ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Вебинар

Этапы соответствия по ОУД 4

Спикеры

Пушкин Александр

«Внедрение SDLC»

Паршина София

«Разработка
и анализ документов
для оценки ОУД4»

Каргина Татьяна

«Виды исследований
при оценке ОУД 4
и что для этого нужно»

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Внедрение SDLC

Пушкин Александр Несергеевич

Технический директор
компании «Перспективный мониторинг»

Положения Банка России

- **719-П**

ОПДС, БПА, БПС, ОУИС, ОУПИ

- **757-П**

Некредитные финансовые организации

- **683-П (проект)**

Кредитные организации

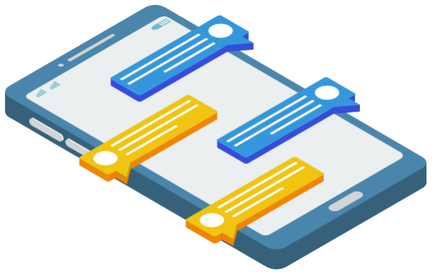
Что оценивается?

- **Мобильные приложения**

  Прикладное ПО АС и приложения, распространяемые клиентам для совершения операций

- **Серверная часть ДБО**

  ПО, предназначенное для приёма поручений от клиентов



Уязвимости подстерегают на каждом шагу

- Выбор архитектуры
- Внедрение
- Непосредственное кодирование
- Эксплуатация

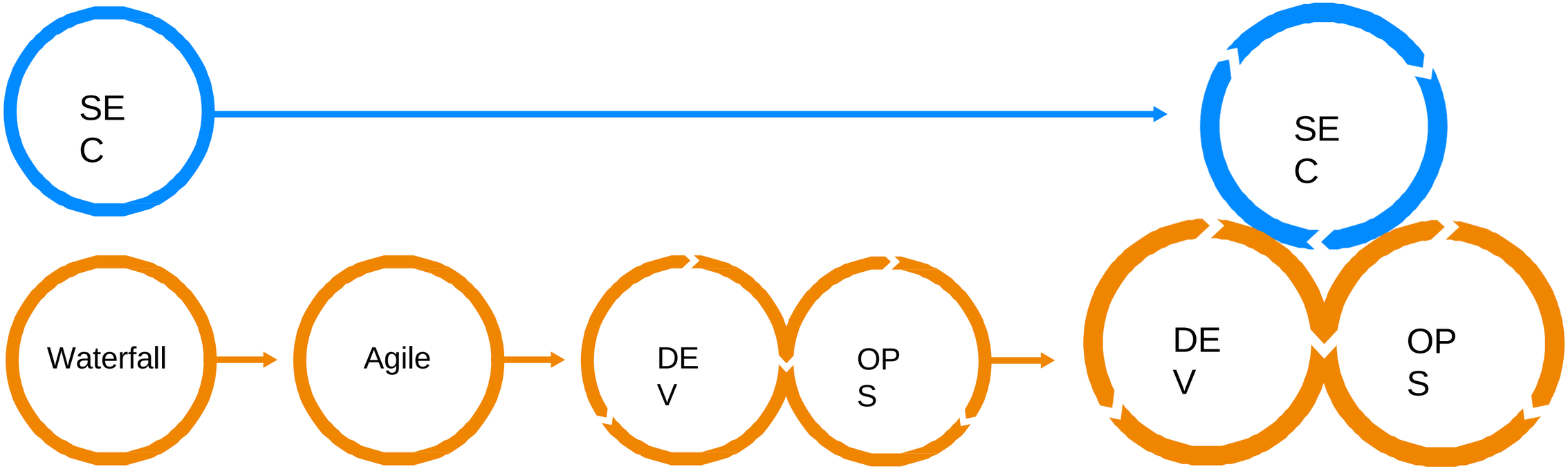
Концепция SDLC

Внедрение на каждый этап разработки дополнительных процессов и инструментов с задачей минимизировать появление уязвимостей

Основные этапы и инструментарий

1. Подготовительный этап
2. Формирование требований к безопасности
3. Проектирование архитектуры
4. Реализация программного решения
5. Тестирование с акцентом на безопасность
6. Установка в продуктовую среду
7. Эксплуатация и сопровождение
8. Вывод из эксплуатации

