

## ДИСКЛЕЙМЕР / DISCLAIMER

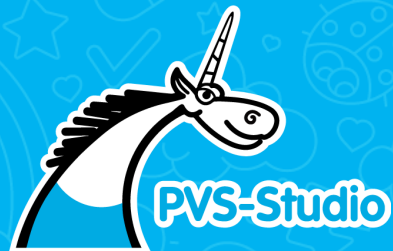
Данное выступление содержит материалы, которые могут быть неприемлемы, неуместны или оскорбительны для некоторых зрителей. Просмотр данного выступления рекомендуется только лицам старше 18 лет в соответствии с законодательством. Выступление предназначено исключительно для юмористических целей и не несет в себе намерения оскорбить или унижить кого-либо. Все сценарии, персонажи и ситуации являются вымышленными и не имеют отношения к реальным событиям или личностям. Юмористический контент данного выступления может содержать ненормативную лексику, сексуальные сцены, насилие, кровь, резкие и/или громкие звуки, а также световые вспышки или другие элементы, которые могут вызвать дискомфорт или неприязнь при просмотре. Просмотр выступления происходит на собственное усмотрение и риски зрителя, который берет на себя ответственность за свой выбор. Все действия были выполнены профессиональными актерами и исполнителями с использованием спецэффектов и безопасного оборудования. Не пытайтесь повторить или воссоздать какие-либо сцены из выступления. Автор не несёт ответственности за любые возможные негативные последствия, вызванные просмотром данного выступления, и рекомендует обратиться за помощью к квалифицированным специалистам в случае возникновения психологических или эмоциональных проблем в результате просмотра.

Данное выступление не рекомендуется к просмотру лицам младше 18 лет, носит исключительно юмористический характер и не используется для распространения информации с целью опорочить людей по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, не содержит призывов к осуществлению террористической и экстремистской деятельности, участию в массовых мероприятиях, проводимых с нарушением установленного порядка, не демонстрирует неуважение к обществу, государству, официальным государственным символам Российской Федерации, конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации.

Мнения, озвученные в данном выступлении, являются оценочными суждениями и в соответствии с принципами свободы слова, выраженными в ст. 10 европейской конвенции по правам человека, свободны к распространению и не являются призывом к совершению противоправных действий. Выступление может содержать информацию, просмотр которой в соответствии с федеральным законом Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», доступен только для лиц старше 18 лет.

**Как учить РБПО/БРПО?  
Как мы создавали лучшие курсы  
по безопасной разработке в УЦ МАСКОМ**

**Опыт привлечения партнёров  
(на примере PVS-Studio)**

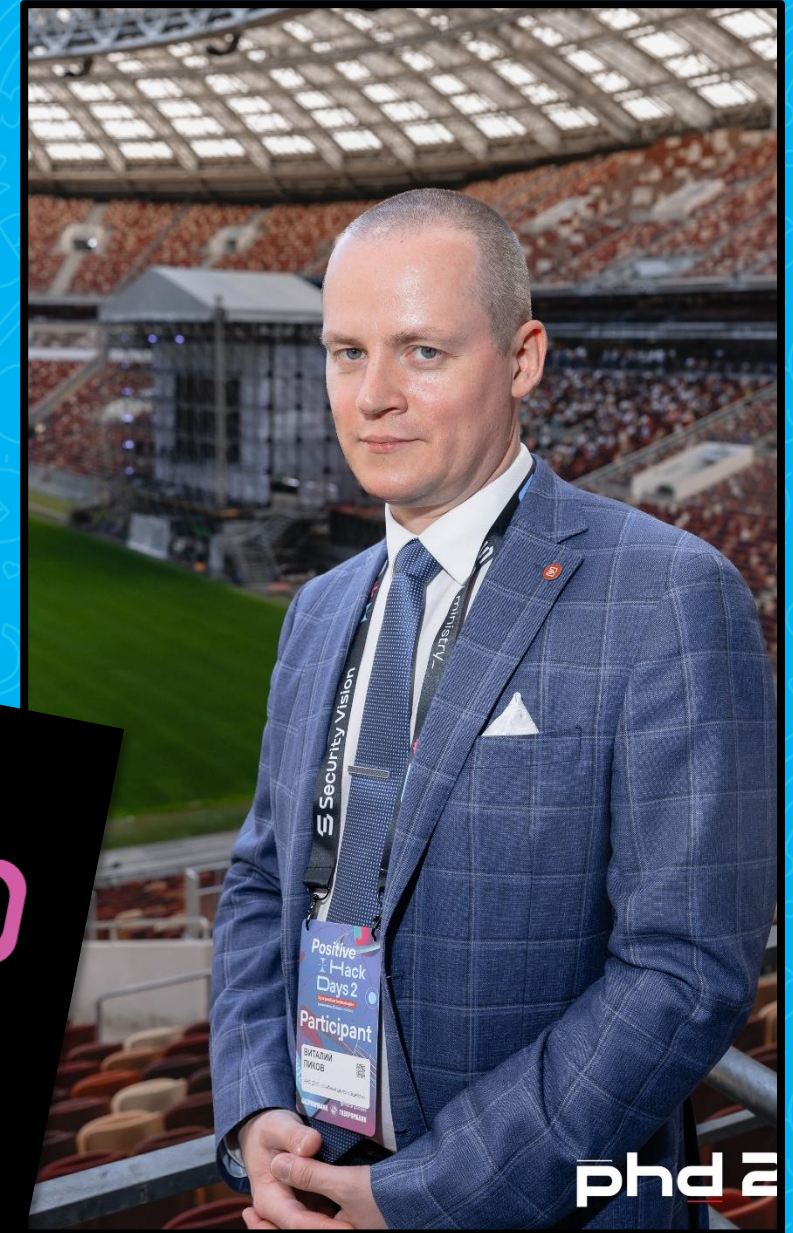


**Виталий Пиков**

руководитель направления обучения  
по РБПО/БРПО, преподаватель  
НОУ ДПО «УЦБИ «МАСКОМ»

# Виталий Пиков

- **Общий стаж работы:** более 26 лет.
- **Стаж преподавательской работы:** более 10 лет.
- **Microsoft Certifications Earned:** MCT, MCPS, MCSA, MCTS.
- Автор **более 30** научных публикаций.
- Читаю курсы, провожу занятия в области информационной безопасности, защиты информации и информационных технологий.



Некоммерческое образовательное учреждение  
дополнительного профессионального образования  
«Учебный центр безопасности информации «МАСКОМ» 1(4)



**НОУ ДПО «УЦБИ «МАСКОМ»** создан в 1998 году. Это отраслевая образовательная площадка для руководителей и специалистов в области безопасности и защиты информации предприятий, а также руководителей и специалистов предприятий оборонно-промышленного комплекса (ОПК) участвующих в государственном оборонном заказе (ГОЗ).

Лидер в сегменте дополнительного профессионального образования по вопросам информационной безопасности, защиты государственной тайны и ИТ.



**УЧЕБНЫЙ ЦЕНТР  
БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Год основания: **1998**

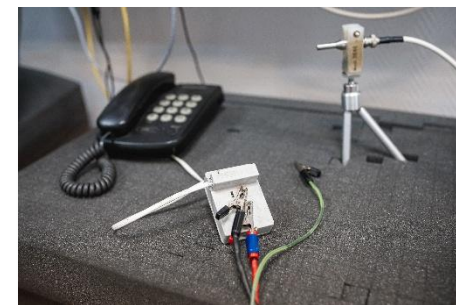


### Факты об НОУ ДПО «УЦБИ «МАСКОМ»:

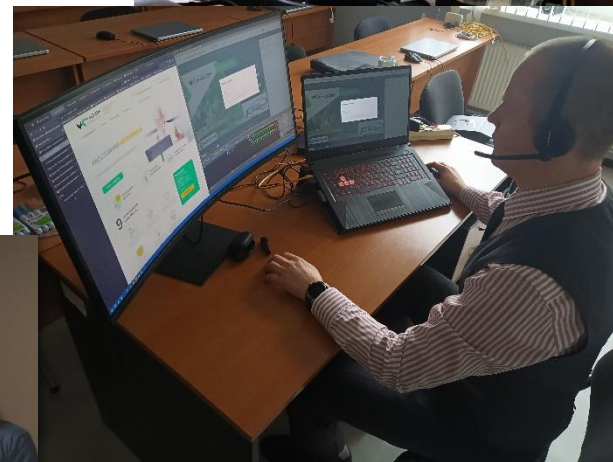
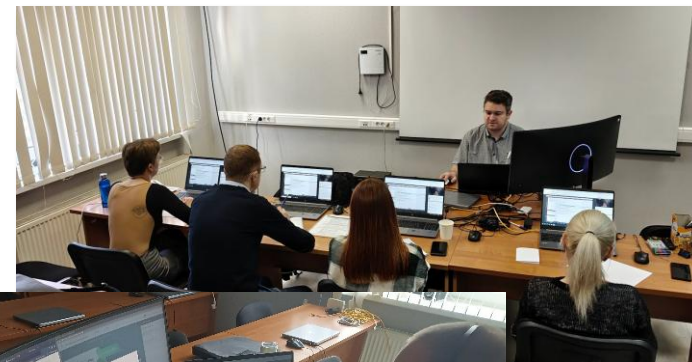
- Более **27 лет** на рынке образовательных услуг.
- Ежегодно повышают квалификацию или приобретают новые знания **более 2,000 человек**.
- Обучаем: офлайн (**более 15 уч. классов**), онлайн, смешанный формат обучения.
- **Более 50** различных программ обучения, повышения квалификации и профессиональной переподготовки.
- Занятия проводятся в комфортабельных классах, оборудованных всем необходимым для учебного процесса
- Курсы включают в себя практические занятия на новом современном оборудовании.
- Мы постоянно развиваемся, обновляя учебные программы и оборудование.
- Преподаватели действующие практики, имеющие ученые степени профессоров и доцентов, кандидатов и докторов наук, а также многолетний преподавательский и научно-прикладной опыт работы.
- Обучение по ряду программам **согласовано с ФСТЭК России и ФСБ России**.
- Гибкие ценовые предложения, скидки.
- Выездные корпоративные мероприятия на территории заказчика
- Удобное расположение (рядом с метро «Воронцовская» / «Калужская»).



