AKTIV.
CONSULTING

Ноябрь 2022

Внедрение процесса безопасной разработки прикладного ПО в соответствии с требованиями ГОСТ Р 56939

Александр Моисеев
Ведущий консультант по информационной безопасности AKTIV.CONSULTING

О чем сегодня пойдет речь

AKTIV.
CONSULTING

Блок I

Подходы к безопасной разработке

Блок II

Проект внедрения безопасной разработки

AKTIV.
CONSULTING

Блок I

Подходы к безопасной разработке

Предпосылки внедрения БРПО

01 Требования финансовой отрасли

ГОСТ 57580.1 Безопасность финансовых (банковских) операций

п.9.5 (ЖЦ.8)

Проект ГОСТ Обеспечение операционной надежности

п.7.3.4. (УИ.26)

02 Требования для КИИ

Приказ ФСТЭК России от 25 декабря 2017 г. N 239

п.29.3 «...Прикладное ПО должно соответствовать требованиям безопасной разработки...»

03 Бизнес-потребность

Помощь в достижении целей бизнеса за счет:

- снижения стоимости разработки
- управления рисками ИБ

Существующие подходы к безопасной разработке ПО

01 Национальные стандарты и НПА

- 239 приказ ФСТЭК России
- ГОСТ Р 56939 (+проекты новых стандартов)

- 76 приказ ФСТЭК России (выписка)
- *Методика ВУ и НДВ (2020)

**ограниченного распространения*

02 Гармонизированные стандарты

- ГОСТ Р ИСО/МЭК 27034xx «Безопасность приложений»
- ГОСТ Р ИСО/МЭК 15408xx «Общие критерии»

03 Международные практики и стандарты

- Microsoft SDL
- Cisco SDL
- NIST
- и др.

Система стандартов ГОСТ Р 56939

Описание мер БРПО
+ рекомендаций по их внедрению
+ оценке внедренных мер

1. ГОСТ Р 56939-2016 ЗИ. БРПО.
Общие требования

2. ГОСТ Р проект ЗИ. БРПО.
Руководство по реализации мер по БРПО

3. ГОСТ Р проект ЗИ. БРПО.
Руководство по оценке БРПО

Требования к методикам и инструментам,
реализующим конкретные меры

4. ГОСТ Р проект ЗИ. БРПО.
Руководство по проведению статистического анализа

5. ГОСТ Р проект ЗИ. БРПО.
Руководство по проведению динамического анализа

6. ГОСТ Р проект ЗИ. БРПО.
Доверенный компилятор языков С/С++. Общие требования

Этапы по ГОСТ Р 56939

Основные Этапы ЖЦ* ПО

*более подробно описаны в ГОСТ Р ИСО МЭК 12207

Этап 1 «Анализ требований»

Этап 2 «Проектирование архитектуры ПО»

Этап 3 «Конструирование и комплексирование ПО»

Этап 4 «Квалификационное тестирование ПО»

Этап 5 «Инсталляция и приемка ПО»

Этап 6 «Поддержка в процессе эксплуатации»

Обеспечивающие процессы

Процесс А «Менеджмент конфигурации»

Процесс В «Менеджмент среды разработки»

Процесс С «Менеджмент персонала»

Меры безопасности по ГОСТ Р 56939

ОСНОВНЫЕ ПРОЦЕССЫ		ОБЕСПЕЧИВАЮЩИЕ ПРОЦЕССЫ
1. Определение требований по безопасности	9. Функциональное тестирование	17. Процедуры уникальной маркировки версий ПО
2. Анализ и моделирование угроз*	10. Тестирование на проникновение	18. Использование системы управления конфигурацией ПО
3. Уточнение проекта архитектуры ПО	11. Динамический анализ	19. Защита от НСД к элементам конфигурации
4. Идентифицированные средства разработки	12. Фаззинг	20. Резервное копирование
5. Создание ПО на основе уточненного проекта архитектуры	13. Обеспечение целостности ПО в процессе передачи пользователю	21. Регистрация событий, связанных с изменениями элементов конфигурации
6. Порядок оформления исходного кода	14. Поставка пользователю эксплуатационных документов	22. Обучение сотрудников и анализ программы обучения
7. Статический анализ	15. Процедуры отслеживания и исправления ошибок и уязвимостей ПО в ходе ЖЦ	
8. Экспертиза исходного кода	16. Систематический поиск уязвимости	*меры соответствуют требованиям 239 приказа ФСТЭК России

239 приказ ФСТЭК России

01 Руководство по безопасной разработке программного обеспечения

02 Анализ угроз

03 Обеспечение прослеживаемости (только для 1 КЗ)

04 Статический анализ

05 Динамический анализ (только для 1 КЗ)

06 Фаззинг

07 Отслеживание и исправление ошибок и уязвимостей в ходе ЖЦ

08 Информирование разработчиком конечных пользователей

09 Оповещение об окончании поддержки ПО в ходе ЖЦ (только для 1 КЗ)

Мера 1 Этап ЖЦ 1
Руководство по безопасной разработке ПО

Регламентация содержания руководства:

- Описание области действия руководства
- Цели организации в области БРПО
- Распределение ролей и обязанностей
- Перечень документации (+ указатели на ИС, в которых ведутся записи и свидетельства по процессам)
- Правила и требования к планированию и проведению проверок реализации мер БРПО
- Описание действий по улучшению процесса

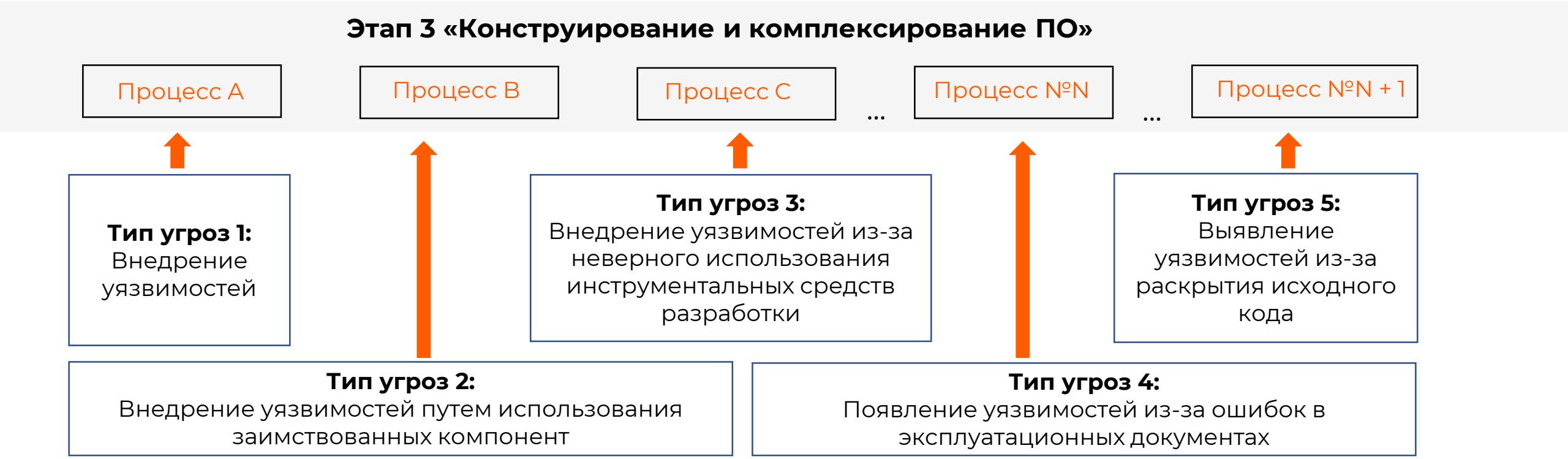
Проблема !

Требуется большое кол-во изменений вслед за развитием проектов и стека используемых ИТ-технологий. Традиционный подход с «бумажным» документом тормозит процессы разработки и обеспечения безопасности.

