



КОД БЕЗОПАСНОСТИ



Выполнение требований по уровням доверия при производстве средств защиты информации

Андрей Голов, 12.02.2020



Это бессмысленно!

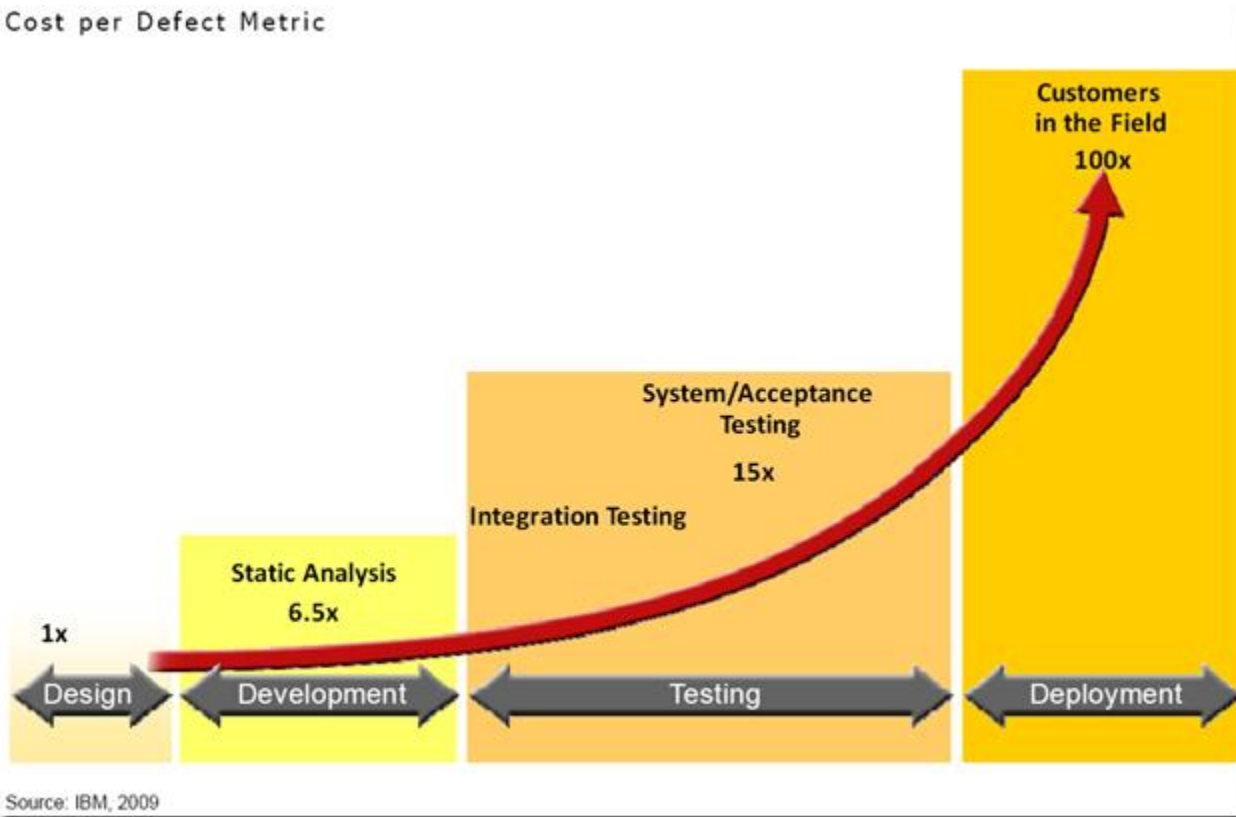
Это долго!

Это дорого!



Как растет стоимость бага на различных этапах жизненного цикла ПО

Cost per Defect Metric



Две редакции:

- Защита конфиденциальной информации
- Защита государственной тайны

Сертифицирован ФСТЭК по пяти направлениям:

- СЗИ от НСД
- Антивирус
- Межсетевой экран
- Система контроля съемных носителей
- Система обнаружения вторжений





Требования	Профили
• 4-й уровень отсутствия НДВ • 5-й класс защищенности для СВТ • 4-й класс защиты для МЭ тип «В» • 4-й класс защиты СКН • 4-й класс защиты САВЗ типов «А», «Б», «В», «Г» • 4-й класс защиты СОВ	7 профилей защиты: • 7 наборов функциональных требований • 7 наборов требований доверия



Задерживает
выход на рынок



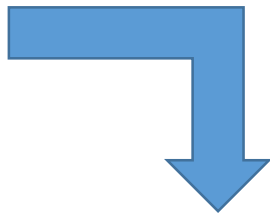
Повышает нагрузку
при сертификации



Косвенно влияет
на сертификацию
остальных
продуктов



Требования	Профили
4-й уровень отсутствия НДВ 5-й класс защищенности для СВТ 4-й класс защиты для МЭ тип «В» 4-й класс защиты СКН 4-й класс защиты САВЗ типов «А», «Б», «В», «Г» 4-й класс защиты СОВ	7 профилей защиты: 7 наборов функциональных требований 7 наборов требований доверия



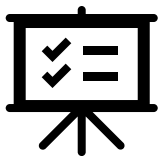
Оптимизация за
счет объединения
требований

Требования	Профили
5-й класс защищенности для СВТ 4-й класс защиты для МЭ тип «В» 4-й класс защиты СКН 4-й класс защиты САВЗ типов «А», «Б», «В», «Г» 4-й класс защиты СОВ 4-й класс УД	7 наборов функциональных требований 1 набор требований доверия



КОД БЕЗОПАСНОСТИ

Ключевые этапы цикла безопасной разработки



Подготовка



Разработка



Поддержка



Ключевые компоненты КБ SDL

Подготовка

Компетентные
сотрудники

Безопасная
инфраструктура

Разработка

Управление
требованиями

Ответственное
проектирование

Безопасная
реализация

Независимая
верификация ИБ

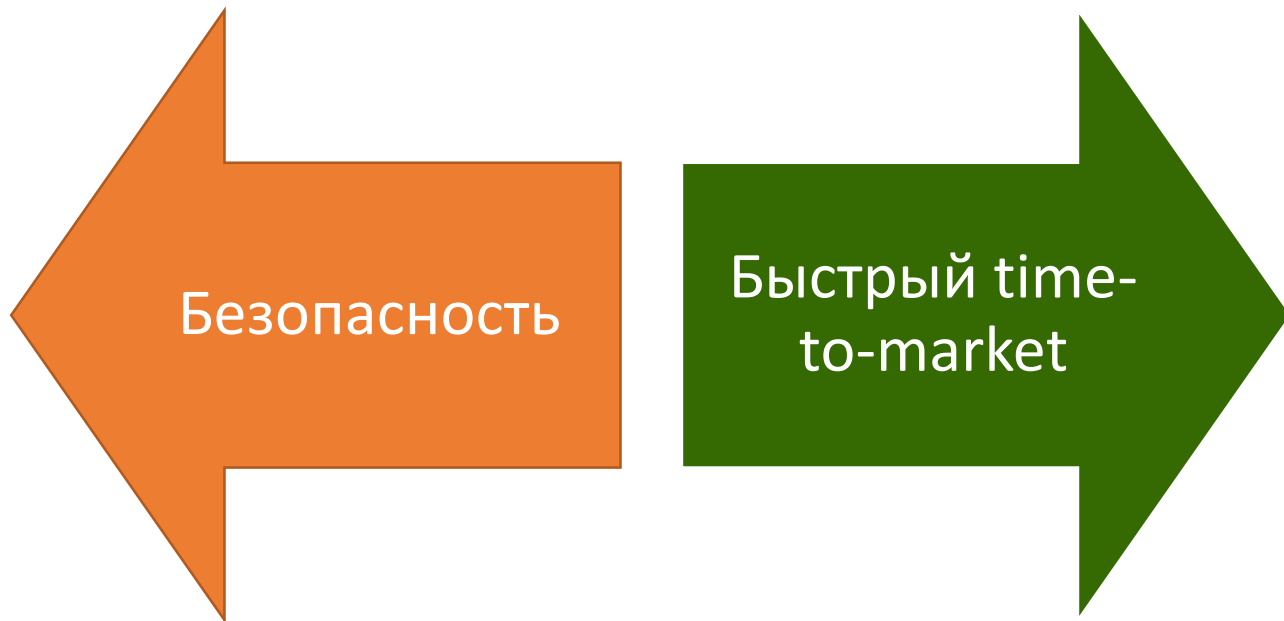
Поддержка

Поддержка

Устранение
уязвимостей



Парадокс разработчика СЗИ



Решение:

- Вывод ответственных за безопасность людей за пределы продуктовой команды
- Анализ архитектуры с точки зрения безопасности

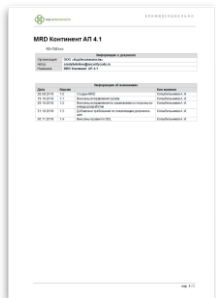


- Трекинг требований и задач – Team Foundation server
- Защищенное хранение кода
- Процедуры Code review
- Автоматизированный статический анализ кода
- Continuous Integration
- Автоматизированное Unit тестирование
- Функциональное тестирование
(ручное и автоматизированное)





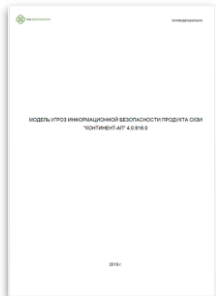
Анализ и декомпозиция



MRD



Архитектура



Модель УИБ Тех. требования



Требования и задачи



Team Foundation Server





Иерархическая структура

- версия
- требования
- функции
- задачи

Задачи

- исполнитель
- статус
- история

Скриншот интерфейса системы SNES (Система Непрерывного Элементарного Следования) для отслеживания безопасности реализации. Визуализация иерархической структуры задач (Epics, Features, Backlog Items).

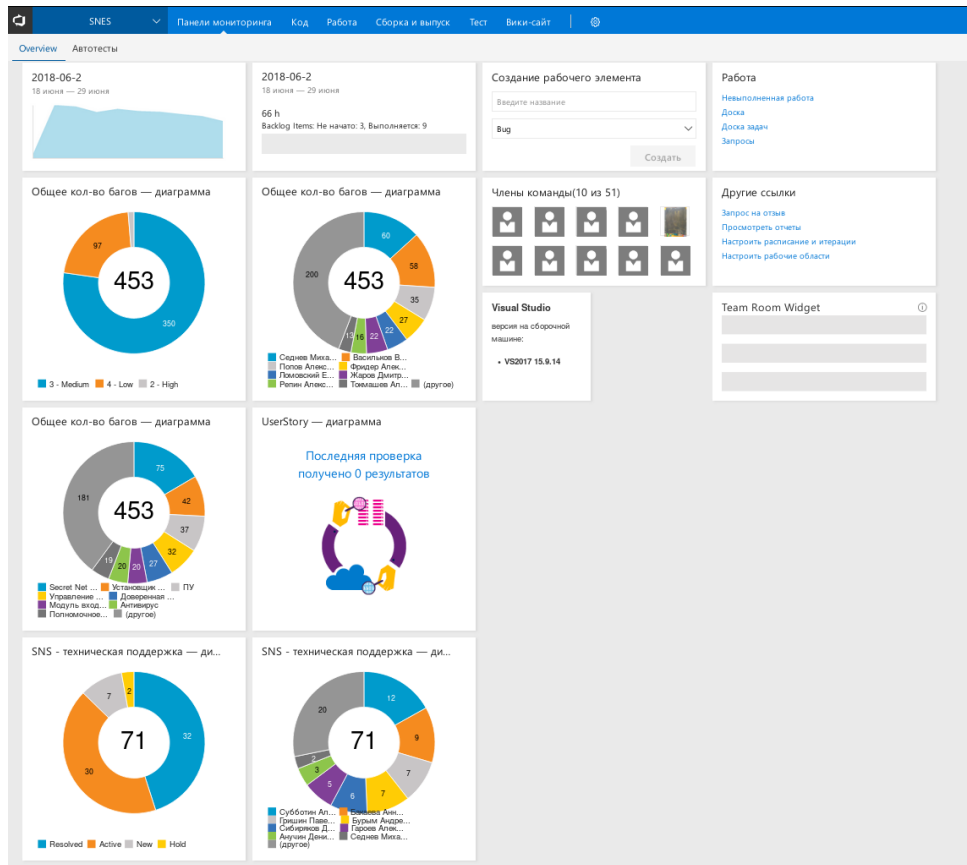
Видимая часть интерфейса:

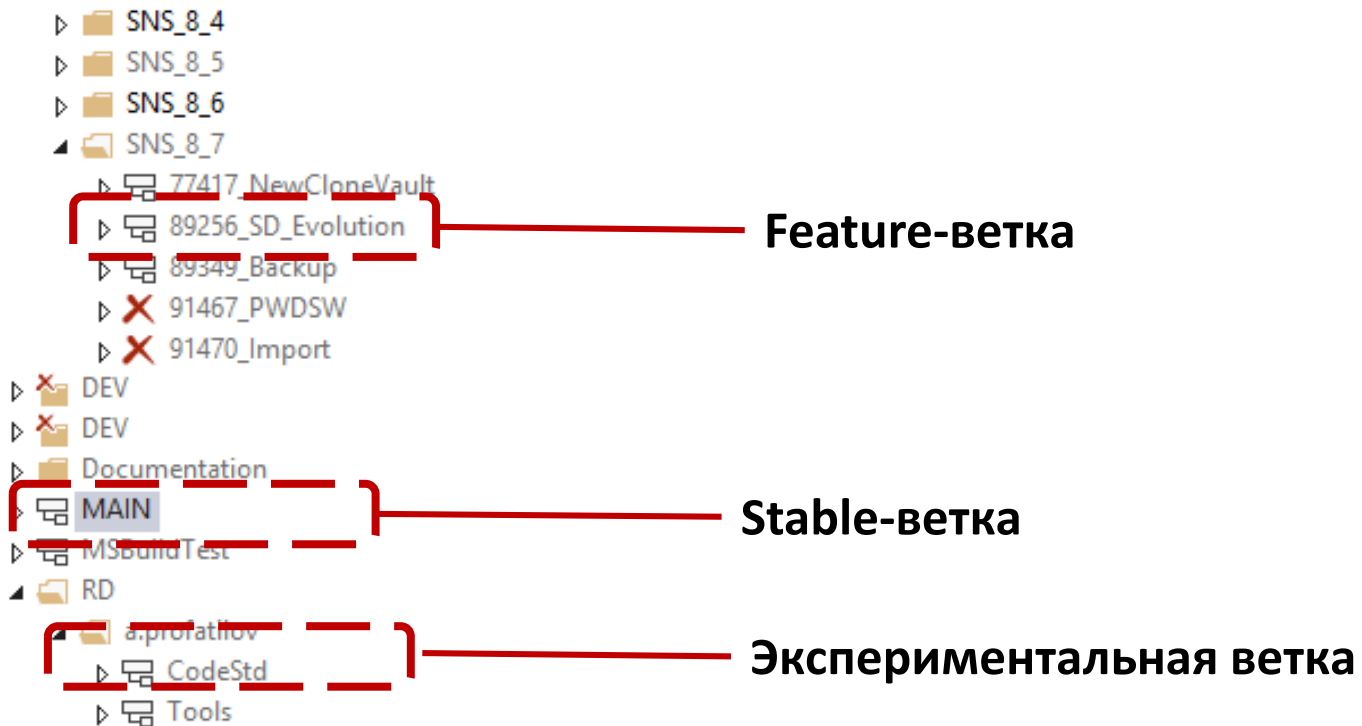
- Верхняя панель: SNES, Панели мониторинга, Код, Работа, Сборка и выпуск, Тест, Вики-сайт.
- Левая панель: Невыполненная работа, Запросы, Contributions Graph.
- Список элементов: Epics, Features, Backlog Items.
- Фильтры: Прошлые, Текущий (2018-06-2).
- Таблица данных:

Поря...	Work Item Type	Title	State	Effort	Busin...	Value Area
1	Epic	SNS 8.6	Active			Business
+	Feature	1. Функциональные требования	Active			Container
	Feature	1.1. Базовая защита	Active			Container
	Feature	1.2. Локальная защита	Active			Container
	Feature	1.3. Межсетевой экран	Resolved			Container
	Feature	1.4. Система обнаружения вторжений	Development			Container
	Feature	1.5. Антивирус	Development			Container
	Feature	1.6. Централизованное управление	Active			Container
	Feature	1.7. Развертывание	Active			Container
	Feature	2. Требования к криптографии	Active			Business
	Feature	3. Нефункциональные требования	Active			Container
	Feature	4. Требования к пользовательскому интерфейсу	Active			Business
	Feature	5. Требования к совместимости	Active			Container
	Feature	6. Системные требования	Development			Container
	Feature	7. Требования к производительности и масштабируемости	Active			Business
	Feature	8. Требования к локализации продукта	Active			Business



Контроль всех параметров
процесса разработки практически
в реальном времени

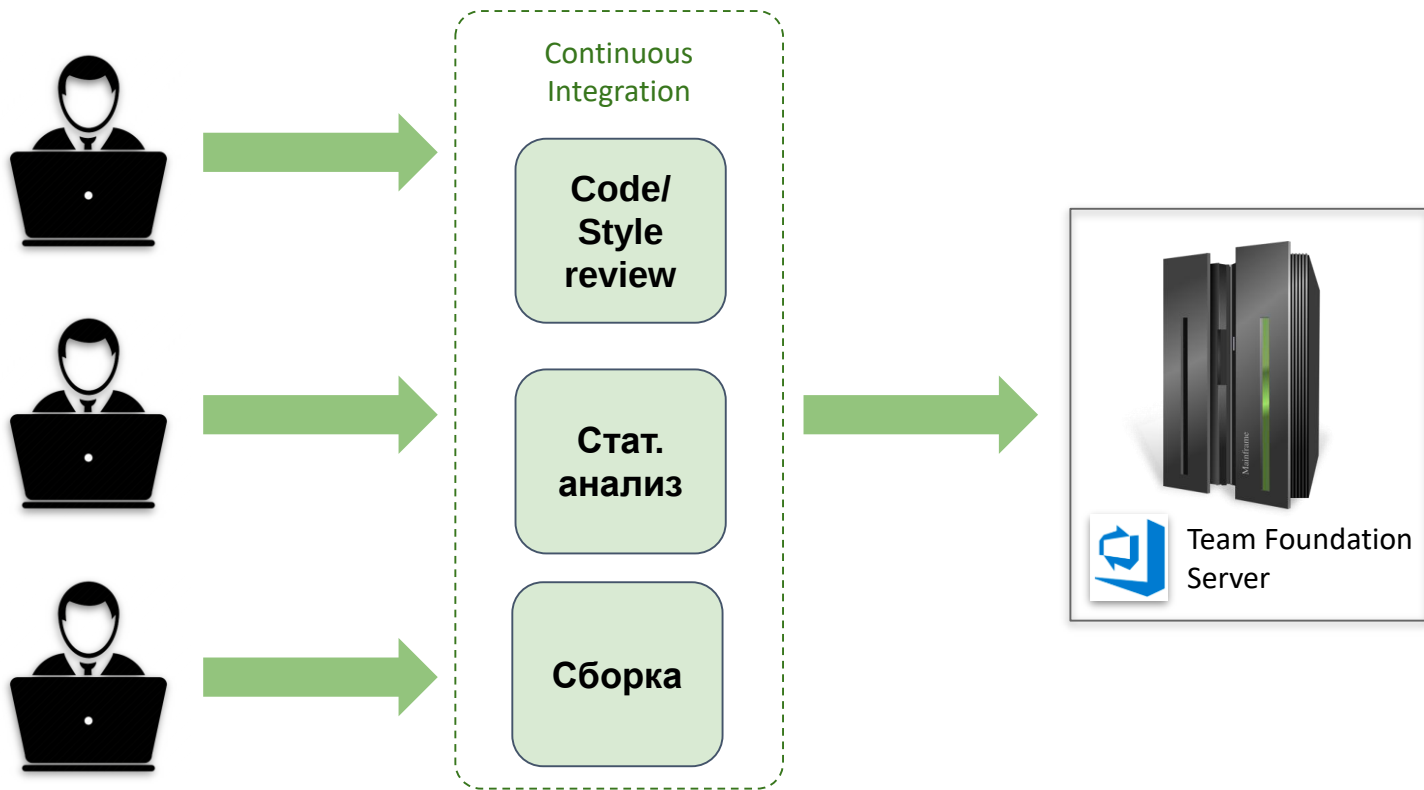






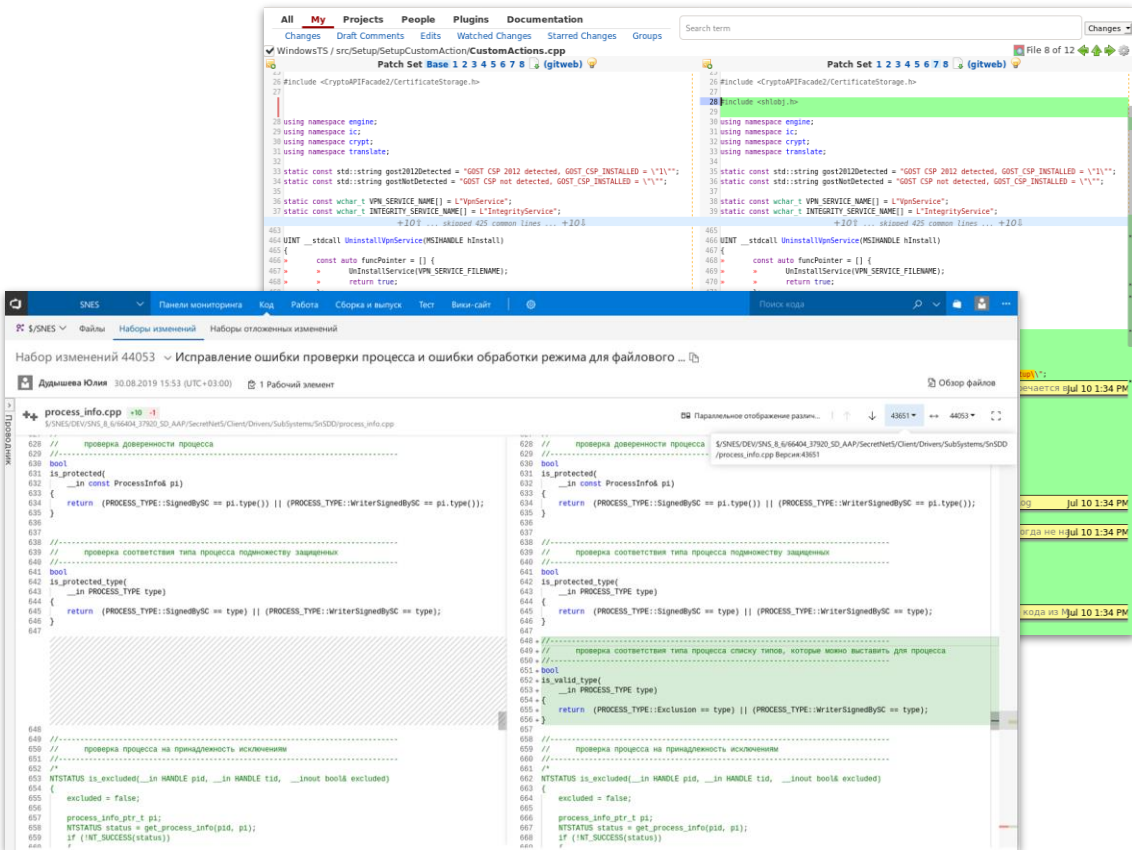
КОД БЕЗОПАСНОСТИ

Безопасная реализация – хранение кода



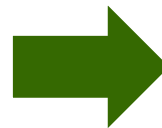
Любой код проверяет как минимум 2 специалиста:

- Поиск ошибок
- Поиск потенциально опасных конструкций
- Документирование
- Искключение НДВ
- Знакомство с кодом
- Обучение





- Единый анализатор для продуктов под Гостайну и «Конфиденциалку»
- Низкое число ложных срабатываний
- Выполняется на каждом этапе сборки от компьютера разработчика до финальной сборки релиз-кандидата



Svace





Анализ и разработка
ПМИ



Экспериментальные
исследования



Формирование
отчета с
рекомендациями



Анализ и разработка ПМИ

Идентифицируется
потенциальная
“поверхность” атаки

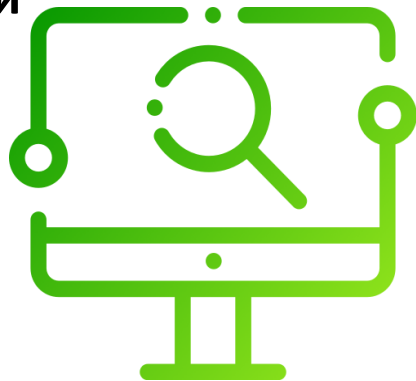
Разрабатываются
специализированные
инструменты

Разрабатывается
программа и
методики испытаний

**Команда специалистов опирается, но “не доверяет”
исходным данным в заявке**



- Задача непростая, но решаемая
- Тестируем доступные пользователю интерфейсы
- Тест считается выполненным если **на 1 тысячу** наборов входных данных через **100 тысяч итераций** перестает расти покрытие кода **в течение 3-4 часов**
 - Фаззер перебрал большинство возможных комбинаций





КОД БЕЗОПАСНОСТИ

Тестирование на проникновение

- Является неотъемлемой частью разработки
- Проводится компанией-партнером
- Эмуляция атаки на стенд с объектом испытаний (Black box)
- Ручная работа + специализированные средства



БЕЗОПАСНЫЕ
ПРОГРАММНЫЕ
РЕШЕНИЯ



Retina



w3af





Как это влияет на бизнес?

+20% ко времени
вывода продукта на
рынок

Можно сократить до
+10%

+5 сотрудников в
штат без учета
команды пентестеров



- Внедрить процедуры связанные с уровнями доверия в крупном разработчике – возможно
- Эффект окупает все затраты
- Улучшенное качество продукта помогает на международном рынке
- Можно реализовать российскими продуктами

Спасибо за внимание!

Андрей Голов
A.Golov@securitycode.ru



КОД БЕЗОПАСНОСТИ

info@securitycode.ru
<http://securitycode.ru>