# НОУ ДПО «УЦБИ «МАСКОМ» 3 (4)



# НОУ ДПО «УЦБИ «МАСКОМ» 4 (4)



# РБПО/БРПО

– весьма «горячая» тема!



10:00 - 16:30 | СИНИЙ ЗАЛ

Эксперты и экспертиза РБПО.  
Вызовы нашего времени

13 февраля 2025

Встреча сообщества, сформировавшегося под эгидой партнерства ФСТЭК России и ИСП РАН по развитию методик, практик и инструментов разработки безопасного ПО. Практически единственная площадка, позволяющая активным участникам сообщества обмениваться информацией о реалиях внедрения практик разработки безопасного ПО, укреплять горизонтальные связи в кругу единомышленников

10:00 - 16:30 | КОНФЕРЕНЦ-ЗАЛ 3

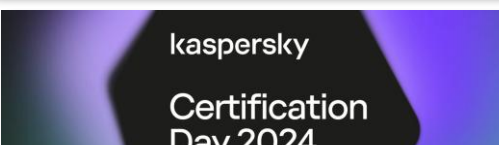
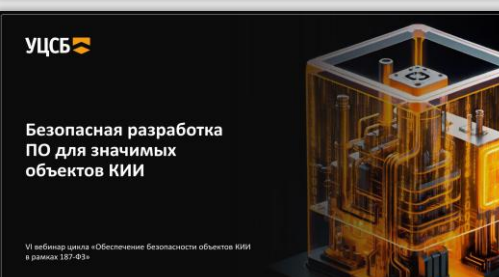
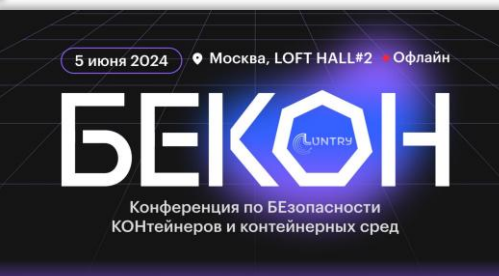
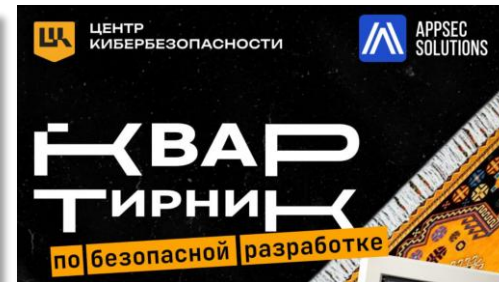
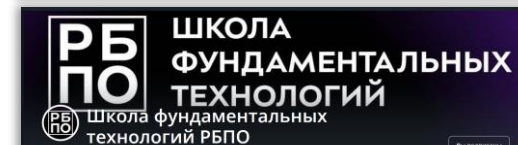
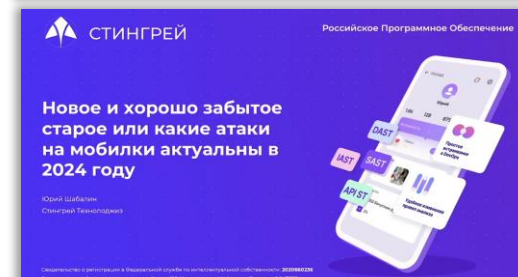
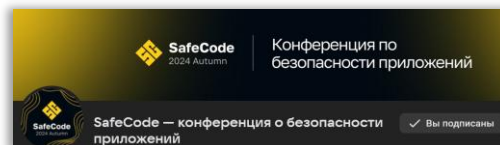
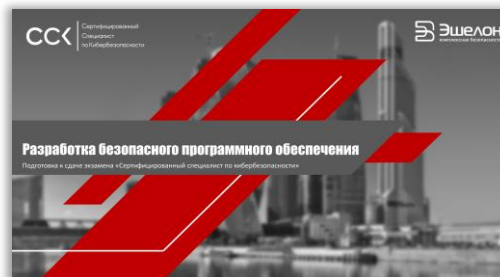
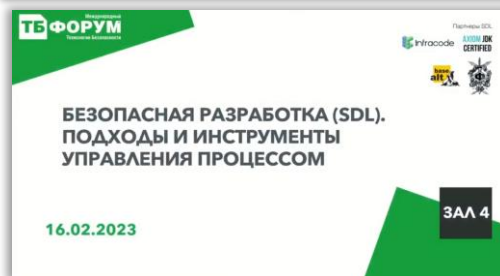
Подходы и инструменты управления процессом РБПО

13 февраля 2025

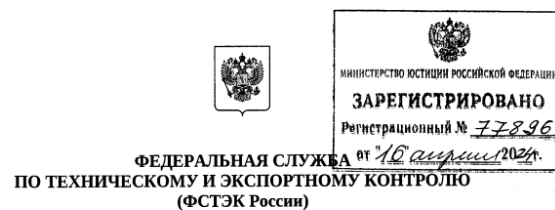
Мастер-трек, семинары, технологическая экспертиза

Реальный опыт по внедрению безопасной разработки и практики пост-релизного сопровождения, актуальные изменения в ГОСТах и сертификации процессов безопасной разработки. Практический опыт внедрения РБПО в компаниях: предпосылки, затраты, кадры. Собственные наработки в области инструментов и методик РБПО.

ОТКРЫТАЯ КОНФЕРЕНЦИЯ ИСП РАН  
МОСКВА, ИННОВАЦИОННЫЙ КЛАСТЕР «ЛОМОНОСОВ»  
11-12 ДЕКАБРЯ 2024 ГОДА  
ПОСВЯЩАЕТСЯ 30-ЛЕТИЮ ИСП РАН И 300-ЛЕТИЮ РАН



# Реалии... 1(6)



## ПРИКАЗ

«1» декабря 2023 г.

Москва

№ 240

### Об утверждении Порядка проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации

В соответствии с подпунктом 13 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и пунктом 9 приложения, утвержденного постановлением Правительства Российской Федерации от 15 мая 2010 г. № 330, **ПРИКАЗЫВАЮ:**

1. Утвердить прилагаемый Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации.
2. Установить, что настоящий приказ вступает в силу с 1 июня 2024 г.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ  
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

**В.СЕЛИН**

УТВЕРЖДЕН  
приказом ФСТЭК России  
от 1 декабря 2023 г. № 240

### **Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации**

1. Сертификация процессов проектирования и производства программного обеспечения (далее – процессы безопасной разработки программного обеспечения) средств защиты информации, содержащей сведения, составляющие государственную тайну или относимые к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, осуществляется на соответствие требованиям национального стандарта Российской Федерации ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 458-ст<sup>1</sup> (далее – требования по безопасной разработке).

2. Сертификация процессов безопасной разработки программного обеспечения (далее – сертификация) осуществляется на основании договора, заключаемого изготовителем средства защиты информации (далее – изготовитель) с органом по сертификации<sup>2</sup>.

3. Изготовитель при намерении сертифицировать процессы безопасной разработки программного обеспечения выбирает для проведения сертификации аккредитованный ФСТЭК России орган по сертификации, согласовывает с ним сроки проведения сертификации.

4. Для получения сертификата соответствия изготовитель представляет в ФСТЭК России заявку на сертификацию (далее – заявка).

В заявке указываются:

- а) полное и сокращенное (при наличии) наименование изготовителя, его организационно-правовая форма;
- б) адрес юридического лица в пределах места нахождения юридического лица – изготовителя;
- в) адрес для корреспонденции изготовителя;
- г) фамилия, имя и отчество (при наличии) лица, ответственного за сертификацию;

<sup>1</sup> М., «Стандартинформ», 2016.

<sup>2</sup> Пункт 11 Положения о сертификации средств защиты информации, утвержденного постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

# Реалии... 2(6)



Kaspersky

## Сертификат №1 ФСТЭК России

«Лаборатория Касперского» первой  
прошла сертификацию процессов  
безопасной разработки



kaspersky

Просто оставим это здесь: мы стали первой (и пока единственной) компанией, получившей сертификат ФСТЭК о соответствии процессов безопасной разработки ПО требованиям ГОСТ Р 56939.

