КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КОД ИБ ИТОГИ 2023

МОСКВА

07 ДЕКАБРЯ 2023

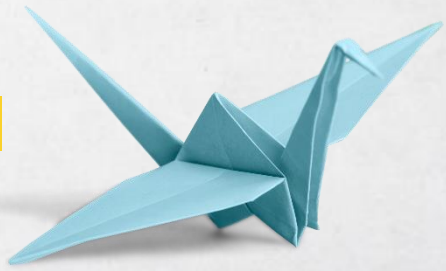
ПАЛЬМИРА БИЗНЕС КЛУБ

ПРИМЕНЕНИЕ МЕТОДОЛОГИИ SCRUM ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Макаров Владимир

Руководитель направления информационной безопасности

Кошелёк



Коротко о себе

- 10+ лет практического опыта работы в области ИБ
- 5+ лет опыта руководства подразделениями ИБ
- **ISO/IEC 27001 Lead Auditor**
- **Certified Ethical Hacker (CEH)**
- Аудитор по ГОСТ Р 57580 (АБИСС)
- Руководитель направления ИБ в приложении «Кошелек»

Кошелёк

Кошелек — приложение, с которым покупают

12 млн

Человек каждый день пользуются Кошельком

250

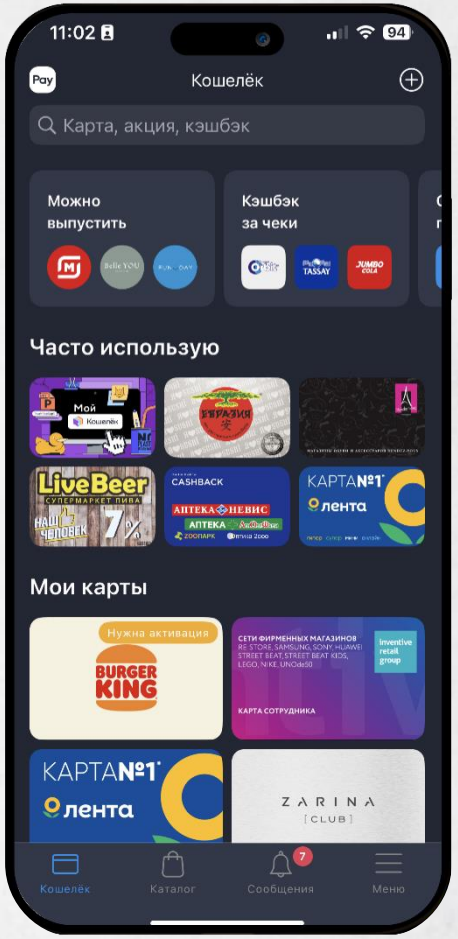
Сотрудников в штате

414+ млн

Карт выпущено и добавлено в приложении

525 тонн

Оцифрованного пластика



Кошелёк

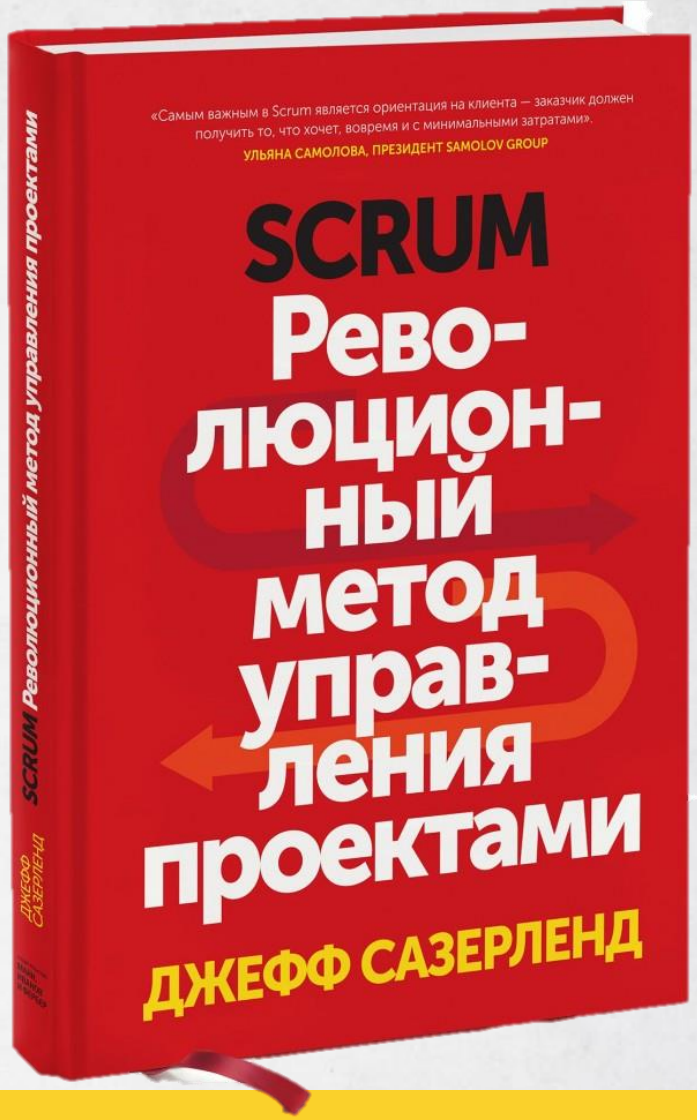
SCRUM Гайд

1995 год

Кен Швабер и **Джефф Сазерленд** впервые представили **SCRUM гайд** на конференции OOPSLA

- Дали определение методологии
- Это руководство описывает Scrum в том виде, в котором он был разработан и дополнялся авторами **>30 лет**

Скачать



SCRUM –

Это проектная методология, которая помогает командам правильно приоритизировать задачи и работу над продуктом.

Его основа — итеративная разработка и получение регулярной обратной связи от заказчиков и пользователей

Принципы SCRUM

Прозрачность

Весь объем и процесс работы прозрачен и понятен всей команде

Инспекция

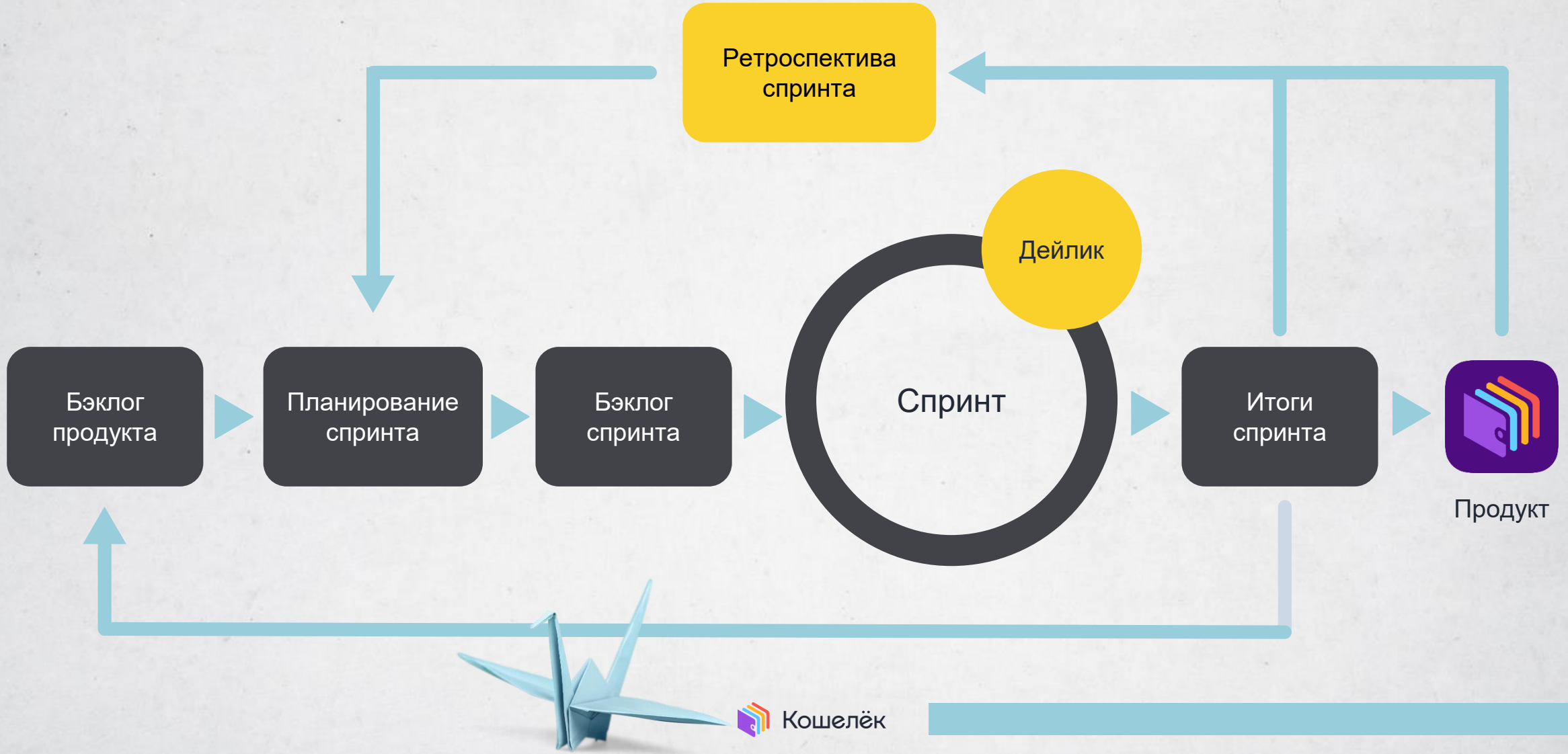
Инспекция прогресса работ происходит регулярно на каждой итерации (спринте)

Адаптация

Адаптация результата работы происходит регулярно на каждой итерации (спринте)

Кошелёк

Типовой цикл Scrum



Применимость SCRUM

1. Разработка продуктов **с длительным циклом жизни**, в том числе и **на весь период существования компании**
2. Все требования к продукту формируют **бэклог**, в котором расположены основные задачи по улучшению продукта
3. Команде приходится решать самостоятельно **нестандартные задачи** на всех этапах жизненного цикла продукта
4. Для качественного процесса разработки **требуется документирование и ретроспективный анализ**
5. Решения по внесению изменений и улучшений в продукт принимаются владельцем продукта **на основании изменяющегося пользовательского опыта**
6. Задачи из бэклога **могут быть разбиты на более мелкие подзадачи** для повышения эффективности их выполнения

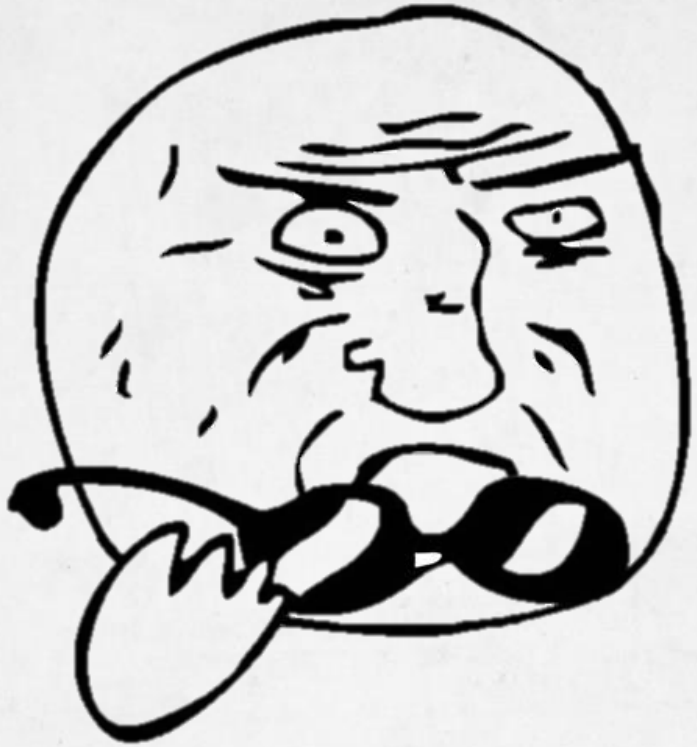
Кошелёк

Применимость SCRUM

1. Разработка продуктов **с длительным циклом жизни**, в том числе и **на весь период существования компании**
2. Все требования к продукту формируют **бэклог**, в котором расположены основные задачи по улучшению продукта
3. Команде приходится решать самостоятельно **нестандартные задачи** на всех этапах жизненного цикла продукта
4. Для качественного процесса разработки **требуется документирование и ретроспективный анализ**
5. Решения по внесению изменений и улучшений в продукт принимаются владельцем продукта **на основании изменяющегося пользовательского опыта**
6. Задачи из бэклога **могут быть разбиты на более мелкие подзадачи** для повышения эффективности их выполнения

1. СУИБ существует **на протяжении всего цикла жизни компании**, а ИБ сама по себе – бесконечный процесс
2. Для построения эффективных систем ИБ требуется годовое и ежеквартальное **планирование**
3. СУИБ на протяжении всего своего существования многократно проходит **цикл Деминга (PDCA)**
4. Для управления системами защиты информации **требуется детальное документирование процессов ИБ**
5. **На основании ежегодной оценки рисков** руководитель направления ИБ может вносить изменения в СУИБ с учетом новых рисков ИБ
6. В рамках годового и ежеквартального планирования ставятся **макро цели на улучшение системы ИБ**, которые **дробятся** на более мелкие для удобства их выполнения

Это что получается —



Система управления ИБ = Разрабатываемый продукт

Как это работает на практике

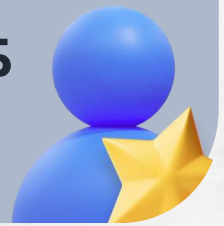
Кошелёк

Роли

Владелец продукта +
SCRUM Мастер

=

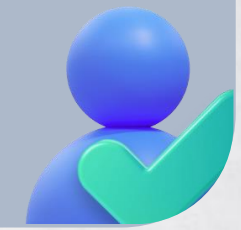
Руководитель по ИБ



Команда

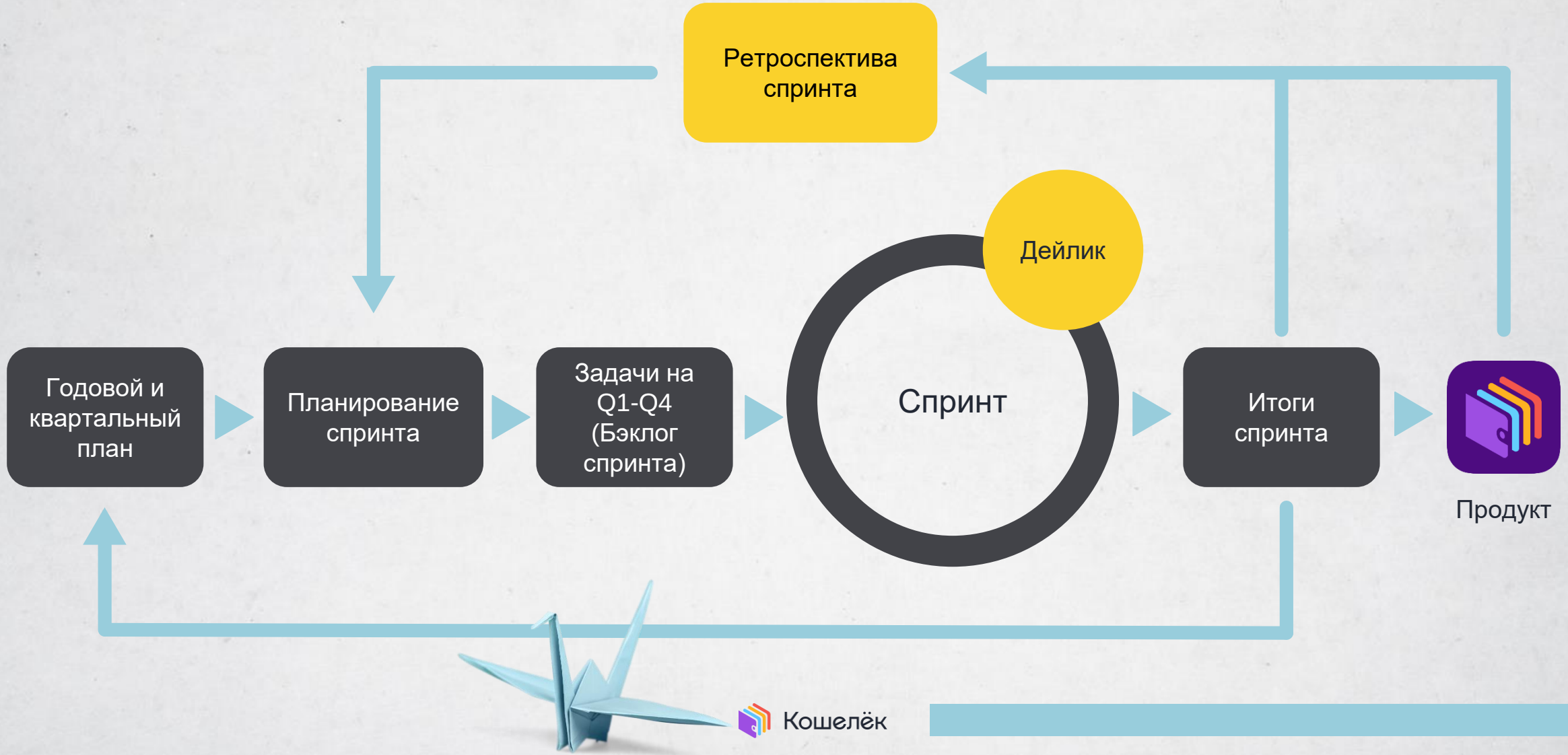
=

Отдел ИБ



Кошелёк

Цикл SCRUM в ИБ



Проблемные вопросы, с которыми вы столкнетесь

- Правильное внедрение и поддержание SCRUM (возможно потребуется наличие SCRUM Мастера)
- Высокий уровень требований к самоорганизации Команды. Кадры решают!
- Наличие АС по управлению проектами и документированию (Jira, Bitrix, Wiki, Confluence и т.п.)
- Строгое соблюдение задачности в спринтах
- Использование предоставляемых методологией точек контроля работ (отказ от «Чайка-менеджмента»)
- Выделение резерва времени спринта на поддержание ИБ систем
- Наличие годового и квартального планирования на основе оценки рисков ИБ

И самое важное

- Наличие прозрачной системы оценки результатов личной работоспособности сотрудников (1х1, ежемесячная оценка, оценка 360 и т.п.)
- Наличие системы премирования сотрудников (Квартальное, полугодовое, годовое, проектное и т.п.)
- Контроль отсутствия сверхурочной работы
- Наличие системы повышения квалификации сотрудников

Что нам это дало?

- Больше выполненных работ по ИБ в единицу времени
- Задачи перестали теряться, а сроки нарушаться
- Более адекватная оценка сроков выполнения
- Отсутствие переработок и улучшение мотивации отдела ИБ
- Отпала необходимость в переработке сегментов проекта целиком (делаем все с 1й попытки)
- Наличие четких метрик оценки эффективности сотрудников отдела ИБ