От Waterfall к Agile



Источник: https://habr.com/ru/company/swordfish_security/blog/596817/

Подход ASOC

(Application Security Orchestration and Correlation)

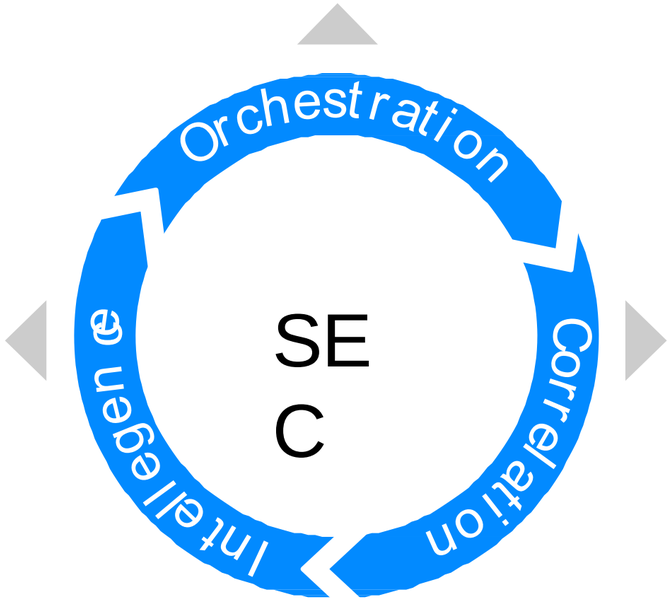
- интегрирует инструменты анализа защищённости – **Application Security Tools (AST)** со стеком разработки программного обеспечения (DevOps)
- обеспечивает прозрачное взаимодействие в реальном времени между инженерными командами и экспертами информационной безопасности **(Software Security Group)**
- Реализует автоматизированное управление процессом создания защищённых программных продуктов на основе данных, получаемых из производственных конвейеров **(DevSecOps pipelines)**

Подход ASOC

(Application Security Orchestration and Correlation)

Software Engineering Tools

- CI/CD
- Defect Tracking
- Source Code Mgmt.
- Artifact Management
- Containers



Application Security Tools

- OSA
- SCA
- SAST
- DAST
- IAST
- BAST
- RASP
- BCA
- API ST
- WAF

Источник: https://habr.com/ru/company/swordfish_security/blog/596817/

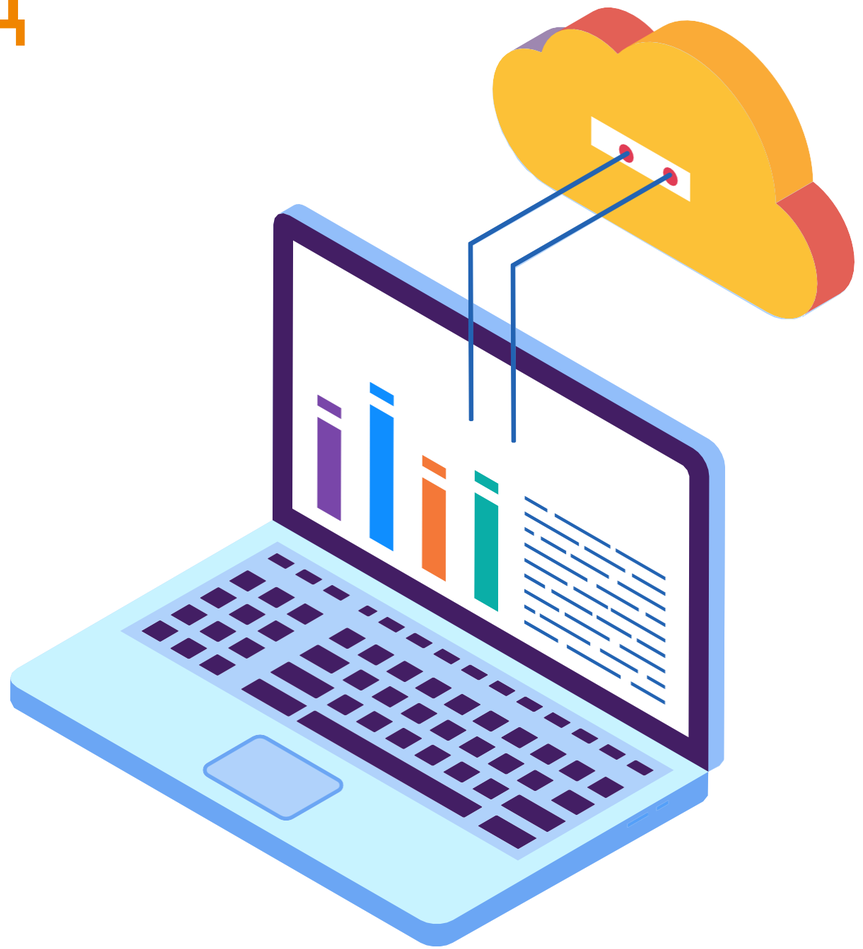
Требования к безопасной разработке в рамках ОУД

Профиль защиты

Прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций

Требования к безопасной разработке в рамках ОУД

- Требования настоящего раздела могут заменить требования доверия к безопасности (ТДБ)
- Могут использоваться методологии **SDLC, DevSecOps , BSIMM , OWASP**



Критерии для реализации безопасного жизненного цикла ОО

- Состав команды должен иметь необходимые компетенции
- Должно быть обеспечено наличие соответствующего специального ПО для реализации процессов жизненного цикла безопасной разработки
- функциональные требования и описание реализации ОО должны быть документированы

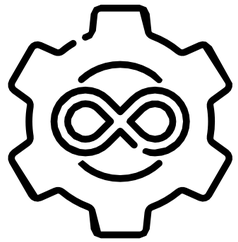
Составзадач безопасного жизненного цикла ОО

- Задача «Организационной подготовки»
- Задача «Формирования требований к ОО»
- Задача «Архитектуры и проектирования ОО»
- Задача «Реализации (разработки) ОО»
- Задача «Тестирования ОО»
- Задача «Подготовки и переноса ОО в промышленную эксплуатацию»
- Задача «Эксплуатации и сопровождения ОО»
- Задача «Вывода из эксплуатации ОО»

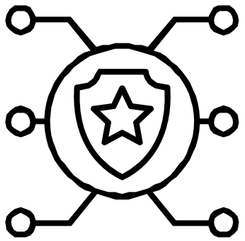
Организационная модель команды

Роль аналитика ИБ («Application Security», «AppSec»)

Роль чемпиона по безопасности («Security Champion»)



Участник команды разработки («Application Security», «AppSec»)



Роль офицера безопасности

Базовое определение ролей

Роль	Контрольные мероприятия безопасности	Задача жизненного цикла	Необходимые компентенции
Аналитик ИБ	Определение требований ИБ к ОО	Задача «Формирование требований»	Владение риск-ориентированным подходом при анализе рисков нарушения ИБ, знание актуальных рисков, уязвимостей, атак, принципов, методов и средств обеспечения ИБ, требований и лучших практик обеспечения ИБ, понимание безопасного жизненного цикла ОО и лучших практик гибких подходов к разработке, внедрению и тестированию
	Анализ рисков нарушения ИБ		
	Требования ИБ и меры для минимизации рисков		

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Пушкин Александр
Несергеевич

Технический директор компании
«Перспективный мониторинг»

Aleksandr.Pushkin@amonitoring.ru

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Разработка и анализ документов для оценки ОУД4

София Паршина

Руководитель проектов
АО «Перспективный мониторинг» в г. Пензе

Стандарты

- **ГОСТ Р ИСО/МЭК 15408-1-2012**

  «Введение и общая модель»

- **ГОСТ Р ИСО/МЭК 15408-3-2013**

  «Компоненты доверия к безопасности»

