ИТ-Экспертиза

DevSecOps

Безопасная разработка

IT EXPERTISE

КАКИЕ РИСКИ МОЖНО ВЫЯВИТЬ И УСТРАНИТЬ БЛАГОДАРЯ DEVSECOPS

DevSecOps – методология, которая интегрирует практики безопасности **на каждом этапе** жизненного цикла разработки программного обеспечения, **а не в конце** этого процесса. Этот подход базируется на культуре, где безопасность является общей ответственностью всех команд, включая разработчиков, специалистов по безопасности и операционную команду

Основная идея – автоматизировать проверки безопасности в процессе **DevOps**, чтобы снизить уязвимости и ускорить выход продукта на рынок

Риск / Проблема	Как это устраняет подход DevSecOps
Позднее обнаружение уязвимостей	Сканеры и тесты запускаются при каждом коммите, а не после релиза
Высокие затраты на исправление после инцидента	Удаление дефектов в ранних стадиях экономит до 90% расходов
Непредсказуемый time-to-market	Автоматический пайплайн гарантирует, что безопасность не тормозит релиз, а лишь фильтрует критические риски
Штрафы и отказ в лицензировании	Автоматическая проверка соответствия ГОСТ/ФСТЭК – отчет готов к проверке регулятора
Конфликты между командами разработки и информационной безопасности	Совместные правила, общие метрики и «security champions» делают безопасность частью ежедневной работы
Зависимость от иностранных инструментов	Отечественные сканеры работают в изолированных сетях, удовлетворяя требование импортозамещения
Отсутствие контроля над инфраструктурой как кодом	IaC-сканеры фиксируют конфигурационные риски до их применения
Отсутствие измеримых KPI по безопасности	Дашборды и метрики позволяют руководству видеть реальное состояние защиты и принимать решения

ОСНОВНЫЕ ПРИНЦИПЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

- **Безопасность контура разработки ПО** позволяет исключить риски ее компрометации, и, как следствие, компрометации продуктовой инфраструктуры и самого продукта
- **Осуществление безопасного проектирования** охватывает определение требований ИБ и установление конкретных архитектурных решений
- **Идентификация и управление уязвимостями** включает в себя исследование и анализ уязвимостей, их устранение и дальнейшее отслеживание возможных проблем
- **Интеграция безопасности в CI/CD** (Continuous Integration/Continuous Delivery) необходима для автоматической проверки кода на наличие уязвимостей и угроз
- **Защита данных** предполагает использование шифрования и других методов для безопасной передачи, хранения и удаления информации
- **Тестирование** – проверка ПО на уязвимости и устойчивость к атакам, сканирование кода, а также постоянный выпуск обновлений и патчей
- **Мониторинг ИБ** позволяет выявлять угрозы в режиме реального времени и оперативно реагировать на них
- **Постоянное обучение** – систематическое повышение квалификации и получение актуальных знаний в сфере ИБ. Примечательно, что это обязательно не только для разработчиков, но и для остальных сотрудников организации

ОСНОВНЫЕ НОРМАТИВНЫЕ ТРЕБОВАНИЯ ДЛЯ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В России разработаны и приняты национальные стандарты по разработке безопасного программного обеспечения (РБПО)

ГОСТ Р 58412-2019 Моделирование угроз безопасности при разработке.
Перечень документов: Модель угроз.
Регулярность и частота: пересмотр регулярно и при изменении (изменения среды, состава ПО и пр.)

