Успешные практики

обеспечения безопасности разработки в рамках автоматизации управления
жизненным циклом разработки ПО

LOGROCON
SOFTWARE ENGINEERING

О компании Logrocon

О нас

Клиенты:
ТОП-10 банков России,
Телеком ТОП-5,
Производители ПО

90+
сотрудников

6 лет в деле

3 офиса:
Москва,
Санкт-Петербург,
Калуга

250+
проектов

Мы гордимся

Наши достижения

Gold
Microsoft Partner
DevOps
Microsoft

LOGROCON
SOFTWARE ENGINEERING

Повышение эффективности процессов разработки ПО

DevOps (CI/CD, IAC)

Аудит и оптимизация процессов разработки ПО

Консалтинг

Внедрение ALM решений

Регламентация процессов

Разработка индикаторов качества / эффективности ALM процессов (PI/KPI). Формирование мотивационных схем

LOGROCON
SOFTWARE ENGINEERING

О чем эта презентация

Как гибкие подходы к разработке могут помочь обеспечению информационной безопасности

- Потребность в обеспечении информационной безопасности в разработке
- Почему традиционные подходы не работают
- Ключевые противоречия из-за разных предпосылок
- Использование гибких подходов и ALM к обеспечению ИБ
- Интеграция требований ИБ и контролей ИБ в автоматизированный процесс разработки ПО (ALM-систему)
- Контроль за изменениями исходных кодов
- Повышение управляемости процессов обеспечения ИБ за счет ALM-системы
- Сила обратной связи
- Примеры

LOGROCON
SOFTWARE ENGINEERING

Контекст

«По итогам 2018 года ущерб российской экономике может составить 1,1 триллиона рублей.
Ущерб мировой экономике может достигнуть около 1,5 триллиона»
Заместитель председателя Сбербанка Станислав Кузнецов

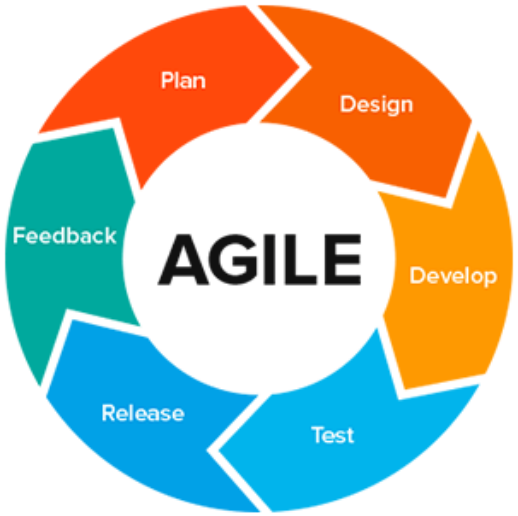
https://www.securitylab.ru/news/494280.php

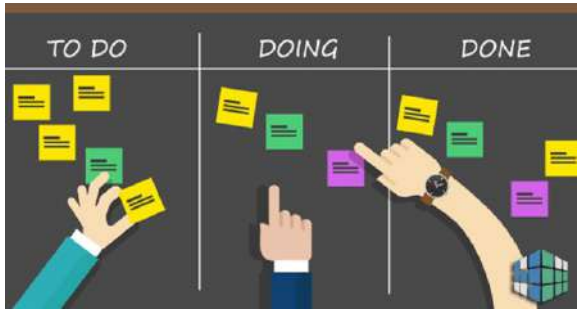
«В первом полугодии текущего года в РФ было зарегистрировано 80 127 преступлений, совершенных при помощи компьютерных и телекоммуникационных технологий. Это в два раза больше, чем за аналогичный период прошлого года (39 993).»

https://rg.ru/2018/09/05/kolichestvo-kiberprestuplenij-v-rf-vyroslo-vdvoe.html

LOGROCON
SOFTWARE ENGINEERING

Современная разработка





Явно выраженная тенденция к **ускорению поставки ПО** путем конвейерного подхода и деления задачи на небольшие партии

LOGROCON
SOFTWARE ENGINEERING

Проблемы обеспечения безопасности обостряются

- Сроки выпуска спринта крайне сжатые – нет времени на задачи информационной безопасности
- Не выбираем задачи обеспечения безопасности из бэклога - нам нужно быстрее нарастить функциональность и начать приносить прибыль
- Подразделение информационной безопасности блокирует выпуск версий – давайте найдем обходные пути
- Требования ТБ – прошлый век, и вообще не могут быть обеспечены в нашем проекте.

LOGROCON
SOFTWARE ENGINEERING

Конфликт разработчики-безопасники

LOGROCON
SOFTWARE ENGINEERING

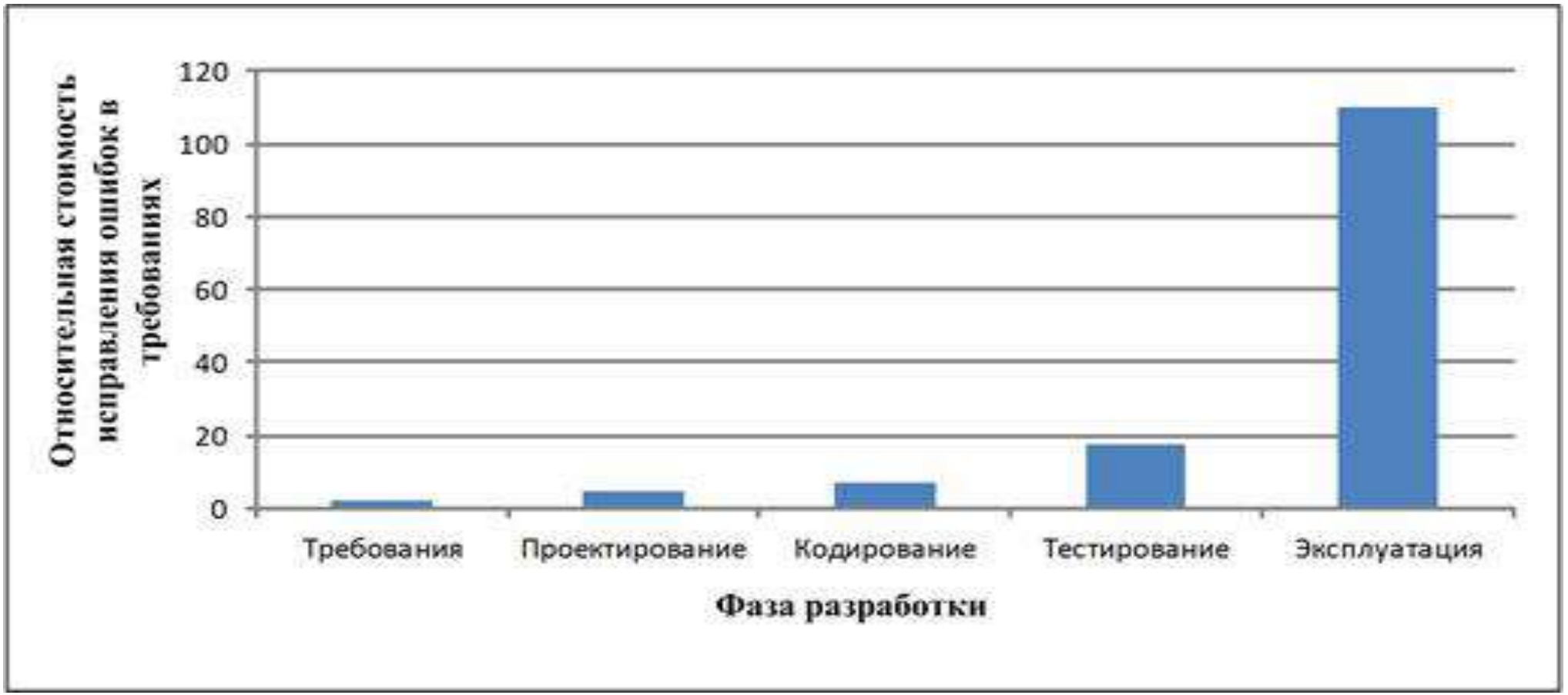
Отторжение в команде разработки

- Политика запретов – приводит к тому, что разработчики рассматривают требования ИБ как препятствие, мешающее проекту
- Неадаптивные требования – применение нормативных требований, которые невыполнимы или противоречат функциональным требованиям
- Длительные проверки проекта/кода на безопасность
- Отсутствие делегирования ответственности за обеспечение информационной безопасности

LOGROCON
SOFTWARE ENGINEERING

Причина в исходных посылках

Исправлять ошибки после выпуска в 30 раз дороже, чем на стадии проектирования



LOGROCON
SOFTWARE ENGINEERING

Причина в исходных посылках

Современные итерационные методы разработки нацелены на постоянное внесение изменений и снижение стоимости внесения таких изменений

LOGROCON
SOFTWARE ENGINEERING

Разработчики чувствуют себя беспомощными

LOGROCON
SOFTWARE ENGINEERING

Повышение гибкости обеспечения ИБ

- Итеративная разработка, гибкие методики и DevOps – не преходящее увлечение, а тенденция, обусловленная требования бизнеса
- Соответственно, обеспечение ИБ также должно стать гибким и итеративным, обеспечивать обратную связь для последующих итераций
- С учетом конвейеризации и повышения скорости поставки ПО, контроль безопасности может быть только автоматизированным

LOGROCON
SOFTWARE ENGINEERING

Повышение гибкости обеспечения ИБ

Разработка

- Должна брать на себя ответственность за обеспечение ИБ
- Учитывать обратную связь от проверок ИБ
- Предлагать свои решения по обеспечению требований ИБ

Информационная безопасность

- Должна адаптировать требования к новым решениям
- Должна предлагать варианты контроля ИБ
- Принимать решения по обеспечению ИБ от разработки, если они решают свои задачи

LOGROCON
SOFTWARE ENGINEERING

Помощь и защита

LOGROCON
SOFTWARE ENGINEERING

Согласование процессов

- Процесс обеспечения информационной безопасности должен подстроиться под более современный и гибкий процесс DevOps

- Необходимо потратить усилия, чтобы разработчики осознали задачи обеспечения ИБ как повышение качества кода и «приняли вызов»

LOGROCON
SOFTWARE ENGINEERING

Гибкие требования

Традиционно

- Стандартный фиксированный набор требований ИБ
- Требования прорабатываются подразделением ИБ
- Требования ИБ обсуждению не подлежат

Гибко

- Требования ИБ прорабатываются с разработчиками, чтобы получить минимально необходимый набор
- Прорабатываются средства автоматизации контроля требований ИБ
- Требования формулируются в виде пользовательстких историй, как и функциональные требования

LOGROCON
SOFTWARE ENGINEERING

Гибкие требования

Традиционно

- Построение частой модели угроз в виде документа
- Оценка рисков по стандартной методике
- Команда разработчиков к оценке угроз и рисков не привлекается

Гибко

- Безопасность должна стать неотъемлемой частью мышления разработчиков, так же как и качество кода
- Разработчики вовлекаются в оценку рисков и являются их основными оценщиками
- Модель угроз в виде «антиисторий» входит в требования к системе

LOGROCON
SOFTWARE ENGINEERING

Гибкие требования

Традиционно

- Проверка кода вручную или автоматизированно вне процесса разработки ПО
- Отчеты об анализе кода подлежат прочтению и проработке разработчиками

Гибко

- Проверки кода максимально автоматизированы
- Все проверки кода, даже ручные, должны завершаться внесением результатов в виде действий в ALM-систему
- Разработчики, по мере возможности, освобождаются от чтения и анализа отчетов

LOGROCON
SOFTWARE ENGINEERING

Гибкие требования

Традиционно

- Планы реагирования на инциденты не затрагивают процесс разработки ПО
- Сведения об обнаруженных попытках атак рассматриваются как конфиденциальные

Гибко

- Планы реагирования на инциденты должны включать обратную связь с процессом разработки
- Сведения об обнаруженных попытках атак рассматриваются как «антиистории» и подлежат обработке группой разработки

LOGROCON
SOFTWARE ENGINEERING

Примеры

LOGROCON
SOFTWARE ENGINEERING

Контроль кода с обратной связью

- Решение реализовано в Банке, входящем в ТОП-10
- Код, предназначенный к выпуску в релиз, проверяется инструментом (в данном случае - Fortify Static Code Analyzer)
  в рамках автоматизированного релизного конвейера
- Отчет автоматически анализируется. В случае нахождения критичных уязвимостей, выпуск релиза останавливается
- Обратная связь – найденные уязвимости регистрируются в ALM-системе как баги, обнаруженные в данном релизе
- Подход может применять для любых сканеров кода или сходных инструментов

LOGROCON
SOFTWARE ENGINEERING

Тест на уязвимость с обратной связью

- Решение реализовано в известной Oil&Gas компании
- В рамках регламентов, выполняется регулярное (ежегодное) тестирование на уязвимость инструментом MaxPatrol в режиме PenTest
- Отчет автоматизированно анализируется. Замечания и рекомендации регистрируются в системе ServiceDesk как проблемы, с разными приоритетами (в зависимости от критичности)

LOGROCON
SOFTWARE ENGINEERING

Контроль изменений исходных кодов

- Решение реализовано в крупной Oil&Gas компании
- Обязательное привязывание коммитов в Git к задачам из ALM
- Контроль изменений службо й безопасности в коде перед переносом в основную ветвь
- Автоматизированная проверка кода на безопасность является частью автоматизированного тестирования и формирует баги к исправлению

LOGROCON
SOFTWARE ENGINEERING

СПАСИБО ЗА ВНИМАНИЕ

Сергей Белолипецкий
Директор по консалтингу

sbelolipetskiy@logrocon.com
+7 903 724 0649

+7 (495) 777-00-84
info@logrocon.ru
www.logrocon.ru
Москва, Барабанный переулок, д. 3