- **ГОСТ Р 57628-2017**

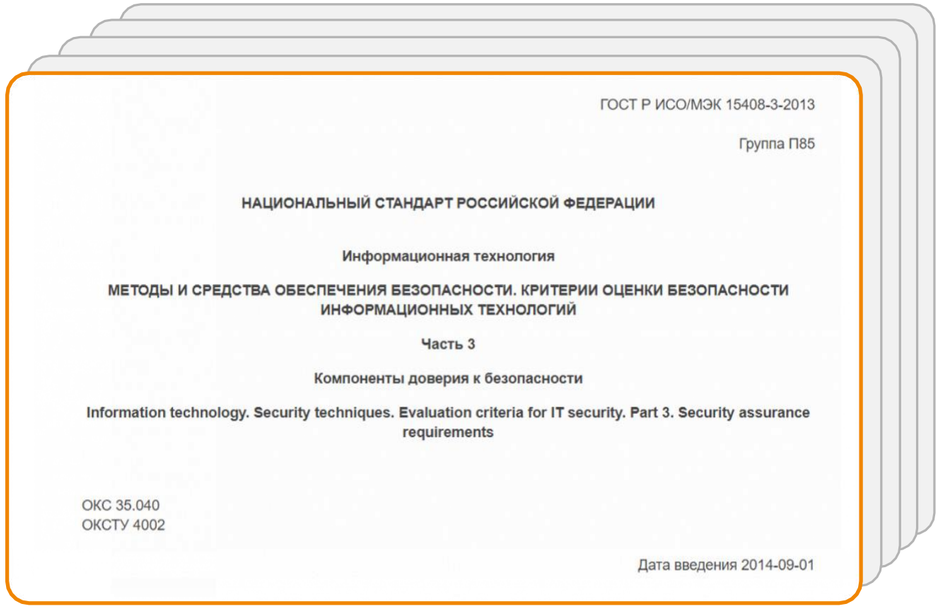
  «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»

- **ГОСТ Р ИСО/МЭК 18045**

  «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

- **ГОСТ Р ИСО/МЭК 15408-2-2013**

  «Введение и общая модель»


ГОСТ Р ИСО/МЭК 15408-3-2013

Группа П85

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 3

Компоненты доверия к безопасности

Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements

ОКС 35.040
ОКСТУ 4002

Дата введения 2014-09-01

Документация
для оценки по ОУД4

Документация должна включать описание самого объекта оценки (ОО), процесса безопасной разработки и его функциональных возможностей безопасности

Ожидание

Документация для оценки по ОУД4 разрабатывалась в параллели с ОО

Реальность

Документация для оценки по ОУД4 разработана частично или не разработана

Через тернии…

Внешний разработчик

Отсутствие разработчика

Отсутствие понимания состава работ

Классы доверия по ОУД4

ASE

Оценка задания по безопасности

ADV

Разработка

AGD

Руководства

AGD_OPE.1

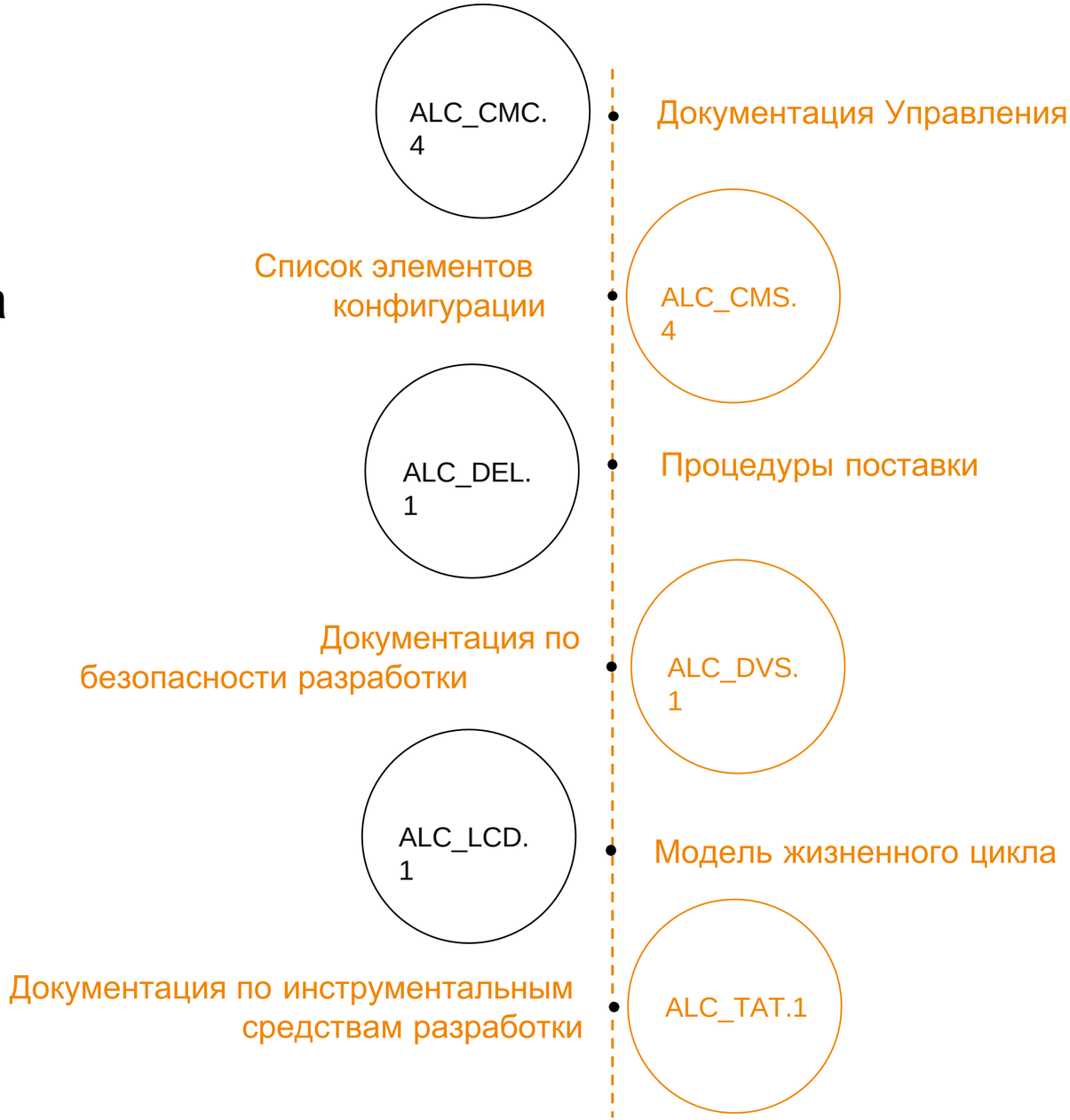
Руководство пользователя по эксплуатации

Подготовительные процедуры

AGD_PRE.1

ALC

Поддержка жизненного цикла



ATE

Тестирование

ATE_FUN.1

Тестовая документация

Свидетельство анализа глубины тестирования

ATE_DPT.2

ATE_COV.2

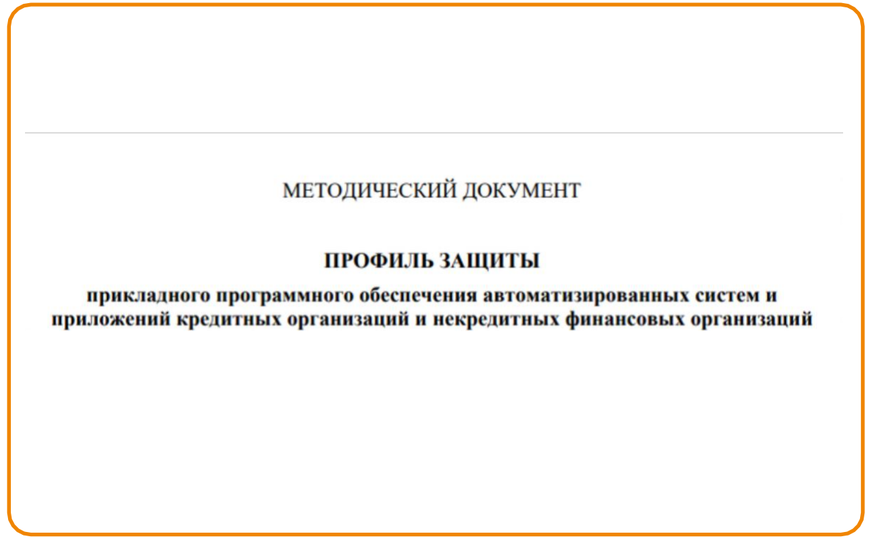
Свидетельство анализа покрытия тестами

Минимальный состав документов

1) Описание архитектуры безопасности
2) Функциональная спецификация
3) Представление реализации
4) Проект ОО
5) Руководство пользователя
6) Подготовительные процедуры
7) Документация Управления Конфигурацией
8) Список элементов конфигурации
9) Документация поставки
10) Документация по безопасности разработки
11) Модель жизненного цикла ПО
12) Документация инструментальных средств разработки
13) Тестовая документация
14) Свидетельство анализа глубины тестирования
15) Свидетельство анализа покрытия тестами

Профиль защиты

- Носит рекомендательный характер
- Включает ряд дополнительных требований к документации для оценки по ОУД4
- При указании в ЗБ соответствия ПЗ – ОО должен соответствовать всем требованиям данного ПЗ



МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ

прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций

Опубликован Банком России
от 02.02.2022

Перечень документов по Профилю защиты

Документация
для оценки по ОУД4

1) Реализация ОО
2) Процедуры устранения недостатков
3) Руководство по устранению недостатков
4) Процедуры обновления программного обеспечения
5) Декларация о сроке поддержки ОО
6) Документация по анализу скрытых каналов
7) Свидетельства анализа влияния обновлений на безопасность ОО

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

София Паршина

Руководитель проектов
АО «Перспективный мониторинг»
в г. Пензе

Sofia.Parshina@amonitoring.ru

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Виды исследований при оценке ОУД 4
и что для этого нужно

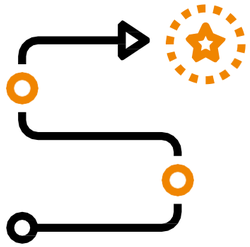
Каргина Татьяна

Менеджер по работе с заказчиками
компании «Перспективный мониторинг»

Требования доверия безопасности

- Оценка задания по безопасности
- Оценка безопасности процессов разработки и поддержки ЖЦ
- Оценка предоставленных руководств по эксплуатации ОО
- Оценка программ тестирования ОО

Что разберём?

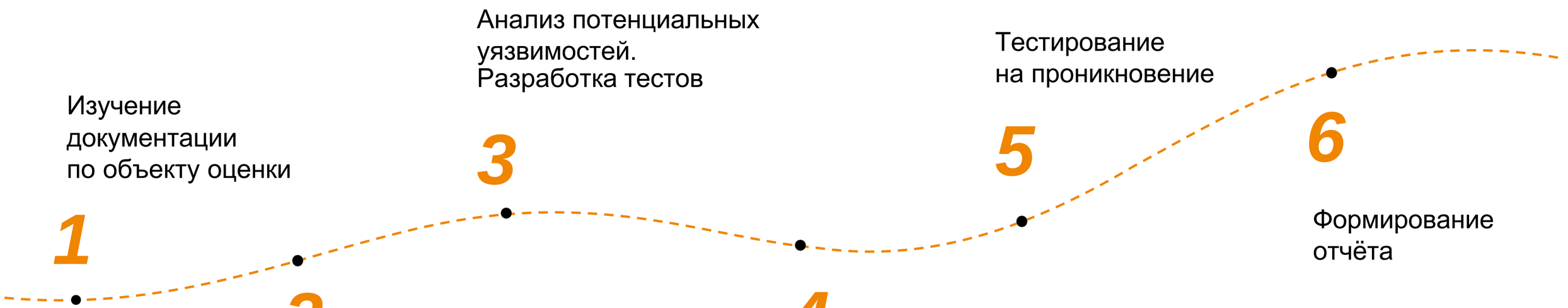


Этапы проведения работ

Основные виды исследований

- Анализ уязвимостей
- Анализ исходного кода (статический и динамический)
- Тестирование на проникновение

Этапы проведения работ



Анализ уязвимостей

Что требуется?

1) Задание по безопасности
2) Документация руководств
3) Функциональная спецификация
4) Проект ОО
5) Описание архитектуры безопасности и представления реализации

Результат

Перечень потенциальных уязвимостей, классифицированных по степени критичности

Статический анализ исходного кода

Что требуется?

Исходный код:

1) Файловый архив
2) Сборочный пакет
3) Виртуальная машина со средствами компиляции

Результат

1) Список обнаруженных слабостей исходного кода
2) Перечень слабостей ПО, которые могут являться источником уязвимостей и которые необходимо проверить при проведении тестов на проникновения
3) Рекомендации по устранению
4) Оценка текущего уровня качества написания исходного кода с точки зрения разработки безопасного ПО

Динамический анализ исходного кода

Что требуется?

1) Дистрибутив
2) Виртуальная машина
3) Доступ к уже развёрнутому стенду
4) Краткая инструкция по работе
5) Список учётных данных

Результат

1) Перечень выявленных уязвимостей исследуемого ПО
2) Рекомендации по повышению безопасности программирования

Тестирование
на проникновение

Что предоставить?

