

10 декабря 2025 г.

Вебинар 22.

Обеспечение поддержки программного обеспечения при эксплуатации пользователями

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



ПИКОВ
Виталий
Александрович

Общий стаж работы: более 27 лет.

Стаж преподавательской работы: более 11 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.

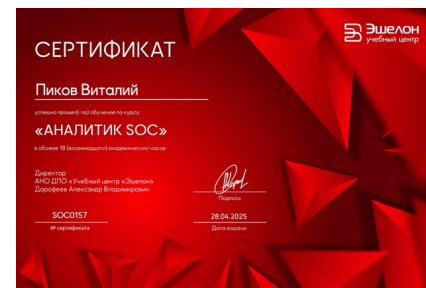
Автор более 40 научных публикаций.

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.

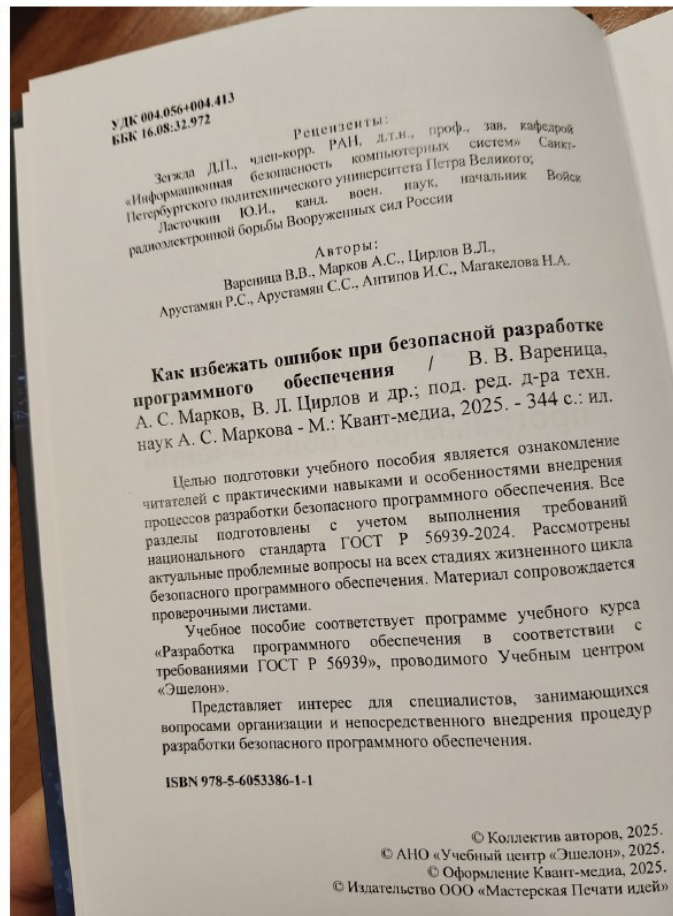
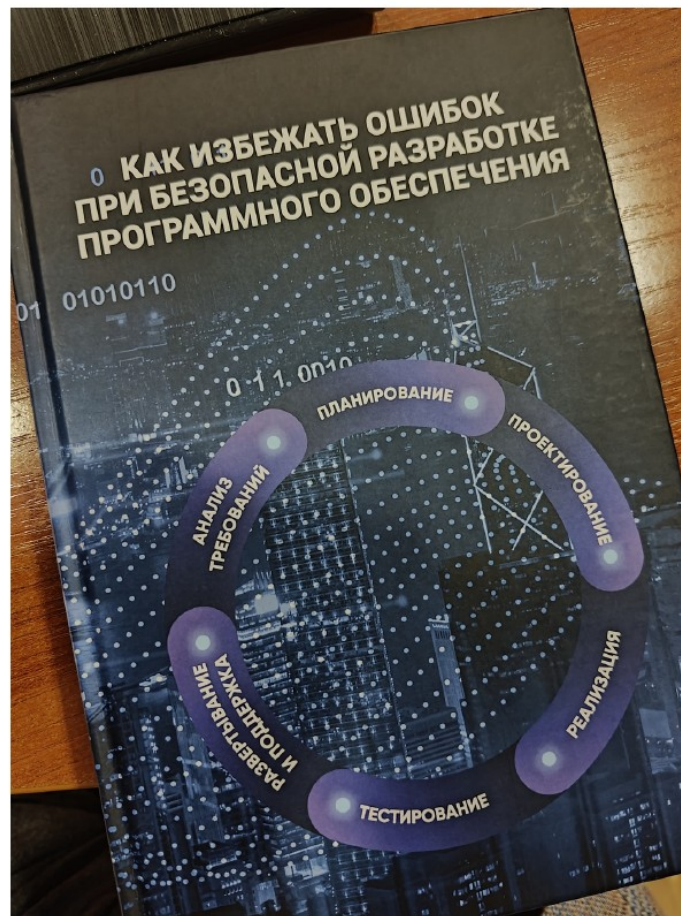
Авторизованный преподаватель по продуктам «Группы Астра» с правом проведения курсов по ОС Astra Linux Special Edition 1.8