ГОСТ Р 56939-2019 Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования.
(перечень мер и документов см. ниже ГОСТ Р 56939-2024)

ГОСТ Р 56939-2024 Защита информации. Разработка безопасного программного обеспечения. Общие требования (Стандарт описывает: 25 процессов разработки.
Перечень необходимых документов - 30)

ГОСТ Р 56939-2024. ЗАЩИТА ИНФОРМАЦИИ. РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ОБЩИЕ ТРЕБОВАНИЯ

ОБЩИЕ ПОЛОЖЕНИЯ

При реализации мер по разработке безопасного программного обеспечения по ГОСТ Р 56939-2016 можно выделить следующие ключевые моменты:

- стандарт устанавливает общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного ПО. Детали соответствующих процессов стандартом не регламентируются
- меры по разработке безопасного ПО применяются в течение всего жизненного цикла ПО. При этом есть связь с процессами, описанными в ИСО/МЭК 12207-2010
- стандартом вводится базовый набор мер по разработке безопасного ПО. При невозможности реализации в среде разработки ПО отдельных мер из базового набора, разработчик имеет право реализовать компенсирующие меры
- в стандарте предусмотрены шесть видов испытаний ПО: статический анализ и экспертиза кода, функциональное тестирование программы, тестирование на проникновение, динамический анализ кода и фаззинг-тестирование
- учитывается необходимость защиты инфраструктуры среды разработки ПО, а также обеспечения конфиденциальности информации, получаемой в ходе анализа кода и тестирования ПО

ГОСТ Р 56939-2024. ЗАЩИТА ИНФОРМАЦИИ. РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. БАЗОВЫЙ НАБОР МЕР

- При выполнении анализа требований к ПО разработчик ПО должен определить требования по безопасности, предъявляемые к разрабатываемому ПО
- Моделирование угроз безопасности информации
- Уточнение проекта архитектуры программы с учетом результатов моделирования угроз безопасности информации
- Использование при разработке ПО идентифицированных инструментальных средств
- Создание программы на основе уточненного проекта архитектуры программы
- Создание (выбор) и использование при создании программы порядка оформления исходного кода программы
- Статический анализ исходного кода программы
- Экспертиза исходного кода программы
- Функциональное тестирование программы
- Тестирование на проникновение
- Динамический анализ кода программы

- Фаззинг-тестирование программы
- Обеспечение защиты ПО от угроз безопасности информации, связанных с нарушением целостности в процессе его передачи пользователю
- Поставка пользователю эксплуатационных документов
- Реализация и использование процедуры отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы
- Систематический поиск уязвимости программы
- Реализация и использование процедуры уникальной маркировки каждой версии ПО
- Использование системы управления конфигурацией ПО
- Защита от несанкционированного доступа к элементам конфигурации
- Резервное копирование элементов конфигурации
- Регистрация событий, связанных с фактами изменения элементов конфигурации
- Периодическое обучение сотрудников
- Периодический анализ программы обучения сотрудников

ГОСТ Р 56939-2024. ЗАЩИТА ИНФОРМАЦИИ. РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ПЕРЕЧЕНЬ ДОКУМЕНТОВ В СООТВЕТСТВИИ СО СТАНДАРТОМ

- Политика информационной безопасности в соответствии с ИСО/МЭК 27001
- Руководство по разработке безопасного ПО
- Перечень требований по безопасности
- Модель угроз безопасности
- Проект архитектуры программы (логическая структура программы)
- Перечень инструментальных средств разработки ПО
- Описание проектных решений, обеспечивающих выполнение требований по безопасности
- Порядок оформления исходного кода программы
- Регламент и протоколы статического тестирования программы
- Регламент и протоколы экспертизы исходного кода программы
- Регламент и протоколы функционального тестирования программы
- Регламент и протоколы тестирования на проникновение
- Регламент и протоколы динамического анализа кода программы
- Регламент и протоколы фаззинг-тестирования программы
- Эксплуатационная документация

- Регламент передачи ПО пользователю
- Регламент отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы
- Регламент приема и обработки сообщений от пользователей об ошибках ПО и уязвимостях программы
- Регламент доведения до пользователей информации об уязвимости программы и рекомендаций по их устранению
- Журнал ошибок и уязвимостей программы
- Регламент экстренного выпуска обновлений ПО
- Регламент, протоколы и журналы поиска уязвимостей программы
- Регламент маркировки версий ПО
- Регламент управления конфигурацией ПО
- Регламент защиты инфраструктуры среды разработки ПО
- Регламент резервного копирования конфигурации ПО
- Регламент регистрации событий изменений конфигурации ПО
- Журнал регистрации изменений конфигурации ПО
- Программа обучения сотрудников в области разработки безопасного ПО
- Журнал обучения сотрудников в области разработки безопасного ПО

