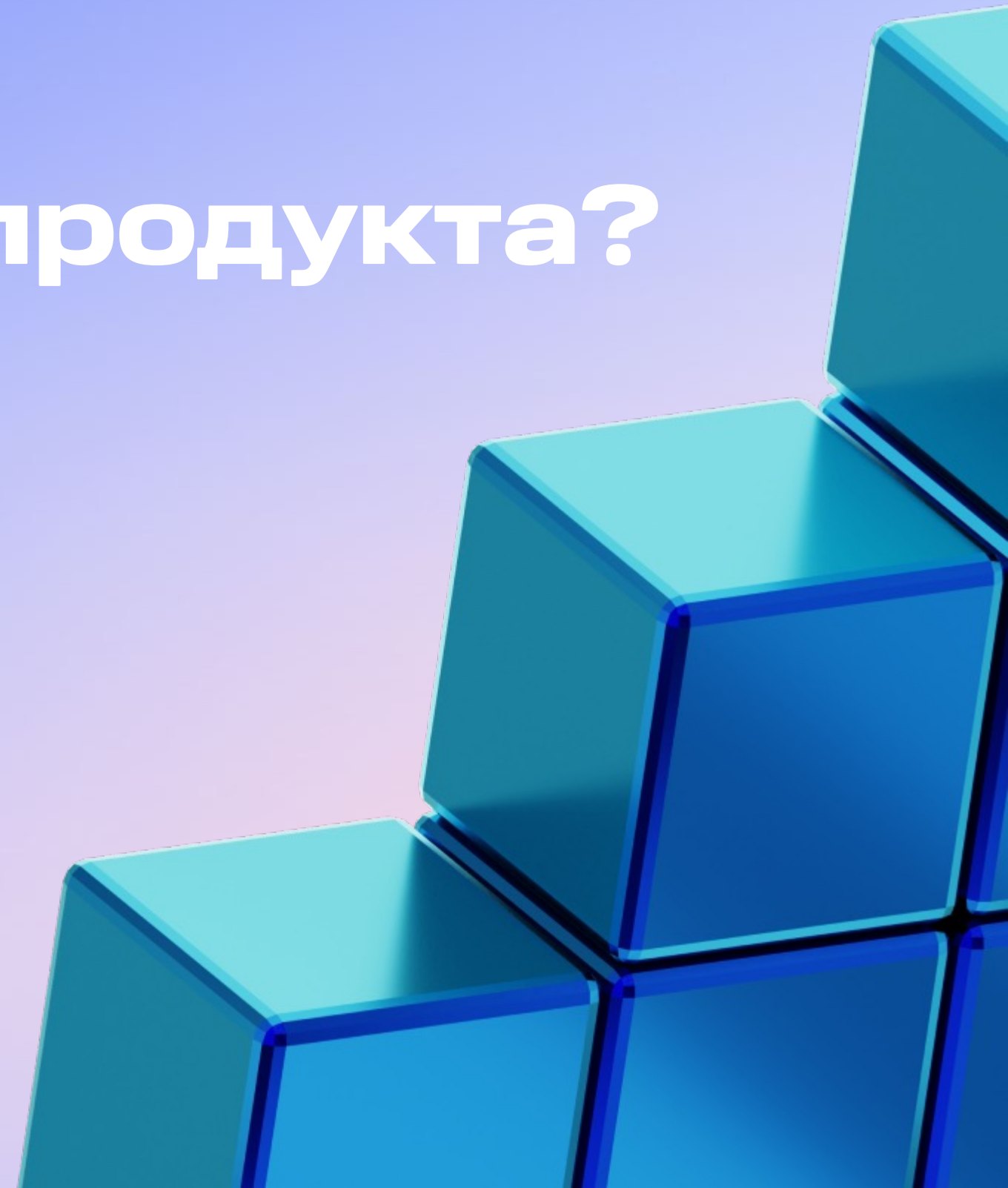


Как обезопасить смерть продукта?

