

28 января 2026

г.

Вебинар 25.

Обеспечение безопасности при выводе программного обеспечения из эксплуатации

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

ДИСКЛЕЙМЕР / DISKLAIMER

• 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. Некоторые высказывания, сказанные в ходе выступления, предназначены исключительно для юмористических целей и не несут 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. 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 несет 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, а некоторые высказывания, сказанные в ходе выступления, предназначены исключительно для юмористических целей и не используются 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.



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 40 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.



РБПО — это сокр. от «Разработка безопасного программного обеспечения» (РБПО).

ГОСТ Р 56939-2024

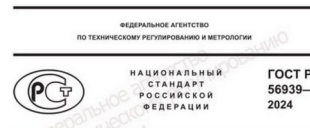
«**3.1 безопасное программное обеспечение:** Программное обеспечение, разработанное в ходе реализации совокупности процессов (мер), **направленных на предотвращение появления и устранение недостатков программы**».

ГОСТ Р 56939-2016

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

ГОСТ Р 56939-2024

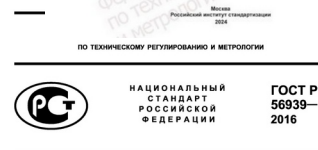
«**3.8 недостаток программы:** Любое несоответствие программы заданным требованиям или любая ошибка, допущенная в ходе проектирования или реализации программы, которая в случае её неисправления может являться причиной невозможности выполнения требуемых функциональных возможностей или уязвимости программы».



Защита информации
РАЗРАБОТКА БЕЗОПАСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

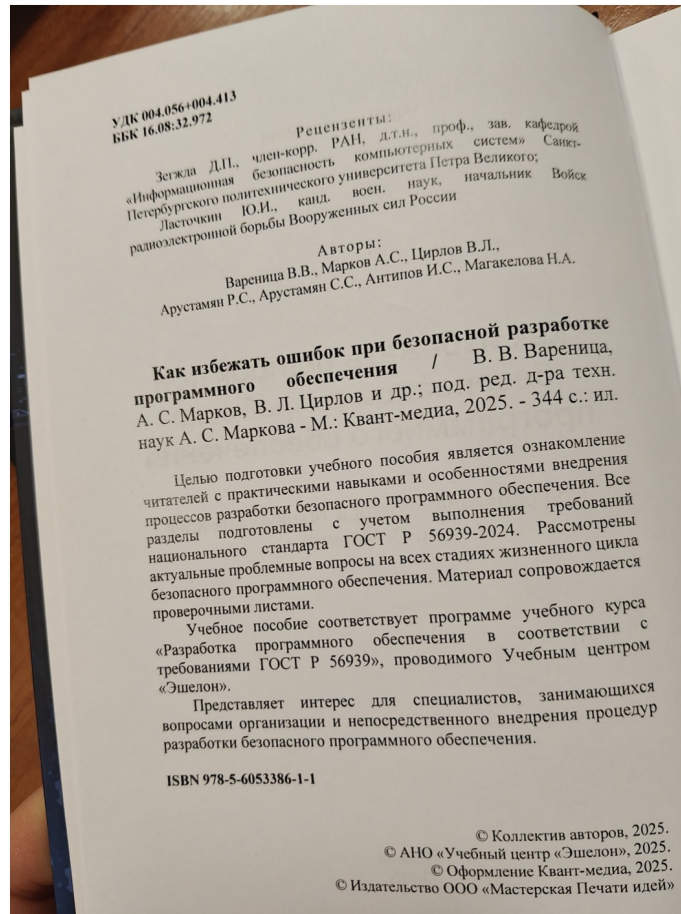
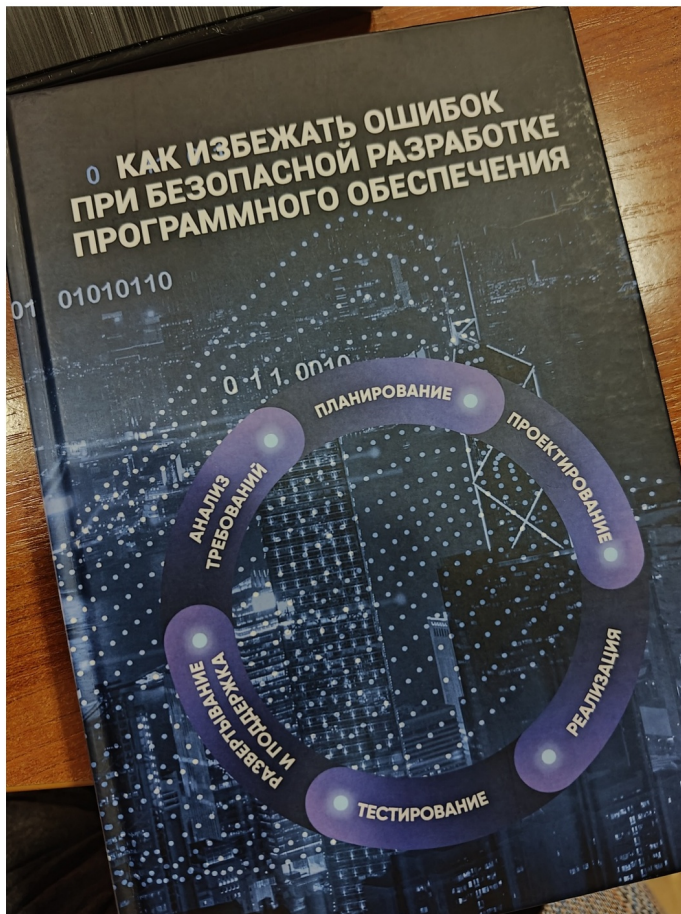
Издание официальное



Защита информации
РАЗРАБОТКА БЕЗОПАСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Общие требования

Издание официальное





Цель процесса (1/2)

Целью данного процесса является **недопущение реализации угроз безопасности, связанных с эксплуатацией неподдерживаемой версии ПО.**

Данный процесс реализуется **на этапе эксплуатации** - завершающей стадии жизненного цикла, как показано на рисунке.

*Место процесса
обеспечения безопасности
при выводе ПО из эксплуатации*



Требования национального стандарта к обеспечению безопасности при выводе ПО из эксплуатации включают следующее:

- разработку регламента;
- информирование пользователей;
- четкое определение условий и процедур.

Необходимо определить условия вывода из эксплуатации исходя из особенностей разрабатываемого ПО.

Как правило, **к основным условиям вывода ПО (версий ПО) из эксплуатации можно отнести следующие случаи:**

- окончание жизненного цикла, объявленного поставщиком;
- техническое устаревание: несовместимость с современными ОС, аппаратурой или стандартами безопасности;
- переход на новую версию/платформу (например, миграция на облачное решение);
- отсутствие возможности обеспечения поддержки;
- высокие риски безопасности (например, обнаружение критических уязвимостей, которые невозможно устранить).

Роли и обязанности сотрудников

Здесь следует установить **обязанности сотрудников**, которые будут вовлечены в процесс вывода из эксплуатации и будут нести за него ответственность.

В таблице приведены примеры ролей и соответствующих им обязанностей.

Роль	Обязанности
Руководитель проекта	Утверждает план вывода, контролирует сроки, распределяет ресурсы.
Ответственный за вывод ПО	Координирует процесс, готовит документацию, взаимодействует с пользователями.
Технический специалист	Обеспечивает миграцию данных, архивацию, отключение сервисов.
Служба поддержки	Информирует пользователей, собирает обратную связь, помогает с переходом.

Необходимо информировать пользователей о планах прекращения технической поддержки ПО (версии ПО) и своевременно уведомлять их об этом.

Для соответствия данному требованию должны быть определены и реализованы методы уведомления, например, такие как:

- рассылка по электронной почте с четким указанием сроков и возможных альтернатив;
- уведомление в интерфейсе ПО;
- обновление документации: добавление раздела «Планы прекращения поддержки»;
- публикация на корпоративном сайте/портале.

Рекомендуется установить конкретные сроки уведомлений, например:

- первое уведомление - за 6 месяцев до прекращения поддержки.
- повторное уведомление - за 3 месяца с деталями миграционного плана.
- финальное уведомление - за 1 месяц до отключения.

Процесс информирования пользователей. Практические рекомендации (1/2).

Приведем практические рекомендации для разработчиков, сотрудников службы поддержки и руководителей.

1. Для разработчиков:

- внедрите автоматические уведомления в интерфейс ПО (например, pop-up при запуске);
- добавьте в код метку EOL_DATE для автоматической блокировки ПО после указанной даты;
- обеспечьте архивацию данных и инструменты для их экспорта в новую систему.