УЧАСТИЕ DEVSECOPS В ЭТАПАХ КОНВЕЙЕРА CI/CD

Методология devSECops охватывает те же этапы, что и методология DevOps, расширяя следующие этапы функционалом с фокусом на безопасность:

- **Планирование.** Анализ и предварительная оценка состояния безопасности, выбор оптимальных инструментов и моделирование угроз
- **Разработка/написание кода.** Поиск уязвимостей с помощью инструментов статического (SAST, Sonar cube) анализа. Проверка выполняется при добавлении кода в репозиторий
- **Сборка.** Повторная проверка собранного исходного кода программы (SAST), анализ на уязвимости, взаимодействия с интерфейсом (DAST, Vanessa Automation). Проверка выполняется после сборки на тестовой среде
- **Тестирование.** Проведение пен тестов, фаззинг (тест на корректные данные в граф. формах программы), сканеры анализа защищенности
- **Развертывание** релиза. Проверка среды установки программы, политик безопасности и конфигурации, настройка системы мониторинга, сбор логов, назначение прав доступа. Настройка систем безопасности
- **Мониторинг.** Непрерывное наблюдение за всеми частями системы, включая инфраструктуру (WAF, SIEM и пр.)

DEVSECOPS МЕТОДОЛОГИЯ И ПРИМЕНЯЕМЫЕ КЛАССЫ ИНСТРУМЕНТОВ

SAST – инструмент для статического анализа кода. Помогает находить потенциальные уязвимости и выявлять ошибки в исходном коде

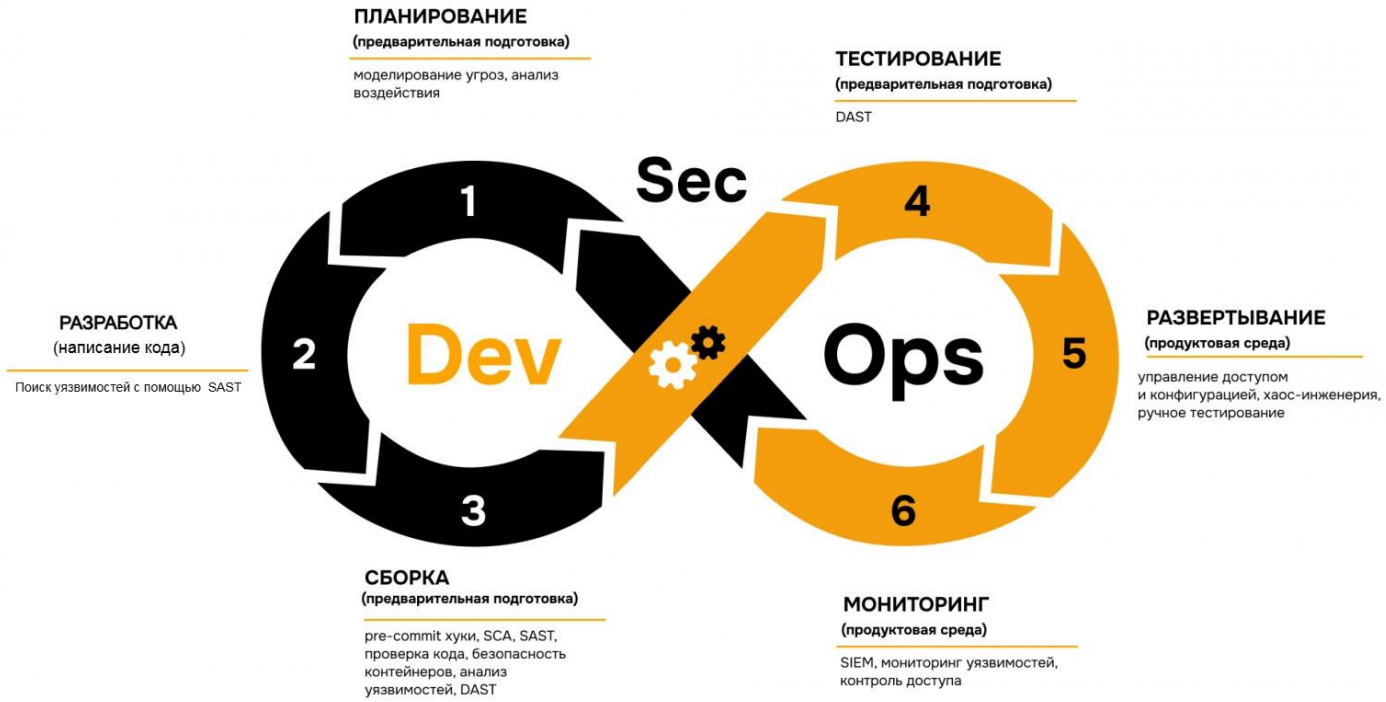
DAST – инструмент для динамического анализа. Обнаруживает уязвимости в работающем приложении

