РАСУ
РОСАТОМ

DevSecOps в действии: автоматизация проверки кода в локальных доверенных репозиториях

Форум ITSEC 2025: информационная и кибербезопасность России

Сплюхин Денис Валерьевич
Главный специалист обособленного подразделения АО «РАСУ» в г. Саров

Важность применения DevSecOps при разработке программного обеспечения и программно-аппаратных комплексов

ПО и ПАК занимают ключевую роль во многих сферах деятельности, включая финансы, медицину, транспорт, энергетику и другие

- Небезопасное программное обеспечение может привести к серьезным последствиям, включая утечку конфиденциальных данных, нарушение работы критически важных систем и даже угрозу жизни людей

Разработка программного обеспечения - это сложный и многоэтапный процесс, который включает в себя множество различных аспектов, таких как проектирование, кодирование, тестирование, развертывание и поддержка

- Каждый из этих этапов может содержать уязвимости, которые могут быть использованы злоумышленниками для атаки на программное обеспечение. Поэтому важно разработать комплексную процессную модель, которая позволит обеспечить безопасность на каждом этапе разработки

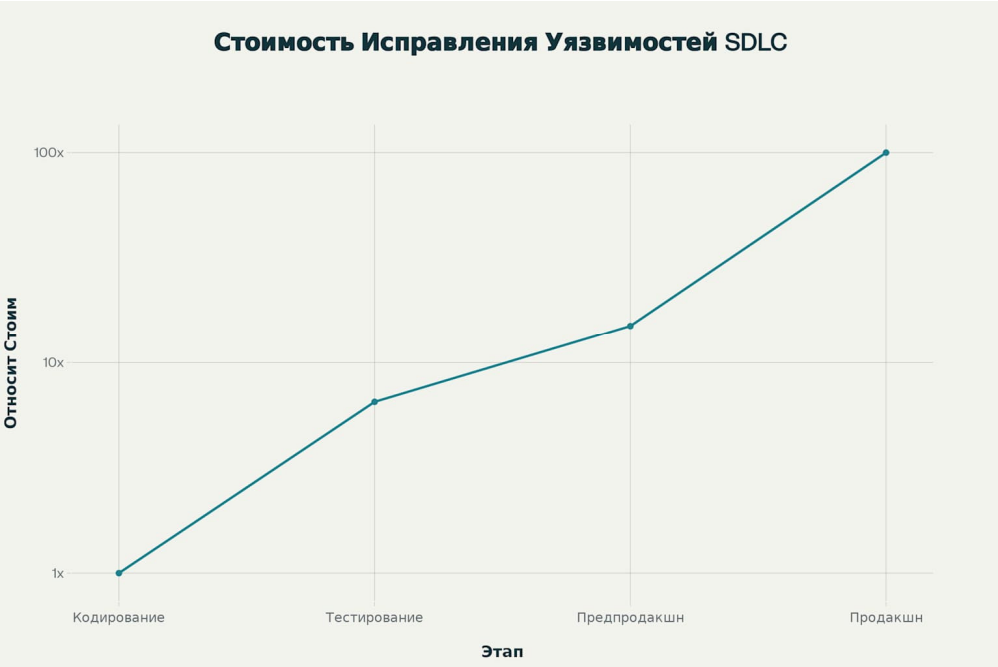
Проведение тестирования и отладки программного обеспечения необходимо выполнять в условиях, максимально приближенных к реальным, но без риска нарушения работы критически важных систем

- Позволяет выявлять и устранять уязвимости на ранних стадиях разработки, что значительно повышает безопасность программного обеспечения

Принципы интеграции безопасности в разработку ПО

Традиционные модели разработки рассматривали безопасность как отдельную фазу, выполняемую в конце цикла разработки

DevSecOps кардинально меняет этот подход, делая безопасность неотъемлемой частью каждого этапа разработки и операций



Экспоненциальный рост стоимости исправления уязвимостей на поздних этапах разработки

Проблемы традиционной разработки ПО

RASU
ROSATOM

Отсутствие безопасности на ранних этапах

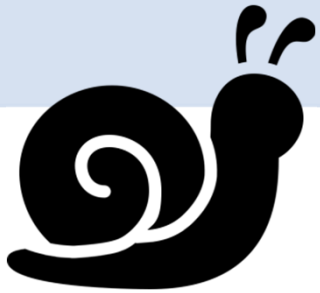
- *Без внедрения проверок безопасности на стадии проектирования и кодирования уязвимости попадают в продукт с самого начала*

Риски внедрения уязвимостей

- *Использование сторонних библиотек и отсутствие контроля зависимостей увеличивают вероятность появления уязвимостей в приложении*

Медленная реакция на угрозы

- *Отсутствие автоматизированного мониторинга и оповещений приводит к задержкам в обнаружении и устранении проблем*



Высокая стоимость исправления проблем безопасности

- *Чем позже обнаружена проблема, тем дороже и сложнее её устранить — исправление уязвимостей на продакшене в 30 раз дороже, чем на этапе проектирования*

Основные принципы DevSecOps

Shift-left security. Безопасность внедряется на самых ранних этапах жизненного цикла ПО, что позволяет выявлять уязвимости до релиза

Автоматизация процессов безопасности. Использование автоматических сканеров и тестов ускоряет обнаружение и устранение проблем