Результаты всех предыдущих этапов

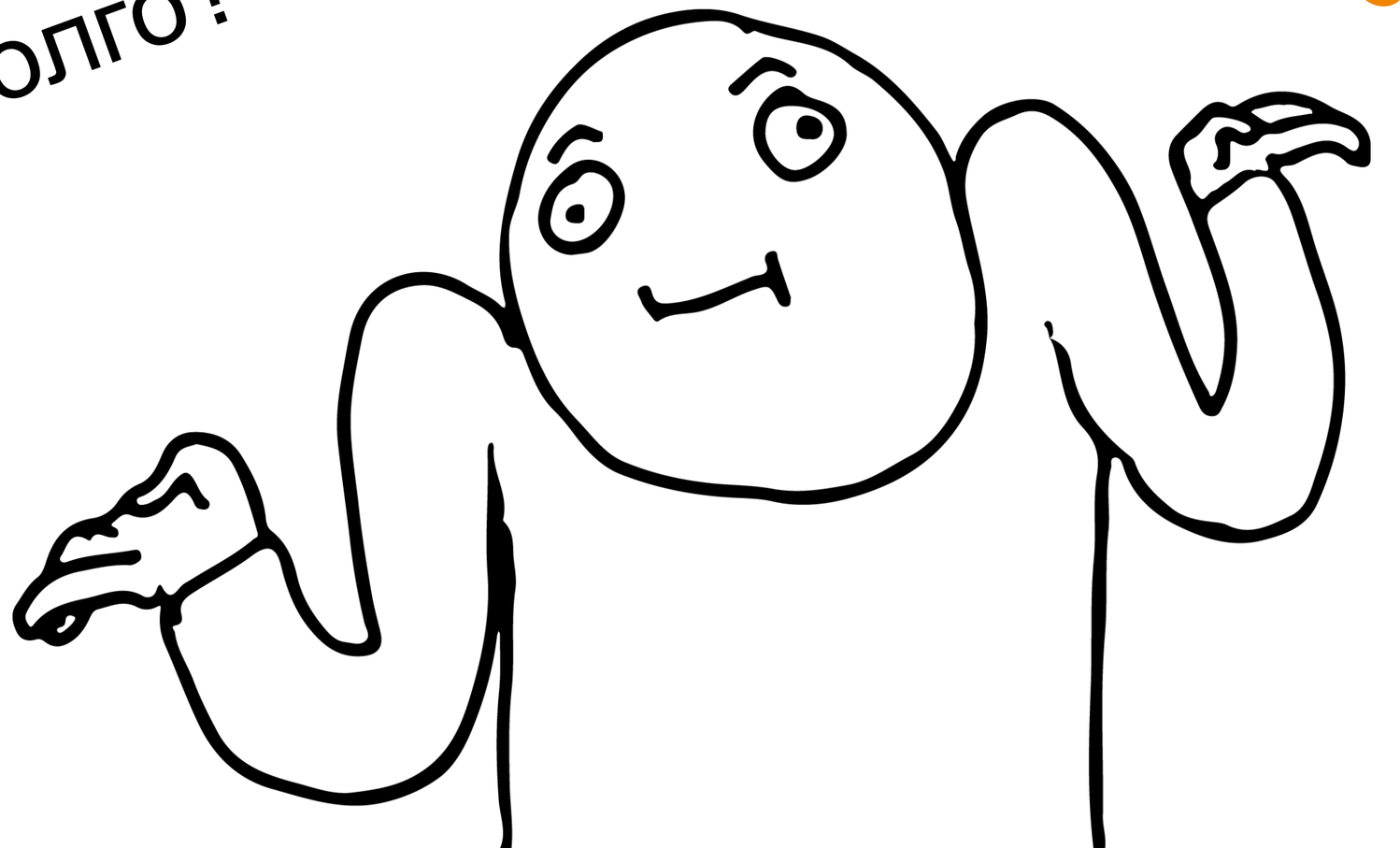
Результат

Список уязвимостей, обнаруженных при проведении тестирования на проникновение и анализа уязвимостей.

По каждой найденной уязвимости дано детальное описание, а также рекомендации по их устранению или существенному снижению потенциальных угроз

Как долго?

Как часто?



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Каргина Татьяна

Менеджер по работе
с заказчиками в компании
«Перспективный мониторинг»

+7 (495) 737-61-97, доб. 4113
Tatiana.Kargina@amonitoring.ru