Сертификацию проводили на соответствие двум редакциям: 2016 года и обновленной — 2024 года. Это значит, что «Лаборатория Касперского» отвечает всем требованиям к безопасной разработке не только на уровне отдельного ПО, но и всей компании.

Подробнее о нашем пути к сертификату №1 и о том, почему мы занимались безопасной разработкой до того, как это стало мейнстримом обязательным для всех — Карина Нападовская, руководитель центра сертификации и соответствия стандартам

❤️ 21 👍 11 🔥 9 🗨️ 6 🙌 1

👁 3638 edited 17:46

kaspersky

Для дома Для бизнеса Партнеры О компании

🌐 🔍

Мой Аккаунт

Главная > О нас > Пресс-релизы > «Лаборатория Касперского» первой в России прошла сертификацию процессов безопасной разработки и получила сертификат №1 в ФСТЭК России

## «Лаборатория Касперского» первой в России прошла сертификацию процессов безопасной разработки и получила сертификат №1 в ФСТЭК России

7 октября 2024 г.

Сертификат даёт значительные конкурентные преимущества

## Сертификат № 1 о соответствии процессов безопасной разработки АО «Лаборатория Касперского» ГОСТ Р 56939



### СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

#### СЕРТИФИКАТ СООТВЕТСТВИЯ № 1

Выдан: 25 сентября 2024 г.  
Действителен до: 25 сентября 2029 г.

Настоящий сертификат удостоверяет, что процессы безопасной разработки, реализованные акционерным обществом «Лаборатория Касперского» (АО «Лаборатория Касперского»), соответствуют требованиям национального стандарта ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 458-ст.

Сертификат выдан на основании результатов сертификации, проведенной органом по сертификации федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (аттестат аккредитации от 24.05.2024 № СЗИ RU.0001.01БИ00.A009) — экспертное заключение от 30.08.2024.

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

[https://t.me/kasperskylab\\_ru/5468](https://t.me/kasperskylab_ru/5468)

<https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-pervoj-v-rossii-proshla-sertifikaciyu-processov-bezopasnoj-razrabotki-i-poluchila-sertifikat-1-v-fstek-rossii>

# ФСТЭК России подтвердила статус безопасности процессов разработчика Astra Linux

Пресс-релиз - 25.02.2025



ООО «РусБИТех-Астра» (входит в ПАО «Группа Астра») объявила о получении сертификата ФСТЭК России № 3 от 28.01.2025 г., подтверждающего соответствие процессов безопасной разработки национальному стандарту Российской Федерации ГОСТ Р 56939, сообщает компания во вторник.

Документ оформлен на основании заключения Института системного программирования им.

В.П. Иванникова РАН. При подготовке к сертификации и стандартизации процессов безопасной разработки были учтены положения новой редакции ГОСТ Р 56939-2024, введенной в действие с 20.12.2024.

Полученный сертификат подтверждает, что в штате компании трудятся квалифицированные ИБ-специалисты и выстроены надежные процессы безопасной разработки, что позволяет самостоятельно проводить исследования, связанные с внесением изменений в сертифицированные продукты без привлечения испытательной



**Сертификат № 3 о соответствии процессов безопасной разработки ООО «РусБИТех-Астра» ГОСТ Р 56939**

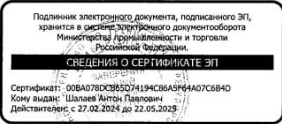
# Реалии...4(6)



  
МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ  
(Росстандарт)  
**ПРИКАЗ**  
24 октября 2024 г. № 1504-ст

Москва  
Об утверждении национального стандарта  
Российской Федерации  
В соответствии со статьей 24 Федерального закона от 29 июня 2015 г.  
№ 162-ФЗ «О стандартизации в Российской Федерации» п р и к а з ы в а ю:  
1. Утвердить национальный стандарт Российской Федерации  
ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного  
программного обеспечения. Общие требования» с датой введения в действие  
20 декабря 2024 г.  
Взамен ГОСТ Р 56939–2016.  
2. Управлению стандартизации обеспечить размещение информации  
об утвержденном настоящим приказом стандарте на официальном сайте  
Росстандарта в информационно-телекоммуникационной сети «Интернет»  
(далее – официальный сайт) с учетом законодательства о стандартизации.  
3. Федеральному государственному бюджетному учреждению  
«Российский институт стандартизации» разместить утвержденный настоящим  
приказом стандарт на официальном сайте в установленном порядке.  
4. Закрепить утвержденный настоящим приказом стандарт  
за техническим комитетом по стандартизации № 362 «Защита информации»  
(ТК 362).

Руководитель  
А.П.Шалаев



ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ  
  
НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ГОСТ Р  
56939—  
2024


Защита информации  
РАЗРАБОТКА БЕЗОПАСНОГО  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
Общие требования  
Издание официальное

Москва  
Российский институт стандартизации  
2024

**РБПО** – это сокр. от «Разработка  
Безопасного Программного Обеспечения»  
(РБПО).

**ГОСТ Р 56939-2024**  
**«3.2 безопасное программное**  
**обеспечение:** Программное обеспечение,  
разработанное с использованием совокупности  
мер, направленных на предотвращение  
появления и устранение уязвимостей  
программы».

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ  
  
НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ГОСТ Р  
71207—  
2024  
Защита информации  
РАЗРАБОТКА БЕЗОПАСНОГО  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
Статический анализ программного обеспечения.  
Общие требования  
Издание официальное  
Москва  
Российский институт стандартизации  
2024

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ  
  
НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ГОСТ Р  
58412—  
2019  
Защита информации  
РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО  
ОБЕСПЕЧЕНИЯ  
Угрозы безопасности информации при разработке  
программного обеспечения  
Издание официальное  
Москва  
Российский институт стандартизации  
2019

# Реалии...5(6)



## BIS JOURNAL

ИНФОРМАЦИОННАЯ  
БЕЗОПАСНОСТЬ  
БИЗНЕСА

№1 (56) 2025

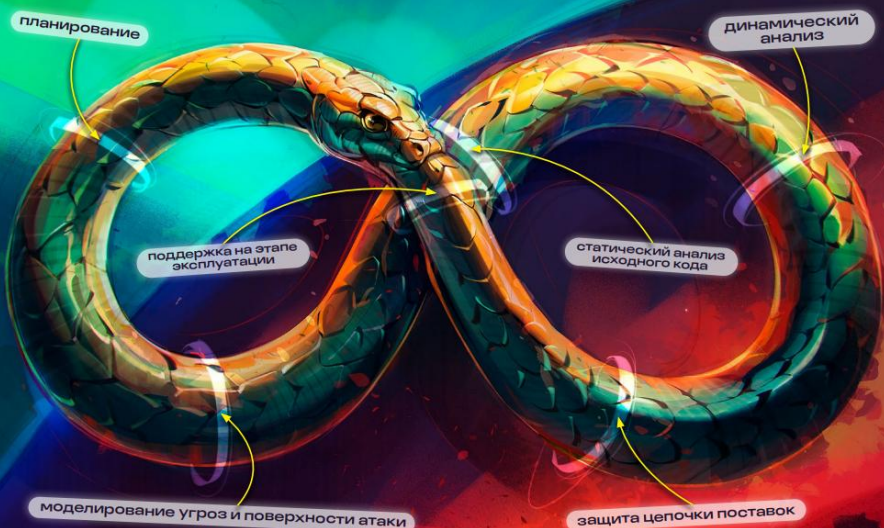
Владимир  
МАТЮХИН  
По случаю юбилея  
Пионеру  
русской ИБ –  
80 лет!  
→ 106



Сергей ГУСЕВ  
АО «Северсталь  
Менеджмент»  
«Броня крепка,  
а будет крепче!»  
→ 4



