РЕГУЛЯТОРНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОЙ РАЗРАБОТКЕ В ЭПОХУ AGILE

Бакин Александр

Руководитель Группы защиты приложений
Центр информационной безопасности
АО «Инфосистемы Джет»

2023

СТРУКТУРА ПРЕЗЕНТАЦИИ

ОБЗОР СУЩЕСТВУЮЩИХ ТРЕБОВАНИЙ В ОБЛАСТИ БЕЗОПАСНОЙ РАЗРАБОТКЕ ПО

СУЩЕСТВУЮЩИЕ НОРМАТИВНЫЕ ТРЕБОВАНИЯ

ПРИКЛАДНОЕ ПО ЗОКИИ

Приказ ФСТЭК №239

- Требования по безопасной разработке ПО (наличие руководства по безопасной разработке ПО, проведение анализа угроз безопасности информации ПО, *наличие описания структуры ПО**)
- Проведение испытаний по выявлению уязвимостей в ПО (статический анализ исходного кода, фаззинг-тестирование, *динамическое тестирование**)
- Требования к поддержке безопасности ПО (наличие процедуры управления дефектами ПО и процедуры информирования пользователей ПО)

**для ЗОКИИ 1-ой категории*

СУЩЕСТВУЮЩИЕ НОРМАТИВНЫЕ ТРЕБОВАНИЯ

ПРИКЛАДНОЕ ПО ЗОКИИ

Приказ ФСТЭК №239

- Требования по безопасной разработке ПО (наличие руководства по безопасной разработке ПО, проведение анализа угроз безопасности информации ПО, *наличие описания структуры ПО**)
- Проведение испытаний по выявлению уязвимостей в ПО (статический анализ исходного кода, фаззинг-тестирование, *динамическое тестирование**)
- Требования к поддержке безопасности ПО (наличие процедуры управления дефектами ПО и процедуры информирования пользователей ПО)

**для ЗОКИИ 1-ой категории*

ПРИКЛАДНОЕ ПО ФО*

Положение 719-П | **Положение 683-П** | **Положение 757-П** | **ГОСТ Р 57580.1-2017**

- Оценка соответствия по требованиям не ниже ОУД 4 (24+ требования доверия к безопасности, включающие требования к проектной, эксплуатационной документации, жизненному циклу разработки ПО, тестированию и оценке уязвимостей)

или

- Сертификация в системе сертификации ФСТЭК России

**ПО, распространяемое клиентам для совершения финансовых операций, а также ПО, обрабатывающее ЗИ при приеме ЭС к исполнению с использованием «Интернет»*

КЛАССИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ СООТВЕТСТВИЯ ПО ТРЕБОВАНИЯМ ОУД

ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

Оценка задания по безопасности

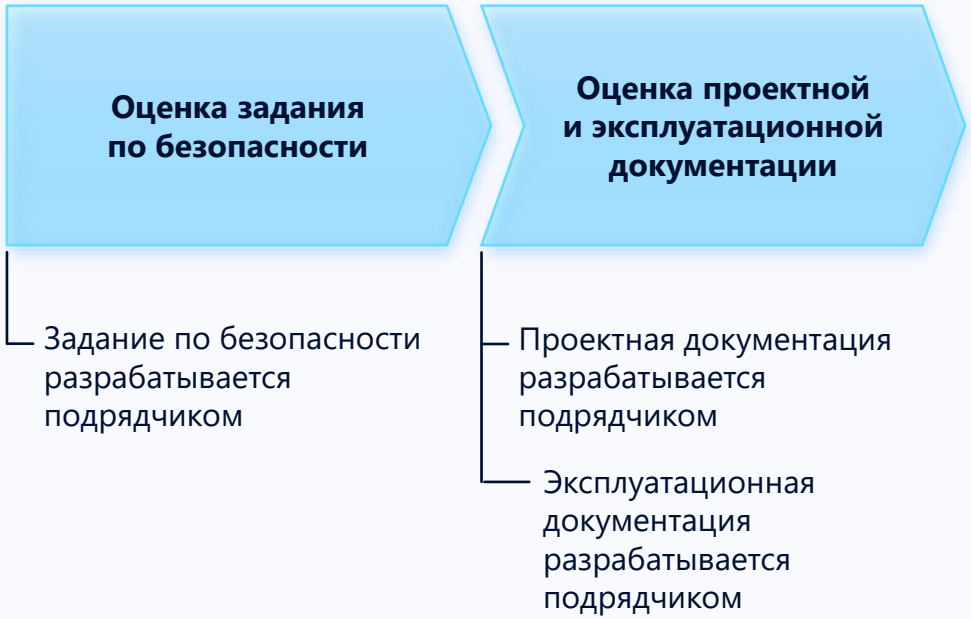
ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

Оценка задания по безопасности

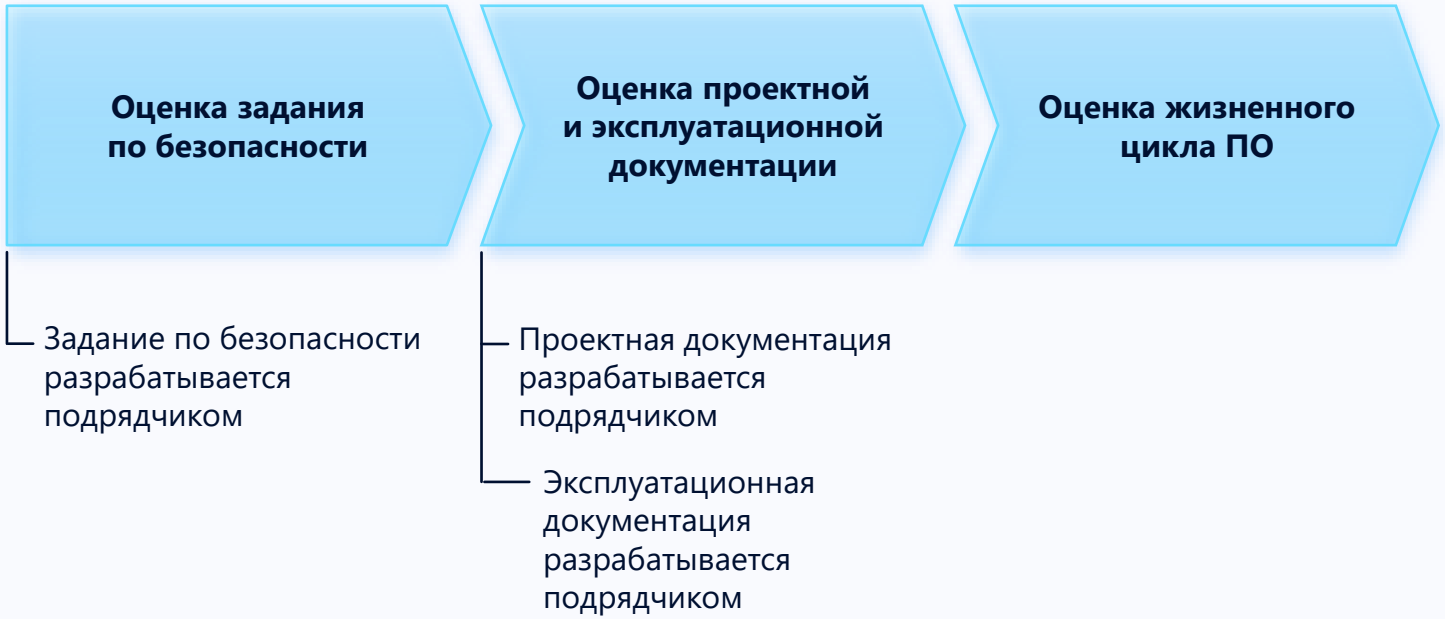
Задание по безопасности разрабатывается подрядчиком

ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

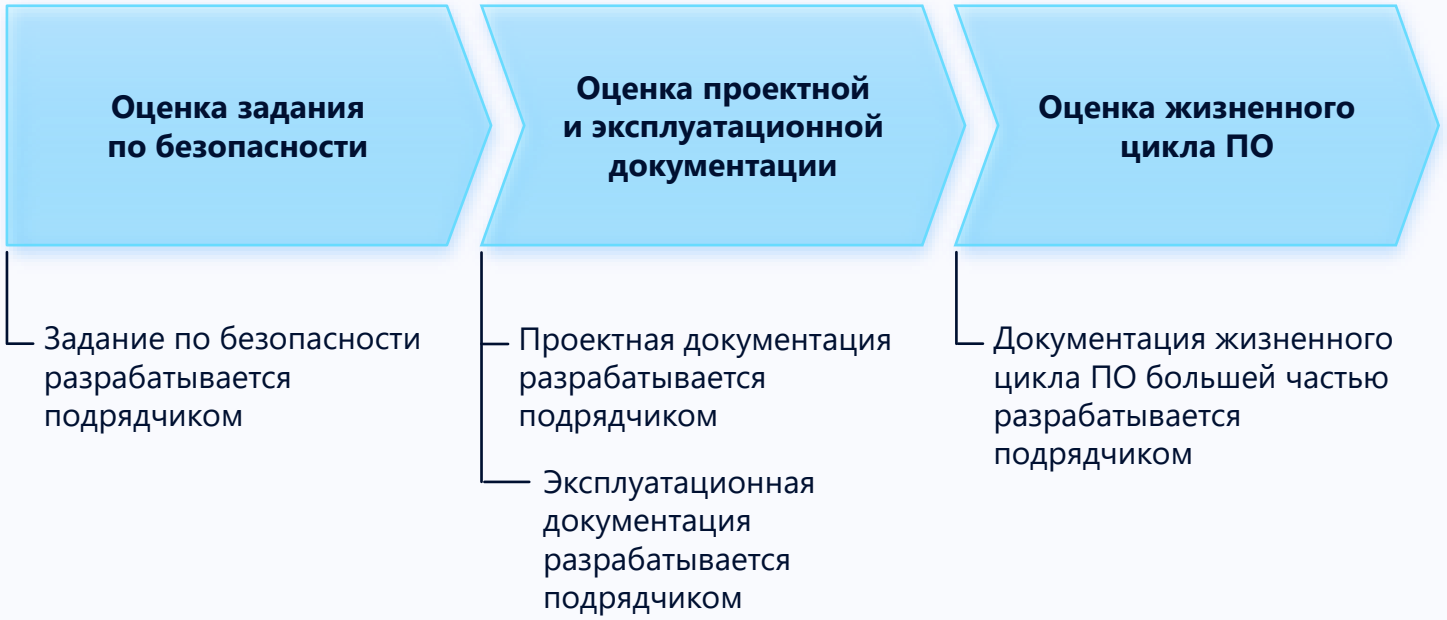
ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ



ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

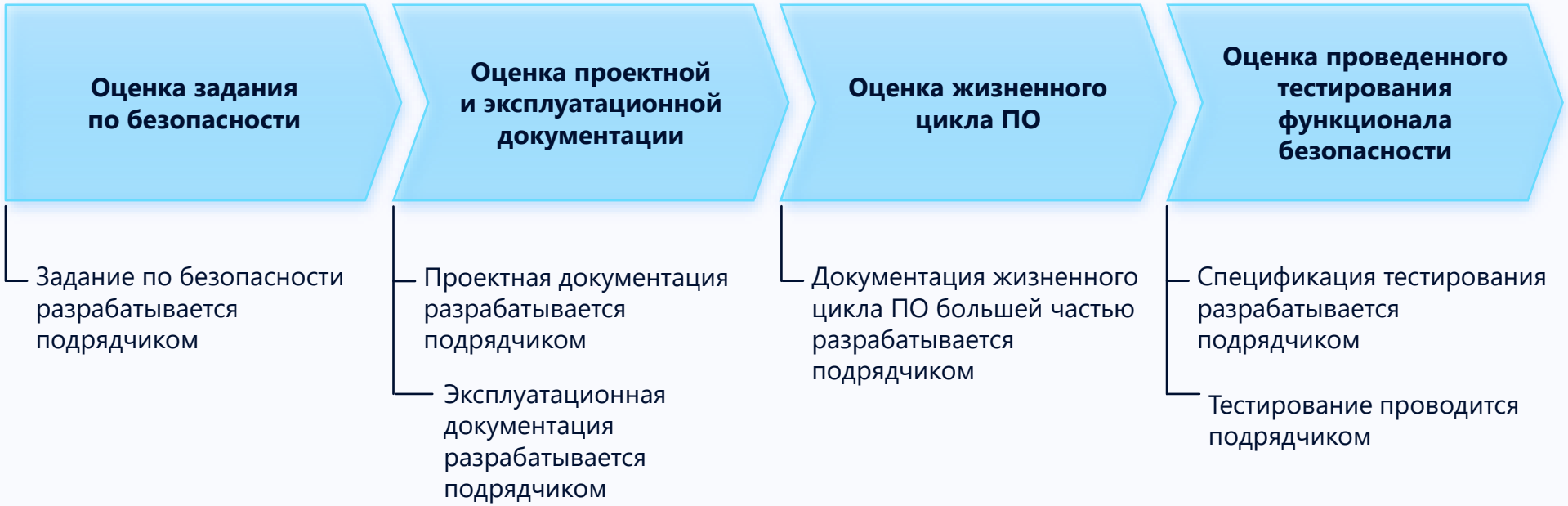


ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ



ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ



ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ

Оценка задания по безопасности	Оценка проектной и эксплуатационной документации	Оценка жизненного цикла ПО	Оценка проведенного тестирования функционала безопасности	Оценка уязвимостей
Задание по безопасности разрабатывается подрядчиком	Проектная документация разрабатывается подрядчиком Эксплуатационная документация разрабатывается подрядчиком	Документация жизненного цикла ПО большей частью разрабатывается подрядчиком	Спецификация тестирования разрабатывается подрядчиком Тестирование проводится подрядчиком	Подрядчик анализирует исходный код и сторонние компоненты на уязвимости Подрядчик формирует тестовые сценарии и проводит тестирование на проникновение

ПО РЕЗУЛЬТАТАМ ПРОЕКТА ЗАКАЗЧИК ПОЛУЧАЕТ:

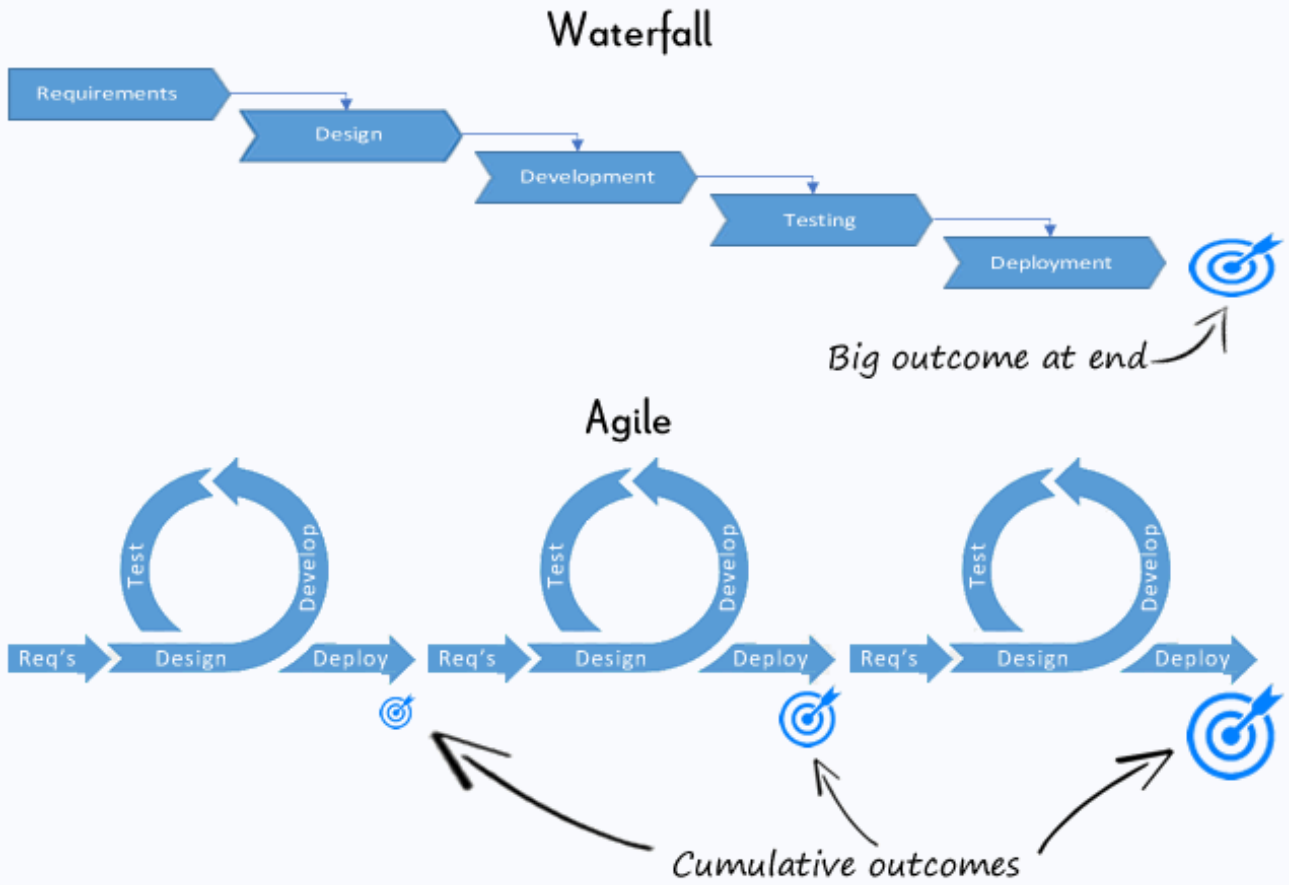
- Документацию на ПО и жизненный цикл его разработки
- Повышение защищенности ПО
- Документ о соответствии ПО регуляторным требованиям ЦБ

Оценке подвергается конкретный релиз ПО

Средняя длительность Проекта ~ 6-8 месяцев*

ПРОБЛЕМАТИКА И ВАРИАНТЫ РЕШЕНИЯ

ПОДХОДЫ К РАЗРАБОТКЕ ПО



WATERFALL

- Определение и последовательное продвижение к конечной цели
- Максимум несколько major релизов в год

AGILE

- Порционное внедрение продукта
- До нескольких обновлений ПО в день

ПРОБЛЕМАТИКА

ВАРИАНТЫ РЕШЕНИЯ

МЕХАНИЗМЫ ГОСТ 15408

AMA_SIA_EXT.3
Анализ влияния обновлений на безопасность ПО*

ALC_FPU_EXT.1
Процедуры обновления ПО**

Для каждого релиза ПО необходимо проводить анализ влияния обновлений на безопасность ПО.

Материалы анализа должны содержать:

- краткое описание влияние обновлений на ЗБ и реализацию ФБО (или логическое обоснование отсутствия такого влияния);
- подтверждение устранения уязвимости (уязвимостей), на устранение которой(-ых) направлен выпуск данных обновлений, и невнесения иных уязвимостей в ПО;
- *(в случае влияния на безопасность)* идентификацию функций безопасности и компонентов ПО, на которые влияет данное обновление.

Разработчик должен разработать и реализовать процедуру представления обновлений оценщику для проведения внешнего контроля

** Подробнее Приложение Б.4.1 Профиля защиты ПЗ ЦБ*
*** Подробнее Приложение Б.2.1 Профиля защиты ПЗ ЦБ*

ВАРИАНТЫ РЕШЕНИЯ

МЕХАНИЗМЫ ГОСТ 15408

AMA_SIA_EXT.3
Анализ влияния обновлений на безопасность ПО*

ALC_FPU_EXT.1
Процедуры обновления ПО**

Для каждого релиза ПО необходимо проводить анализ влияния обновлений на безопасность ПО.

Материалы анализа должны содержать:

- краткое описание влияние обновлений на ЗБ и реализацию ФБО (или логическое обоснование отсутствия такого влияния);
- подтверждение устранения уязвимости (уязвимостей), на устранение которой(-ых) направлен выпуск данных обновлений, и невнесения иных уязвимостей в ПО;
- *(в случае влияния на безопасность)* идентификацию функций безопасности и компонентов ПО, на которые влияет данное обновление.

Разработчик должен разработать и реализовать процедуру представления обновлений оценщику для проведения внешнего контроля

** Подробнее Приложение Б.4.1 Профиля защиты ПЗ ЦБ*
*** Подробнее Приложение Б.2.1 Профиля защиты ПЗ ЦБ*

АЛЬТЕРНАТИВНЫЙ

Оценка процесса гибкой безопасной разработки и тестирования ПО***

Реализовать документированный безопасный жизненный цикл ПО, основанный на современных гибких практиках разработки, тестирования и внедрения ПО, в основе которых лежат различные методологии безопасного жизненного цикла программных продуктов (например, SDL, DevSecOps, BSIMM, OWASP и др.)

**** Раздел 7.4 Профиля защиты ПЗ ЦБ*

АЛЬТЕРНАТИВНЫЙ ПОДХОД

УСЛОВИЯ ПЕРЕХОДА

Выполнены все функциональные требования безопасности из раздела 7.1 Профиля защиты ЦБ

УСЛОВИЯ ПЕРЕХОДА

Выполнены все функциональные требования безопасности из раздела 7.1 Профиля защиты ЦБ

Разработчик должен иметь документированный процесс разработки, тестирования и эксплуатации, включая описания реализуемых мер, контролей (security controls) и проверок по обеспечению ИБ.

УСЛОВИЯ ПЕРЕХОДА

Выполнены все функциональные требования безопасности из раздела 7.1 Профиля защиты ЦБ

Разработчик должен иметь документированный процесс разработки, тестирования и эксплуатации, включая описания реализуемых мер, контролей (security controls) и проверок по обеспечению ИБ.

Инфраструктура Разработчика, на которой выполняются процессы разработки, тестирования и развертывания, а также среды постоянной эксплуатации, должна соответствовать требованиям ГОСТ Р 57580.1-2017.

УСЛОВИЯ ПЕРЕХОДА

Выполнены все функциональные требования безопасности из раздела 7.1 Профиля защиты ЦБ

ПО не должно использоваться в составе ЗОКИИ

Разработчик должен иметь документированный процесс разработки, тестирования и эксплуатации, включая описания реализуемых мер, контролей (security controls) и проверок по обеспечению ИБ.

Инфраструктура Разработчика, на которой выполняются процессы разработки, тестирования и развертывания, а также среды постоянной эксплуатации, должна соответствовать требованиям ГОСТ Р 57580.1-2017.

УСЛОВИЯ ПЕРЕХОДА

Выполнены все функциональные требования безопасности из раздела 7.1 Профиля защиты ЦБ

ПО не должно использоваться в составе ЗОКИИ

Разработчик должен иметь документированный процесс разработки, тестирования и эксплуатации, включая описания реализуемых мер, контролей (security controls) и проверок по обеспечению ИБ.

Разработчик должен иметь документированный процесс управления версиями и изменениями ПО

Инфраструктура Разработчика, на которой выполняются процессы разработки, тестирования и развертывания, а также среды постоянной эксплуатации, должна соответствовать требованиям ГОСТ Р 57580.1-2017.

УСЛОВИЯ ПЕРЕХОДА

Выполнены все функциональные требования безопасности из раздела 7.1 Профиля защиты ЦБ

Разработчик должен иметь документированный процесс разработки, тестирования и эксплуатации, включая описания реализуемых мер, контролей (security controls) и проверок по обеспечению ИБ.

Инфраструктура Разработчика, на которой выполняются процессы разработки, тестирования и развертывания, а также среды постоянной эксплуатации, должна соответствовать требованиям ГОСТ Р 57580.1-2017.

ПО не должно использоваться в составе ЗОКИИ

Разработчик должен иметь документированный процесс управления версиями и изменениями ПО

Главное условие перехода….

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка

- Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями
- Обеспечить безопасность сред разработки и эксплуатации
- Обеспечить наличие необходимых инструментов

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка

- Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями
- Обеспечить безопасность сред разработки и эксплуатации
- Обеспечить наличие необходимых инструментов

Формирование требований к ОО

- Определение требований ИБ к ОО
- Анализ рисков нарушения ИБ
- Требования ИБ
- и меры для минимизации рисков
- Заключение по ИБ

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка	Формирование требований к ОО	Архитектура и проектирование ОО
• Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями • Обеспечить безопасность сред разработки и эксплуатации • Обеспечить наличие необходимых инструментов	• Определение требований ИБ к ОО • Анализ рисков нарушения ИБ • Требования ИБ • и меры для минимизации рисков • Заключение по ИБ	• Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО • Проверка соответствия требованиям ИБ стороннего ПО • Уточнение и последующий анализ проекта архитектуры и требований по безопасности •Документирование проектных решений по ИБ

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка	Формирование требований к ОО	Архитектура и проектирование ОО	Реализация (разработка) ОО
• Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями • Обеспечить безопасность сред разработки и эксплуатации • Обеспечить наличие необходимых инструментов	• Определение требований ИБ к ОО • Анализ рисков нарушения ИБ • Требования ИБ • и меры для минимизации рисков • Заключение по ИБ	• Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО • Проверка соответствия требованиям ИБ стороннего ПО • Уточнение и последующий анализ проекта архитектуры и требований по безопасности •Документирование проектных решений по ИБ	• Анализ заимствованных компонент на наличие уязвимостей • Анализ кода, компонентов на соответствие ИБ • Разработка решений по ИБ для ПО • Разработка автоматизированных тестов по безопасности • Обеспечение контроля целостности всего программного кода • Статический анализ кода на уязвимости • Подтверждение соответствия архитектуры требованиям ИБ

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка	Формирование требований к ОО	Архитектура и проектирование ОО	Реализация (разработка) ОО	Тестирование ОО
• Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями • Обеспечить безопасность сред разработки и эксплуатации • Обеспечить наличие необходимых инструментов	• Определение требований ИБ к ОО • Анализ рисков нарушения ИБ • Требования ИБ • и меры для минимизации рисков • Заключение по ИБ	• Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО • Проверка соответствия требованиям ИБ стороннего ПО • Уточнение и последующий анализ проекта архитектуры и требований по безопасности •Документирование проектных решений по ИБ	• Анализ заимствованных компонент на наличие уязвимостей • Анализ кода, компонентов на соответствие ИБ • Разработка решений по ИБ для ПО • Разработка автоматизированных тестов по безопасности • Обеспечение контроля целостности всего программного кода • Статический анализ кода на уязвимости • Подтверждение соответствия архитектуры требованиям ИБ	• Проверка соответствия ОО требованиям безопасности • Динамическое тестирование защищенности ПО • Проведение авт. тестирования безопасности • Фаззинг-тестирование • Проведение интеграционного тестирования с сервисами СОИБ • Функциональное тестирование ФБО

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка	Формирование требований к ОО	Архитектура и проектирование ОО	Реализация (разработка) ОО	Тестирование ОО	Подготовка и перенос ОО в промышленную эксплуатацию
• Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями • Обеспечить безопасность сред разработки и эксплуатации • Обеспечить наличие необходимых инструментов	• Определение требований ИБ к ОО • Анализ рисков нарушения ИБ • Требования ИБ • и меры для минимизации рисков • Заключение по ИБ	• Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО • Проверка соответствия требованиям ИБ стороннего ПО • Уточнение и последующий анализ проекта архитектуры и требований по безопасности •Документирование проектных решений по ИБ	• Анализ заимствованных компонент на наличие уязвимостей • Анализ кода, компонентов на соответствие ИБ • Разработка решений по ИБ для ПО • Разработка автоматизированных тестов по безопасности • Обеспечение контроля целостности всего программного кода • Статический анализ кода на уязвимости • Подтверждение соответствия архитектуры требованиям ИБ	• Проверка соответствия ОО требованиям безопасности • Динамическое тестирование защищенности ПО • Проведение авт. тестирования безопасности • Фаззинг-тестирование • Проведение интеграционного тестирования с сервисами СОИБ • Функциональное тестирование ФБО	• Проверка соответствия выполнения требований ИБ проектной и эксплуатационной документации • Контроль корректности версий и целостности ПО

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка	Формирование требований к ОО	Архитектура и проектирование ОО	Реализация (разработка) ОО	Тестирование ОО	Подготовка и перенос ОО в промышленную эксплуатацию	Эксплуатация и сопровождение ОО
• Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями • Обеспечить безопасность сред разработки и эксплуатации • Обеспечить наличие необходимых инструментов	• Определение требований ИБ к ОО • Анализ рисков нарушения ИБ • Требования ИБ • и меры для минимизации рисков • Заключение по ИБ	• Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО • Проверка соответствия требованиям ИБ стороннего ПО • Уточнение и последующий анализ проекта архитектуры и требований по безопасности •Документирование проектных решений по ИБ	• Анализ заимствованных компонент на наличие уязвимостей • Анализ кода, компонентов на соответствие ИБ • Разработка решений по ИБ для ПО • Разработка автоматизированных тестов по безопасности • Обеспечение контроля целостности всего программного кода • Статический анализ кода на уязвимости • Подтверждение соответствия архитектуры требованиям ИБ	• Проверка соответствия ОО требованиям безопасности • Динамическое тестирование защищенности ПО • Проведение авт. тестирования безопасности • Фаззинг-тестирование • Проведение интеграционного тестирования с сервисами СОИБ • Функциональное тестирование ФБО	• Проверка соответствия выполнения требований ИБ проектной и эксплуатационной документации • Контроль корректности версий и целостности ПО	• Тестирование на проникновение • Резервное копирование каждого выпуска ПО и всех его компонентов • Мониторинг ПО на наличие уязвимостей • Периодический пересмотр, анализ и тестирование кода ПО для выявления ранее не обнаруженных уязвимостей

ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

Организационная подготовка	Формирование требований к ОО	Архитектура и проектирование ОО	Реализация (разработка) ОО	Тестирование ОО	Подготовка и перенос ОО в промышленную эксплуатацию	Эксплуатация и сопровождение ОО	Вывод из эксплуатации ОО
• Обеспечить наличие ответственных лиц с определенными ролями и соответствующими компетенциями • Обеспечить безопасность сред разработки и эксплуатации • Обеспечить наличие необходимых инструментов	• Определение требований ИБ к ОО • Анализ рисков нарушения ИБ • Требования ИБ • и меры для минимизации рисков • Заключение по ИБ	• Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО • Проверка соответствия требованиям ИБ стороннего ПО • Уточнение и последующий анализ проекта архитектуры и требований по безопасности •Документирование проектных решений по ИБ	• Анализ заимствованных компонент на наличие уязвимостей • Анализ кода, компонентов на соответствие ИБ • Разработка решений по ИБ для ПО • Разработка автоматизированных тестов по безопасности • Обеспечение контроля целостности всего программного кода • Статический анализ кода на уязвимости • Подтверждение соответствия архитектуры требованиям ИБ	• Проверка соответствия ОО требованиям безопасности • Динамическое тестирование защищенности ПО • Проведение авт. тестирования безопасности • Фаззинг-тестирование • Проведение интеграционного тестирования с сервисами СОИБ • Функциональное тестирование ФБО	• Проверка соответствия выполнения требований ИБ проектной и эксплуатационной документации • Контроль корректности версий и целостности ПО	• Тестирование на проникновение • Резервное копирование каждого выпуска ПО и всех его компонентов • Мониторинг ПО на наличие уязвимостей • Периодический пересмотр, анализ и тестирование кода ПО для выявления ранее не обнаруженных уязвимостей	• Архивирование информации, содержащейся в ОО • Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации

НЕОБХОДИМЫЙ ИНСТРУМЕНТАРИЙ И ОРГ. МЕРЫ

Инструменты

Сканеры безопасности:

- SAST;
- DAST;
- SCA;
- Средства сканирования уязвимостей контейнеров и инфраструктуры.

Инфраструктурные сервисы:

- Хранилище артефактов (репозитории);
- GitOps;
- CI/CD;
- Система резервного копирования

НЕОБХОДИМЫЙ ИНСТРУМЕНТАРИЙ И ОРГ. МЕРЫ

Инструменты

Сканеры безопасности:

- SAST;
- DAST;
- SCA;
- Средства сканирования уязвимостей контейнеров и инфраструктуры.

Инфраструктурные сервисы:

- Хранилище артефактов (репозитории);
- GitOps;
- CI/CD;
- Система резервного копирования

Люди (роли)

- ИТ-архитектор;
- Аналитик ИБ (Application Security/AppSec);
- DevOps и QA инженеры;
- Security Champion

НЕОБХОДИМЫЙ ИНСТРУМЕНТАРИЙ И ОРГ. МЕРЫ

Инструменты

Сканеры безопасности:

- SAST;
- DAST;
- SCA;
- Средства сканирования уязвимостей контейнеров и инфраструктуры.

Инфраструктурные сервисы:

- Хранилище артефактов (репозитории);
- GitOps;
- CI/CD;
- Система резервного копирования

Люди (роли)

- ИТ-архитектор;
- Аналитик ИБ (Application Security/AppSec);
- DevOps и QA инженеры;
- Security Champion

Процессы

- Процесс разработки документации интегрирован в разработку;
- Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО;
- Наличие формализованного подхода к управлению конфигурацией;
- Наличие формализованного подхода к тестированию на уязвимости

НЕОБХОДИМЫЙ ИНСТРУМЕНТАРИЙ И ОРГ. МЕРЫ

Инструменты

Сканеры безопасности:

- SAST;
- DAST;
- SCA;
- Средства сканирования уязвимостей контейнеров и инфраструктуры.

Инфраструктурные сервисы:

- Хранилище артефактов (репозитории);
- GitOps;
- CI/CD;
- Система резервного копирования

Люди (роли)

- ИТ-архитектор;
- Аналитик ИБ (Application Security/AppSec);
- DevOps и QA инженеры;
- Security Champion

Процессы

- Процесс разработки документации интегрирован в разработку;
- Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ПО;
- Наличие формализованного подхода к управлению конфигурацией;
- Наличие формализованного подхода к тестированию на уязвимости

Инфраструктура

- Соответствие ГОСТ Р 57580.1-2017 (включая непродуктивные среды)

ПЛЮСЫ И МИНУСЫ АЛЬТЕРНАТИВНОГО ПОДХОДА

ПЛЮСЫ

- Аудиту подвергается не конкретный релиз, а процесс безопасной разработки
- Подходит для современных практик разработки ПО – Agile
- Необходимость проведения повторного аудита, только после существенных изменений в процессе безопасной разработки
- Позволяет существенно повлиять на уровень защищенности ПО через оценку процессов SSDLC

ПЛЮСЫ И МИНУСЫ АЛЬТЕРНАТИВНОГО ПОДХОДА

ПЛЮСЫ

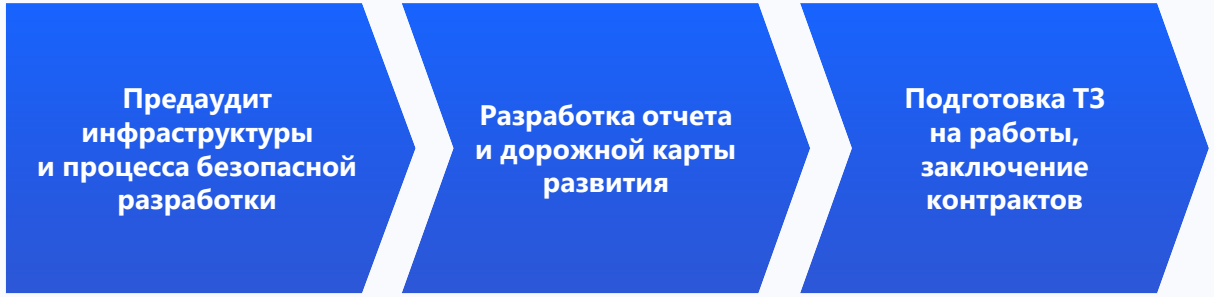
- Аудиту подвергается не конкретный релиз, а процесс безопасной разработки
- Подходит для современных практик разработки ПО – Agile
- Необходимость проведения повторного аудита, только после существенных изменений в процессе безопасной разработки
- Позволяет существенно повлиять на уровень защищенности ПО через оценку процессов SSDLC