Интеграция инструментов анализа кода. Проверка кода на уязвимости встроена в пайплайн CI/CD

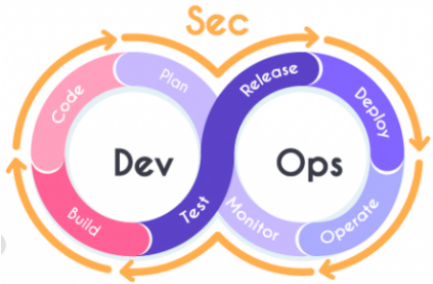
Непрерывное тестирование безопасности. Непрерывный поиск и выявление потенциально опасных недостатков на всех этапах разработки

Безопасная разработка программного обеспечения и программно-аппаратных комплексов

RASU
ROSATOM

Безопасная разработка ПО и ПАК

- **Разработка, производство и техническая поддержка**
  - Проектирование
    Управление конфигурацией
    Управление средой разработки и тестирования
  - Производство ПО или ПАК
    Техническая поддержка (устранение уязвимостей, обновление, внесение изменений)
- **Испытания по требованиям инф. безопасности**
  - Экспертный анализ архитектуры
    Идентификация потенциальных уязвимостей
    Тестирование на проникновение
  - Статический анализ
  - Динамический анализ и фаззинг-тестирование
  - Функциональное тестирование ФБО
  - Аудит кода
  - Анализ уязвимостей компонентов
  - Тестирование на проникновение
  - Анализ скрытых каналов
- **Документирование продукта (ПО или ПАК)**
  - Архитектура/ архитектура безопасности
    Схемы информационных потоков ФБО
    Модель безопасности
    Функциональная спецификация
  - Инструментальные средства разработки и анализа
    Документация по безопасной разработке ПО или ПАК
    Модель угроз
    ПМИ, отчеты, протоколы, заключения …

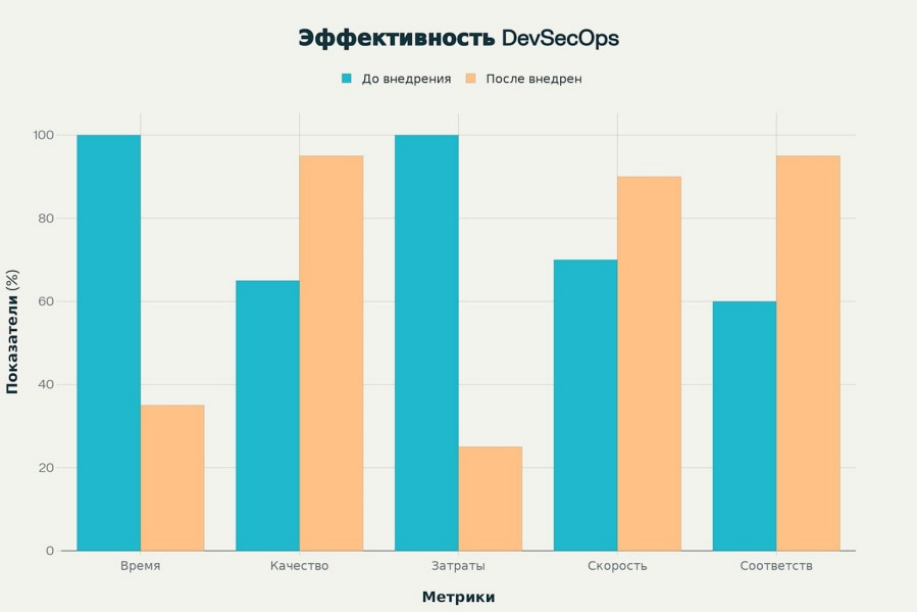


Автоматизация как основа эффективности

Ключевые преимущества автоматизации включают:

- сокращение человеческих ошибок
- ускорение процессов обнаружения уязвимостей
- обеспечение консистентности проверок безопасности

Исследования показывают, что только 6.83% из 8,243 анализируемых open-source проектов применяют автоматизацию безопасности в своих CI-пайплайнах, несмотря на признание важности безопасности разработчиками



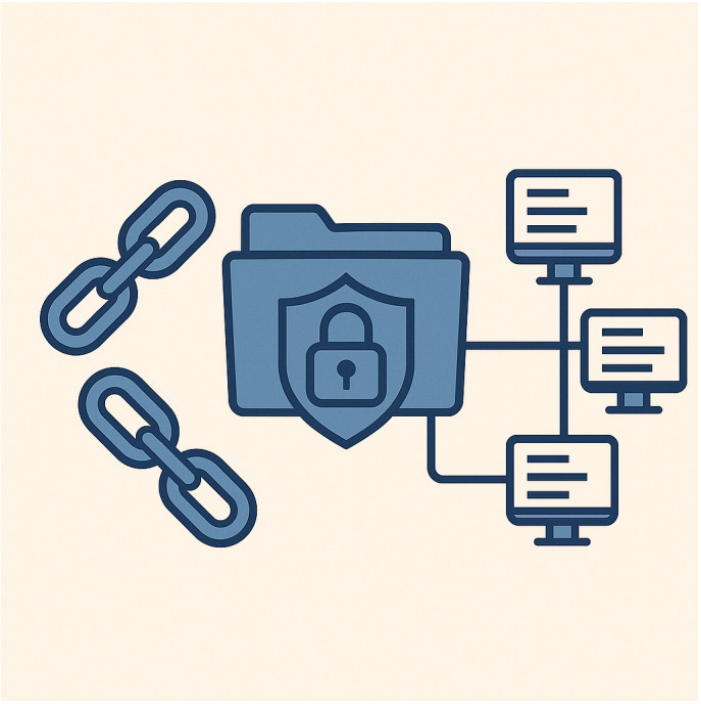
Эффективность внедрения DevSecOps: сравнение ключевых показателей до и после внедрения

Локальные доверенные репозитории

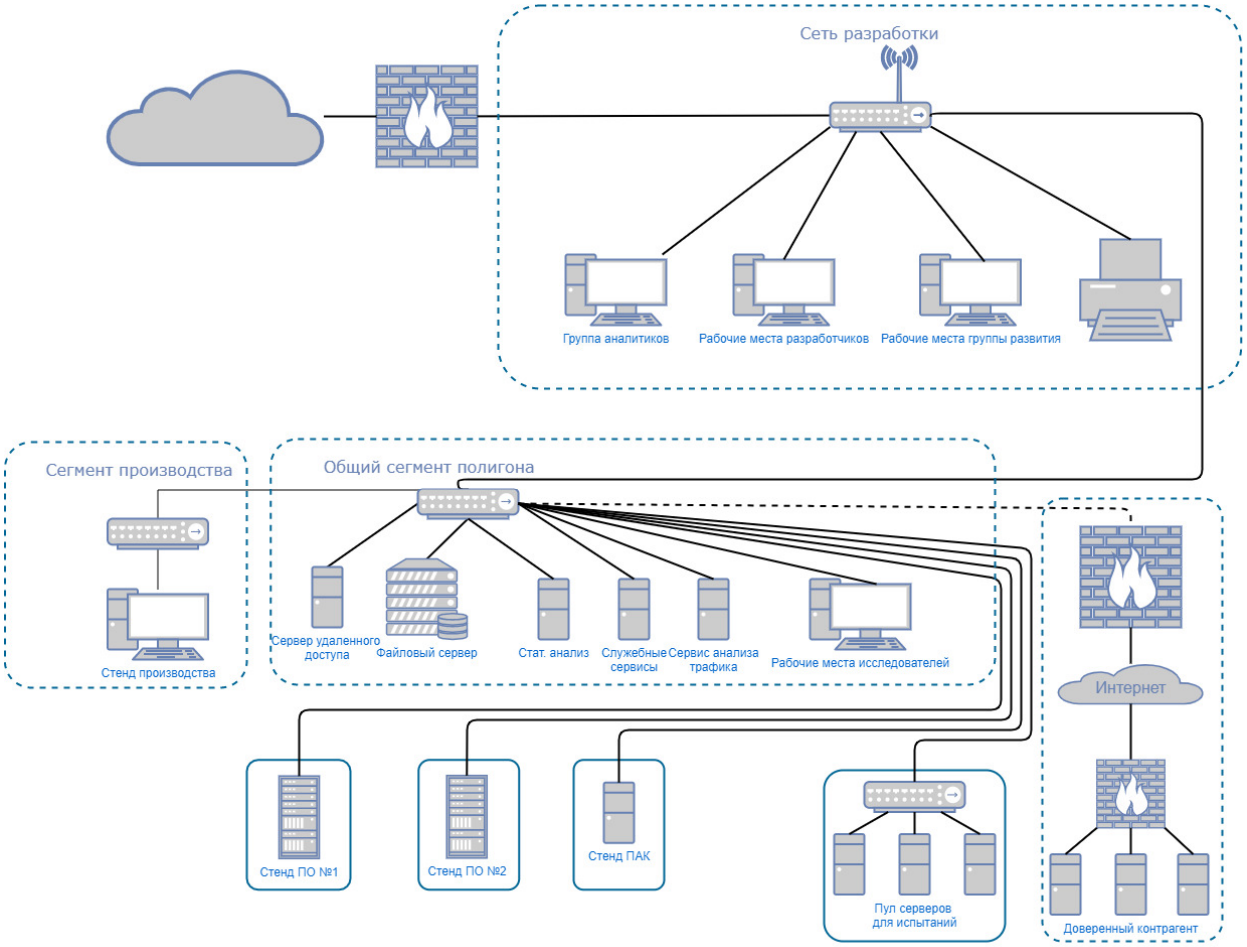
Локальное защищённое хранилище исходного кода и зависимостей, полностью контролируемое организацией

Роль в цепочке поставок ПО

- Централизует хранение и распространение компонентов
- Обеспечивает проверку и цифровую целостность артефактов
- Позволяет отслеживать происхождение каждого компонента
- Автоматически сканирует на наличие уязвимостей и вредоносного кода
- Ограничивает доступ по ролям (RBAC) и журналирует все изменения



Инфраструктура разработки безопасных информационных систем (ИРБИС)



- Подтвержденная применимость в отраслевых задачах
- Подробное документирование процессов разработки и испытаний
- Импортонезависимое решение
- Контейнеризация и изоляция ПО
- Использование программного обеспечения с открытым исходным кодом (Opensource)
- Формирование замкнутой среды