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



Обеспечение поддержки программного обеспечения при эксплуатации пользователями





Цель процесса

После того, как разработанное ПО было протестировано в ходе приёмки и поставлено пользователям, происходит переход на **этап поддержки и сопровождения ПО** на последней стадии жизненного цикла.

Целью данного процесса является обеспечение технической поддержки ПО при его эксплуатации с целью устранения выявляемых в ходе использования и обновления ПО недостатков.



Требования к реализации (1/7)

Для обеспечения технической поддержки **необходимо реализовать целый ряд требований.**

Первое требование - организовать работу службы технической поддержки.

Для этого следует сначала определить обязанности сотрудников и их роли при оказании технической поддержки.

Обычно для технической поддержки используется **трёхуровневая модель, включающая 3 линии**, описание задач и ролей сотрудников каждой из них представлено в таблице.

Уровни технической поддержки (2/7)

Уровень поддержки	Основные задачи	Роли
Первый уровень (L1)	Первичный приём заявок от пользователей. Решение тривиальных проблем. Фильтрация и передача проблем, требующих более детального анализа на уровень L2.	Операторы колл-центра. Специалисты первой линии техподдержки.
Второй уровень (L2)	Решение технических проблем, связанных с настройками и конфигурацией ПО. Взаимодействие с пользователями, передача проблем разработчикам ПО. Анализ системных сбоев.	Инженеры поддержки. Специалисты по базе знаний. Разработчики ПО.
Третий уровень (L3)	Первичное исправление багов и выпуск патчей. Оптимизация производительности. Работа с инфраструктурой.	Разработчики ПО. DevOps-инженеры. Архитектор ПО.

Для каждого уровня технической поддержки необходимо определить перечень используемых инструментов.

Например, это могут быть различные инструменты.

Следующее требование - разработка процедуры оповещения пользователей о выходе обновлений и необходимости их установки.

Данные уведомления делятся на 2 вида:

- критические уведомления;
- плановые уведомления.

Категория	Инструментарий
Управление заявками (тикетами)	Service Desk
	Help Desk
Мониторинг и регистрирование	Prometheus
	Grafana
	Zabbix
	Elasticsearch + Logstash + Kibana (ELK Stack)
	Graylog
Организация удалённого доступа	AnyDesk
	TeamViewer
	Virtual Network Computing (VNC)
	Secure Shell (SSH)
	Remote Desktop Protocol (RDP)
Анализ сетевого трафика, сетевых служб и системных процессов	Wireshark
	Process Explorer
	Strace
	nmap
	iperf
Документирование	Confluence
	MediaWiki
	MkDocs
Автоматизация процессов технической поддержки (рутинных операций)	Ansible
	PowerShell
	Terraform
	Jenkins
	GitLab CI/CD
	Rundeck
Управление конфигурацией	Microsoft System Center Configuration Manager (SCCM)
	SaltStack
	Puppet
	Chef

Критические уведомления - сообщения пользователям о серьезных уязвимостях, критических ошибках или угрозах безопасности, требующих немедленного реагирования, например, установки обновления.

