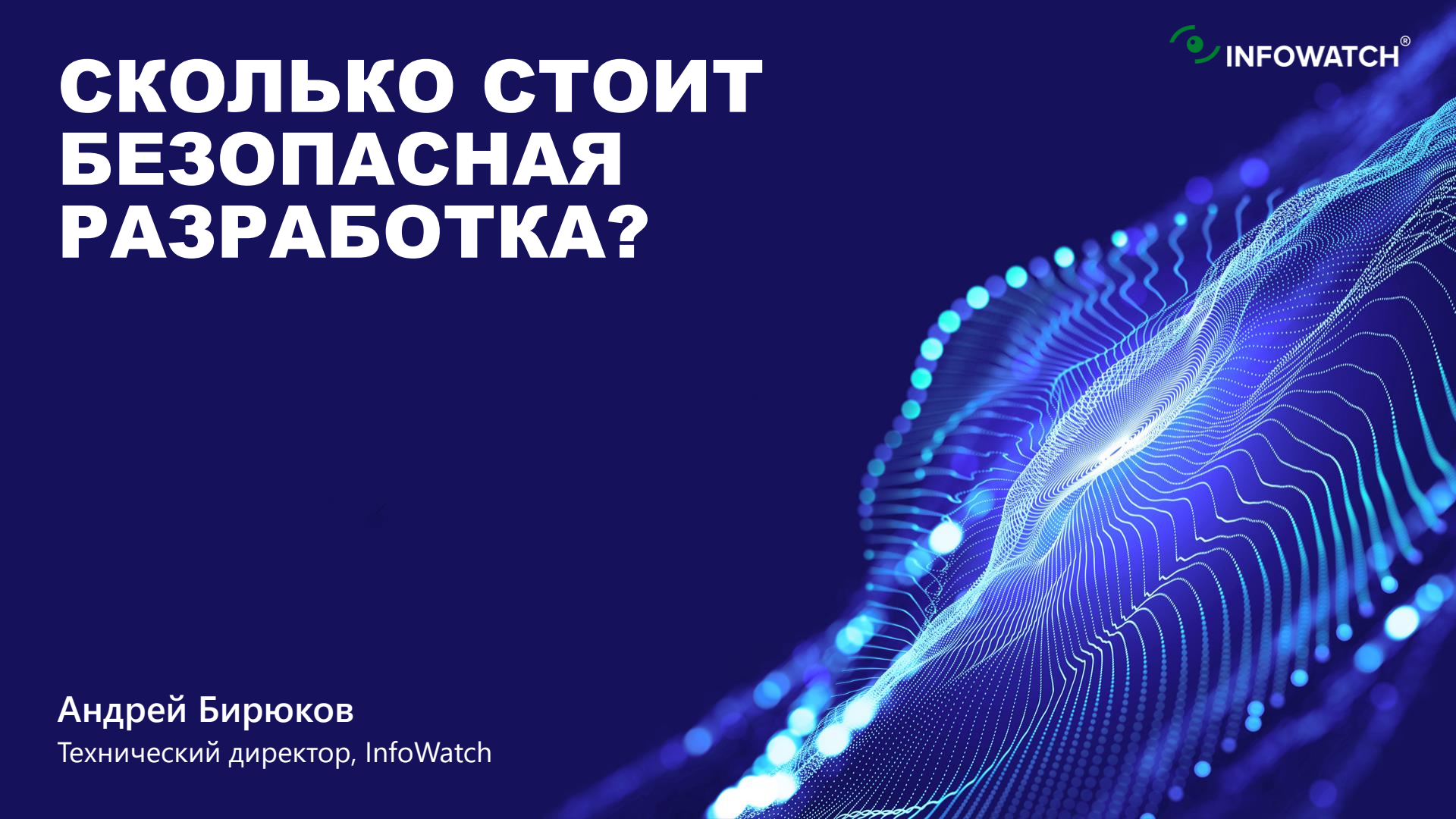
СКОЛЬКО СТОИТ БЕЗОПАСНАЯ РАЗРАБОТКА?



Андрей Бирюков
Технический директор, InfoWatch

Практики безопасной разработки

С чего все начинают?

INFOWATCH®

Бизнесу для успеха всегда нужна «ещё одна фича»

И ещё качество, но это после того, как клиенты приходят с проблемами

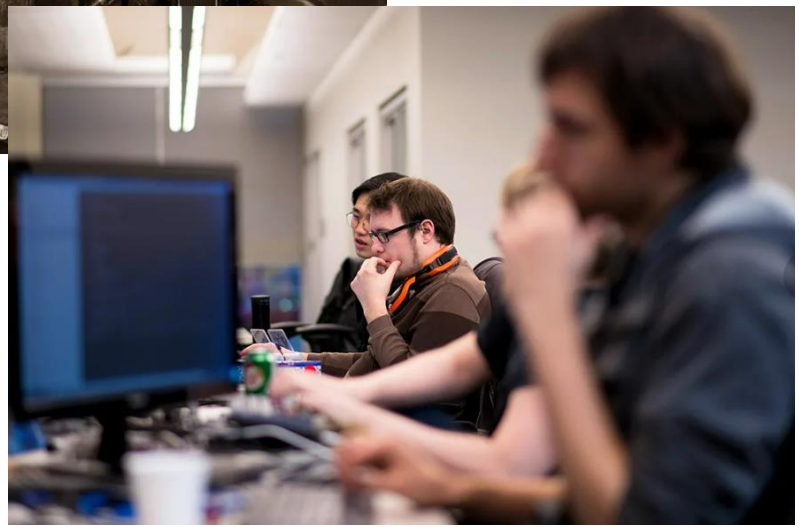
~~Техдолг~~	~~Code review~~	~~Пофиксить баги~~

Почему такая несправедливость

Зачем вкладываться, если проблем не видно?

- Требует ресурсов — как человеческих, так и софта, железа и т. п.
- Сколько багов найдет фаззинг-тестирование — заранее не очевидно

Как выглядят редкие истории успеха?



Технический лидер с административным ресурсом:

> **Мы будем делать так**

Разработчики-энтузиасты:

> **Внедряем полезные практики разработки, потому что это правильно**

Хорошо заходят в R&D:

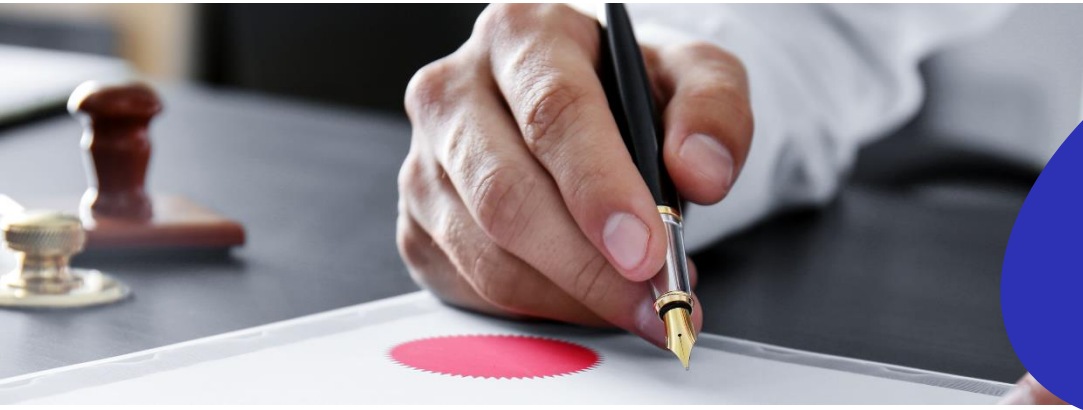
- Требования
- Модульное тестирование / юнит-тесты
- Статический и динамический анализ кода
- Фаззинг-тестирование

Безопасная разработка — тоже фича!

...если она нужна для получения сертификата

...или в случае взлома ПО и ущерба репутации продукта

Как это было в InfoWatch?



Нужен сертификат!

И это был не ФСТЭК

- Решили не строить потёмкинскую деревню, а делать, как надо, — разовые затраты и последующее поддержание.
- Практики безопасной разработки внедрили для успешного прохождения сертификации:
  - — В испытательной лаборатории были хорошие специалисты
  - — Нам выдали дельные замечания

Первый подход к снаряду — было больно, но результат понравился

- **Что сделали:**
  - — Статический анализ
  - — Вычистили сторонние библиотеки (неиспользуемые)
  - — Обновили сторонние библиотеки, закрытие CVE
  - — Динамический анализ
  - — Юнит-тесты и т. п.
  - — Обучение / тренинги

Второй подход к снаряду — стало сильно легче

- **Добавили фаззинг-тестирование**

Активная фаза — 2 недели

Остальное — документы, контракты и т. п.

Сколько это нам стоило?

Первый подход к снаряду	
Люди	6 месяцев работы команды
Деньги	5% от выручки
Второй подход к снаряду	
Люди	2 недели работы команды
Деньги	<1% от выручки

Сколько стоит безопасная разработка?

INFOWATCH®

Security Development Lifecycle является описанием того, какие практики разработки надо использовать, чтобы сделать качественный продукт

Она стоит качества продукта

Ещё есть документальное сопровождение...

INFOWATCH®

Как быстро устаревает описание процесса софтверной разработки в 2023?

Описание процессов, требований, выдвигаемых к продукту, и прочих документов, а также поддержание их в актуальном состоянии — вторая большая задача.

План, что и говорить, был превосходный; простой и ясный, лучше не придумать. Недостаток у него был только один: было совершенно неизвестно, как привести его в исполнение.

ЖДЁМ ВАС НА СТЕНДЕ INFOWATCH

B70

и в наших соцсетях

/InfoWatchOut /InfoWatch

infowatch.ru