

«Опасная разработка. Дорожная карта движения к катастрофе»

Практика внедрения в организациях цикла безопасной разработки программного обеспечения



ЗАО «Перспективный мониторинг»


Качалин Алексей

Зам. Генерального директора

О наших работах по теме

- Инструментальный анализ ПО и ИС
- С 2012 года – работаем по направлению повышения безопасности разработки
- Принимаем участие в работе ГК с регуляторами
 - ФСТЭК: требования к СЗИ и ИБ платформ, база угроз, безопасная разработка
 - ФСБ: СОПКА

Безопасная разработка: этапы осознания проблем

-  Мониторинг и реагирование
- Проверка и выпуск продукта
- Разработка
- Проектирование
- Требования
- Подготовка команды
- Внедрение цикла безопасной разработки

Шаг 1. Такая безопасность не нужна



2010 год. Эксперт по ИБ/соответствию требованиям:
«... работы по инструментальному анализу не будут
востребованы, нет таких требований у регуляторов»

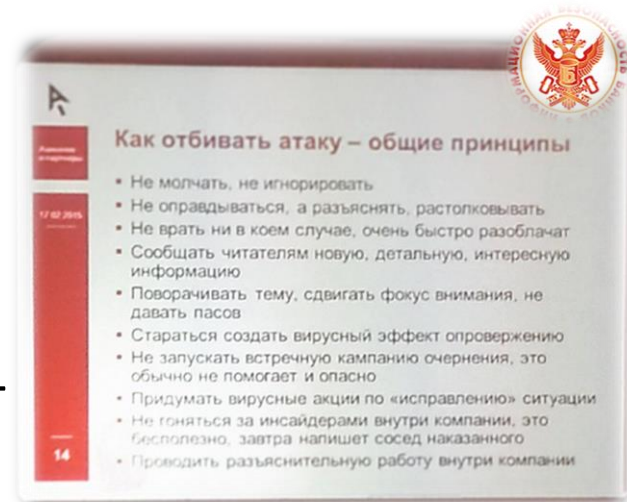
- ФСТЭК: о безопасной разработке
- «Банки будут стремиться оптимизировать расходы, а самый оптимальный способ – вывести операции в Интернет»
- «Анализ безопасности ПО - одно из немногих за что в кризис банки будут готовы платить»



Февраль 2015. Конференция ИБ Банков

Безопасность разработки - требование рынка

- Уязвимости и инциденты ИБ
 - Репутация невозможно контролировать раскрытие информации
 - Раскрытие информации об уязвимостях используемых компонентов
 - Обращения к регулятору с вопросами от пользователей
- Необходимость реакции
 - Взаимодействие с «атакующим» сообществом
- Требования НПА и регуляторов
- Требования 3-их лиц по гарантиям ИБ



Шаг 2. Соответствие как самоцель



«При выполнении работ должны применяться практики безопасной разработки программного обеспечения»

Из ТЗ

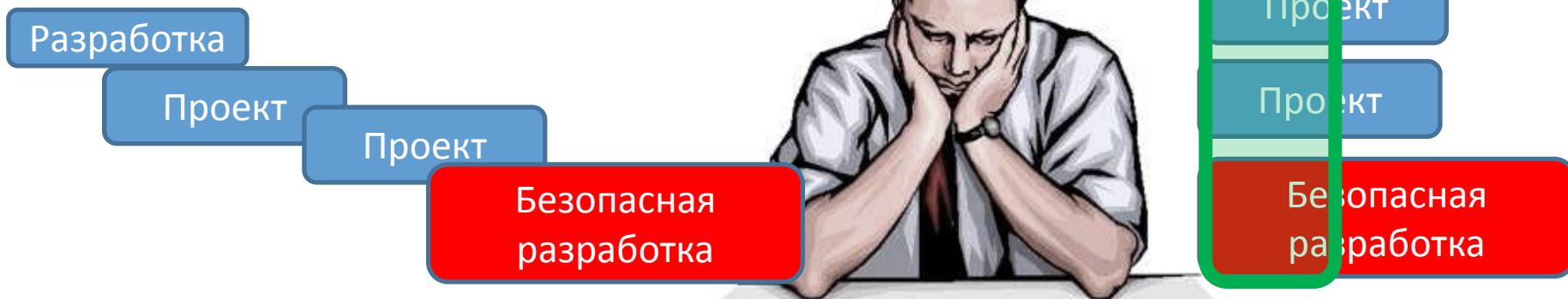
Подтверждение соответствия ПО

Как устроена разработка

- Водопад – не модно?
- Итеративные и гибкие методики

В худшем случае – после разработки

- Внутренние требования организации
- Требования регуляторов отрасли (БР, PCI DSS)
