Путешествие к безопасному ПО: идти медленно одному или далеко вдвоем?

Степан Харитонов

Руководитель направления безопасной разработки ООО «КСБ-СОФТ»

КСБ-СОФТ

Системный интегратор
в сфере информационной
безопасности и импортозамещения
информационных технологий

Входим в ГК «Кейсистемс»

Лицензиат ФСТЭК России

Лицензиат ФСБ России

Проекты компании курируют опытные
ИБ-специалисты, аккредитованные
по международным сертификациям
OSCP, CISM, CGEIT и CISA

80+

регионов
внедрения

4000+

реализованных
проектов

С чего мы начинали, и куда движемся

ГК «Кейсистемс»

КСБ-СОФТ

НПЦ КСБ

информационные технологии КЕЙСИСТЕМС

2021-2022 гг.	• Внедрение процессов РБПО для разработчика • Сопровождение разработчика при сертификации СЗИ • Встраивание в образовательную и научную деятельность по безопасной разработке
2023-2024 гг.	• Масштабирование процессов РБПО во всей ГК, и развитие их по настоящий день • Участие в деятельности Центра исследований безопасности системного ПО • Проведение аудита РБПО в производственных командах разработки • Приведение процессов РБПО в соответствие с ГОСТ Р 56939-2024

Активно помогаем нашим клиентам с выстраиванием и развитием процессов РБПО

Почему стоит задуматься?

35 000+

уязвимостей обнаружили по итогам 2024 года (число растёт с каждым годом)

до 78%

доля открытого исходного кода в ПО в некоторых отраслях

90%

инцидентов безопасности вызваны дефектами исходного кода

80%

веб-приложений имеют хотя бы 1 опасную уязвимость

21%

утечек данных вызван уязвимостями программного обеспечения

Высокая

стоимость устранения уязвимостей на поздней стадии

Что мы обнаружили при внедрении/развитии РБПО по ГОСТ?

- Большинство специалистов производственных подразделений не понимают, для чего им менять уже сформированные и работающие процессы
- Технически процессы выстроены – хорошо, однако отсутствует регламентация процессов РБПО (ответственные, порядки, объемы и пр.)
- «Поддерживающие» процессы показывают более высокий уровень зрелости
- Проблемные места: планирование и обучение, МУ и ПА, динамический анализ, безопасная сборка, безопасность сборочной среды, НФТ

Три столпа безопасной разработки – процессы, технологии и люди!

Пути внедрения/развития процессов РБПО

Самостоятельная работа	• Постепенное встраивание в уже сформированные процессы компании • Подготовка собственной команды по внедрению и обеспечению безопасной разработки	• Неразборчивость в последовательности встраивания различных практик • Долгое погружение сотрудников в «новый» уклад работы
Привлечение сторонних ресурсов	• На порядок быстрее, чем при самостоятельной процедуре • Внедрение гарантировано работающих практик и методологий • Отсутствие необходимости отвлечения специалистов от профильной деятельности • Обучение специалистов навыкам использования необходимого инструментария	• Медленное развитие внутренних компетенций в области РБПО • Отсутствие собственного опыта борьбы с «проблемными ситуациями»

Истории из жизни #1

Исходные данные

Проведенная «просветительская» встреча по практикам РБПО

Состав участников

~15 человек: разработчики, тестировщики, аналитики, DevOps

Результат

Разработчики – начали в проактивном режиме отслеживать и обновлять применяемые зависимости в проекте

Тестировщики – вовлеклись в процесс формирования фаззинг-целей с последующим их тестированием

DevOps – обеспечили сборку всех составных частей проекта из исходников, с требуемым уровнем контроля на уровне конвейера

Как просвещение ваших сотрудников по теме РБПО может оказать влияние на их заинтересованность для участия в процессах?

Истории из жизни #2

Исходные данные

Система багтрекинга с открытым исходным кодом, доработанная под собственные нужды

Особенности

Применяется «исторически» в производственных процессах компании-разработчика >10 лет

Вердикт

Не удовлетворяет.
Требуется применять более «зрелые» инструменты, используемые в рамках жизненного цикла разработки ПО, также как и задействованные в этом процессе технологии

Действительно ли применяемая система багтрекинга позволяет покрыть требования РБПО?

Истории из жизни #3

Исходные данные

Студент (-ка) 3-4 курса направлений подготовки: Разработка ПО/Информационная безопасность

Условия

Высокая персональная заинтересованность, горящие глаза и прямые руки

Вердикт

Не только возможно, а очень даже рабочий вариант. Способны решать задачи различного уровня сложности: формирование регламентов по РБПО, участие в процессе сертификации, разметка результатов статического анализа, проведение фаззинг-тестирования и пр.

Обеспечение процессов РБПО при помощи молодых специалистов-инженеров. А такое вообще возможно?

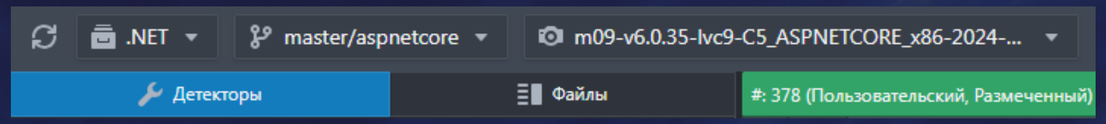
Образовательная и научная деятельность

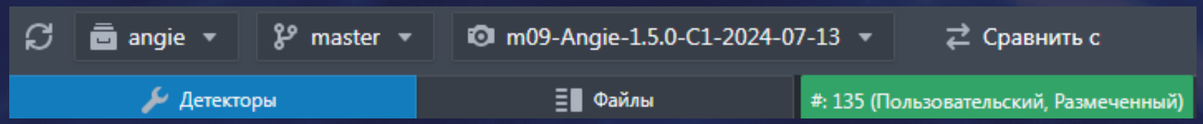
Лаборатория безопасной разработки и системного программирования ЧГУ им. И.Н. Ульянова:

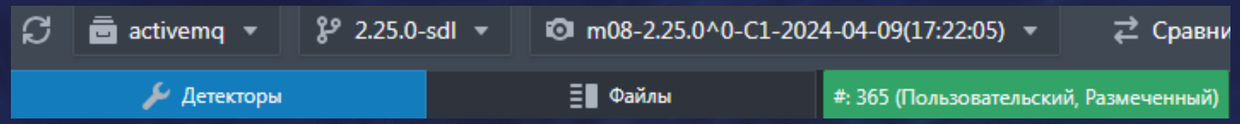
- участие в образовательном процессе студентов
- проведение интенсивов, научно-популярных лекций и семинаров по безопасной разработке
- поддержка студентов при выполнении выпускных квалификационных работ
- выполнение научно-исследовательских работ по тематикам разработки безопасного программного обеспечения

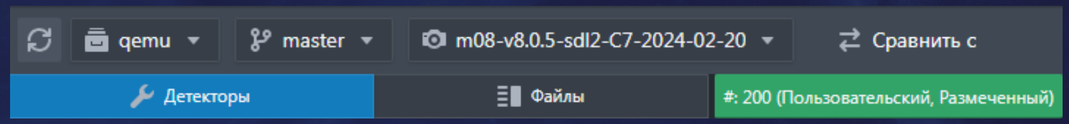
Приглашаем экспертов из отрасли принять участие в лекциях для студентов по вопросам лучших подходов и технологий в области РБПО

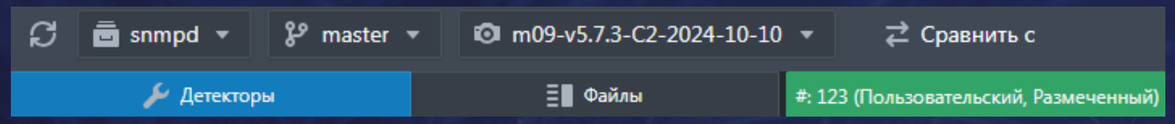
Исследование безопасности системного ПО

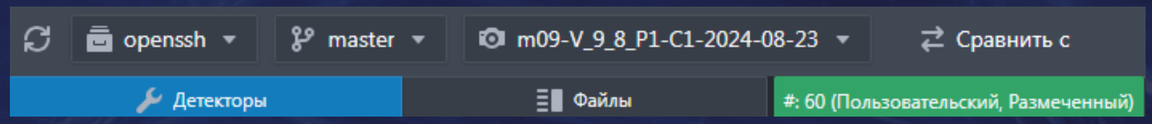












>1500
разметок статического анализа

40+
исправлений на рассмотрении

25
фаззинг-целей разработано

20+
исправлений принято в upstream

В фокусе исследования: activemq, apacheds, dotnet (aspnetcore, runtime), libvirt, libvirt-exporter, qemu, gnutls, openssh, snmpd, nginx, angie и пр.

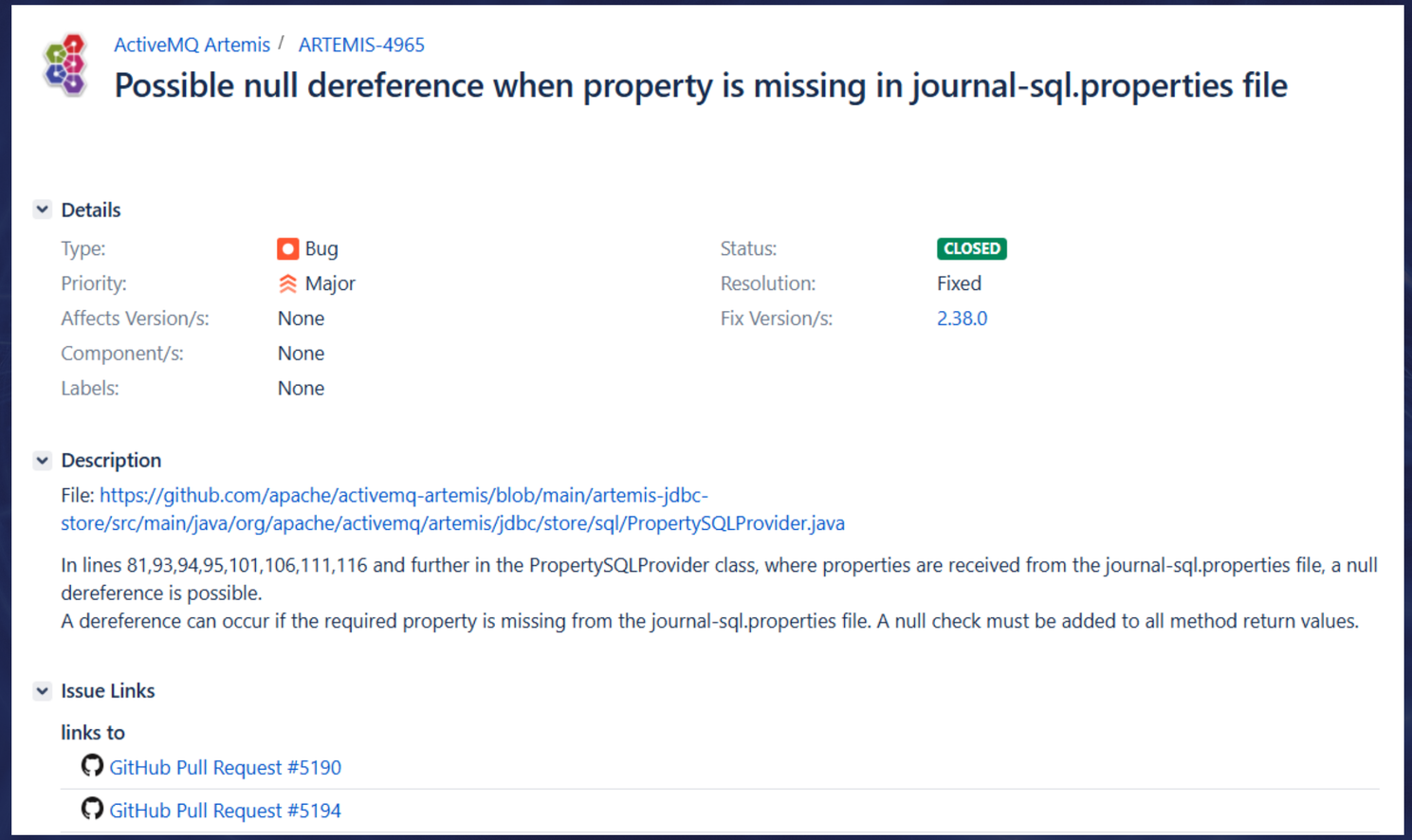
Кейс (Исследование безопасности системного ПО)

Проект Active MQ Artemis
v.2.25.0

Результат

Благодаря одному исправлению, удалось закрыть одновременно 42 ошибки, связанных с разыменованием нуля, без возможности появления подобных проблем в будущем.

Этот случай ярко демонстрирует масштабность эффекта от одного issue, а также насколько важно решать проблемы комплексно, а не каждую из них по отдельности.



ActiveMQ Artemis / ARTEMIS-4965

Possible null dereference when property is missing in journal-sql.properties file

Details

Type:	Bug	Status:	CLOSED
Priority:	Major	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	2.38.0
Component/s:	None		
Labels:	None		

Description

File: https://github.com/apache/activemq-artemis/blob/main/artemis-jdbc-store/src/main/java/org/apache/activemq/artemis/jdbc/store/sql/PropertySQLProvider.java

In lines 81,93,94,95,101,106,111,116 and further in the PropertySQLProvider class, where properties are received from the journal-sql.properties file, a null dereference is possible.
A dereference can occur if the required property is missing from the journal-sql.properties file. A null check must be added to all method return values.

Issue Links

links to

GitHub Pull Request #5190

GitHub Pull Request #5194

Построение процессов РБПО совместно с Центром экспертизы КСБ-СОФТ

01 Внедрение и развитие процессов безопасной разработки

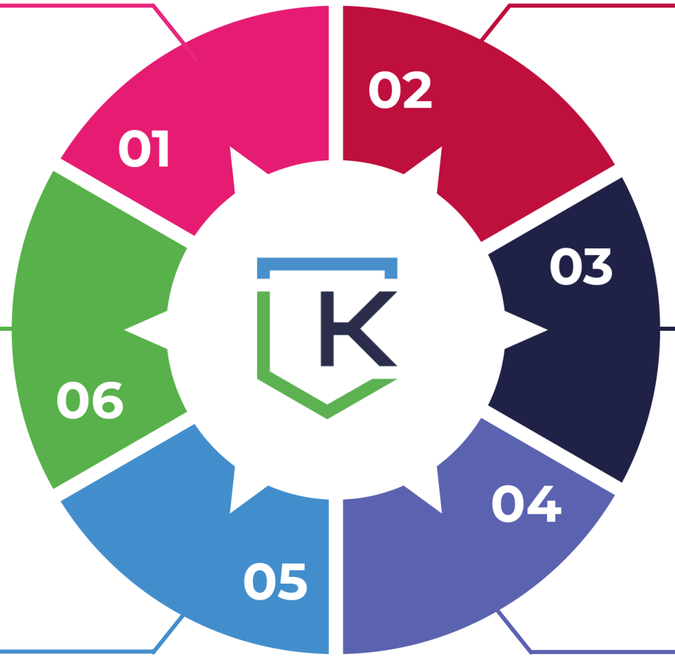
02 Подготовка документации, описывающей разработку безопасного программного обеспечения

03 Проверка соответствия требованиям стандартов и нормативных документов

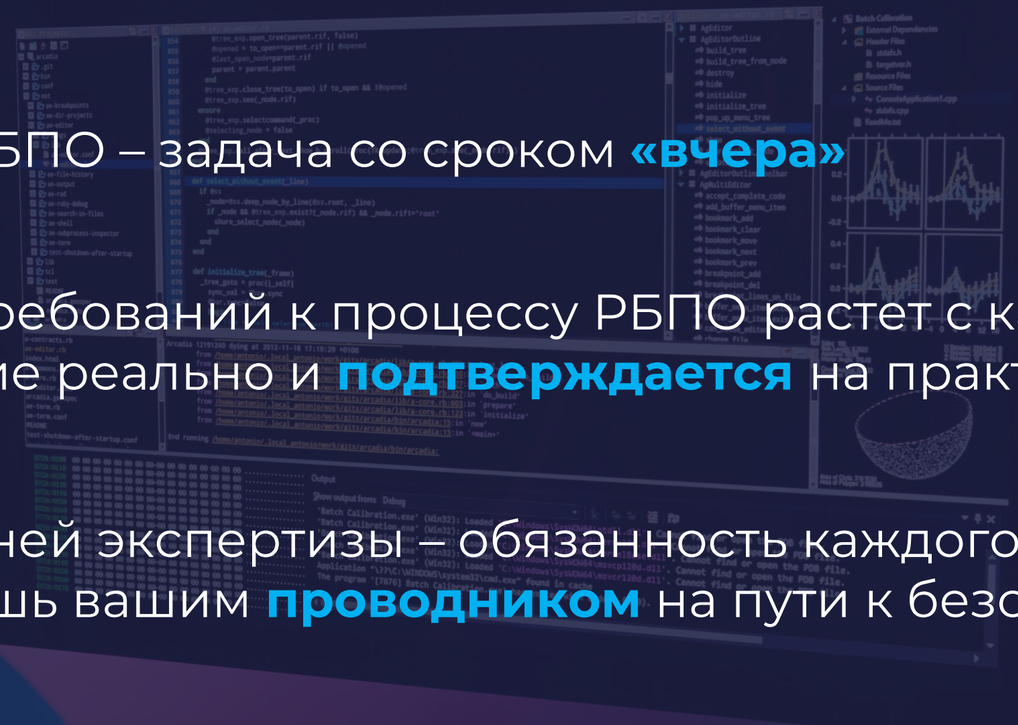
04 Проведение аудита процессов разработки безопасного ПО