Этапы автоматизации проверки кода

Этапы автоматизации проверки кода

Идентификатор	Описание	Комментарий
2025-02-26 crypto CVE-2025-22869 UNASSIGNED	SSH servers which implement file transfer protocols are vulnerable to a denial of service attack from clients which complete the key exchange slowly, or not at all, causing pending content to be read into memory, but never transmitted.	SSH не используется
2022-02-16 qt BDU-2022-00893 (CVE-2022-25255) Средний	Уязвимость пакета qt/qtbase библиотеки Qt связана с неверным ограничением имени пути к каталогу с ограниченным доступом. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	пакет qt/qtbase не используется При условии использования рекомендаций производителя для ОС Astra Linux Уязвимость считается устраненной (есть в сводной таблице устраненных уязвимостей для ОС Astra Linux), бюллетень № 2022-0819SE17 (1.7.2)
2023-06-04 qt BDU-2023-03689 (CVE-2023-34410) Средний (CVSSv3=5.3)	Уязвимость кроссплатформенного фреймворка для разработки программного обеспечения Qt связана с ошибками процедуры подтверждения подлинности сертификата. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти существующие ограничения безопасности	При условии использования рекомендаций производителя для ОС Astra Linux Уязвимость считается устраненной (есть в сводной таблице устраненных уязвимостей для ОС Astra Linux), бюллетень № 2023-0630SE17MD (1.7.4.UU1)
2023-05-22 qt BDU-2023-03802 (CVE-2023-32763) Высокий (CVSSv3=7.5)	Уязвимость компонента QTextLayout кроссплатформенного фреймворка для разработки программного обеспечения Qt связана с копированием буфера без проверки входных данных. Эксплуатация уязвимости позволяет нарушителю, действующему удаленно, вызвать отказ в обслуживании с помощью специально созданного файла SVG	Не применимо, т.к QTextLayout не используется в frontend Уязвимость считается устраненной (есть в сводной таблице устраненных уязвимостей для ОС Astra Linux), бюллетень № 2023-0630SE17MD (1.7.4.UU1)

Наименование	Анализатор, снимок	Размечено / Общее кол-во	Подтверждённые (Критические и высокие / Средние и низкие)	Комментарии, %
backend-cpp	Svace 3.4.240902 25-05-31-ec369ee16	931 / 931	109 (3 / 106)	37.97%
backend-golang	Svace 3.4.240902 25-05-31-ec369ee16	59 / 59	0 (0 / 0)	100%

Описание	Пункт требования	frontend	backend-cpp	backend-golang
Отсутствие пробела между условием/циклом и открывающей скобкой	4.6.2	6	3	-
else должно быть на одной строке с закрывающейся скобкой предыдущего блока	4.6.4	0	3	-
if и else должны находиться на одном логическом уровне	4.6.7	0	0	-

2.2.4.20250423-so-release ✓ Пре-релиз

robot выпустил(-а) это 3 часа назад | -23 коммиты main с этого релиза

Actions
frontend version:
backend version:
gui-func-testing version:

Coverage:

Component	Date
Admin-panel, HMI-engineer	23.04.2025
AuthGateway	23.04.2025
AuthRepository	23.04.2025
Reserv	23.04.2025
Director	23.04.2025

▼ Загрузки

Исходный код (ZIP)	
Исходный код (TAR.GZ)	
2.2.4.20250423-120629-so-release-dbg.tar.gz	524 MiB
2.2.4.20250423-120629-so-release.tar.gz	179 MiB
AV_backend-address-sanitize.log	867 B
AV_backend-thread-sanitize.log	867 B
AV_backend-undefined-sanitize.log	867 B
AV_b_linux_frontend-gis_release.log	171 B
AV_b_linux_frontend_release.log	155 B
AV_b_windows_frontend.log	283 B
AV_frontend-address-sanitize.log	155 B
AV_frontend-thread-sanitize.log	155 B
AV_frontend-undefined-sanitize.log	155 B
AV_linux_backend_debug.log	867 B
AV_linux_backend_release.log	815 B
AV_linux_frontend_debug.log	155 B
AV_linux_frontend-gis_debug.log	171 B

Процесс автоматизированного проведения испытаний по требованиям безопасности информации

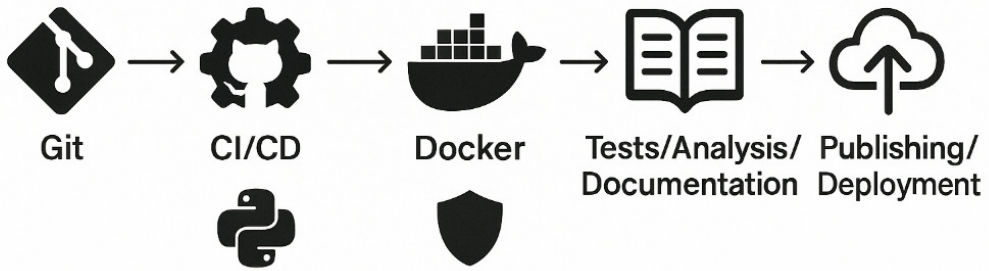
Интеграция тестирования ПО в CI/CD

Использование
Gitea Actions — автоматизация тестов и сборки
Gitea CI — глубокая интеграция с Git, гибкая настройка пайплайнов