## БЕЗОПАСНАЯ РАЗРАБОТКА ЭВОЛЮЦИЯ ПО ГОСТУ



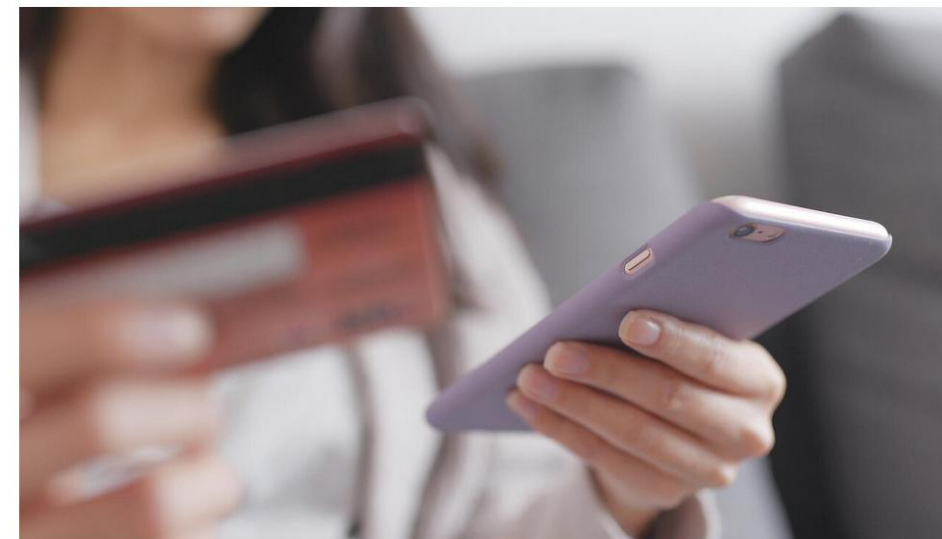
05:35 26.02.2025

РИА НОВОСТИ

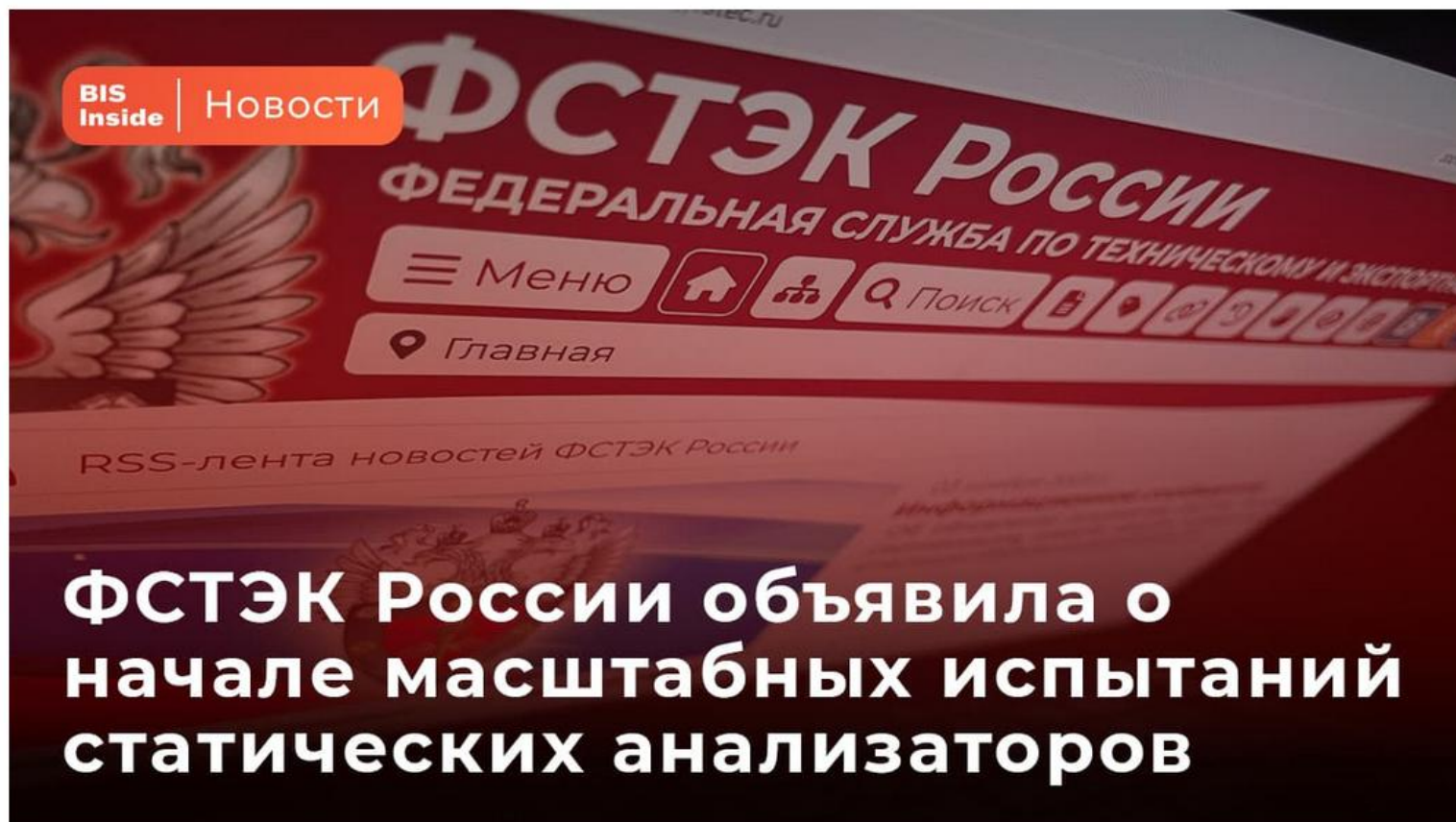
Поделиться

## Эксперты нашли критические уязвимости в каждом втором банковском приложении

В каждом втором банковском приложении нашли критические уязвимости



# Реалии...6(6)



**«Испытания статических анализаторов исходных кодов компилируемых и динамических языков программирования под руководством ФСТЭК России»**

3 февраля ФСТЭК России провела встречу представителей заинтересованных организаций, где обсуждались детали предстоящего масштабного мероприятия «Испытания статических анализаторов».

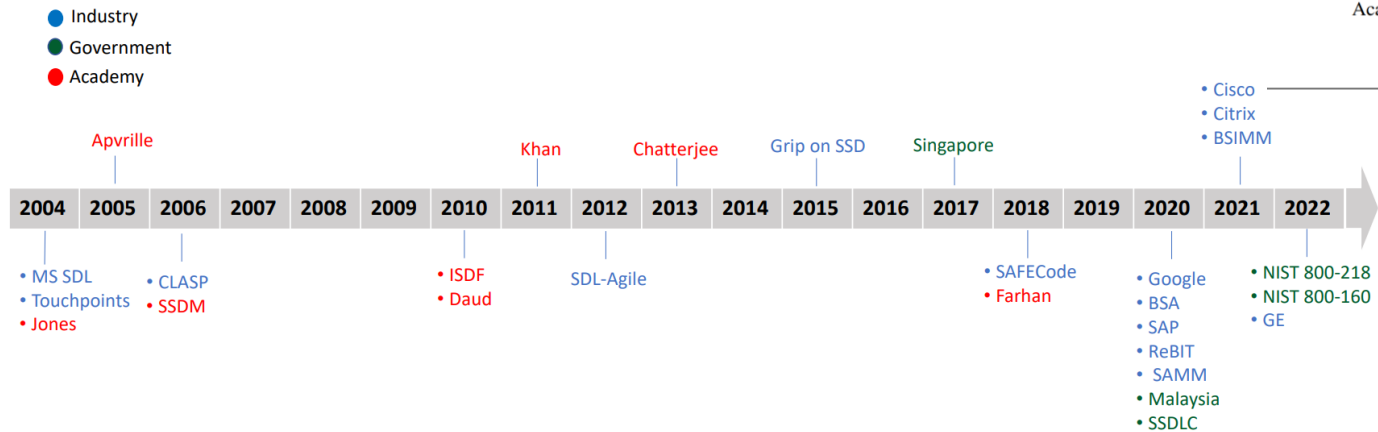
<https://ib-bank.ru/bisjournal/news/21667>

# Как давно это началось? 1(2)



## Secure Software Development Methodologies: A Multivocal Literature Review

Arina Kudriavtseva, Olga Gadyatskaya



SECURE SOFTWARE DEVELOPMENT METHODOLOGIES ORDERED CHRONOLOGICALLY		
The source of methodology	Name	Year of publication
Industry	Microsoft Software Development Life Cycle (SDL) [4], [26]	2006
	McGraw's Secure Software Development Lifecycle Process [57], [66]	2006
	Comprehensive, Lightweight Application Security Process (CLASP) [67]	2006
	Microsoft SDL version 5.2 for Agile Development [68]	2012
	Software Assurance Forum for Excellence in Code (SAFECode) [69]	2018
	Building Secure and Reliable Systems [70]	2020
	BSA framework [30]	2020
	The Secure Software Development Lifecycle at SAP [11]	2020
	ReBIT Application Security Framework [61]	2020
	OWASP Software Assurance Maturity Model [39]	2020
	Cisco Secure Development Lifecycle [13]	2021
	Citrix Security Development Lifecycle [12]	2021
	Building Security in Maturity Model [71]	2021
Government	GE Secure Development Lifecycle [27]	2022
	Grip on Secure Software Development [34]	2015
	CSA Singapore Security-by-Design [29]	2017
	SSDLC guidelines Malaysia [35]	2020
	Security in SDLC Romania [24]	2021
	NIST 800-218 [28]	2022
Academia	NIST 800-160 [72]	2022
	Secure Coding: Building Security into the Software Development Life Cycle [73]	2004
	Secure Software Development Life Cycle Process [25]	2005
	The Secure Software Development Model (SSDM) [36]	2006
	The Integrated Security Development Framework (ISDF) [31]	2010
	Secure Software Development Model: A Guide for Secure Software Life Cycle [37]	2010
	Secure Software Development: a Prescriptive Framework [32]	2011
	Framework for Development of Secure Software [33]	2013
	Methodology for Enhancing Software Security During Development Processes [38]	2018

# Как давно это началось? 2(2)



## ГОСТ Р 56939-2016 (проект ГОСТ Р 56939-20XX)

**«3.2 безопасное программное обеспечение:** Программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы».

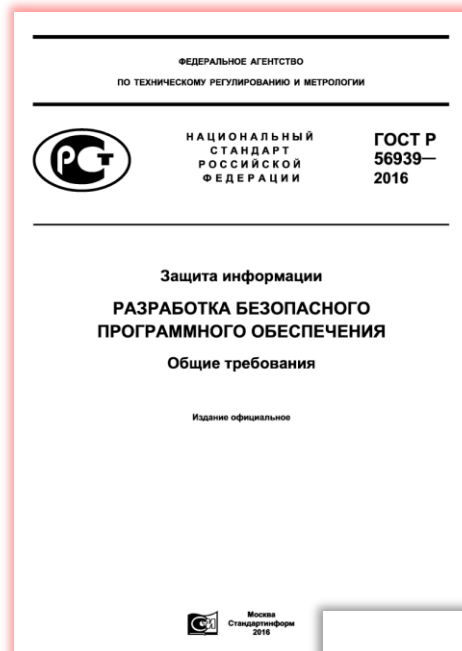
**Методический документ. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций (Банк России, 2021)**

### «7.4.1. Общие положения

Целью применения методологий безопасного жизненного цикла к ОО является обеспечение высокой конкурентоспособной скорости разработки и внедрения безопасных программных продуктов при сохранении гарантированного и достаточного уровня защищенности ОО в условиях изменяющихся требований, при высокой вовлеченности и ответственности компетентных подразделений (от разработчиков, специалистов по информационной безопасности до служб эксплуатации и поддержки), одновременно привлекаемых на самых ранних этапах жизненного цикла ОО, включая обновления ОО, и сопровождающих жизненный цикл ОО вплоть до вывода ОО из эксплуатации».