- Требования гос.регуляторов



Шаг 3. ИБ будет протестировано

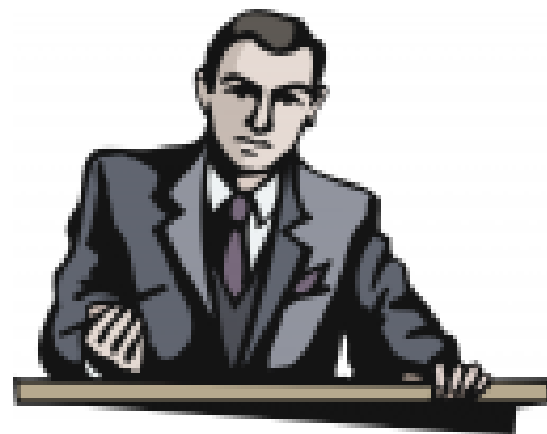


«... в случае возникновения проблем у внедряемого сервиса мы обратимся за анализом уязвимостей»

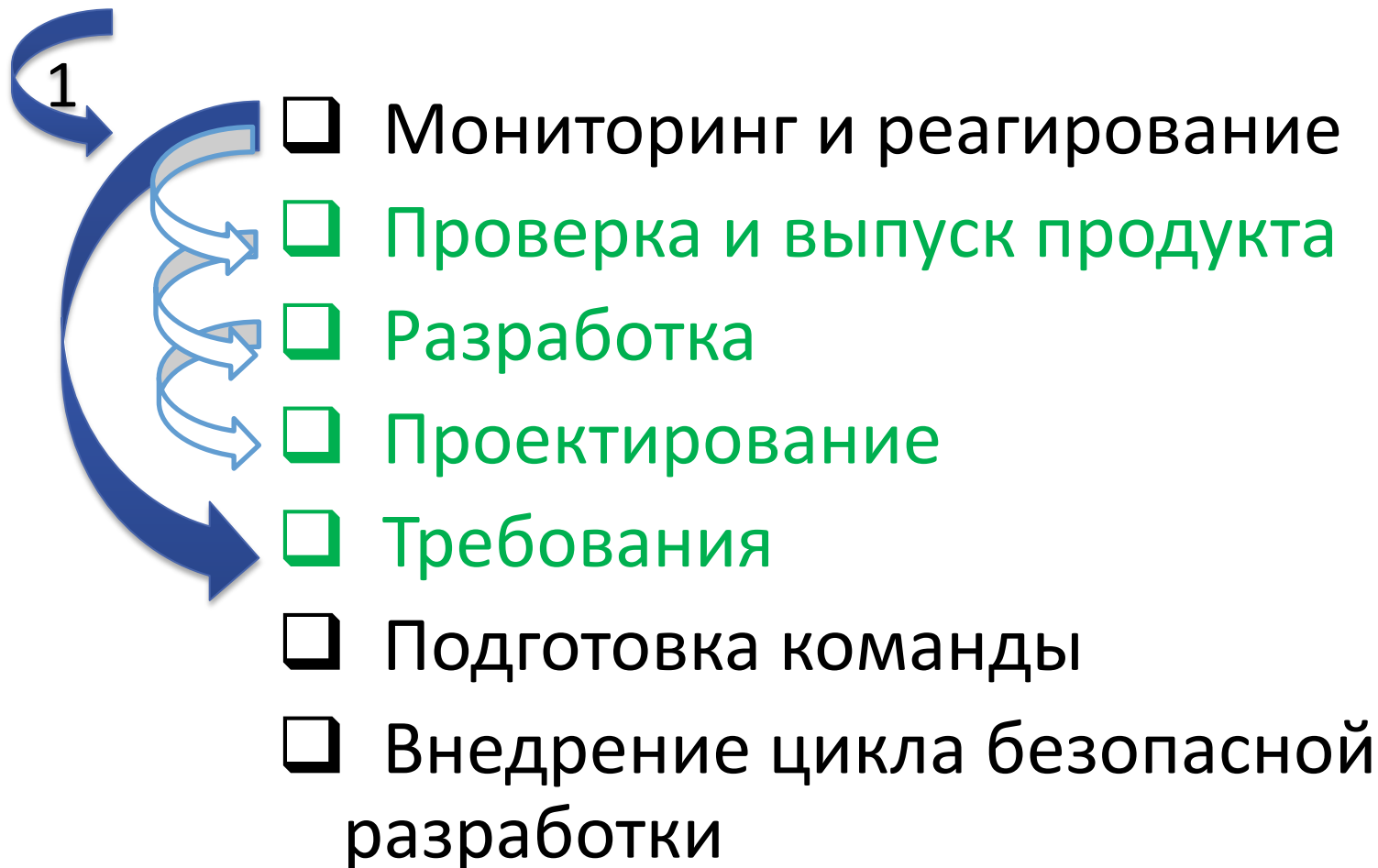
Руководитель службы эксплуатации сервиса в первом проекте