Автоматизация документации:
MkDocs — генерация статических сайтов из Markdown

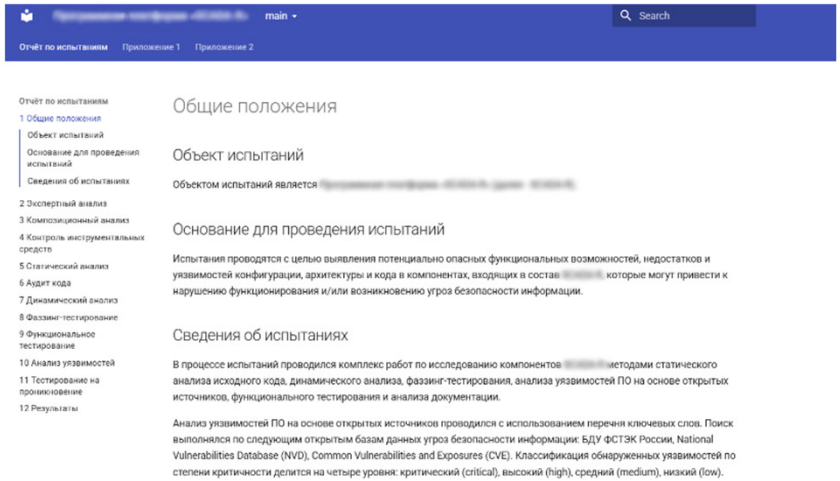
Оркестрация и воспроизводимость:
Docker — создание изолированных окружений для сборки и тестирования

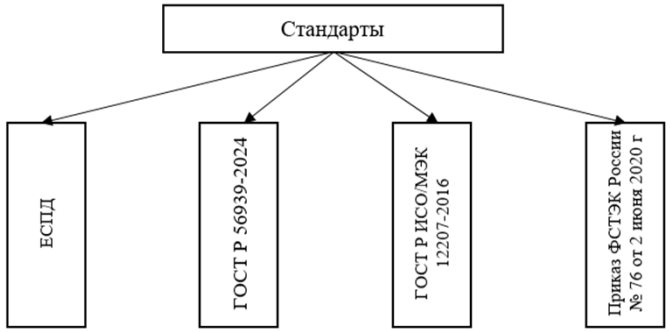
Интеграция внешних систем и автоматизация анализа:
Python CLI-скрипты для работы с API Svacer и Dependency Track

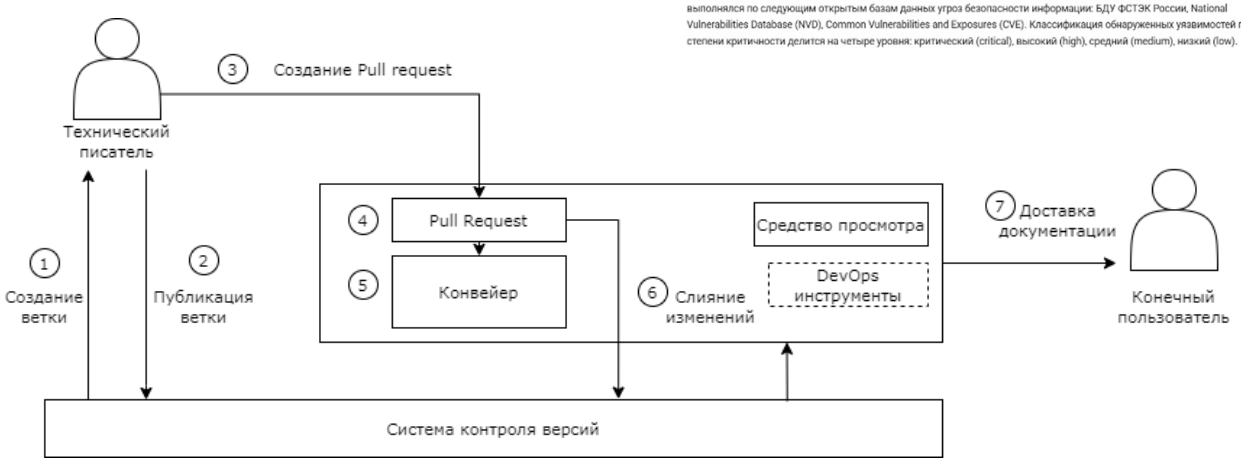


Формирование отчетной документации по испытаниям ПО

Отчет генерируется автоматически в виде страницы сайта и в формате PDF со стилями CSS

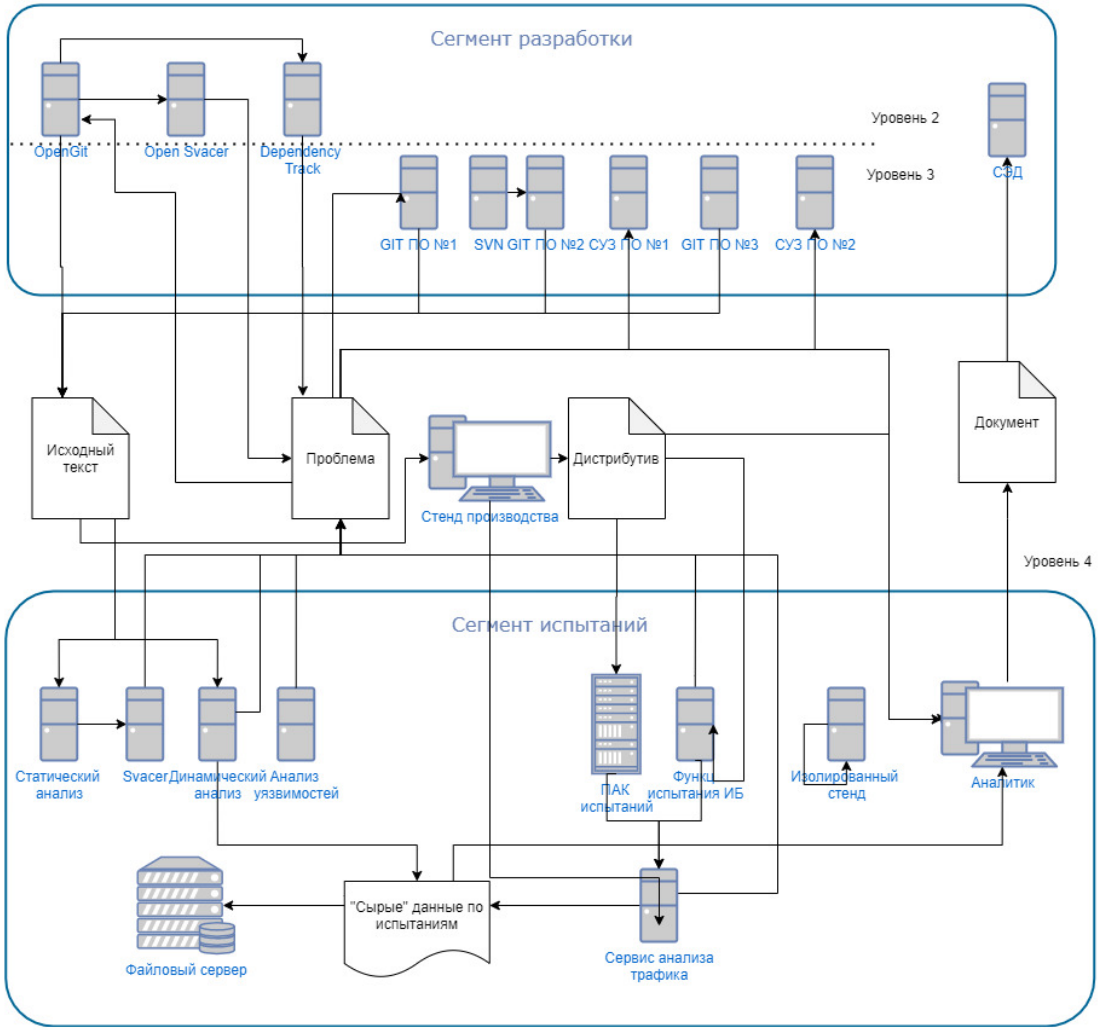






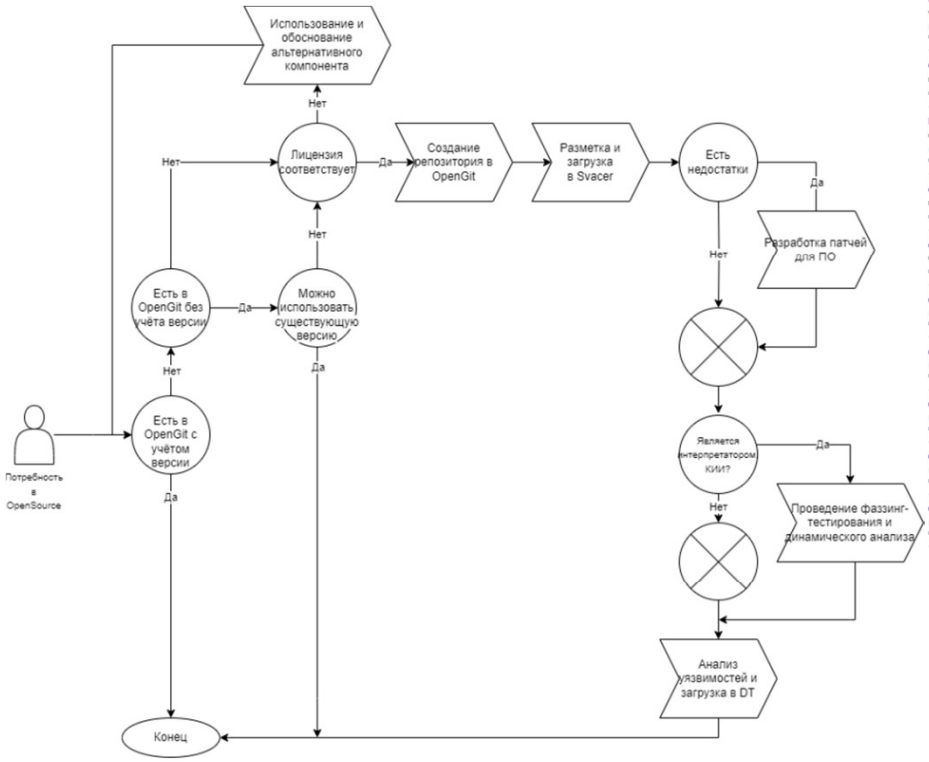
Процесс создания документации с использованием «Документация как код»

