guardant DAY

КОМПАНИЯ АКТИВ

AKTIV. CONSULTING

Внедрение процесса безопасной разработки прикладного ПО

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

Драйверы внедрения процесса БРПО

ЭЛЕМЕНТ СУОР	Разработчики ПО и ПАК	
	Разработчики прикладного ПО	Разработчики СЗИ
Бизнес-цели	**Увеличение объемов продаж за счет:** • новых конкурентных преимуществ • новые клиентские сегменты **Сокращение стоимости разработки за счет:** • стандартизации процессов разработки • повышения стабильности релизов	
Комплаенс	**ПО для ФО** ГОСТ Р ИСО/МЭК 15408 ПО для Атомной энергетики **ГОСТ Р 60880** **ПО для КИИ** Приказ ФСТЭК РФ №239	**СЗИ** Приказ ФСТЭК РФ №55, №76

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.

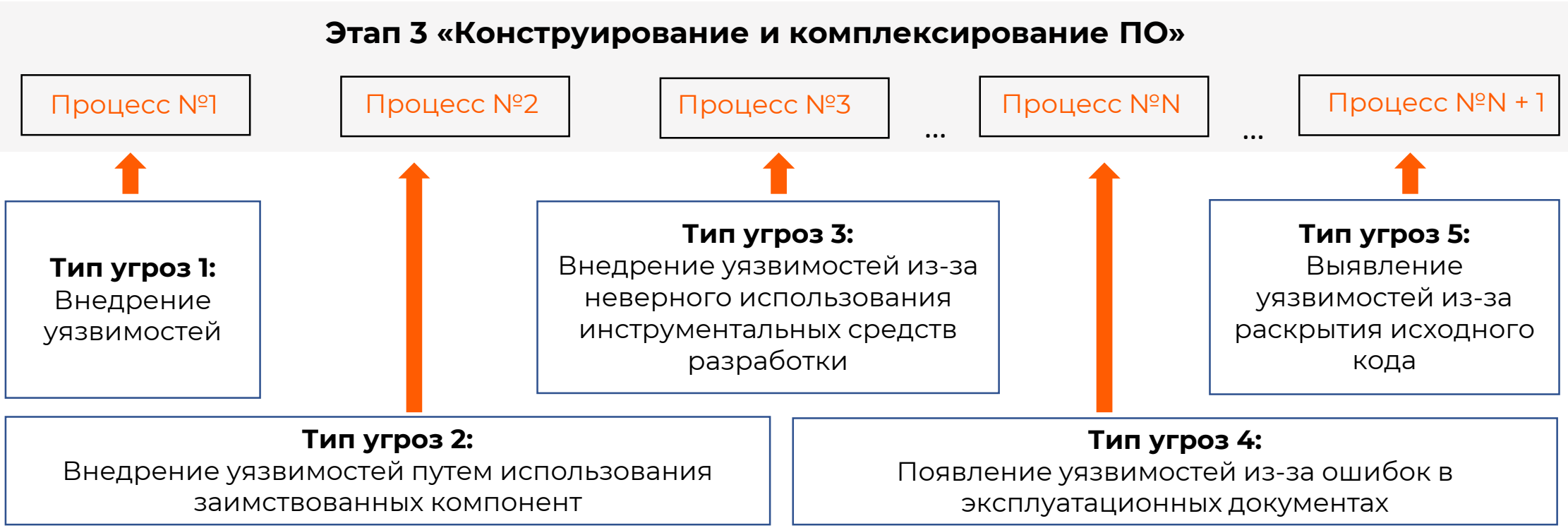
Меры безопасности по ГОСТ Р 56939

Основные Процессы	1. Определение требований по безопасности 2. Анализ и моделирование угроз* 3. Уточнение проекта архитектуры ПО 4. Использование идентифицированных инструментальных средств разработки 5. Создание ПО на основе уточненного проекта архитектуры 6. Порядок оформления исходного кода 7. Статический анализ 8. Экспертиза исходного кода 9. Функциональное тестирование 10. Тестирование на проникновение 11. Динамический анализ 12. Фаззинг 13. Обеспечение целостности ПО в процессе передачи пользователю 14. Поставка пользователю эксплуатационных документов 15. Процедуры отслеживания и исправления ошибок и уязвимостей ПО в ходе ЖЦ 16. Систематический поиск уязвимости
Обеспечивающие процессы	17. Процедуры уникальной маркировки версий ПО 18. Использование системы управления конфигурацией ПО 19. Защита от НСД к элементам конфигурации 20. Резервное копирование 21. Регистрация событий, связанных изменения элементов конфигурации 22. Периодическое обучение сотрудников и анализ программы обучения

*меры соответствуют требованиям 239 приказа ФСТЭК России

Мера 2. Анализ и моделирование угроз

Пример рассмотрения типов угроз
(на примере этапа 3):