- Рекомендуем: Выполнять руководство в форме электронного документа по 63-ФЗ

Мера 2 Этап ЖЦ 2
Анализ и моделирование угроз

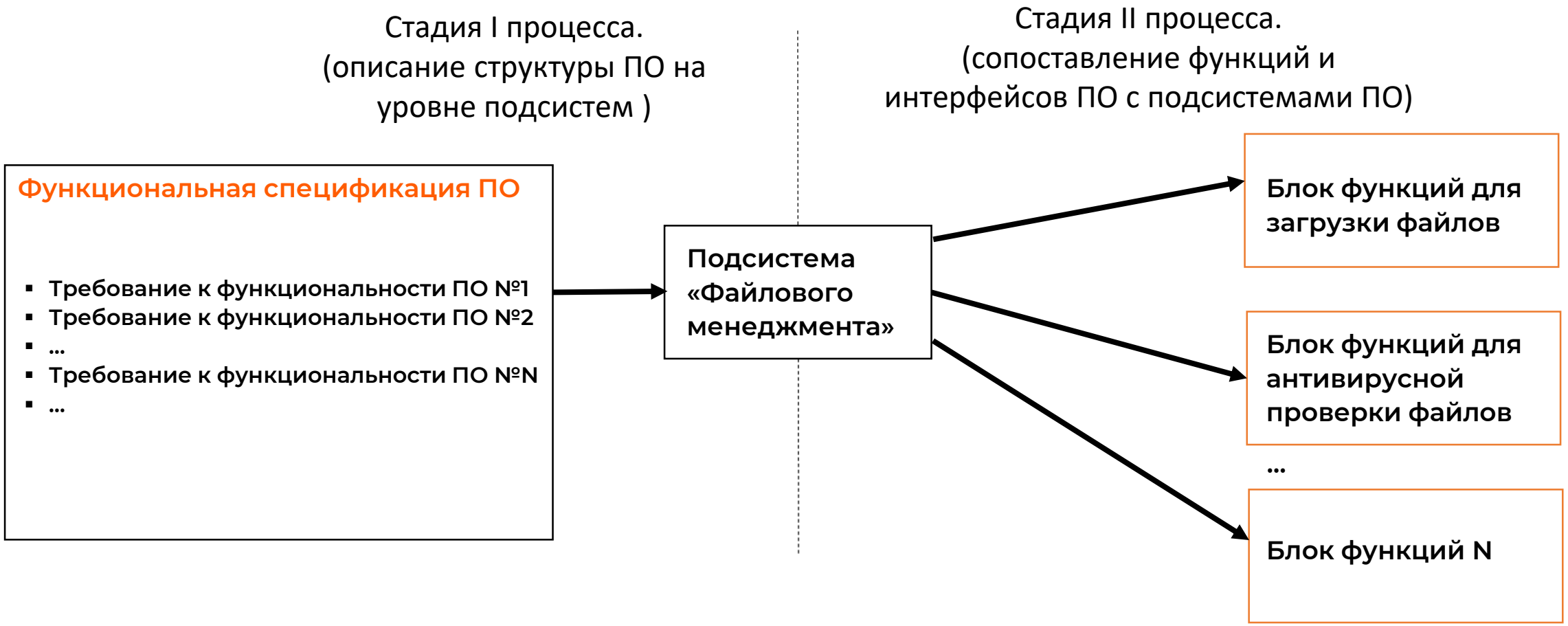
Пример рассмотрения типов угроз
(на примере этапа 3):



Рекомендуем: Перечень угроз ПО в соответствии с ГОСТ Р 58412. Методика моделирования угроз ФСТЭК (от 2021)

Мера 3 Этап ЖЦ 2
Обеспечение прослеживаемости

Пример обеспечения прослеживаемости:

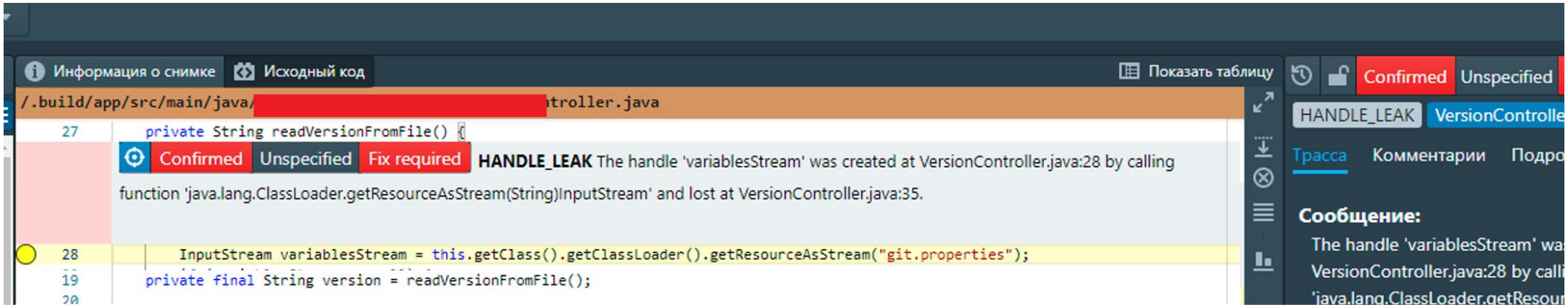


Мера 4 Этап ЖЦ 3
Статический анализ кода

- Выбор инструментов SAST
- Классификация ошибок

- Классификация применяемых методов
- Сопоставление типов предупреждений анализатора списку критических ошибок

Пример выявленной анализатором проблемы утечки из-за незакрытого потока:



Проблема! Не все ЯП поддерживаются инструментами статического анализа

Важное по первому блоку

1. Изменение в постановлении о категорировании объектов КИИ с высокой вероятностью затронет ФО

2. На требования семейства ГОСТов 56939 можно опираться, внедряя процессы БРПО

3. ГОСТ Р 56939 устанавливает 22 меры, которые полностью покрывают требования 239 Приказа ФСТЭК РФ

AKTIV.
CONSULTING

AKTIV.
CONSULTING

Блок II

Проект внедрения процесса БРПО

Пример проекта по внедрению БРПО

01 этап **Обоснование**

- Определение целей и задач проекта
- Формирование команды проекта
- Разработка ТЭО

Результат этапа:

Управленческое решение по внедрению проекта

02 этап **Аудит**

- Обследование текущих бизнес процессов разработки
- Формирование целевого состояния процессов
- GAP-анализ
- Разработка организационных и технических мер безопасности

Результат этапа:

Подготовка перечня организационных и технических мер безопасности

Пример проекта по внедрению БРПО

03 этап

Разработка дорожной карты

- Ранжирование организационных и технических мер
- Разработка «Плана перехода...»
- Разработка «Пояснительной записки...»

Результат этапа:
подготовка «Дорожной карты...»

04 этап

Внедрение процессов

Внедрение процессов и мер, которые включают:

- Организационные меры (ОРД, ЛНА, обучение)
- Технические меры (SAST, DAST, Fuzzing, пентест, code review, КЦ)
- Обеспечивающие меры (менеджмент БРПО и политики лицензирования)

Результат этапа:
функционирующие процессы БРПО

05 этап

Контроль

Проверка полноты и достаточности внедренных мероприятий

Результат этапа:
свидетельства функционирования БРПО

Важное по второму блоку

01 Необходимо выбрать единую точку ответственности – руководителя проекта

02 Собрать команду проекта

03 Определить этапы проекта и промежуточные результаты

04 Оценить и запланировать ресурсы: время, специалистов, финансы

05 Подготовить ТЭО и пояснительные записки к принятым техническим решениям

AKTIV. CONSULTING

AKTIV.
CONSULTING

В качестве резюме

01 Внедрение процессов БРПО упрощает прохождение процедур сертификационных испытаний, оценки соответствия, анализа уязвимостей

02 Оптимальное разделение ролей: техническое лидерство должно быть за разработкой, организационное лидерство за ИБ

03 Для внедрения процесса БРПО можно использовать отечественную регуляторную базу: ГОСТ Р 56939*

*Требования ГОСТа совпадают с 239 Приказом ФСТЭК России, это будет важно для ФО, которые категорируются как ЗО КИИ

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting