

27 августа 2025 г.

Вебинар № 8
Вокруг РБПО за 25 вебинаров
Процесс № 8 ГОСТ Р 56939 – 2024:
Формирование и поддержание
в актуальном состоянии
правил кодирования

Виталий Александрович Пиков, руководитель направления обучения по РБПО,
преподаватель НОУ ДПО «УЦБИ «МАСКОМ».



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.



СТО TTTT.02.005—2024

УТВЕРЖДАЮ
Генеральный директор
ПАО «ИИИИИИИИ»

А.К. Петров

СТО TTTT.02.005—2024

СТАНДАРТ ОРГАНИЗАЦИИ

Система менеджмента качества РУКОВОДСТВО ПО РАЗРАБОТКЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Москва
2024

Приложение В (обязательное)

Требования к оформлению исходного кода программного обеспечения

к п. 6.3.1, приложению Л

Требования к оформлению исходного кода ПО могут быть разработаны индивидуально, согласовав их с Лабораторией БПО. Требования ниже используются как действующий пример, если не было предложено и согласовано другого варианта.

В.1 Именованние исходных файлов:

- все файлы должны иметь смысловое название;
- расширения файлов должны быть строчными буквами.

Модуль всегда начинается с описания, которое оформляется в виде комментария, достаточного для понимания его назначения.

Каждая правка в исходном коде модуля должна быть помечена датой и именем автора правки. Правки должны сопровождаться ясными комментариями, которые располагаются в начале файла исходного кода.

Если модуль содержит описание класса, то перед его объявлением должен присутствовать комментарий, содержащий назначение этого класса.

Для процедур, функций и методов класса необходимо краткое описание выполняемого действия, а также краткое описание смысла передаваемых параметров и возвращаемого результата.

Каждая функция, процедура или метод класса должны разделяться между собой строкой, состоящей из символов минуса «-», закомментированных однострочным комментарием. Длина строки должна составлять 80 символов.

Текст далее относится только к исполняемому коду.

Запись операторов:

- если оператор содержит блок более трёх размеров экрана, то закрывающая операторная скобка должна иметь поясняющий комментарий, указывающий, какой оператор закрывается;
- реализация набора, состоящего из четырёх и более операторов, повторяющихся 2 и более раз, должна быть оформлена в виде отдельной процедуры или функции;
- не рекомендуется использование вложенных процедур.

СТО ТТТТ.02.005—2024

Использование пустых строк:

- пустые строки должны использоваться в следующих местах:
- после декларации пакета;
- после секции импорта;
- между объявлениями классов;
- между объявлениями пользовательских типов;
- между реализациями методов;
- между интерфейсными секциями, которые логически связаны между собой.

V.2 Использование пробелов:

Не допускается использовать вместо пробелов табуляцию.

Пробелы должны использоваться в следующих местах:

- до и после оператора присваивания;
- до и после арифметических операторов в выражениях;
- до и после логических операторов в выражениях;
- после запятой при перечислении параметров функции во время вызова функции;
- после точки с запятой при перечислении параметров функции во время объявления функции;
- после двоеточия при объявлении переменной, параметров функции и типа результата функции;
- до и после знака «=» при объявлении типов и констант.

Не допускается использование пробелов в следующих местах:

- между именем метода и открывающей скобкой;
- после открывающей скобки или перед закрывающей;
- после открывающей квадратной скобки [или перед закрывающей];
- перед точкой с запятой;
- перед двоеточием при объявлении переменной, параметров функции и типа результата функции;
- между унарным оператором и его операндом.

V.3 Использование отступов:

Не допускается использовать для отступов символ табуляции.

Всегда необходимо использовать одно и то же количество пробелов, по отношению к предыдущему, для всех уровней отступа (либо два, либо четыре пробела).

СТО ТТТТ.02.005—2024

Первым уровнем считаются объявления функции, классов. На первом уровне отступы делать не нужно. Во всех остальных случаях необходимо наличие отступа.

Код внутри блока должен располагаться на следующем уровне. Завершающая операторная скобка должна находиться на том же уровне, что и открывающая операторная скобка.

Операторы одного уровня вложенности должны начинаться с одинаковыми отступами.

При объявлении класса области видимости располагаются на одном уровне с идентификатором класса. Все данные внутри класса располагаются на следующем уровне.

Суть и значение процесса № 8: почему это больше, чем «Code Style»?

Что такое «правила кодирования» в трактовке ГОСТ?