«...мы хотим сделать новый сервис, представляющий следующие возможности:..., насколько это безопасно?»

Он же, несколько проектов спустя



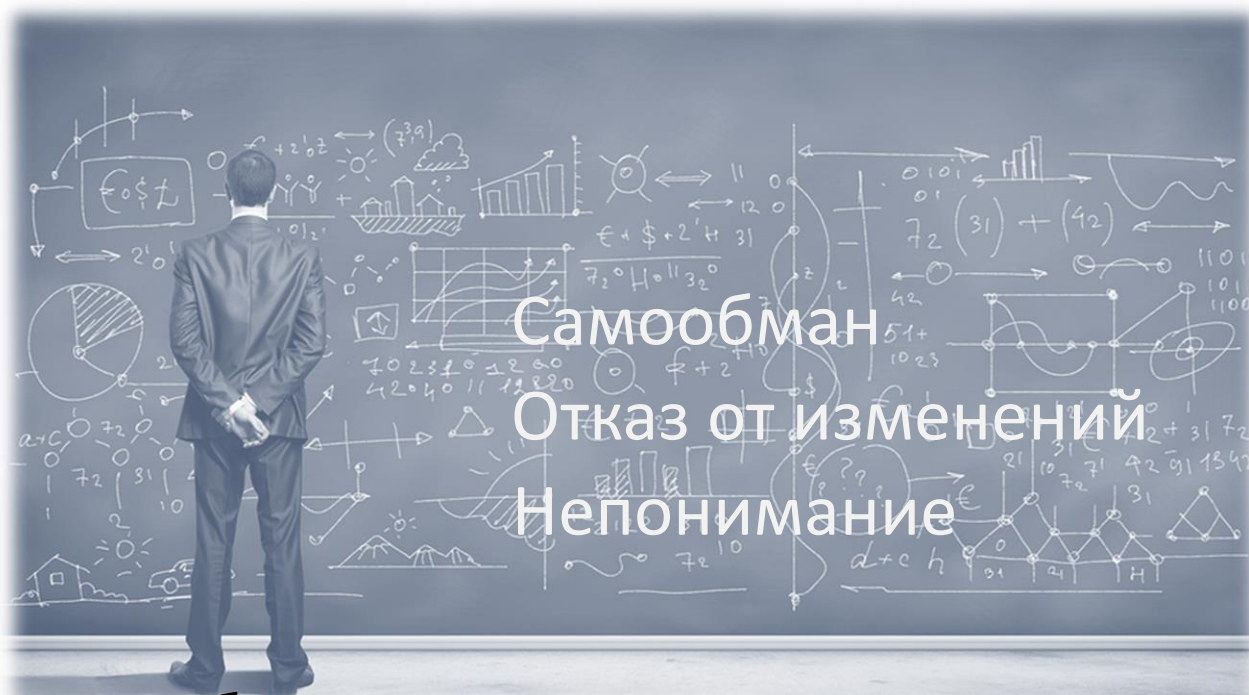
Эволюция требует повторений



Эффект от внедрения безопасной разработки

- Осязаемые результаты: **отдача** от инвестиций
 - ~~Возврат инвестиций~~
 - ПО финансовых, подверженных фроду систем – возможно
 - Снижение количества инцидентов
 - Оперативность реагирования на инциденты
- **Встраивание** в существующий процесс разработки (заказа и эксплуатации ПО)
- Часто применение к **имеющимся** продуктам или компонентам
 - Вам продают «задел по теме», свой или чужой
- Вовлечение **команды** (мотивация исполнителя и легитимизация затрат) на дополнительные практики ИБ

Шаг 4. Какая-то безопасность разработки



«Мы себя проверили – у нас **многое** есть.

Программисты что-то такое делают. Не надо ничего менять»

В ответ на предложение развивать практики

Не так уж и сложно соответствовать SDL

	Basic	Standardized (Activities are expert led)	Advanced (Activities are led by central security team)	Dynamic (Activities are co-ordinated by product teams and a central security team)
Training, Policy Organization Capabilities	+ Setting baseline and goals for SDL	+ Executive support + Enterprise coverage SDL pilot projects +/- Training: Basic +/- Basic security	+ Executive support: Explicit coverage: New, project +/- Training: Common baseline +/- Security team exists	- Executive support: SDL mandated and enforced - Enterprise coverage: All project with meaningful risk +/- Training: Custom training - SDL is adopted to the development methodology
Requirement Design	Undefined or inconsistent	- Risk assessment	- Requirements for	- Threat models: dynamically created by group
Implementation	Undefined or inconsistent			- Product-specific tools development organization
Verification	Undefined or inconsistent	- File fuzzing - Basic Web application scanning + Penetration testing by third party as appropriate	+ Intensive fuzzing + Application scanning + Model based verification	- In-house development and customization tools to: + Detect vulnerabilities - Audit compliance with SDL
Release Response	Undefined or inconsistent	- Final Security Review internal and external compliance + Project archiving + Response: Basic	+ Plan in place, tracking cause and effect	- Real-time incident tracking - Advanced root-cause analysis and formal feedback into policy

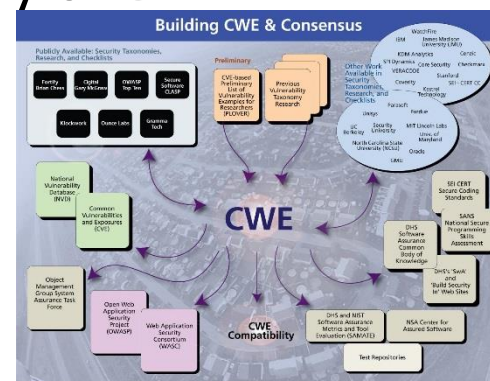
Ловушки инструментов и практик “as is”

- Выбор инструментов и компонентов
 - Удобство среды разработки
 - Использование знакомых компонентов
 - Борьба с унаследованным кодом
- «Безопасное программирование» == ИБ?
 - Утечки памяти, переполнение буфера, падения/повисания
 - Безопасные опции компилятора
- Инструменты безопасности при разработке
 - Анализаторы кода
 - Генераторы нагрузки без тонкой настройки
 - Системы автоматизированного тестирования
- Практики управления
 - Менеджер форсирует: бюджет, сроки, функционал
 - Унаследованный долг: было 500 предупреждений, будет 507 – ок?

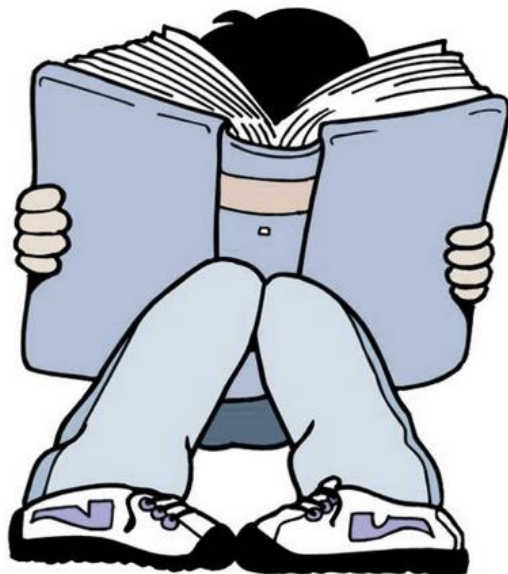


Кстати о говоря – о границах понимания

- «Уязвимость» – все говорят, скоро зафиксируют в НПА
- Различные этапы проявления уязвимостей
 - Уязвимости эксплуатации
 - Уязвимости, вносимые на этапе формирования требований
- CVE vs CWE - Уязвимость vs Слабость
 - Необходимость логичной замкнутой системы определений и понятий
- Корректность «атакующей» терминологии
 - «Василий провёл с своего компьютера DDoS»
 - Пользователи устроили DDoS сервиса
 - В вашем ПО – эксплоит



Шаг 5. Строим безопасную разработку по учебнику

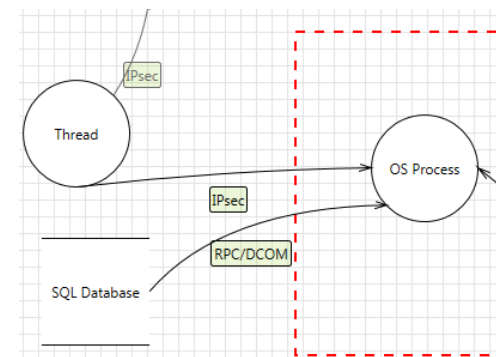


«Я не читаю курсы по SDL»

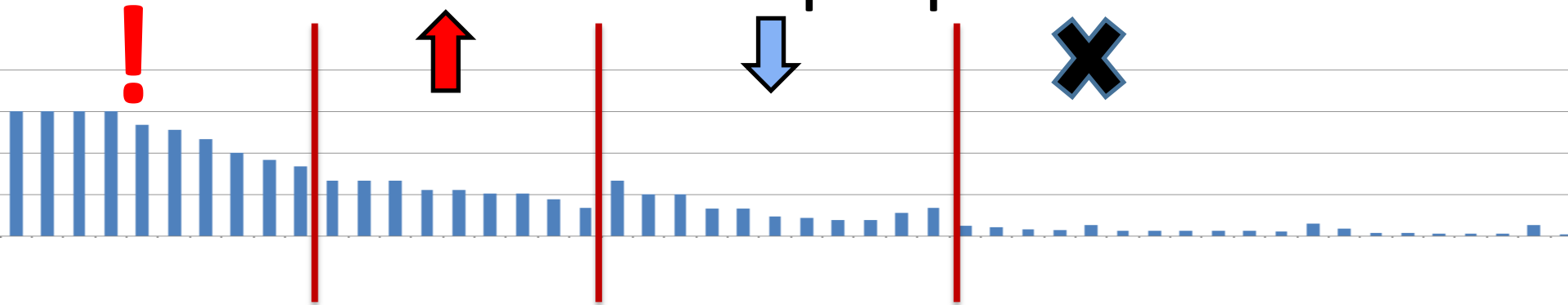
Алексей Лукацкий, кладезь по ИБ

Что можно почерпнуть из практик MSDL, CSDL, ...