Процесс информирования пользователей. Практические рекомендации (3/2).

Приведем практические рекомендации для разработчиков, сотрудников службы поддержки и руководителей.

2. Для службы поддержки:

- создайте FAQ по переходу на новую версию;
- организуйте обратную связь через тикет-систему или форму на сайте; ведите журнал обращений, чтобы выявить пользователей, которые не завершили миграцию.

3. Для руководителей:

- по возможности включите дату окончания поддержки в договоры с новыми клиентами;
- регулярно проводите аудит используемых версий ПО для своевременного вывода устаревших.

Стало быть, при выводе ПО из эксплуатации требуется убедиться, что:

- пользователи были заранее уведомлены;
- данные экспортированы и архивированы;
- серверы/сервисы отключены;
- документация обновлена.

В ГОСТ Р 56939-2024 имеется требование к разработке регламента вывода ПО из эксплуатации, который должен содержать:

- описание условий вывода ПО из эксплуатации;
- обязанности сотрудников;
- роли сотрудников при осуществлении вывода ПО из эксплуатации ПО;
- порядок оповещения пользователей о планах прекращения технической поддержки ПО (версии ПО).

В таблице представлен вариант чек-листа, который определяет требования к обеспечению безопасности при выводе ПО из эксплуатации.

Проверочный лист требований к обеспечению безопасности:

№ п/п	Требование	Выполнение
5.25.2.1	Разработан регламент вывода ПО из эксплуатации, который должен содержать описание условий, при которых ПО (версию ПО) необходимо выводить из эксплуатации, обязанности сотрудников и их роли при осуществлении вывода ПО из эксплуатации ПО и порядок оповещения пользователей о планах прекращения технической поддержки ПО (версии ПО).	
5.25.3.1		
5.25.2.2	Реализовано своевременное информирование пользователя о планах прекращения технической поддержки ПО (версии ПО)	

Процесс № 25 — не просто «завершение», а активная мера защиты.

Грамотный вывод ПО из эксплуатации:

- снижает риски компрометации;
- сохраняет доверие пользователей;
- обеспечивает соответствие ГОСТ Р 56939-2024.

Не забывайте, безопасность ПО должна быть обеспечена на всех этапах его жизненного цикла — от проектирования до окончательного вывода.

Распространённые ошибки

- отсутствие формального (действующего) регламента;
- молчаливое прекращение поддержки без уведомления;
- недостаточная информация о рисках использования старой версии;
- отсутствие рекомендаций по миграции.

Эти ошибки могут привести к инцидентам ИБ и юридическим последствиям.

СПАСИБО БОЛЬШОЕ ЗА ВНИМАНИЕ! ПРИХОДИТЕ К НАМ УЧИТЬСЯ!



@MASCOM_UC

ПОДПИСЫВАЙТЕСЬ
НА ОФИЦИАЛЬНЫЙ ТЕЛЕГРАМ-КАНАЛ!



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



@UNDERLINESECURITY

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



**Учебные курсы
по обеспечению безопасности
значимых объектов КИИ
Российской Федерации**

Учебные курсы: «ПМ 5», «М 3.7»,

Информационная безопасность. Безопасность значимых объектов критической информационной инфраструктуры

С 01 января 2021 г. вступили в силу требования Приказа ФСТЭК России 2017 г. №235 к уровню подготовки специалистов подразделений обеспечения безопасности значимых объектов КИИ: Работники структурного подразделения по безопасности, специалисты по безопасности должны соответствовать следующим требованиям:

- наличие у руководителя структурного подразделения по безопасности высшего профессионального образования по направлению подготовки в области ИБ или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению «Информационная безопасность»;
- прохождение не реже одного раза в 3 года обучения по программам повышения квалификации по направлению «Информационная безопасность».

По окончании обучения слушатели получают Диплом о профессиональной переподготовке.

ВНИМАНИЕ!
ДАТЫ НА КУРС ОБСУЖДАЮТСЯ ИНДИВИДУАЛЬНО ПРИ ЗАКЛЮЧЕНИИ ДОГОВОРА!

В соответствии с Указом Президента РФ 2022 г. №250 и Постановлением Правительства РФ 2022 г. №1272, организации, являющиеся субъектами КИИ, обязаны «возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты». Указанное должностное лицо «должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки

Стоимость:	
Очное обучение	130 000 Р
Длительность:	502 ч
Форма обучения	очно-заочная



Открытый курс

По окончании обучения вы получаете:



Необходимые документы:

при отсутствии – прохождение курса невозможно

- Копия СНИЛС и диплома о высшем профессиональном образовании.



Согласовано с ФСТЭК России

Серия учебных курсов по направлению «Обеспечение безопасности ЗО КИИ Российской Федерации»

Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

С 01 января 2021 г. вступают в силу требования ФСТЭК к уровню подготовки специалистов подразделений по безопасности значимых объектов КИИ (см. изменения в Приказ ФСТЭК от 2017 г. №235):

- Руководитель подразделения (в зависимости от базового образования) должен иметь документ о профессиональной переподготовке по направлению «Информационная безопасность». Предлагаем к изучению курс ПМ 2 «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»;
- Работники подразделения (в зависимости от базового образования) должны иметь документ о повышении квалификации по направлению «Информационная безопасность».

По окончании обучения слушатели получают Удостоверение о повышении квалификации.

С 01 января 2021 г. вступают в силу требования ФСТЭК к уровню подготовки специалистов подразделений по безопасности значимых объектов КИИ (см. изменения в Приказ ФСТЭК от 2017 г. №235):

Руководитель подразделения (в зависимости от базового образования) должен иметь документ о профессиональной переподготовке по направлению «Информационная безопасность». Предлагаем к изучению курс ПМ 2 «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну». Работники подразделения (в зависимости от базового образования) должны иметь документ о повышении квалификации по направлению «Информационная безопасность».

Предлагаем к изучению курс М 3.7 «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».

Стоимость:	
Очное обучение	53 000 Р
Длительность:	108 часов
Форма обучения	очная очно-заочная дистанционная



Открытый курс

По окончании обучения вы получаете:



Необходимые документы:

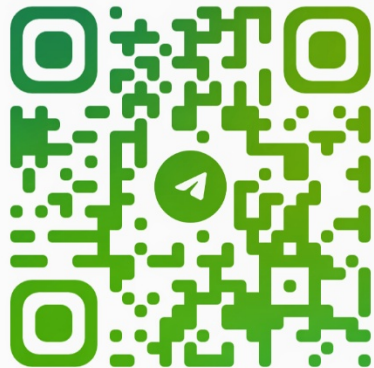
при отсутствии – прохождение курса невозможно

- Копия СНИЛС и диплома о высшем профессиональном образовании.



Согласовано с ФСТЭК России

ПОДПИСЫВАЙТЕСЬ НА ОФИЦИАЛЬНЫЙ ТЕЛЕГРАМ-КАНАЛ!



@MASCOM_UC



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



@UNDERLINESECURITY

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

Серия учебных курсов: «М БРПО...»

Серия учебных курсов по направлению «Безопасная разработка программного обеспечения»



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.

М БРПО-Спец



02.09.2024-27.09.2024
30.09.2024-25.10.2024



Пиков Виталий
Александрович

Время
200 часов / 20 дней



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.

М БРПО-01



03.09.2024-06.09.2024
01.10.2024-04.10.2024



Пиков Виталий
Александрович

Время
40 часов / 4 дня



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.

М БРПО-02



02.09.2024-06.09.2024
30.09.2024-04.10.2024



Пиков Виталий
Александрович

Время
50 часов / 5 дней



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.

М БРПО-03



03.09.2024-23.09.2024
01.10.2024-21.10.2024



Пиков Виталий
Александрович

Время
140 часов / 14 дней



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.

М БРПО-04



03.09.2024-23.09.2024
01.10.2024-21.10.2024



Пиков Виталий
Александрович

Время
140 часов / 14 дней



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.

М БРПО-05

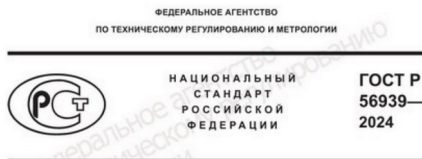


03.09.2024-05.09.2024
01.10.2024-03.10.2024



Пиков Виталий
Александрович

Время
30 часов / 3 дня



Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

рологии

ГОСТ Р
56939—
2016

Москва
Российский институт стандартизации
2024

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва
Стандартинформ
2016



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» и в целях:

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.