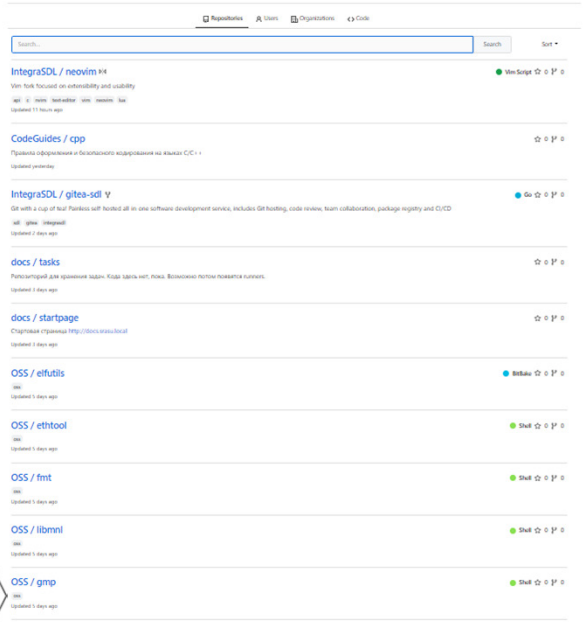
Взаимодействие разработчиков и испытателей



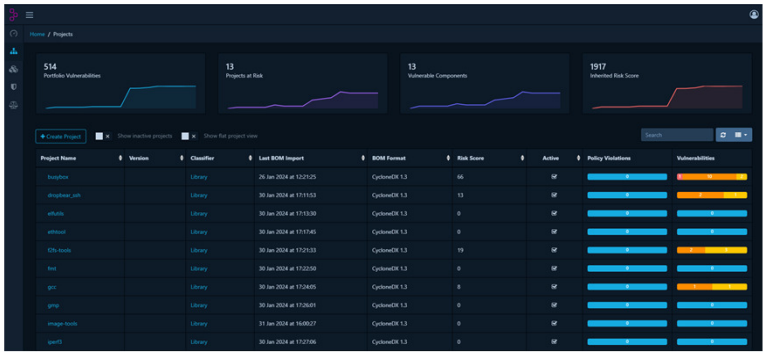
- Организация единого информационного пространства
- Отслеживание в системе управления задачами истории запросов
- Комплексное решение задач по ИБ
- Документирование процессов
- Независимость проведения испытаний

OpenGIT РАСУ – репозиторий безопасного OpenSource





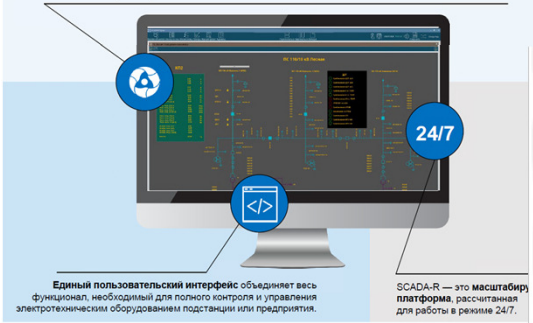
- Более 50 компонентов проверено и использовано в проектах
- Доступность для сотрудников всего предприятия
- Высокая степень прозрачности и доверия



Результаты внедрения DevSecOps при разработке ПО и ПАК

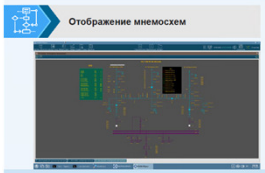
RASU
ROSATOM

Программный комплекс SCADA-R является собственным отраслевым продуктом Госкорпорации «Росатом» и предназначен для создания систем диспетчеризации на объектах электроэнергетики.



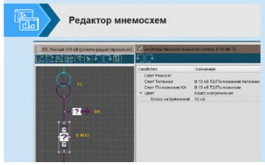
Единый пользовательский интерфейс объединяет весь функционал, необходимый для полного контроля и управления электротехническим оборудованием подстанции или предприятия.

SCADA-R — это **масштабир платформа**, рассчитанная для работы в режиме 24/7.



Отображение мнемосхем

- Оконный менеджер позволяет удобно группирова различные окна.
- Динамическая раскраска мнемосхем в зависимос от состояния технологического оборудования и положения коммутационных аппаратов.
- Непрерывная индикация измеряемых значений параметров оборудования.
- Представление обслуживающему персоналу информации о техническом состоянии объекта контроля и обнаружение его изменения.

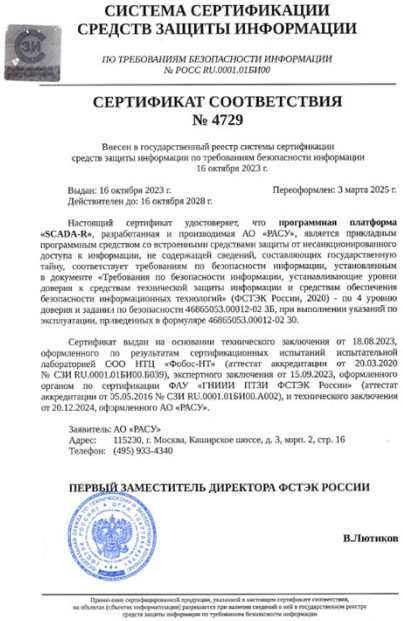


Редактор мнемосхем

Редактор мнемосхем позволяет:

- создавать и открывать мнемосхемы из реестра мнемосхем;
- работать с редактором мнемосхем и палитрой элементов;
- создавать привязки объектов дерева к элемента на мнемосхеме.