Fuzzing – техника тестирования ПО, основанная на передаче приложению неправильных или случайных данных

WAF – защищает от уязвимостей путем фильтрации вредоносного трафика

OSA (Open-Source Analysis) – инструмент для анализа компонентов с открытым исходным кодом

SCA (Software Composition Analysis) – инструмент для анализа состава программного кода



ИТ-Экспертиза

О компании

IT EXPERTISE

ФАКТЫ О КОМПАНИИ

ООО «ИТ-Экспертиза»
ООО «Умные решения»

группа компаний

18+ лет

опыта команды в сфере оптимизации 1С

150 +

участий в оптимизационных проектах по всей России

ISO 9001:2015

Сертификация ISO

Являемся официальным партнером Фирмы «1С»

Входим в рейтинг Центр компетенций 1С:КОРП

Призер конкурса стартапов с решением САКУРА

Победитель конкурса 1С Проект года

Проект года 2019

ИТ-ЭКСПЕРТИЗА: НАПРАВЛЕНИЯ РАБОТЫ

Информационная безопасность

Комплекс информационной безопасности САКУРА для контроля состояния защищенности удаленных рабочих мест и активного реагирования на угрозы

Консалтинг по информационной безопасности - аудит и разработка рекомендаций по совершенствованию систем информационной безопасности (ГИС, КИИ, персональные данные), подготовка необходимой документации для регуляторов

Умный мониторинг

Система сбора и анализа данных, оперативного реагирования и прогнозирования

«Умный мониторинг» позволяет эффективно выявлять и быстро реагировать на возникающие ситуации в ИТ-ландшафте

Благодаря идеям AIOps может предугадывать поведение системы и заранее предотвращать потенциальные аварии

«ПУСК» входит в состав «Умного мониторинга»

1С:Интеграция КОРП

Корпоративная шина предприятия (ESB) с универсальным коннектором 1С и открытым кодом, использующая каноническую модель данных, поставляемая как типовое решение 1С

Решение выпускается совместно с Фирмой «1С»

Технологическая экспертиза

Корпоративная технологическая поддержка систем на платформе 1С:Предприятие (РКЛ)