**«7.4.3.1 Описание процесса безопасного жизненного цикла ОО. Определение методологии и практик процесса безопасного жизненного цикла ОО**

**Под методологией безопасного жизненного цикла ОО в настоящем документе понимается соблюдение совокупности принципов, правил, мер, требований, а также последовательности выполнения мероприятий жизненного цикла для целей предотвращения появления и устранения уязвимостей в ОО, поддержания доверия к ОО на всем протяжении жизненного цикла ОО и обеспечения необходимого и достаточного уровня безопасности ОО».**

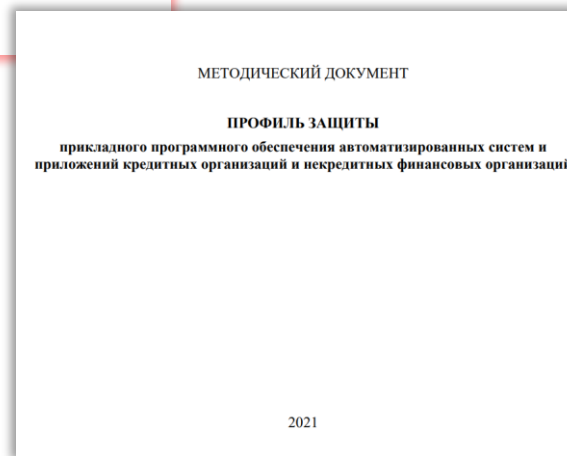


## К вопросу о выявлении дефектов безопасности методом статического сигнатурного анализа

Алексей Марков, к.т.н., с.н.с., CISSP, SBCI  
Андрей Фадин, CISSP

НПО «Эшелон»  
mail@cnpo.ru

ТипВСИТ - 2012



# А есть ли смысл учить РБПО/БРПО?



Максим Горшенин | imaxai  
25 903 subscribers

**Pinned message**  
На фоне стены, где стоит кресло и колонки, я снимаю все нов

Профессия «программист» полностью исчезнет через год

По словам CEO одной из самых мощных нейросетей по написанию кода Claude, уже через 3–6 месяцев 90% кода будет генерироваться ИИ, а через год — 100%

В системах МТС уже 8% строк программного кода пишется с помощью искусственного интеллекта (ИИ)

А к 2027 г. доля созданного нейросетями кода вырастет до 25% – втрое больше, чем сейчас

Если говорить о российском рынке в целом, то количество кода, сгенерированного ИИ, будет расти примерно такими же темпами

@imaxairu Подписаться

👍 140 👤 19 👍 8 🗨️ 6 📢 5

👁 4308 16:20

AS 5 comments



Битва Low-code и нативного программирования: RPA против Python — эволюция разработки или война подходов

Сергей Вотяков

GR директор PIX Robotics, член Правления RUSOFT, ректор NARPA  
info@narpa.ru | www.narpa.ru

Март 13, 2025





Утверждаю  
Зам. директора по УВР  
Жуковский А. Г.  
« 29 » 08 2022 г.

Кафедра «Информатика и вычислительная техника»  
 Направление подготовки: 10.03.01 Информационная безопасность  
 Профиль: Безопасность компьютерных систем.  
 Формы обучения: очная

ОДОБРЕНО УМС ИИКС  
Протокол № УМС-575/01-1  
от 30.08.2021 г.

Направление подготовки (специальность)	[1] 10.04.01 Информационная безопасность
-------------------------------------------	------------------------------------------

Семестр	Трудоёмкость, крел.	Общий объем курса, час.	Лекции, час.	Практик, занятий, час.	Лаборат. работы, час.	В форме проектной/исследовательской работы, час.	СРС, час.	КСР, час.	Форматы контроля,
3	2	72	8	24	0		40	0	3
Итого	2	72	8	24	0	2	40	0	

[записаться](#)[смотреть программу](#) Версия для слабовидящих

 **+7 (499) 877-16-11**  
Info@infosystem.ru

[АКАДЕМИЯ](#)
[КУРСЫ](#)
[УСЛУГИ](#)
[БИБЛИОТЕКА](#)
[КОНТАКТЫ](#)

Курсы • Информационная безопасность • Авторские курсы

**Безопасная разработка программного обеспечения**



**ИСП | РАН**

**ПРОГРАММА № 33 «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. АНАЛИЗ АРХИТЕКТУРЫ И ЭКСПЕРТИЗА ИСХОДНЫХ КОДОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»**

**ПРОГРАММА № 34 «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. СТАТИЧЕСКИЙ АНАЛИЗ ИСХОДНЫХ КОДОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»**

**ПРОГРАММА № 37 «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ОСНОВЫ ИНСТРУМЕНТАЛЬНОЙ И ТЕХНОЛОГИЧЕСКОЙ ПОДДЕРЖКИ ПРОВЕДЕНИЯ ФАЗЗИНГ-ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»**

# Домены знаний (приблизительно...)



1. Методологии РБПО/БРПО (современные и ретроспектива).
2. Основные руководящие нормативные и методические документы, требования НПА РФ.
3. Организация ЭВМ и вычислительных систем. Безопасность операционных систем, безопасность сетей ЭВМ.
4. Хроника языков программирования. Низкоуровневые и высокоуровневые языки.
5. Системная и программная инженерия.
6. Обзор требований к системам менеджмента информационной безопасности (СМИБ). Серия международных стандартов ISO 270XX.
7. Управление уязвимостями программного обеспечения.
8. Сертификация программного обеспечения по требованиям безопасности информации (системы сертификации ФСТЭК России, Минобороны России). Сертифицированные испытания программного обеспечения.
9. Анализ и реверс-инжиниринг программного обеспечения.
10. Тестирование программного обеспечения.
11. Статический анализ программного кода.
12. Архитектурный анализ программного обеспечения.
13. Динамический анализ программного обеспечения.
14. Фаззинг-тестирование программного обеспечения.
15. Анализ защищенности и тестирование на проникновение.
16. Внедрение процессов РБПО/БРПО в организации.



# Серия учебных курсов по направлению РБПО/БРПО в УЦ МАСКОМ 1(4)



## М БРПО- Спец

Специалист по процессам разработки безопасного программного обеспечения

Программа курса направлена на подготовку полноценного специалиста, обладающего всеми необходимыми компетенциями для ведения профессиональной деятельности, имеющего глубокие теоретические знания и практические навыки по направлению разработки безопасного программного обеспечения с учётом актуальной нормативной правовой базы.

02.09.2024-27.09.2024



Пиков Виталий  
Александрович

Время

30.09.2024-25.10.2024

200 часов / 20 дней



## М БРПО-01

Внедрение процессов разработки безопасного программного обеспечения в организации (для руководителей и ответственных)

Программа курса охватывает всё необходимое для руководителей предприятий и ответственных за процессы БРПО для получения знаний теоретических основ и приобретения практических навыков внедрения процессов разработки безопасного программного обеспечения (ГОСТ Р 56939–2016) на предприятии с учётом требований актуальной нормативной правовой базы.

03.09.2024-06.09.2024



Пиков Виталий  
Александрович

Время

01.10.2024-04.10.2024

40 часов / 4 дня



## М БРПО-02

Внедрение процессов разработки безопасного программного обеспечения для специалистов по информационной безопасности

Программа курса охватывает всё необходимое для получения знаний у специалистов по информационной безопасности теоретических основ актуальной отечественной и зарубежной нормативной правовой базы по направлению разработки безопасного программного обеспечения, а также приобретения практических навыков внедрения процессов разработки безопасного программного обеспечения (ГОСТ Р 56939–2016) в организации.

02.09.2024-06.09.2024



Пиков Виталий  
Александрович

Время

30.09.2024-04.10.2024

50 часов / 5 дней



## М БРПО-03

Сертификационные испытания с учётом требований по разработке безопасного программного обеспечения для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации

Программа курса охватывает всё необходимое для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации для получения знаний теоретических основ актуальной отечественной и зарубежной нормативной правовой базы по направлению сертификации программного обеспечения, проведению сертификационных испытаний и по разработке безопасного программного обеспечения, а также для приобретения практических навыков проведения сертификационных испытаний по требованиям доверия согласно требованиям приказа ФСТЭК России от 2 июня 2020 г. № 76 и по требованиям системы сертификации средств защиты информации в Министерстве обороны Российской Федерации.

03.09.2024-23.09.2024

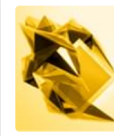


Пиков Виталий  
Александрович

Время

01.10.2024-21.10.2024

140 часов / 14 дней



## М БРПО-04

Формирование практических навыков по разработке безопасного программного обеспечения для разработчиков и программистов

Программа курса будет полезна разработчикам программного обеспечения, программистам и их руководителям для получения знаний теоретических основ актуальной отечественной и зарубежной нормативной правовой базы, а также для приобретения обширных практических навыков по разработке безопасного программного обеспечения, проведения сертификационных испытаний программных продуктов и внедрения процессов разработки безопасного программного обеспечения в организации.

03.09.2024-23.09.2024



Пиков Виталий  
Александрович

Время

01.10.2024-21.10.2024

140 часов / 14 дней



## М БРПО-05

Методология подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России

Программа курса охватывает всё необходимое для подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России, внедрения процессов разработки безопасного программного обеспечения на предприятии с учётом актуальной нормативной правовой базы.

03.09.2024-05.09.2024



Пиков Виталий  
Александрович

Время

01.10.2024-03.10.2024

30 часов / 3 дня

# Серия учебных курсов по направлению РБПО/БРПО в УЦ МАСКОМ 2(4)



## М БРПО- Спец



Специалист по процессам разработки безопасного программного обеспечения

Программа курса направлена на подготовку полноценного специалиста, обладающего всеми необходимыми компетенциями для ведения профессиональной деятельности, имеющего глубокие теоретические знания и практические навыки по направлению разработки безопасного программного обеспечения с учётом актуальной нормативной правовой базы.

02.09.2024-27.09.2024

30.09.2024-25.10.2024



Пиков Виталий  
Александрович

Время

200 часов / 20 дней



## М БРПО-01



Внедрение процессов разработки безопасного программного обеспечения в организации (для руководителей и ответственных)

Программа курса охватывает всё необходимое для руководителей предприятий и ответственных за процессы БРПО для получения знаний теоретических основ и приобретения практических навыков внедрения процессов разработки безопасного программного обеспечения (ГОСТ Р 56939–2016) на предприятии с учётом требований актуальной нормативной правовой базы.

03.09.2024-06.09.2024

01.10.2024-04.10.2024



Пиков Виталий  
Александрович

Время

40 часов / 4 дня

- Для специалистов по процессам РБПО.
- Для руководителей и ответственных за организацию разработки безопасного программного обеспечения в организации.
- Для специалистов по информационной безопасности.
- Для архитекторов, разработчиков программного обеспечения и программистов.
- Для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации (ФСТЭК России, Минобороны России).
- Для организаций, лицензиатов ФСТЭК России и Минобороны России, создающие средства защиты информации.

# Серия учебных курсов по направлению РБПО/БРПО в УЦ МАСКОМ 3(4)



**М**  
**БРПО-02**



Внедрение процессов разработки безопасного программного обеспечения для специалистов по информационной безопасности

Программа курса охватывает всё необходимое для получения знаний у специалистов по информационной безопасности теоретических основ актуальной отечественной и зарубежной нормативной правовой базы по направлению разработки безопасного программного обеспечения, а также приобретения практических навыков внедрения процессов разработки безопасного программного обеспечения (ГОСТ Р 56939–2016) в организации.

02.09.2024-06.09.2024  
30.09.2024-04.10.2024



Пиков Виталий  
Александрович

Время  
50 часов / 5 дней



**М**  
**БРПО-03**



Сертификационные испытания с учётом требований по разработке безопасного программного обеспечения для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации

Программа курса охватывает всё необходимое для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации для получения знаний теоретических основ актуальной отечественной и зарубежной нормативной правовой базы по направлению сертификации программного обеспечения, проведению сертификационных испытаний и по разработке безопасного программного обеспечения, а также для приобретения практических навыков проведения сертификационных испытаний по требованиям доверия согласно требованиям приказа ФСТЭК России от 2 июня 2020 г. № 76 и по требованиям системы сертификации средств защиты информации в Министерстве обороны Российской Федерации.

03.09.2024-23.09.2024  
01.10.2024-21.10.2024



Пиков Виталий  
Александрович

Время  
140 часов / 14 дней

- Для специалистов по процессам РБПО.
- Для руководителей и ответственных за организацию разработки безопасного программного обеспечения в организации.
- Для специалистов по информационной безопасности.
- Для архитекторов, разработчиков программного обеспечения и программистов.
- Для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации (ФСТЭК России, Минобороны России).
- Для организаций, лицензиатов ФСТЭК России и Минобороны России, создающие средства защиты информации.

# Серия учебных курсов по направлению РБПО/БРПО в УЦ МАСКОМ 4(4)



**М**  
**БРПО-04**



**Формирование практических навыков по разработке безопасного программного обеспечения для разработчиков и программистов**

Программа курса будет полезна разработчикам программного обеспечения, программистам и их руководителям для получения знаний теоретических основ актуальной отечественной и зарубежной нормативной правовой базы, а также для приобретения обширных практических навыков по разработке безопасного программного обеспечения, проведения сертификационных испытаний программных продуктов и внедрения процессов разработки безопасного программного обеспечения в организации.

03.09.2024-23.09.2024

01.10.2024-21.10.2024



Пиков Виталий  
Александрович

Время

140 часов / 14 дней



**М**  
**БРПО-05**



**Методология подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России**

Программа курса охватывает всё необходимое для подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России, внедрения процессов разработки безопасного программного обеспечения на предприятии с учётом актуальной нормативной правовой базы.

03.09.2024-05.09.2024

01.10.2024-03.10.2024



Пиков Виталий  
Александрович

Время

30 часов / 3 дня

- Для специалистов по процессам РБПО.
- Для руководителей и ответственных за организацию разработки безопасного программного обеспечения в организации.
- Для специалистов по информационной безопасности.
- Для архитекторов, разработчиков программного обеспечения и программистов.
- Для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации (ФСТЭК России, Минобороны России).
- Для организаций, лицензиатов ФСТЭК России и Минобороны России, создающие средства защиты информации.

# Курсы изначально построены на ГОСТ Р 56939-2024

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ

ГОСТ Р  
56939—  
202X  
(проект, окончательная  
редакция)

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

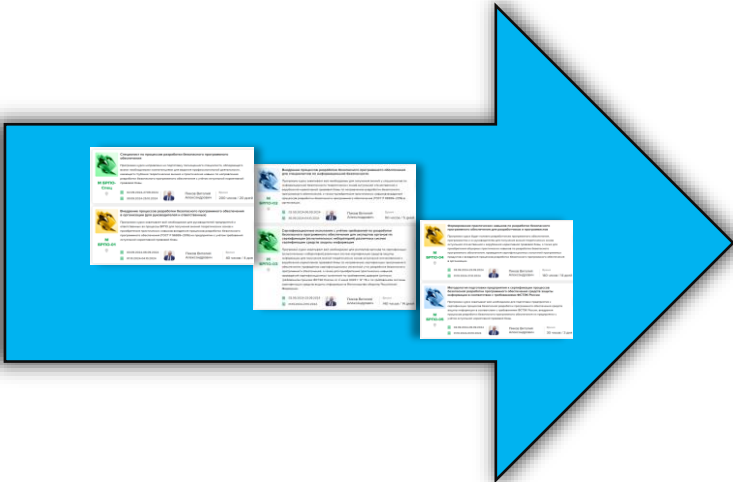
Общие требования

Настоящий проект стандарта не подлежит применению до его утверждения


Москва

ФГБУ «Российский институт стандартизации»

202X



ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ

ГОСТ Р  
56939—  
2024

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва

Российский институт стандартизации

2024

# Официальные программы уч. курсов представлены с учётом подхода «Я – легенда»



# Проведена серия вебинаров (10 шт. + экзамен) по теме: «Разработка безопасного программного обеспечения (РБПО/БРПО). Давайте разбираться вместе!» 1(2)

№ п/п	Дата проведения (по средам в 19:00)	Темы вебинара (примерно по 20–30 мин. каждая тема)	Докладчики
1.	28.08.2024	- Давайте разбираться вместе! РБПО для: ЗО КИИ, Центробанка, Минобороны... и Вашей фирмы Актуальность создания безопасного программного обеспечения или как так получается, что красоты в приложениях стало больше, а безопасности – меньше - Рубрика: «Отечественные решения в РБПО». Критические ошибки в коде программ. Требования нового ГОСТ Р 71207–2024 - Статический анализ программного обеспечения - Рубрика: «Отечественные решения в РБПО». Управления процессом БРПО вместе с AppSec.Hub	- Пиков В.А. - Карпов А.Н. (DevRel ООО «ПВС») - Башарин Антон (директор продукта AppSec.Hub).
2.	04.09.2024	- Специалист по процессам безопасной разработки программного обеспечения - кто он? - Автоматизация процесса РБПО на практике вместе с AppSec.Hub - Формальные методы - разбираемся вместе	- Пиков В.А. - Башарин Антон (директор продукта AppSec.Hub). - Буянов С.В. (доцент МАИ)
3.	11.09.2024	- Быстрая разведка при пентесте внешнего периметра в процессах БРПО - Как влияет лоскутная автоматизация на безопасность программного обеспечения - Процессы РБПО для руководителей и ответственных	- Распопов Н.А. (ООО «УЦСБ») - Щеголев А.Г. (преподаватель ГБПОУ «1-й МОК») - Пиков В.А.
4.	18.09.2024	Рубрика: «Отечественные решения в РБПО». Предотвращение атак через известные уязвимости в open-source компонентах при помощи AppSec.Task - Управление уязвимостями в организации	- Багно В.С. (AppSec-инженер ООО «Свордфиш Секьюрити») - Пиков В.А.
5.	25.09.2024	- Управление уязвимостями: методы, технологии и инструменты (ГК «Эшелон») - Деплоим приложения в контейнерах безопасно - Обзор и применение современных программных инструментов реверс-инжиниринга	- Дорофеев А.В. (ГД АО «Эшелон Технологии», директор УИ «Эшелон», CCK, CISA, CISM, CISSP) - Рахманный А.В. (старший разработчик, ПСБ) - Недогарок А.А.
6.	02.10.2024	- Риски информационной безопасности в генеративных системах искусственного интеллекта: уязвимости моделей, инфраструктурные риски. Перспектива применения генеративных ИИ-систем в цикле безопасной разработки программного обеспечения - «Чтобы никто мой код не смог хакнуть!» - процессы РБПО для разработчиков и программистов - Применение и противодействие методам защиты от реверс-инжиниринга	- Кокуйкин Евгений (директор ИИ продуктов Raft, руководитель лаборатории LLM Security AI Talent Hub/ИТМО) - Гайдаёва Т.В., (преподаватель ГБПОУ «1-й МОК») - Недогарок А.А.
7.	09.10.2024	- Рубрика: «Отечественные решения в РБПО». Статический анализатор PVS-Studio на страже качества, защищённости и безопасности кода - Рубрика: «Отечественные решения в РБПО». Безопасность мобильных приложений, новые вызовы, атаки и как их решить при помощи платформы Стинтрей - Что нам даст сертификация процессов БРПО средств защиты информации предприятия в соответствии с требованиями ФСТЭК России?	- Карпов А.Н. (DevRel ООО «ПВС») - Юрий Шабалин (AppSec Solutions, владелец продукта Стинтрей) - Пиков В.А.
8.	16.10.2024	- Построение автоматизированного конвейера и интегрированных платформ разработки критически безопасных систем - Рубрика: «Отечественные решения в РБПО». Современные программные средства безопасной разработки от ИСП РАН	- Буянов С.В. - Филимонов И.А.
9.	23.10.2024	- Рубрика: «Отечественные решения в РБПО». Анализатор исходных текстов АК-BC 3» обзор функциональных возможностей - Обзор требований по разработке безопасного программного обеспечения ГОСТ Р 56939-20XX	- Представители ГК «Эшелон»: Вареница В.В., Арустамян С.С. - Пиков В.А.
10.	30.10.2024	- Рубрика: «Отечественные решения в РБПО». AppSec.Hub - использование метрик для управления процессом безопасной разработки - «Методология!? Фреймворк? Подход? Учение по безопасной разработке программного обеспечения!?» - рассказ о том, как мы разработали новую «регламентацию» - Формальные модели, как часть процесса РБПО - ИТОГОВЫЙ ОНЛАЙН-ЭКЗАМЕН	- Башарин Антон (директор продукта AppSec.Hub) - Евгений Ильяхин, Артём Кармазин (Positive Technologies) - Буянов С.В. - УЦ МАСКОМ



@MASCOM\_UC

Проведена серия вебинаров (10 шт. + экзамен) по теме:  
«Разработка безопасного программного обеспечения (РБПО/БРПО).  
Давайте разбираться вместе!» 2(2)



[https://vkvideo.ru/@vitaliy\\_pikov](https://vkvideo.ru/@vitaliy_pikov)



[https://dzen.ru/mascom\\_uc?share\\_to=link](https://dzen.ru/mascom_uc?share_to=link)



<https://rutube.ru/channel/4506349/videos/>



<https://www.youtube.com/vpikov>

## Кто научит?

На курсах РБПО/БРПО задействовано **более 10** лучших преподавателей



Опытные преподаватели из ведущих вузов и организаций-партнёров:

- Московский авиационный институт.
- МГТУ им. Н.Э. Баумана.
- Московский политехнический университет.
- Российский новый университет.
- 1 МОК (Первый Московский Образовательный Комплекс).
- ООО «ПВС».
- ООО «Свордфиш Секьюрити».
- ГК «ЭШЕЛОН».
- ГК «АСТРА».



Общий стаж работы:

Стаж преподавательской работы: более 11 лет

Образование: высшее, МГТУ им. Н.Э. Баумана, специальность - инженер. В 2021 г и 2022 г прошел повышение квалификации в АНО ДПО "Корпоративный университет Сбербанка" по программе "Летняя цифровая школа. Трек "Кибербезопасность".

Читает курсы по "Анализу и реверс-инжинирингу программного обеспечения", "Методы и средства криптографической защиты информации" и "Разработка и эксплуатация защищённых автоматизированных систем" в Московском Политехническом университете с 2016 г.



Общий стаж работы: более 35 лет

Стаж преподавательской работы: более 25 лет

Образование: высшее, кандидат технических наук, Московский авиационный институт по специальности «Вычислительные машины, системы, комплексы и сети». В 2021-24 годах прошёл профессиональную переподготовку в Новосибирском, Томском, Орловском университетах, в МГТУ им. Н. Э. Баумана.

Преподает и участвует в курсах: Верификация и валидация вычислительных систем, Компьютерная алгебра, Корпоративные информационные системы, Системы искусственного интеллекта, Проектирование и архитектура вычислительных систем, Научно-исследовательская деятельность.



Общий стаж работы: более 22 лет

Стаж преподавательской работы: стаж наставничества/консультаций/обучения коллег - более 15 лет

Образование: высшее, с отличием Тамбовский военный авиационный инженерный институт по специальности «Автоматизированные системы обработки информации и управления». В 2017 году прошёл повышение квалификации в ДПО «УЦ ЦБИ» по направлению подготовки: «Техническая защита конфиденциальной информации, Информационная безопасность», «Организация и проведение работ по оценке (подтверждению) соответствия, Информационная безопасность», «Аттестация объектов информатизации по требованиям безопасности информации. Защита от несанкционированного доступа, Информационная безопасность».

Ведет занятия на учебных курсах по направлению разработки безопасного программного обеспечения.



Общий стаж работы: более 26 лет

Стаж преподавательской работы: более 10 лет



УЧЕБНЫЙ ЦЕНТР  
БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
Год основания: 1998

Чему научим? – **Лидеры рынка!**



# Чему научим?

## Инструменты и средства



Продуктовый портфель решений  
AppSec Solutions



Платформа управления  
состоянием безопасности  
приложений (ASPM)



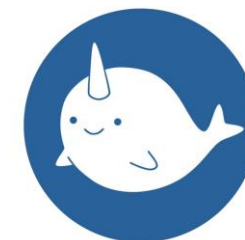
СТИНГРЕЙ

Платформа автоматизированного  
анализа защищённости  
мобильных приложений (MAST)



APPSEC.TRACK

Сервис предотвращения атак  
на цепочку поставок ПО через  
компоненты с открытым  
исходным кодом (OSA, SCA)



Ведутся дальнейшие переговоры с отечественными партнёрами-разработчиками решений для РБПО по вопросу предоставления программных инструментов для наших учебных курсов

# Роль личности в истории



**Карпов Андрей Николаевич, к.ф.-м.н.**  
// Кандидат физико-математических наук

- Более 15 лет занимается темой статического анализа кода и качества программного обеспечения.
- Автор большого количества статей, посвящённых написанию качественного кода на языке C++.
- С 2011 по 2021 год удостоивался награды Microsoft MVP в номинации Developer Technologies.
- Intel Black Belt Software Developer
- Присутствует на **Habrahabr** под именем **Andrey2008**
- Один из основателей проекта PVS-Studio ([pvs-studio.ru](http://pvs-studio.ru))



# Участие команды PVS-Studio в наших курсах по РБПО/БРПО 1(2)

- Минимум 1 день (как правило, 2 дня) участия в уч. программах курсов.
- Участие большой команды преподавателей.
- Лёгкость в подготовке и развертывании стенда (+промокоды).
- Огромное количество материалов в виде статей, видео, книг и пр.

WHOAMI

Глеб Асламов  
C# Developer & Developer Advocate

Занимаюсь разработкой на .NET  
Выступаю с докладами  
Пишу статьи

11.10 Пт.	Лекция	Обзорный доклад о возможностях статического анализатора PVS-Studio. Какие виды ошибок умеет находить, как встраивается в процесс разработки, с какими системами интегрируется, основные настройки. Ответы на вопросы.	с 09:30 по 11:00	Глеб Асламов (ООО «ПВС»)
	Лекция	PVS-Studio с точки зрения БРПО. Обзорное знакомство с ГОСТ Р 71207-2024 (Статический анализ кода). Далее через призму этого стандарта взглянем на инструментальное средство PVS-Studio: технологии, виды выявляемых критических ошибок, фильтрация предупреждений. Ответы на вопросы.	с 11:10 по 12:40	Андрей Карпов (ООО «ПВС»)
Обед: 12:40 — 13:30				
	Дем.	Демонстрация работы PVS-Studio в качестве плагина для Visual Studio. Запуск анализатора, первичная фильтрация отчета, подавление ложных срабатываний, просмотр отчета, исправление критических ошибок, работа с базой разметки (задания baseline-уровня), использование документации. Ответы на вопросы.	с 13:30 по 15:00	Андрей Карпов (ООО «ПВС»)
	ПЗ	Первая часть практического занятия по работе по поиску ошибок в коде с помощью PVS-Studio. Заранее будет предоставлен образ виртуальной Linux машины. В ней будет установлен плагин PVS-Studio для Visual Studio Code и находится отчет уже проверенного проекта на языке C. В течение часа нужно поработать с отчетом и выписать реальные ошибки. Параллельно следует подумать, как можно сократить количество ложных срабатываний (какие настройки можно сделать).	с 15:10 по 16:40	Андрей Карпов, Валерий Филатов (ООО «ПВС»)
	ПЗ	Вторая часть практического занятия, где мы обсуждаем найденные ошибки. Каждый участник обучения по очереди показывает и описывает найденный им баг (почему это баг, насколько он критичен, как его исправить). И разбирает одно из ложных срабатываний. Дискуссия, ответы на вопросы.	с 16:50 по 18:20	Андрей Карпов, Валерий Филатов (ООО «ПВС»)
14.02 Пт.	Лекция	Обзорный доклад о возможностях статического анализатора PVS-Studio. Что из себя представляет статический анализ, какие виды ошибок умеет находить, что за технологии использует. Ответы на вопросы.	с 09:30 по 11:00	Владислав Богданов (ООО «ПВС»)
	Лекция	PVS-Studio с точки зрения БРПО. Обзорное знакомство с ГОСТ Р 71207-2024 (Статический анализ кода). Далее через призму этого стандарта взглянем на инструментальное средство PVS-Studio: технологии, виды выявляемых критических ошибок, фильтрация предупреждений. Ответы на вопросы.	с 11:10 по 12:40	Глеб Асламов, Валерий Филатов (ООО «ПВС»)
Обед: 12:40 — 13:30				
	Дем.	PVS-Studio в Continuous Delivery. Что такое CD и почему это круто? Из чего состоит CD пайплайн? Чем статический анализ поможет в обеспечении непрерывной доставки?	с 13:30 по 15:00	Валерий Филатов (ООО «ПВС»)
	ПЗ	Демонстрация работы PVS-Studio в качестве плагина. Запуск анализатора, первичная фильтрация отчета, подавление ложных срабатываний, просмотр отчета, исправление критических ошибок, работа с базой разметки (задания baseline-уровня), использование документации. Ответы на вопросы.	с 15:10 по 16:40	Владислав Богданов (ООО «ПВС»)
	ПЗ	Первая часть практического занятия по работе по поиску ошибок в коде с помощью PVS-Studio. Заранее будет предоставлен образ виртуальной Linux машины. В ней будет установлен плагин PVS-Studio для Visual Studio Code и находится отчет уже проверенного проекта на языке C. В течение часа нужно поработать с отчетом и выписать реальные ошибки. Параллельно следует подумать, как можно сократить количество ложных срабатываний (какие настройки можно сделать).	с 16:50 по 18:20	Александра Уварова (ООО «ПВС»)
		Вторая часть практического занятия, где мы обсуждаем найденные ошибки. Каждый участник обучения по очереди показывает и описывает найденный им баг (почему это баг, насколько он критичен, как его исправить). И разбирает одно из ложных срабатываний. Дискуссия, ответы на вопросы.		Александра Уварова (ООО «ПВС»)

УЧЕБНЫЙ ЦЕНТР  
МАСКОМ

09 октября 2024 года

Статический анализатор PVS-Studio на страже качества, защищенности и безопасности кода

Андрей Карпов  
PVS-Studio

УЧЕБНЫЙ ЦЕНТР  
МАСКОМ

11 октября 2024 года

PVS-Studio с точки зрения РБПО

PVS-Studio через призму  
ГОСТ Р 71207-2024  
Статический анализ ПО

Андрей Карпов  
PVS-Studio

УЧЕБНЫЙ ЦЕНТР  
МАСКОМ

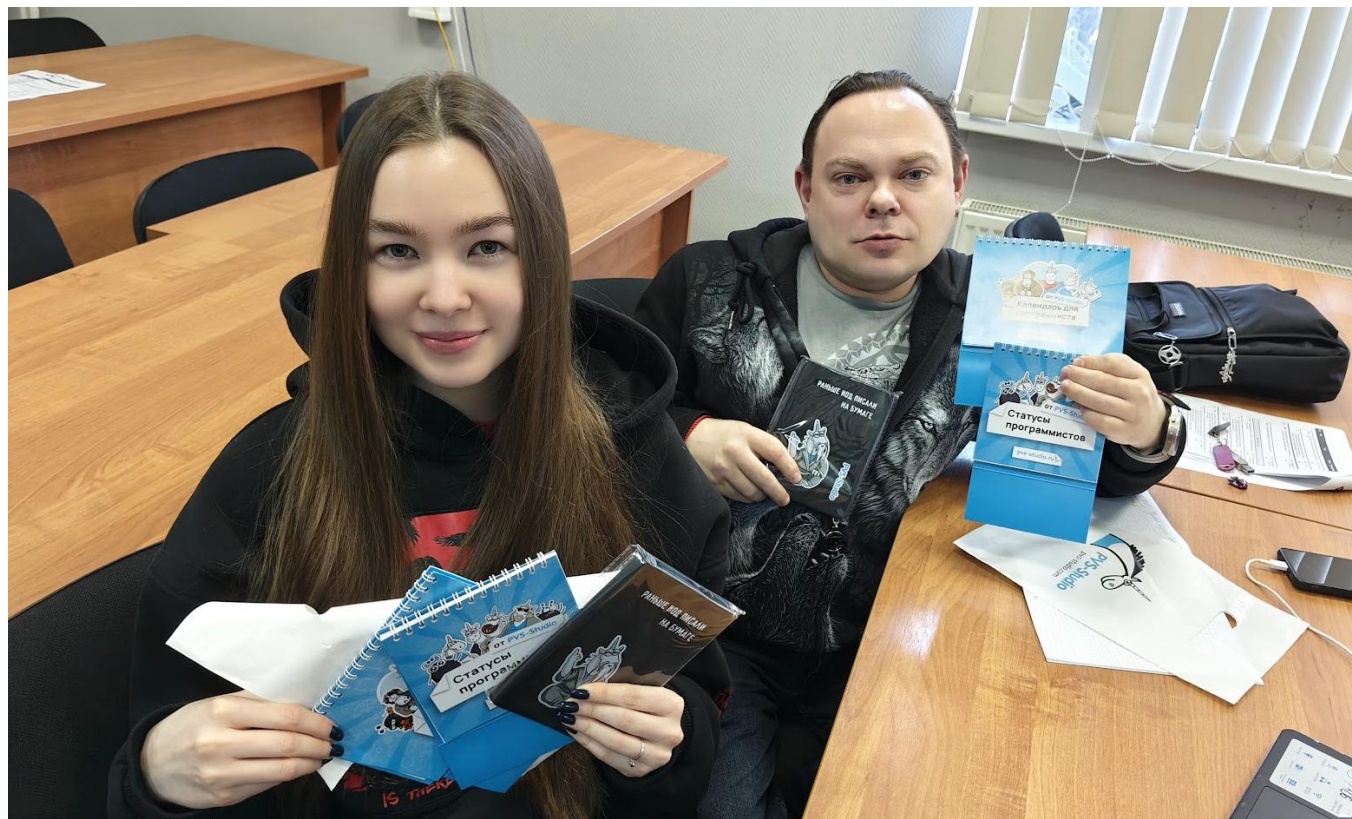
11 октября 2024 года

PVS-Studio с точки зрения РБПО

Статический анализ,  
безопасность и многое другое

Асламов Глеб  
PVS-Studio

# Участие команды PVS-Studio в наших курсах по РБПО/БРПО 2(2)



- <https://pvs-studio.ru>
- Более 15 лет на рынке
- C, C++, C#, Java
- Классификация предупреждений: CWE, MISRA, AUTOSAR, OWASP, CERT
- Работа в закрытом контуре
- Входит в реестр отечественного ПО: №9837
- Можно использовать для сертификации в испытательных лабораториях для проведения исследований до 4 уровня контроля
- Разрабатывается с учётом требований, предъявляемых к статическим анализаторам в ГОСТ Р 71207–2024





<https://mascom-uc.ru/>

**СПАСИБО  
ЗА ВНИМАНИЕ!  
ПРИХОДИТЕ К НАМ  
УЧИТЬСЯ!**

**Q&A**

**Виталий Пиков**

руководитель направления обучения  
по РБПО/БРПО, преподаватель  
НОУ ДПО «УЦБИ «МАСКОМ»

@UnderLineSecurity