Это не только стиль оформления (отступы, имена), но и:

- **стандарты оформления кода:** читаемость, единообразие.
- **архитектурные принципы:** модульность, слабое зацепление.
- **запрещённые приёмы (anti-patterns):** уязвимые конструкции, «магические числа».
- **вопросы безопасности:** правила валидации входных данных, безопасная работа с памятью, шифрование.

Цели и задачи процесса: снижение количества уязвимостей, облегчение коллективной разработки, упрощение поддержки и аудита кода, автоматизация проверок.

Что будет, если процесс не внедрить? На примере кейса о декомпиляции: нечитаемый код невозможно эффективно модернизировать и защищать. Риск «магических чисел» и скрытых уязвимостей.

Детальный разбор требований стандарта:

- **Формирование правил.** Правила должны быть формализованы, документированы и доведены до всех разработчиков. Акцент на том, что правила должны быть практически применимыми, а не «бумажными».
- **Поддержание в актуальном состоянии.** Регулярный пересмотр и актуализация правил с учётом изменений в технологическом стеке, появления новых классов уязвимостей и анализа инцидентов.
- **Контроль соблюдения.** Обязательность автоматизированной проверки (инструменты статического анализа) и периодического ручного контроля (Code Review).

Связь с другими процессами ГОСТ:

- **Процесс про статический анализ (№ 10).** Правила кодирования – это входные данные для настройки анализаторов. Без правил нечего проверять.
- **Процесс про управление заимствованными компонентами (№ 16. 17).** Правила могут регламентировать использование сторонних библиотек.
- **Процесс про проведение тестирования безопасности (№ 10, 11, 18, 19).** Нарушения правил кодирования – это потенциальные объекты для тестирования.

Шаг 1: Разработка правил.

- **Что включать?** Базовые принципы (KISS, DRY, YAGNI), правила именования (``CamelCase``, ``snake_case``) , ограничение сложности функций, правила комментирования (использование ``docstring``), запрет на опасные конструкции.
- **Источники:** Industry best practices (CWE, OWASP), стили кодирования от крупных компаний (Google, Microsoft), собственный опыт.
- **Формат:** живой документ (Wiki, Markdown в Git), конфигурационные файлы для linters (``eslintrc``, ``clang-format``, ``editorconfig``).

Шаг 2: Интеграция в процесс разработки (DevSecOps).

- **Инструменты:** использование линтеров (ESLint, Pylint, SonarQube) и форматтеров (Prettier, Black).

- **Автоматизация:** встроенные проверки в CI/CD-пайплайн.

Коммит с нарушением правил => пайплайн не проходит => код не попадает в основную ветку. Это не рекомендация, а требование стандарта.

- **Code Review:** как последний рубеж защиты. На что смотреть ревьюерам помимо функциональности?

Шаг 3: Обучение и поддержание актуальности.

- **Обучение команды:** проведение воркшопов, ведение чата для вопросов, код-лабы.
- **Актуализация правил:** Регулярный (раз в квартал/полгода) пересмотр правил на основе обратной связи от команды и данных со статических анализаторов.

Типичные ошибки:

- Создание **слишком объёмного и невнятного документа**, которым никто не пользуется.
- **Отсутствие автоматизации** проверок.
- **Неприменимость правил на практике** (например, слишком жёсткие требования к legacy-коду).
- **Игнорирование обратной связи** от разработчиков.

Лучшие практики:

- **Постепенное внедрение**: начните с 10 самых критичных правил.
- **«Живой» документ**: правила должны развиваться.
- **Единообразие**: используйте форматтеры кода для гарантии соблюдения стиля.
- **Лидерство примера**: архитекторы и тимлиды должны сами строго следовать правилам.

Резюме: Правила кодирования по ГОСТ Р 56939–2024 – это обязательный, формализованный и актуальный набор требований, интегрированный в CI/CD и поддерживаемый инструментами.

Ключевой вывод: Качество и безопасность кода закладываются на этапе написания. Правила кодирования – это основной инструмент для обеспечения этого качества.

Совет дня!

Начните с малого – например, с форматера кода и пары правил статического анализа (**PVS-Studio**).

Для погружения в тему рекомендуется изучить следующие ресурсы:

Обязательная литература:

1. ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Первоисточник. Необходимо внимательно изучить раздел, касающийся процесса № 8 и смежных процессов.

2. Макконнелл С. «Совершенный код» (Code Complete).

Фундаментальный труд о качестве кода. Освещает принципы, лежащие в основе хороших правил кодирования: читаемость, организация кода, работа с переменными.

3. Мартин Р. («Дядя Боб») «Чистый код: создание, анализ и рефакторинг».