МИНУСЫ

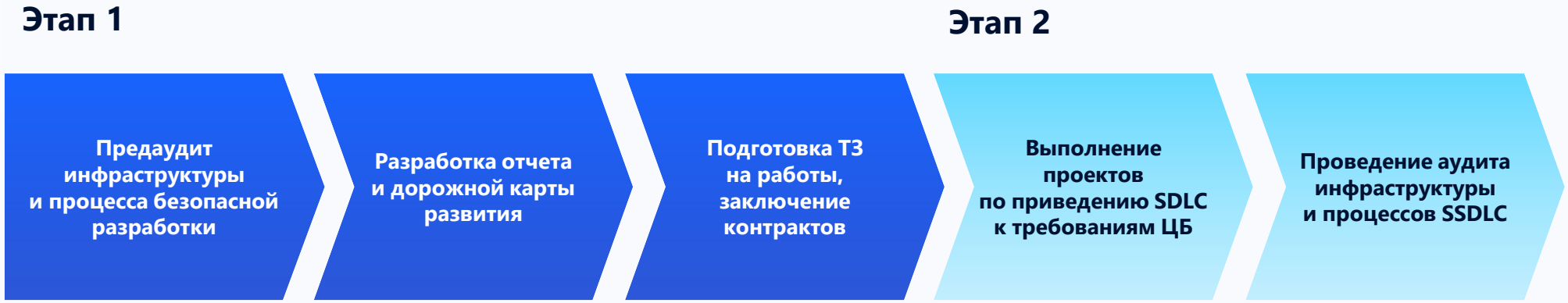
- Необходимость первоначальных инвестиций в безопасную разработку ПО, включая инвестиции на:
  - инструменты,
  - людей,
  - изменение процессов,
  - инфраструктуру.
- Подходит не для всех компаний

ДОРОЖНАЯ КАРТА ПРОЕКТА

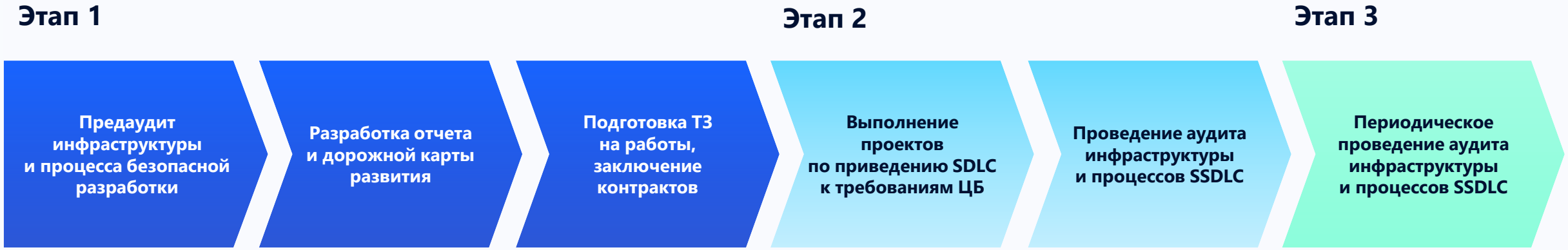
Этап 1



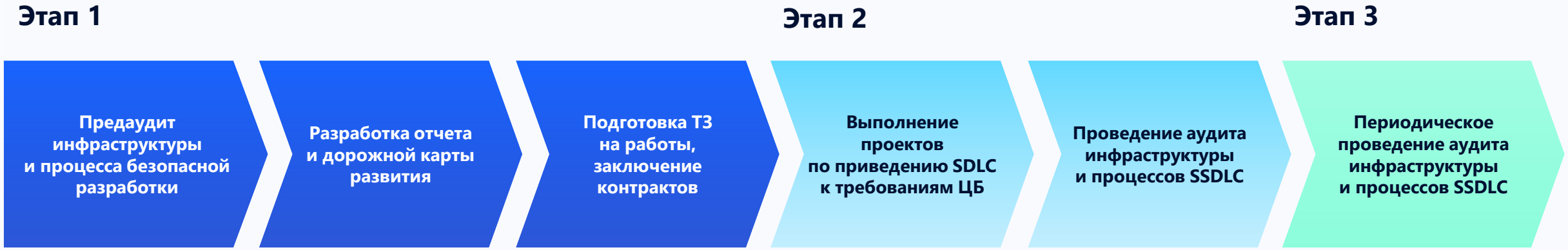
ДОРОЖНАЯ КАРТА ПРОЕКТА



ДОРОЖНАЯ КАРТА ПРОЕКТА



ДОРОЖНАЯ КАРТА ПРОЕКТА



ПО РЕЗУЛЬТАТАМ ПРОЕКТА ЗАКАЗЧИК ПОЛУЧАЕТ:

- Документ о соответствии ПО регуляторным требованиям ЦБ
- Внедрение необходимых контролей ИБ в процесс разработки ПО
- Существенное повышение защищенности ПО

ГЛАВНОЕ УСЛОВИЕ ПЕРЕХОДА НА SSDLC

ГЛАВНОЕ УСЛОВИЕ ПЕРЕХОДА:
ЖЕЛАНИЕ КОМПАНИИ РЕАЛЬНО ПОВЫСИТЬ БЕЗОПАСНОСТЬ ПРОЦЕССА РАЗРАБОТКИ ПО, А НЕ ПРОСТО ПОЛУЧИТЬ БУМАЖКУ О СООТВЕТСТВИИ

INNOVATION distinguishes between a leader and a follower

Steve Jobs 1955-2011 – Business magnate Industrial Designer-Investor

Инфосистемы Джет

СПАСИБО ЗА ВНИМАНИЕ!

Бакин Александр

Руководитель Группы защиты приложений
Центр информационной безопасности
АО «Инфосистемы Джет»

2023