Например, это могут быть уведомления о выпуске исправления уязвимостей «нулевого дня», критических багов, препятствующих корректной работе ПО.

Согласно приказу ФСТЭК России от 2 июня 2020 г. № 76 при выявлении таких недостатков на разработку компенсирующих мер или ограничений по применению средства, а также на доведение информации о таких мерах до потребителя выделяется срок не более 72 и 48 часов для 5 и 4 уровня доверия соответственно с момента уведомления пользователя о наличии такого недостатка.

Плановые уведомления - информация о регулярных обновлениях, новых функциях или незначительных исправлениях.

К таким сообщениям, например, могут быть отнесены уведомления о выпуске минорных версий ПО, обновлений интерфейса.

Иными словами, речь идет об обновлениях, не влияющих на безопасность ПО.

Такой вид уведомлений не имеет фиксированных сроков отправки и может производиться на основе составленного разработчиком плана, например, раз в неделю или раз в месяц.

Требования к реализации (5/7)

Для организации процесса оповещения пользователей, существует множество каналов связи и для каждого ПО необходимо выбирать способ в зависимости от важности обновления, доступности тех или иных механизмов в системе и т.д.

Наиболее распространённые способы для оповещения пользователей это:

- уведомление в пользовательском интерфейсе о выходе обновления;
- принудительное обновление;
- отправка писем по электронной почте с информацией о выходе обновления;
- публикации на официальном сайте разработчика и в соцсетях;
- push-уведомления (в случае мобильных приложений);
- автоматическое обновление через системы корпоративного взаимодействия (для корпоративных клиентов).

Аналогичные процедуры должны быть разработаны и для оповещения пользователей о выявлении уязвимостей.

Дополнительно в организацию работы службы поддержки входит обеспечение обратной связи от пользователя. Команде поддержки следует реализовать сбор и анализ обратной связи, предоставляемой клиентами.

Для получения такой информации могут быть использованы:

- опросы пользователей после обращений в службу поддержки;
- анализ обращений на предмет повторяющихся проблем;
- анализ журналов использования ПО (предоставляемых пользователями);
- отзывы на официальном сайте, платформах предоставления ПО и форумах.

Полученная информация может быть использована для:

- приоритизации исправления проблем в программном обеспечении;
- улучшения пользовательского интерфейса и пользовательской документации;
- добавления новых востребованных функций;
- оценки эффективности работы технической службы поддержки.

Основные метрики, которые могут быть использованы для оценки эффективности:

- время первого реагирования на запрос (First Response Time – FRT);
- время разрешения проблемы;
- процент разрешённых проблем на первой линии поддержки без обращения к высшим уровням;
- уровень удовлетворённости работой технической поддержкой пользователей ПО (Net Promoter Score – NPS).

Следующее требование - **организовать обучение специалистов данной службы работе с программным обеспечением.**

На протяжении всего этапа эксплуатации программного обеспечения специалисты службы должны проходить обучение по работе с поставляемым пользователю ПО, особенностям его установки, настройки и функционирования.

Такое обучение должно включать:

- сведения об ограничениях работы ПО и указаниях по его эксплуатации в соответствии с поставляемыми руководствами;
- сведения о внутренней эксплуатационной документацией на ПО.

Данная мера способна позволить повысить уровень эффективности работы технической службы поддержки.

Главным результатом данного процесса должен стать **регламент технической поддержки**, который содержит такие сведения как:

- обязанности сотрудников и их роли при оказании технической поддержки;
- описание организации службы технической поддержки (режим работы, сроки оказания услуг и т.п.);
- перечень используемых инструментов;
- описание процедуры взаимодействия службы поддержки с пользователями;
- описание процедур оповещения пользователей о выпуске обновлений (включая обновления безопасности) и необходимости их установки;
- описание процедур информирования пользователей ПО о выявленных уязвимостях и способах реализации мер по их нейтрализации до разработки обновлений безопасности, устраняющих уязвимость, по установленным каналам взаимодействия;
- информация об обучении сотрудников службы технической поддержки.