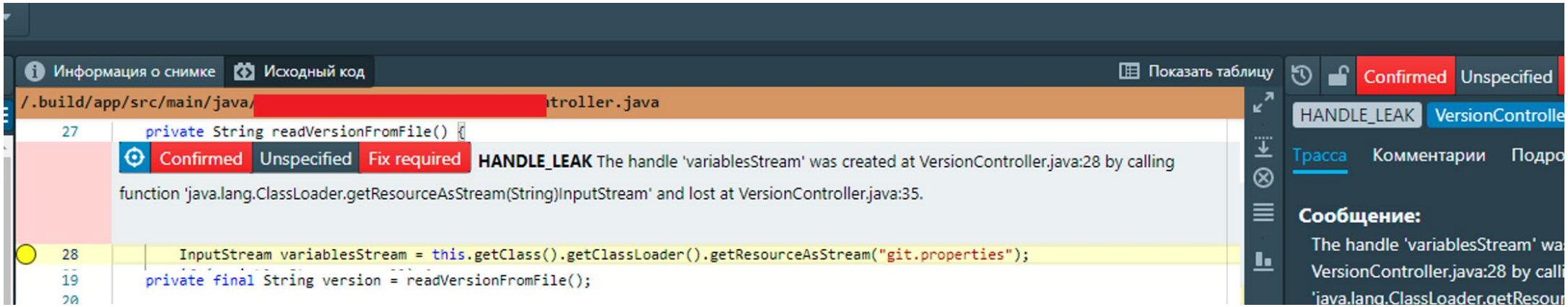
Рекомендуем: Перечень угроз ПО в соответствии с ГОСТ Р 58412. Методика моделирования угроз ФСТЭК (от 2021)

Мера 7. 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

Мера 11. Динамический анализ кода

- Определение функций, принимающих на вход внешние данные
- Инструментирование кода санитайзерами / отладочными аллокаторами
- Проведение модульного и регрессионного тестирования
- Сбор покрытия
- Анализ результатов
- ГОСТы по тестированию:

56920, 56921, 56922

Пример фрагмента отчета о покрытии модульных тестов с нулевым покрытием:

webapp

Element	Missed Instructions	Cov.	Missed Branches	Cov.
[redacted]		0 %		n/a
[redacted]ice.admin.settings.counterpart		0 %		n/a
[redacted]ice.common.logging.event.mq		0 %		0 %
[redacted]		0 %		n/a
[redacted]		0 %		n/a
[redacted]ice.admin.role.authority		0 %		n/a
[redacted]iguration.websocket		0 %		0 %
[redacted]ice.verifier.check.scenario.instance.counterpart		0 %		n/a
[redacted]ain.services.publisher.mq		0 %		0 %
[redacted]ice.admin		0 %		0 %
[redacted]		0 %		n/a
[redacted]ice.common.settings.mq.ldap		0 %		0 %
[redacted]ice.common.settings.mq.general		0 %		0 %
[redacted]ice.verifier.check.scenario.instance.transfer		0 %		0 %
[redacted]ice.verifier.check.routine		0 %		0 %
[redacted]ice.verifier.check.stage.instance		0 %		0 %
[redacted]		0 %		n/a
[redacted]		0 %		0 %
[redacted]		0 %		0 %
[redacted]ice.verifier.check.report		0 %		0 %
[redacted]iguration.db		0 %		n/a
[redacted]		0 %		0 %

Важное по первому блоку

1. Драйверы внедрения БРПО:
   - Регуляторные требования к заказчикам вашего ПО
   - Внутренняя бизнес-потребность

2. Новые клиентские сегменты, конкурентное преимущество

3. Сокращение стоимости разработки

AKTIV. CONSULTING

AKTIV.
CONSULTING

Блок II

Проект внедрения процесса БРПО

Пример проекта по внедрению БРПО

01 этап **Обоснование**

- Определение целей проекта
- Определение задач проекта
- Определение выгод от реализации проекта

Результат этапа:

ТЭО и принятое на его основе решение руководства

02 этап **Аудит**

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

Результат этапа:

Подготовка перечня организационных и технических мер

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 (т.е. руководителя проекта)

02 Собрать команду проекта: ИТ, ИБ, Бизнес

03 Определить этапы проекта и промежуточные результаты

04 Оценить и запланировать ресурсы (время, специалистов, финансы)

AKTIV. CONSULTING

В качестве резюме

AKTIV. CONSULTING

01 С высокой вероятностью вашим клиентам потребуется предоставление свидетельств БРПО, иначе возможен отказ от продукта

02 Основой для внедрения БРПО можно использовать отечественную регуляторную базу – серию ГОСТ Р 56939*

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

*Требования ГОСТа совпадают с 239 Приказом ФСТЭК России,
это будет важно для заказчиков, которые будут использовать ваше ПО

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting