ОЦЕНКА ЗРЕЛОСТИ ПРОЦЕССА БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Сергей Канивец
Ведущий консультант

ДиалогНаука

О ЧЕМ ПОГОВОРИМ

- ✓ Методики оценки зрелости БРПО
- ✓ Концепция стандарта
  - ✓ Основные направления
  - ✓ Структура модулей
- ✓ Что с настройками?
- ✓ Что в итоге?

ДиалОгНаука

МЕТОДИКИ ОЦЕНКИ ЗРЕЛОСТИ БРПО

ДиалогНаука

Методики оценки зрелости

- ✓ OWASP Software Assurance Maturity Model
- ✓ OWASP DevSecOps Maturity Model
- ✓ Synopsys (Microsoft) Building Security In Maturity Model
- ✓ Руководство по оценке БРПО (ФСТЭК России)

КОНЦЕПЦИЯ СТАНДАРТА БЕЗОПАСНОЙ РАЗРАБОТКИ

ДиалогНаука

Основные направления

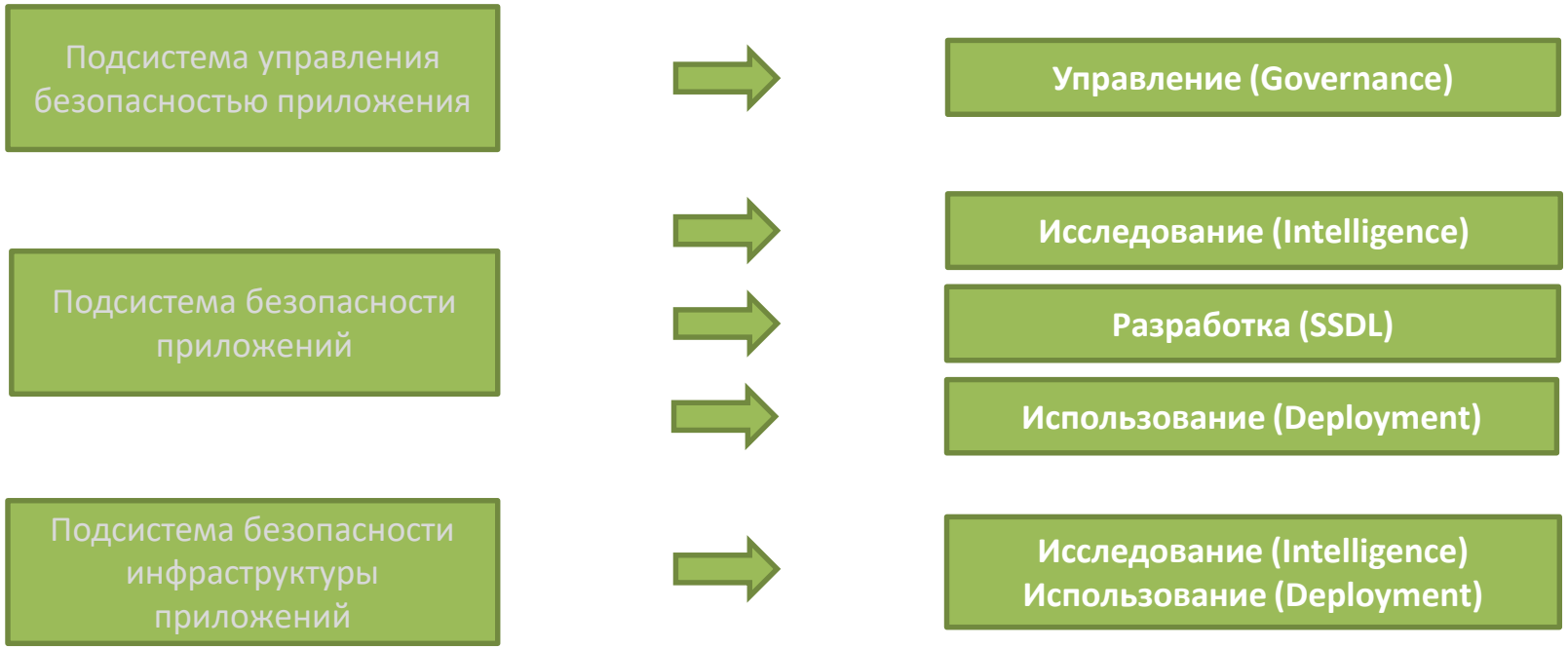
Структура модулей концепции стандарта БРПО