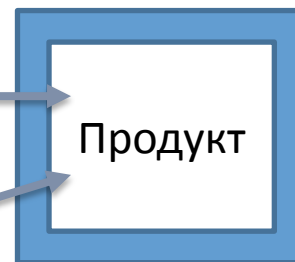
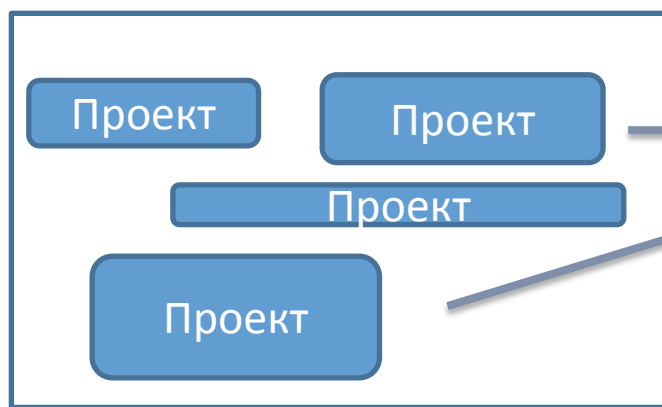
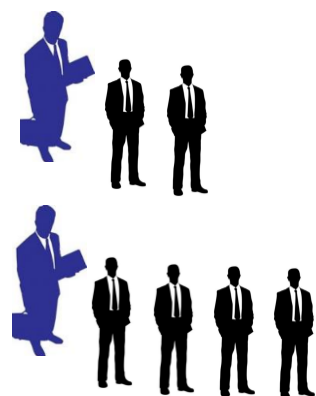
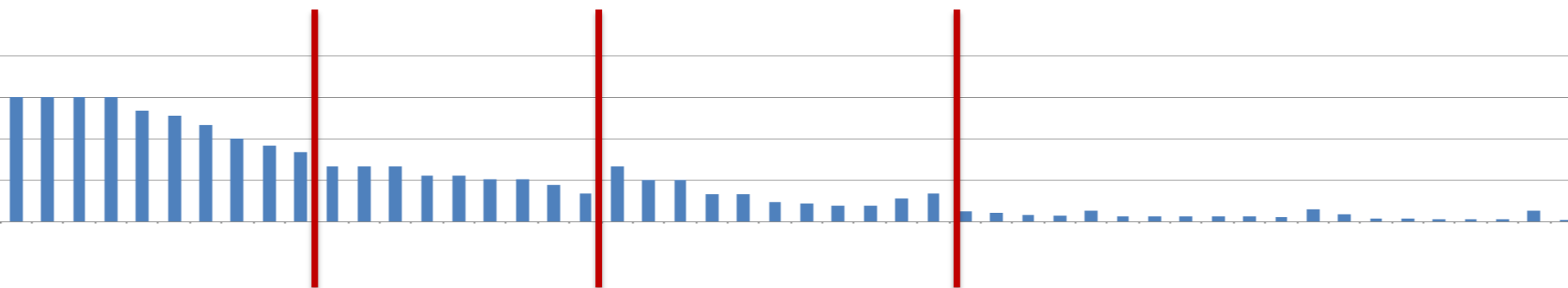
- Модель зрелости *должна быть*
 - Подходящая этапность внедрения?
- Домены
 - Можно суммировать и расширить
- Готовые методы, инструменты, классификации
 - Моделирование угроз, трассировка уязвимостей для оценки ущерба