Рассмотрим более подробно требования, которые предъявляются к регламенту. В первую очередь служба технической поддержки строится на четком распределении ролей, где каждый специалист выполняет конкретные задачи в зависимости от уровня эскалации запроса.

Оператор поддержки (L1) отвечает за первичный приём и классификацию обращений - например, регистрирует запрос в системе управления заявками (Jira, ServiceNow).

Технический специалист (L2) проводит углублённый анализ, включая воспроизведение ошибки в тестовой среде, чтобы точно определить её причину.

Эксперт по безопасности (L3) подключается, если обнаружена уязвимость. Он оценивает её критичность и координирует устранение с командой разработки.

Менеджер поддержки контролирует соблюдение SLA, анализирует метрики качества (время реакции, процент решенных запросов) и готовит отчёты - например, еженедельную сводку по инцидентам высокой важности.

Чтобы обеспечить оперативное реагирование, необходимо четко определить **режим работы технической поддержки**.

Это может быть **круглосуточная поддержка** в случае критических инцидентов и **стандартное рабочее время** для остальных запросов.

Также каждому обращению присваивается **приоритет**, от которого зависят сроки решения.

Далее необходимо указать **конкретный канал связи**, а также последовательность обработки поступающих запросов.

К примеру, **автоматическое присвоение ID запроса**, затем определение **категории ошибки** и далее **последующая эскалация запроса** при обнаружении уязвимости и т.п.

На следующем этапе описывается, как пользователи будут получать информацию об обнаруженных уязвимостях в программном обеспечении и о том, как защитить себя от этих уязвимостей до выхода официального обновления, устраняющего проблему.

Наконец, **на заключительном этапе** требуется подтвердить **компетенции команды технической поддержки** и указать сведения о пройденном обучении (семинары, курсы, вебинары), подтверждающие квалификацию сотрудников в части работы с данным ПО, включая его установку, эксплуатацию и ограничения.

Таким образом, разработанный регламент обеспечивает прозрачность, быстрое реагирование и минимизацию ущерба, а все этапы документируются для упрощения последующего аудита.

Приводим пример **проверочного листа**, который удобно использовать при реализации процесса обеспечения поддержки ПО при эксплуатации пользователями.

Проверочный лист требований к обеспечению поддержки программного обеспечения при эксплуатации пользователями->

Проверочный лист (1/2)

№ п/п	Требование	Выполнение
5.22.2.1	<p>Разработан регламент технической поддержки.</p> <p>Регламент технической поддержки содержит следующие сведения:</p> <ul style="list-style-type: none"> – обязанности сотрудников и их роли при оказании технической поддержки; – описание организации службы технической поддержки: режим работы, сроки оказания услуг по технической поддержке пользователей, иная информация об организации службы технической поддержки; – используемые инструменты; – описание процедуры взаимодействия службы технической поддержки с пользователями (способы получения обращений пользователей, процесс обработки поступающих сообщений и др.); 	

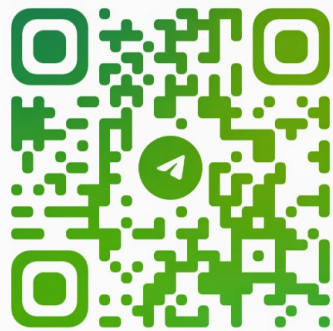
Приводим пример **проверочного листа**, который удобно использовать при реализации процесса обеспечения поддержки ПО при эксплуатации пользователями.