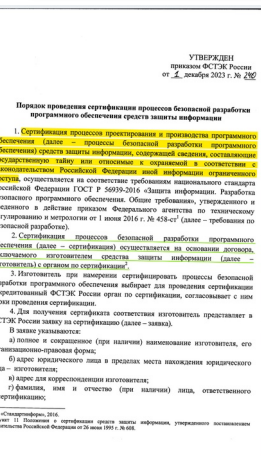
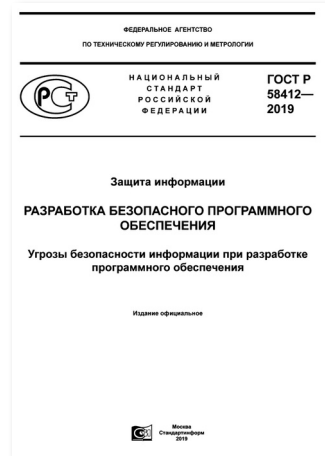
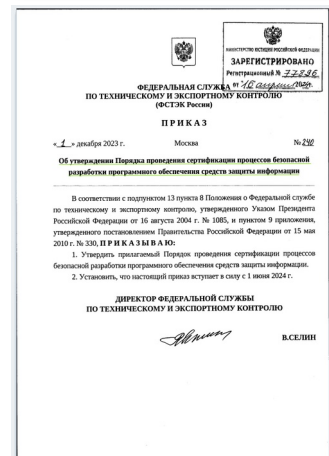
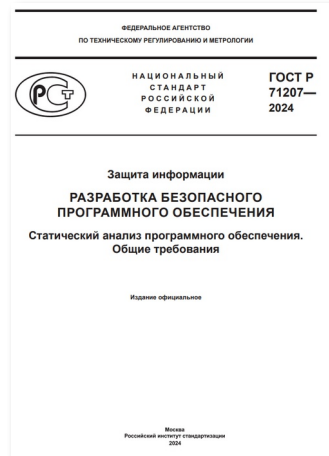
2. Управлению стандартизации обеспечить размещение информации об утвержденном настоящим приказом стандарте на официальном сайте Ростстандарта в информационно-телекоммуникационной сети «Интернет» (далее – официальный сайт) с учетом законодательства о стандартизации.

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



В ногу со временем!!!

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

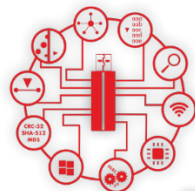
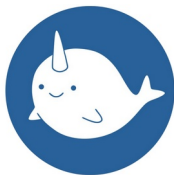
Стаж преподавательской работы: более 10 лет



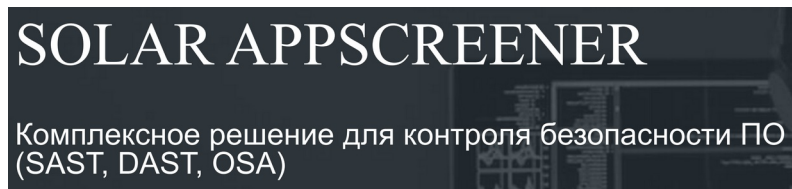
УЧЕБНЫЙ ЦЕНТР
БЕЗОПАСНОСТИ ИНФОРМАЦИИ
Год основания: 1998







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.



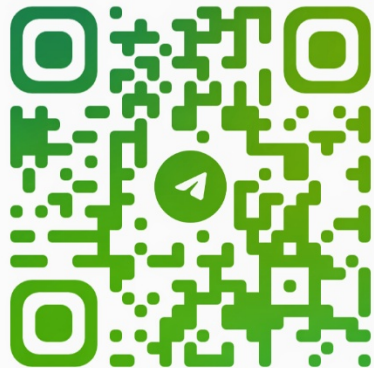
Программы курсов направлены на подготовку полноценного специалиста, обладающего всеми необходимыми компетенциями для ведения профессиональной деятельности и имеющего глубокие теоретические знания и практические навыки по направлению разработки безопасного программного обеспечения с учётом актуальной 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.



ПОДПИСЫВАЙТЕСЬ НА ОФИЦИАЛЬНЫЙ ТЕЛЕГРАМ-КАНАЛ!



@MASCOM_UC



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



@UNDERLINESECURITY