Подсистема управления безопасностью приложения

Подсистема безопасности приложений

Подсистема безопасности инфраструктуры приложений

Структура модулей концепции стандарта БРПО



Структура модулей концепции стандарта БРПО

Подсистема управления безопасностью приложения

Управление (Governance)

- ✓ Стратегия / Планирование процесса разработки
- ✓ Метрики эффективности
- ✓ Повышение осведомленности
- ✓ Контрольные мероприятия
- ✓ Оценка соответствия (в т.ч. требованиям регуляторов)

Состав модулей концепции стандарта БРПО

Подсистема управления безопасностью приложения

Управление (Governance)

- ✓ Стратегия / Планирование процесса разработки
- ✓ Метрики эффективности
- ✓ Повышение осведомленности
- ✓ Контрольные мероприятия
- ✓ Оценка соответствия (в т.ч. требованиям регуляторов)

В части Приказа ФСТЭК России № 239:

- ✓ определение мер обеспечения процесса БРПО
- ✓ документирование и построение процесса БРПО
- ✓ назначение ответственных лиц

В части ПЗ ЦБ:

- ✓ Задача «Формирование требований к ОО»
- ✓ ГОСТ Р 57580.2-2018

Документация

- Руководство по безопасной разработке ПО
  - Периодический анализ текущего состояния, необходимых ресурсов и планов реализации процессов БР
  - Определение области применения БР
- Порядок проведения обучения работников

Подтверждение реализации

- Перечень процессов разработки
- План развития и реализации процессов (Task Management Software)
- План обучения, реестр обучения (кто, какой курс, результат)
- План проведения контрольных мероприятий, отчеты/акты выполнения
- Отчет об оценке соответствия

Состав модулей концепции стандарта БРПО

Подсистема безопасности приложений

Исследование (Intelligence)

- ✓ Подготовка требований безопасности к ПО
- ✓ Моделирование угроз / Оценка рисков
- ✓ Механизмы безопасности и подходы в разработке
- ✓ Соответствие международным стандартам / Best Practice
- ✓ Требования безопасности при использовании зависимостей

Состав модулей концепции стандарта БРПО

Подсистема безопасности приложений

Исследование (Intelligence)

- ✓ Подготовка требований безопасности к ПО
- ✓ Моделирование угроз / Оценка рисков
- ✓ Механизмы безопасности и подходы в разработке
- ✓ Соответствие международным стандартам / Best Practice
- ✓ Требования безопасности при использовании зависимостей

В части Приказа ФСТЭК России № 239:

- ✓ проведение анализа угроз безопасности информации ПО
- ✓ описание структуры ПО

В части ПЗ ЦБ:

- ✓ Задача «Архитектура и проектирование ОО»

Документация

- Процедура управления требованиями безопасности ПО
  - Формализация требований ИБ к ПО
  - Требования к порядку проектирования архитектуры ПО
- Порядок моделирования угроз
  - Порядок пересмотра поверхности атаки
  - Формирование перечня мер по нейтрализации угроз
- Регламент оформления исходного кода и безопасного кодирования
- Регламент использования секретов
- Регламент композиционного анализа
  - Порядок использование компонентов, зависящих от сторонних поставщиков
  - Требования к договорным обязательствам

Подтверждение реализации

- Набор требований безопасности
- Модель угроз
- Перечень мер по нейтрализации угроз
- Описание поверхности атаки
- Перечень зависимостей ПО
- Результаты анализа компонентов и применения корректирующих воздействий

Состав модулей концепции стандарта БРПО

Подсистема безопасности приложений

Разработка (SSDL)

- ✓ Проектирование / Анализ архитектуры
- ✓ Управление конфигурацией ПО
- ✓ Анализ кода
- ✓ Тестирование защищенности

Состав модулей концепции стандарта БРПО

Подсистема безопасности приложений

- ✓ Проектирование / Анализ архитектуры
- ✓ Управление конфигурацией ПО
- ✓ Анализ кода
- ✓ Тестирование защищенности

В части Приказа ФСТЭК России № 239:

- ✓ статический анализ кода
- ✓ фаззинг-тестирование
- ✓ динамический анализ кода

В части ПЗ ЦБ:

- ✓ Задача «Архитектура и проектирование ОО»
- ✓ Задача «Реализация (разработка) ОО»
- ✓ Задача «Тестирование ОО»

Разработка (SSDL)

Документация

- Регламент управления конфигурацией ПО.
- Регламент управления недостатками ПО
- Регламент управления запросами на изменение ПО
- Регламент проведения экспертизы исходного кода ПО
- Регламент проведения статического анализа исходного кода ПО
- Регламент проведения динамического анализа кода ПО (в т.ч. фазинг-тестирование)
- Регламент функционального тестирования
- Регламент нефункционального тестирования

Подтверждение реализации

- Свидетельства регистрации запросов на изменение ПО (в т.ч. в рамках управления конфигурацией ПО) и управления недостатками ПО
- Описание архитектуры ПО
- Формализованные результаты экспертизы исходного кода ПО
- Перечень инструментов статического, динамического анализа
- План функционального тестирования и отчеты по результатам
- Описание объекта нефункционального тестирования
- Отчеты по результатам статического, динамического анализа, функционального и нефункционального тестирования

Состав модулей концепции стандарта БРПО

Подсистема безопасности приложений

Использование (Deployment)

- ✓ Подготовка ввода ПО в эксплуатацию / Доставка ПО
- ✓ Эксплуатация ПО
- ✓ Тестирование на проникновение
- ✓ Управление уязвимостями
- ✓ Вывод из эксплуатации ПО

Состав модулей концепции стандарта БРПО

Подсистема безопасности приложений

- ✓ Подготовка ввода ПО в эксплуатацию / Доставка ПО
- ✓ Эксплуатация ПО
- ✓ Тестирование на проникновение
- ✓ Управление уязвимостями
- ✓ Вывод из эксплуатации ПО

В части Приказа ФСТЭК России № 239:

- ✓ отслеживание и исправление обнаруженных ошибок
- ✓ информирование пользователя (об уязвимостях, об обновлении и порядке их получения и контроля целостности, об окончании поддержки)

В части ПЗ ЦБ:

- ✓ Задача «Подготовка и перенос ОО в промышленную эксплуатацию»
- ✓ Задача «Эксплуатация и сопровождение ОО»
- ✓ Задача «Вывод из эксплуатации ОО»

Использование (Deployment)

Документация

- Регламент приемки ПО
  - Регламент обеспечения целостности ПО при передаче
  - Порядок безопасной доставки ПО пользователям
- Порядок обеспечения поддержки ПО
  - Порядок разработки документации для технической поддержки
  - Порядок работы службы технической поддержки
  - Порядок оповещения пользователей о выпуске обновлений
  - Порядок информирования пользователей ПО о выявленных уязвимостях
- Регламент реагирования на информацию об уязвимостях
- Регламент поиска ошибок и уязвимостей в ПО при его эксплуатации
- Регламент вывода ПО из эксплуатации

Подтверждение реализации

- Результаты анализа влияния на безопасность ПО неустраненных ошибок
- Свидетельства учета информации о дистрибутивах и документации ПО
- Документация технической поддержки
- Отчеты по результатам тестирования на проникновение
- Свидетельства учета запросов пользователей об ошибках и информации о потенциальных уязвимостях и результатах их анализа
- Отчеты об исправлении найденных ошибок
- Свидетельства вывода ПО из эксплуатации

Состав модулей концепции стандарта БРПО

Подсистема безопасности инфраструктуры приложений

Исследование (Intelligence)
Использование (Deployment)

- ✓ Требования к безопасности системы сборки ПО
- ✓ Безопасность инфраструктуры среды разработки, тестирования, продуктовой
- ✓ Обеспечение целостности кода
- ✓ Эксплуатация инфраструктуры приложения

Состав модулей концепции стандарта БРПО

Подсистема безопасности инфраструктуры приложений

Исследование (Intelligence)
Использование (Deployment)

- ✓ Требования к безопасности системы сборки ПО
- ✓ Безопасность инфраструктуры среды разработки, тестирования, продуктовой
- ✓ Обеспечение целостности кода
- ✓ Эксплуатация инфраструктуры приложения

В части Приказа ФСТЭК России № 239:

- ✓ меры защиты информации в зависимости от категории значимости

В части ПЗ ЦБ:

- ✓ ГОСТ Р 57580.1-2017 (в соответствии с требованием к уровню защиты информации)

Документация

- Регламент безопасной сборки ПО
- Регламент обеспечения безопасности сборочной среды
- Политика доступа к исходному коду ПО и обеспечения его целостности
- ВНД в соответствии с ГОСТ Р 57580.1-2017 (ПЗИ, РЗИ, КЗИ, СЗИ)

Подтверждение реализации

- Схема и описание сборочной среды
- Описание ролевой модели доступа к сборочной среде
- Журналы событий процессов сборки
- Журнал аудита сборки ПО (для определения места хранения, контрольных сумм файлов исходного кода, повторяемости сборок ПО и пр.)
- Описание модели управления доступом к исходному коду ПО
- Отчет о соответствии требованиям ГОСТ Р 57580.1-2017 (в соответствии с ГОСТ Р 57580.2-2018)

А что с настройками?

Стандарты конфигурирования

- ✓ Checkpoint, Cisco ASA/Firepower/IOS/ISE/Nexus, F5 BIG IP, Fortigate, Palo Alto, Juniper, Huawei, Mikrotik
- ✓ RHEL 7/8, CentOS 7/8, OEL 7/8, SUSE 15, Ubuntu 20, Debian 9/10, FreeBSD 12, Solaris 11, Windows Server 2016, Windows 10, Astra Linux 1.7, Alt Linux, Ред ОС сервер 7.x
- ✓ VMWare ESXi 6.7/7.0, KVM, Oracle VM
- ✓ Docker, Kubernetes
- ✓ Apache HTTP Server, Apache Tomcat, Nginx
- ✓ СУБД Oracle, Microsoft SQL Server, MySQL, PosgtreSQL, MongoDB, MariaDB,
- ✓ Graphite
- ✓ Clickhouse
- ✓ Airflow
- ✓ JupyterHub
- ✓ OpenSearch
- ✓ Apache Geode
- ✓ Keycloak
- ✓ Grafana
- ✓ WildFly
- ✓ Tarantool Enterprise
- ✓ kafka
- ✓ zookeeper
- ✓ Hashicorp vault
- ✓ Arenadata Streaming (Kafka Manager, Kafka SQL, NiFi, KafkaRestProxy), Arenadata Platform Security (Solr, Knox, Ranger), Arenadata Cluster Manager
- ✓ Arenadata Enterprise Tools, Arenadata Command Center, Arenadata Hadoop (Hive, YARN, HBASE, Poenix, Tez, Zeppelin Atlas, Spark, Flink)
- ✓ Arenadata DB, Arenadata QuickMarts
- ✓ Node.Js
- ✓ BI Intellect
- ✓ Polymatica Analitics
- ✓ HAproxy
- ✓ JVMHotspot
- ✓ JavaSEDevelopmentKit (OpenJDK)
- ✓ ETCD
- ✓ Redis

Что в итоге?


Подсистема управления безопасностью приложения
Подсистема безопасности приложений
Подсистема безопасности инфраструктуры приложений

Спасибо за внимание

?