Классическая книга, посвящённая практике написания чистого, понятного и поддерживаемого кода. Даёт множество конкретных примеров и принципов.

Для углубленного изучения:

4. ГОСТ Р 58412 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения».

Помогает понять, от каких угроз защищают те или иные правила кодирования.

Дополнительные материалы и стандарты:

5. Статья «Оформление кода / Хабр». <https://habr.com/en/articles/145850/>

Практические советы по оформлению кода, именованию переменных и функций, основанные на книге Макконнелла.

6. Статья «Что такое «правильный код» и как его писать». <https://blog.skillfactory.ru/chto-takoe-pravilnyy-kod-i-kak-ego-pisat/>

Отличный современный обзор принципов чистого кода и рефакторинга на русском языке.

7. Microsoft's C# Coding Conventions.

https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82_%D0%BE%D1%84%D0%BE%D1%80%D0%BC%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BE%D0%B4%D0%B0

Пример хорошо структурированного и детализированного стандарта кодирования от крупной IT-компании. Полезно для ознакомления, даже если вы не пишете на C#.

8. Python PEP 8 - Style Guide for Python Code. <https://peps.python.org/pep-0008/>

Яркий пример того, как правила кодирования встроены в культуру языка программирования. Демонстрирует высокий уровень зрелости процесса.

9. Обзор ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». <https://ksb-soft.ru/blog/obzor/obzor-gost-r-56939-2024-rbpo/>

Поскольку правила тесно связаны со статическим анализом, полезно изучить инструменты (например, PVS-Studio) и подходы к их настройке.

10. Статья «Поддержка актуальности документации...» на Хабре. <https://habr.com/en/articles/866198/>

Раскрывает философию подхода «as Code», которую можно и нужно применять к правилам кодирования (правила как код, проверки как код).



Clean Code Principles and Patterns

*A Software Practitioner's
Handbook*

PETRI SILÉN

Copyright © 2023 Petri Silén
All rights reserved.
ISBN: 9780379357732



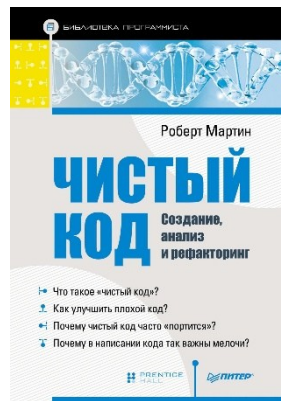
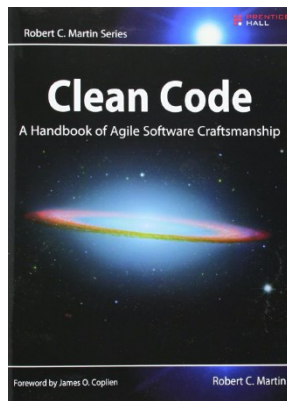
O'REILLY®

Рецепты чистого кода



SPRINT
BOOK

Максимилиано Контьери



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



СПАСИБО ЗА ВНИМАНИЕ!
ПРИХОДИТЕ К НАМ УЧИТЬСЯ!



**Учебные курсы
по процессам разработки
безопасного программного обеспечения**

Серия учебных курсов: «М БРПО...»

Серия учебных курсов по направлению «Безопасная разработка программного обеспечения»



М БРПО-02 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



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 ч



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 к 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 час



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

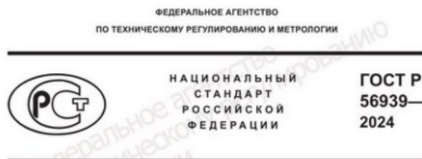
Программа курса охватывает всё необходимое для подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России, внедрения процессов разработки безопасного программного обеспечения на предприятии с учётом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

03.09.2024-05.09.2024
01.10.2024-03.10.2024



Пиков Виталий
Александрович

Время
30 часов / 3 дня



Защита информации
**РАЗРАБОТКА БЕЗОПАСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**
Общие требования

Издание официальное

Метрология

ГОСТ Р
56939—
2016

Москва
Российский институт стандартизации
2024

**РАЗРАБОТКА БЕЗОПАСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**
Общие требования

Издание официальное



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» приказываю:

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.

Внедрен ГОСТ Р 56939-2016.

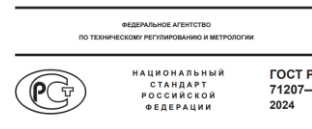
2. Управлению стандартизации обеспечить размещение информации об утвержденном настоящим приказом стандарте на официальном сайте Роставтарга в информационно-телекоммуникационной сети «Интернет» (далее – официальный сайт) с учетом законодательства о стандартизации.