Стратегия внедрения безопасной разработки



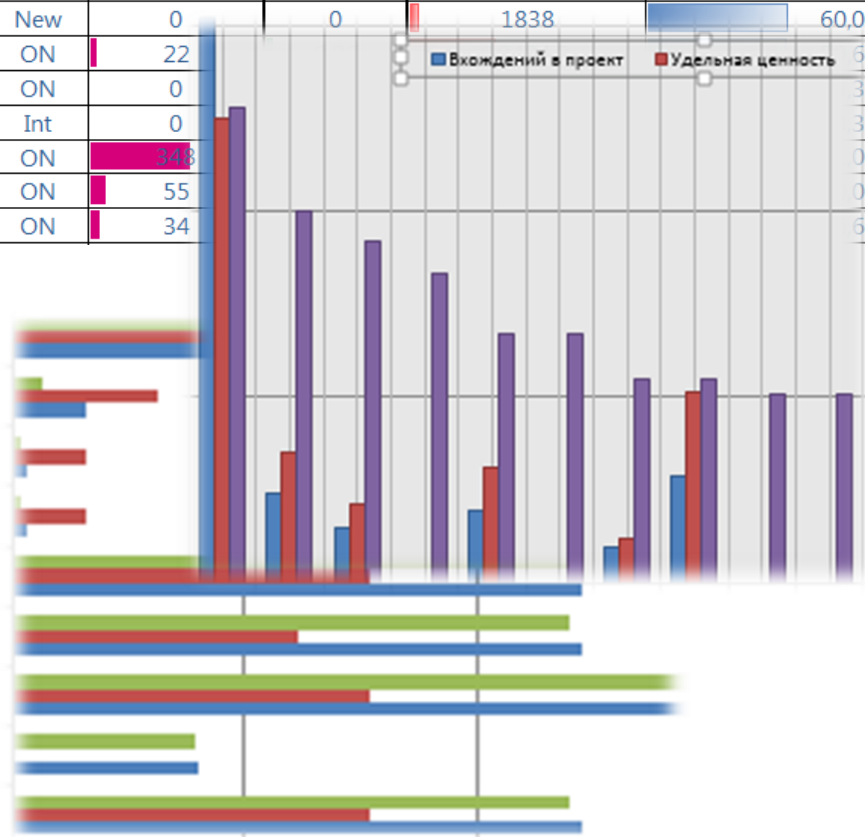
Стратегия внедрения безопасной разработки



Пример одного анализа

- Продуктовый менеджмент
 - Интенсивность разработки
- Бизнес: база внедрений, перспективы продаж
- Разработка:
 - технологические тренды, тех.долг и архитектура
- Установка и сопровождение
 - «Агрессивность среды»
 - Инциденты

Продукт	Статус	Вхождений в проект	Удельная ценность	Статистика трудозатрат	Экспертная усредненная ценность
	ON	248	0,44	22213,4	60,0
	ON	27	0,06	2812,3	60,0
	ON	131	0,32	2271	60,0
	New	0	0	1838	60,0
	ON	22			
	ON	0			
	Int	0			
	ON	348			
	ON	55			
	ON	34			



Шаг 6. Если решать - то все проблемы



«Если нельзя полностью гарантировать доверие начиная от аппаратной базы, ... - то нет смысла вообще заниматься вопросами безопасности»

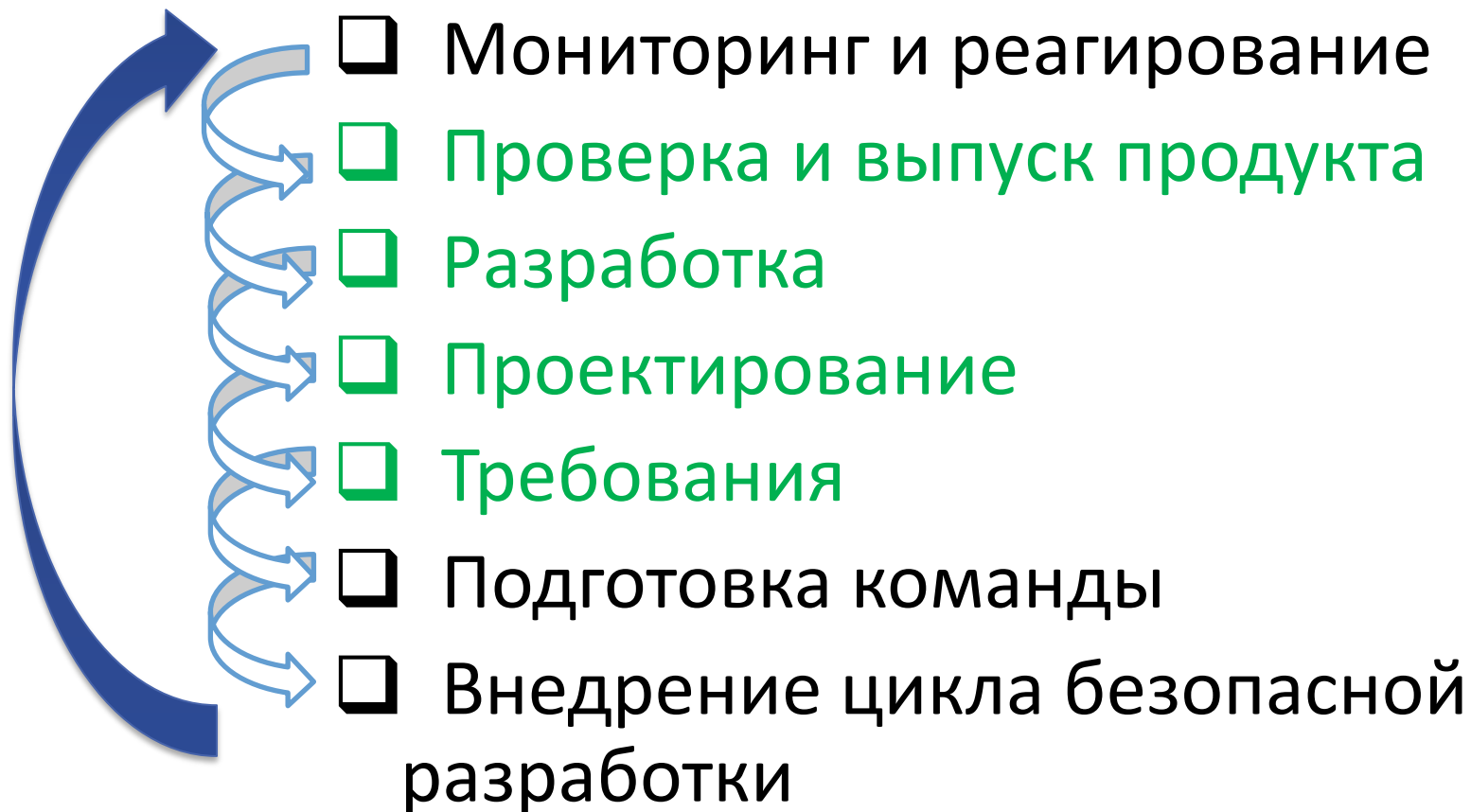
Анализ

Решить проблему нельзя принять риски

- «Крупноузловая» сборка
 - Фреймворки и библиотеки
- Инструменты разработчика
 - Инструменты проектирования
 - Инструменты разработки
 - Инструменты хранения и сборки
- Инфраструктура ПО
 - Магазины мобильных приложений и хранения данных



Внедрение безопасной разработки даёт ценную информацию к размышлению



Развитие мониторинга и реагирования

- Обнаружить публикацию информации об уязвимости
 - Публикация уязвимости в используемом компоненте
 - Публикация информации об уязвимости в Интернет
 - Сети обмена информацией об уязвимостях
 - Технический анализ (состояние узлов, трафик, журналы)
- Интерпретировать **обращения пользователей**
 - Сообщения о «странном поведении программы» (нет явного подозрения на проблемы ИБ)
 - Попытки шантажа и ультиматумы, оскорбления и троллинг
 - Готовый метод компрометации ИБ (пошаговый, в виде PoCE)
 - ...
- Внутренние сообщение от разработчика – **обратить внимание**
 - Указания на строчку кода
 - Развёрнутый анализ с обоснованием неизбежности уязвимости

Итого

- Разрозненные практики ИБ часто **расходы на иллюзию безопасности** – должна быть поставлена цель
 - Синергия безопасной разработки и соответствия требованиям
 - Стратегический план реалистичный по ресурсам и времени
- Очень многое зависит от **автоматизации и инструментов** – но они не панацея
 - Инструменты определяют отдельные сценарии – целостность?
 - Риск автоматизации хаоса
- Реагирование дороже предотвращения
- «Бесплатно» получится плохо
 - Корректировка бюджетов и границ проектов
 - Безопасность – в «системе ценностей» менеджмента
 - Внутренняя команда внедрения



ХУДШАЯ ИЗ УГРОЗ - НЕВЕДЕНИЕ

- ✓ Инструментальный анализ ПО и ИС
- ✓ Внедрение практик безопасной разработки
- ✓ Мониторинг ИБ



Качалин Алексей

kachalin@advancedmonitoring.ru