Повышение стабильности систем на платформе 1С:Предприятие

Повышение производительности систем на платформе 1С:Предприятие

Разработка на платформе 1С:Предприятие 8

НАШИ КЛИЕНТЫ

https://it-expertise.ru/clients

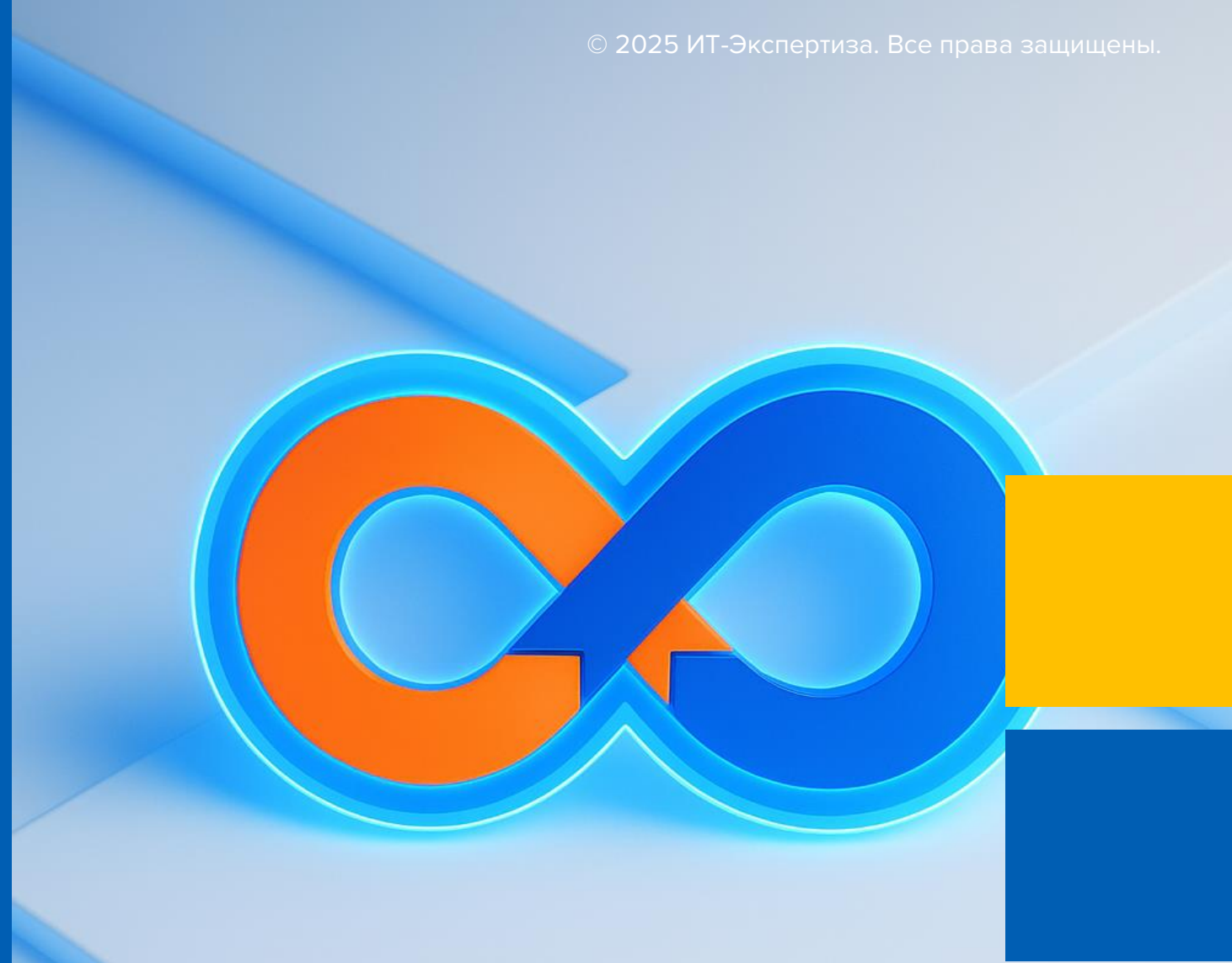
Свяжитесь с нами

САЙТ
it-expertise.ru

EMAIL
info@it-expertise.ru

ТЕЛЕФОН
+7 499 450 28 86

АДРЕС
119435 г. Москва,
ул. Малая Пироговская, 16



IT EXPERTISE