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

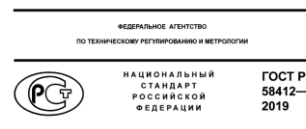
А.П.Шаев



Защита информации
**РАЗРАБОТКА БЕЗОПАСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**
Статический анализ программного обеспечения.
Общие требования

Издание официальное

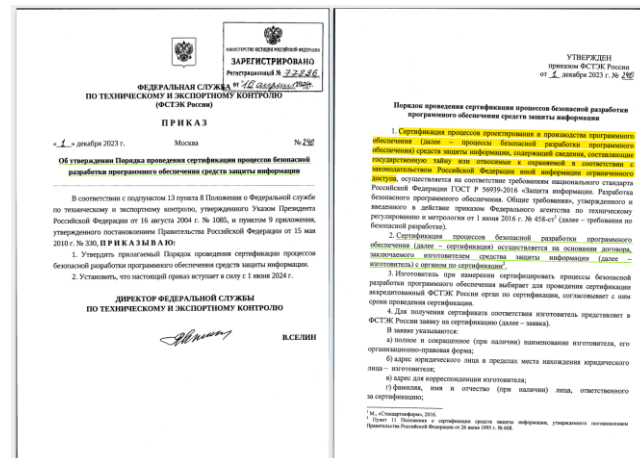
Москва
Российский институт стандартизации
2024



Защита информации
**РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ**
Угрозы безопасности информации при разработке
программного обеспечения

Издание официальное

Москва
Стандартинформ
2019



Кто научит? - УЦ МАСКОМ !

Задействовано более 10 лучших преподавателей

Недогарок Антон Александрович



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.

Буянов Сергей Васильевич



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.

Преподаёт 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.

Большунов Валерий Владимирович



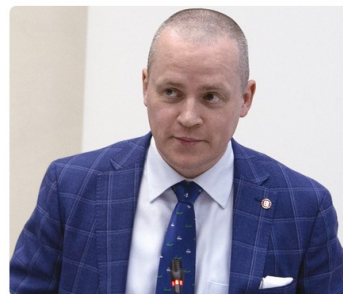
Общий стаж работы: более 22 лет

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.

Пиков Виталий Александрович



Общий стаж работы: более 26 лет

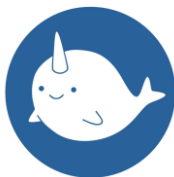
Стаж преподавательской работы: более 10 лет



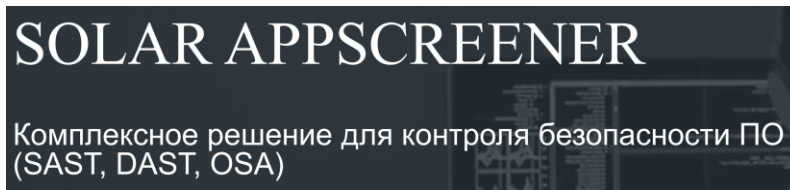
УЧЕБНЫЙ ЦЕНТР
БЕЗОПАСНОСТИ ИНФОРМАЦИИ
Год основания: 1998







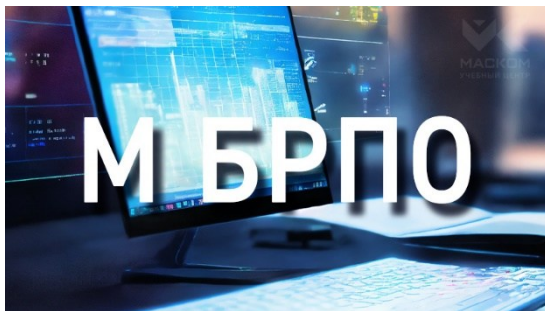
Сканер-ВС
анализ защищённости



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

Курсы предназначены:

- 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.



Программы курсов направлены на подготовку полноценного специалиста, обладающего всеми необходимыми компетенциями для ведения профессиональной деятельности и имеющего глубокие теоретические знания и практические навыки по направлению разработки безопасного программного обеспечения с учётом актуальной нормативной правовой базы (ГОСТ Р 56939–2024/2016, методологий SSDLC и DevSecOps).

Успешно прошедшие обучение смогут самостоятельно разработать для своей организации:

- ✓ дорожную карту (алгоритм) подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России;

- ✓ дорожную карту (алгоритм) внедрения БРПО на предприятии;

- ✓ проект Руководства БРПО предприятия;

- ✓ проекты документов предприятия в соответствии с ГОСТ Р 56939–2024/2016.