05 Обеспечение безопасности приложений во время их выполнения

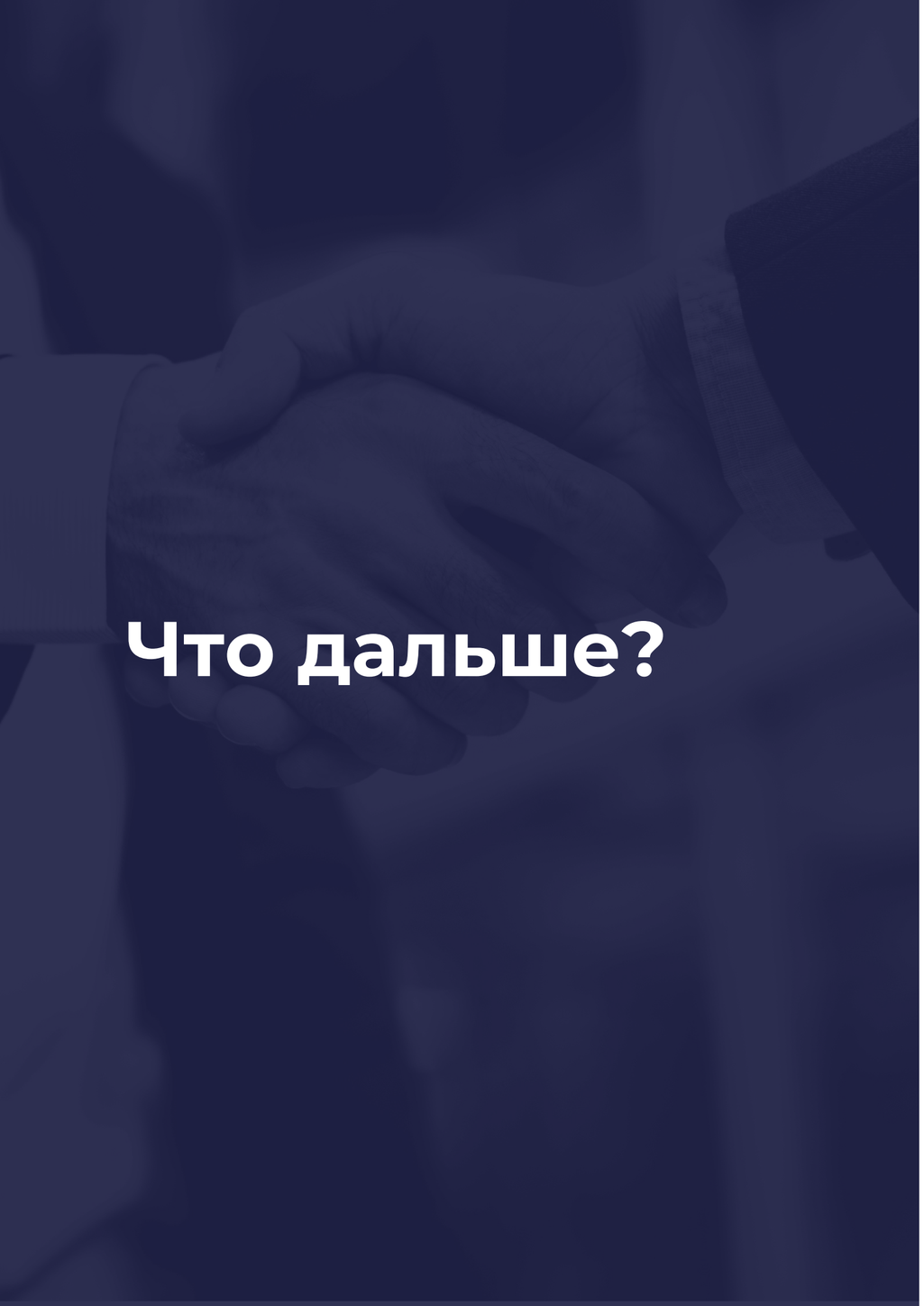
06 Проведение композиционного, статического и динамического анализа, функционального и фаззинг-тестирования



Подводя итоги



1. Внедрение РБПО – задача со сроком **«вчера»**
2. Количество требований к процессу РБПО растет с каждым днем – их выполнение реально и **подтверждается** на практике
3. Рост внутренней экспертизы – обязанность каждого, внешняя компания – выступает лишь вашим **проводником** на пути к безопасному ПО
4. Нет предела совершенству – постоянное развитие процессов безопасной разработки позволит соответствовать **«новым» вызовам**
5. Сторонняя оценка ваших процессов РБПО позволит получить **независимое мнение** о реальном «положении дел»



Что дальше?

1. Регламентирование процессов РБПО (нужна автоматизация?)
2. Самооценка уровня зрелости процессов РБПО на «отечественный лад» (требуется инструмент?)
3. Обеспечение процессов РБПО для компаний, занимающихся разработкой ГИС
4. Создание сетевой магистратуры совместно с ЧГУ им. И.Н. Ульянова и ИСП РАН по профилю: «Разработка безопасного программного обеспечения»
5. Привлечение «большего» студенческого фонда для участия в деятельности Центра исследований безопасности системного ПО

СПАСИБО ЗА ВНИМАНИЕ!

Сделайте первый шаг к новому видению информационной безопасности вместе с нами!

ПРИГЛАШАЕМ ВАС ПОСЕТИТЬ НАШ СТЕНД!

ОСТАЛИСЬ ВОПРОСЫ?

ksb-soft.ru

+7 (8352) 322-322

info@ksb-soft.ru