Проверочный лист требований к обеспечению поддержки программного обеспечения при эксплуатации пользователями->

Проверочный лист (2/2)

№ п/п	Требование	Выполнение
	<ul style="list-style-type: none"> – описание процедур оповещения пользователей о выпуске обновлений (включая обновления безопасности) и необходимости их установки; – описание процедур информирования пользователей ПО о выявленных уязвимостях и способах реализации мер по их нейтрализации до разработки обновлений безопасности, устраняющих уязвимость, по установленным каналам взаимодействия; – информацию об обучении сотрудников службы технической поддержки. 	
5.22.2.2	Организована работа службы технической поддержки.	
5.22.2.3	Разработана процедура оповещения пользователей о выпуске обновлений (включая обновления безопасности) и необходимости их установки.	
5.22.2.4	Организовано обучение специалистов службы технической поддержки работе с поставляемым ПО, особенностями его установки и функционирования, ограничениям и указаниям по эксплуатации.	
5.22.2.5	Разработана процедура информирования пользователей ПО о выявленных уязвимостях и способах реализации мер по их нейтрализации до разработки обновлений безопасности, устраняющих уязвимость, по установленным каналам взаимодействия.	

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



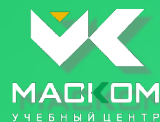
VOKRUG_RBPO25



Получи 10% скидку
на курсы «М БРПО»
в Учебном Центре «МАСКОМ»



VOKRUG_RBPO25





Учебные курсы по 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 ч



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 программ 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 час



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



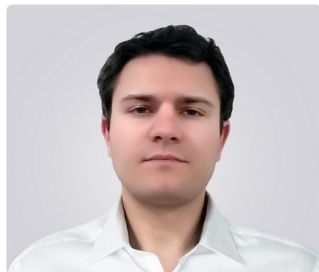
Пиков Виталий
Александрович

Время
30 часов / 3 дня

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.

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.

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



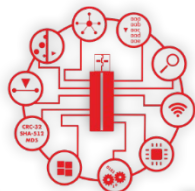
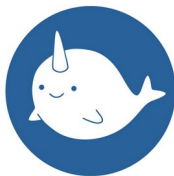
Общий стаж работы: более 26 лет

Стаж преподавательской работы: более 10 лет

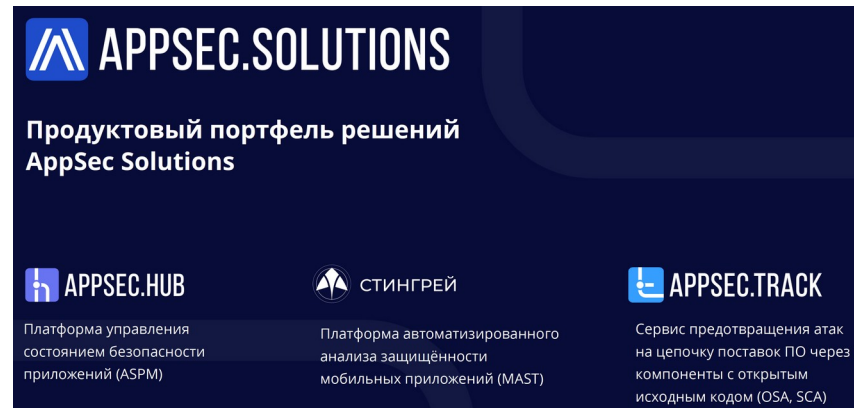
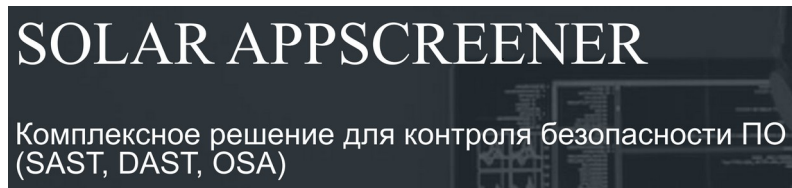


УЧЕБНЫЙ ЦЕНТР
БЕЗОПАСНОСТИ ИНФОРМАЦИИ
Год основания: 1998





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.