Библиотека объектов свободно расширяется собственными средствами редактора.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4729

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 16 октября 2023 г.

Выдан: 16 октября 2023 г. Переоформлен: 3 марта 2025 г.
Действителен до: 16 октября 2028 г.

Настоящий сертификат удостоверяет, что **программная платформа «SCADA-R»**, разработанная и производимая АО «РАСУ», является прикладным программным средством со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия и заданию по безопасности 46865053.00012-02 3Б, при выполнении указаний по эксплуатации, приведенных в формуляре 46865053.00012-02 30.

Сертификат выдан на основании технического заключения от 18.08.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО НТЦ «Фобос-НТ» (аттестат аккредитации от 20.03.2020 № СЗИ RU.0001.01БИ00.Б039), экспертного заключения от 15.09.2023, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 35.05.2016 № СЗИ RU.0001.01БИ00.А002), и технического заключения от 20.12.2024, оформленного АО «РАСУ».

Заявитель: АО «РАСУ»
Адрес: 115230, г. Москва, Каширское шоссе, д. 3, корп. 2, стр. 16
Телефон: (495) 933-4340

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

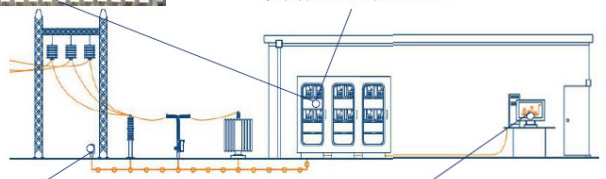
Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС КЛАСТЕРНОЙ ЦИФРОВОЙ ПОДСТАНЦИИ ПАК КЦПС DSC-01R

Платформенное решение кластерной цифровой подстанции с гибкой функциональной структурой. Архитектура «4+» *

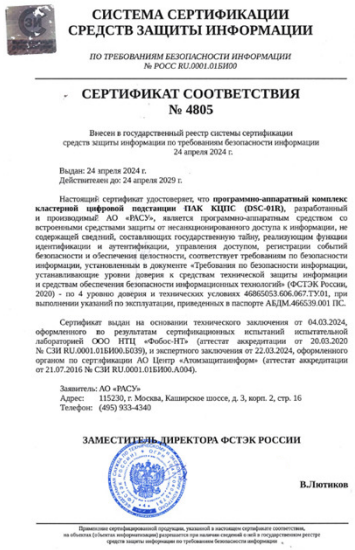
Программно-аппаратная платформа («кластер») –программно-аппаратный комплекс на базе универсальных аппаратных модулей и единого конструктива «шасси», с возможностью гибкой замены оборудования и программного обеспечения для управления подстанцией.

Алгоритмы защиты и управления — Отчуждаемые программные приложения РЗА, АСУ, АИИСКУЭ, ККЭ – специализированное программное обеспечение, обеспечивающее выполнение набора функций автоматизации подстанции, которое может быть запущено на любом из унифицированных аппаратных устройств



Преобразователь аналого-дискретных сигналов (ПАДС) - устройство, преобразующее измерения от электромагнитных трансформаторов тока и напряжения, а также дискретные сигналы в цифровой поток данных в соответствии со стандартом МЭК 61850. Предназначены для реконструкции существующих подстанций с постепенным переходом на цифровые технологии.

SCADA-система подстанционного уровня – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте (мониторинг), а также возможного контроля и управления данным объектом.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4805

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 24 апреля 2024 г.

Выдан: 24 апреля 2024 г.
Действителен до: 24 апреля 2029 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс кластерной цифровой подстанции ПАК КЦПС (DSC-01R)**, разработанный и производимый АО «РАСУ», является программно-аппаратным средством со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом, регистрации событий безопасности и обеспечения целостности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия и техническим условиям 46865053.606.067.ТУ.01, при выполнении указаний по эксплуатации, приведенных в паспорте АБДМ.466539.001 ПС.

Сертификат выдан на основании технического заключения от 04.03.2024, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО НТЦ «Фобос-НТ» (аттестат аккредитации от 20.03.2020 № СЗИ RU.0001.01БИ00.Б039), и экспертного заключения от 22.03.2024, оформленного органом по сертификации АО Центр «Атомзащитинформ» (аттестат аккредитации от 21.07.2016 № СЗИ RU.0001.01БИ00.А004).

Заявитель: АО «РАСУ»
Адрес: 115230, г. Москва, Каширское шоссе, д. 3, корп. 2, стр. 16
Телефон: (495) 933-4340

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

*Продукты АО «РАСУ» - **ПАК «Кластер» и ПО SCADA-R** являются единственными продуктами на сегодняшний день внесенными в реестр ФСТЭК России для возможности использования на ЗО КИИ включая объекты 1 категории значимости*

DevSecOps в действии: автоматизация проверки кода в локальных доверенных репозиториях

Сплюхин Денис Валерьевич

Главный специалист обособленного подразделения АО «РАСУ» в г. Саров

E-mail: dvsplyukhin@rasu.ru
www.rasu.ru