Холод Денис и Молодёнова Александра
Архитекторы ИБ ПАО МТС



МТС: архитектура ИБ



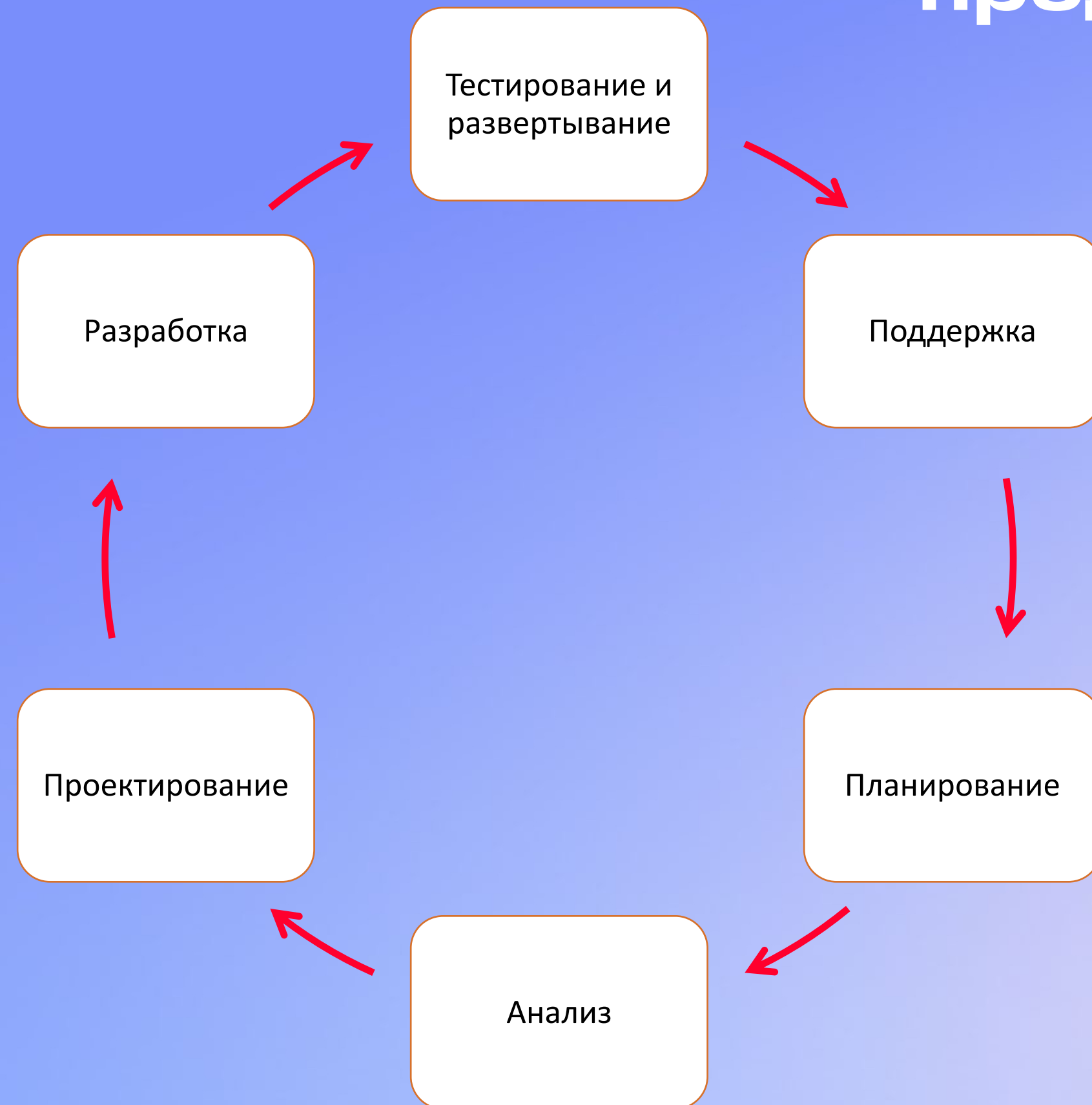
Холод Денис



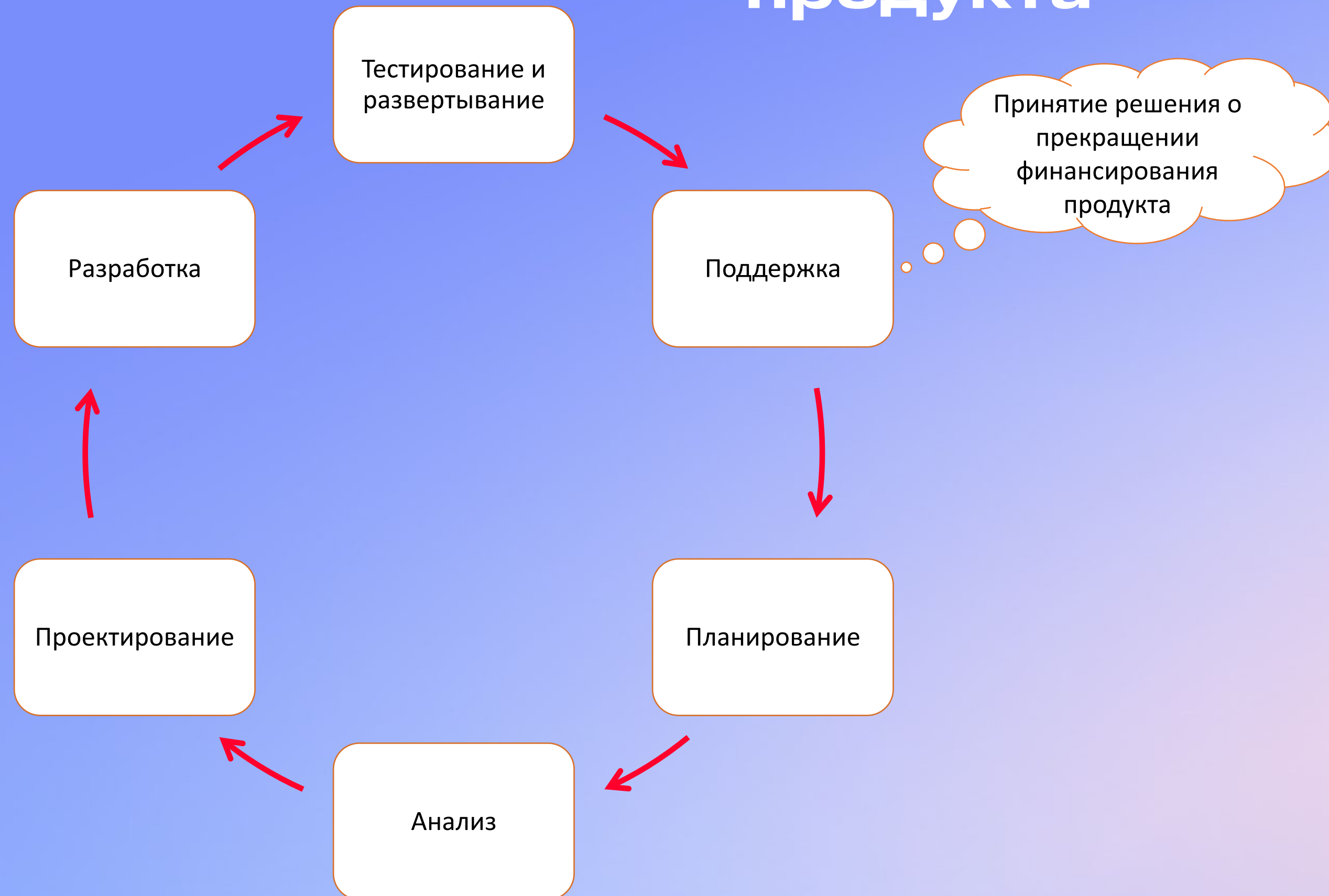
Молодёнова
Александра



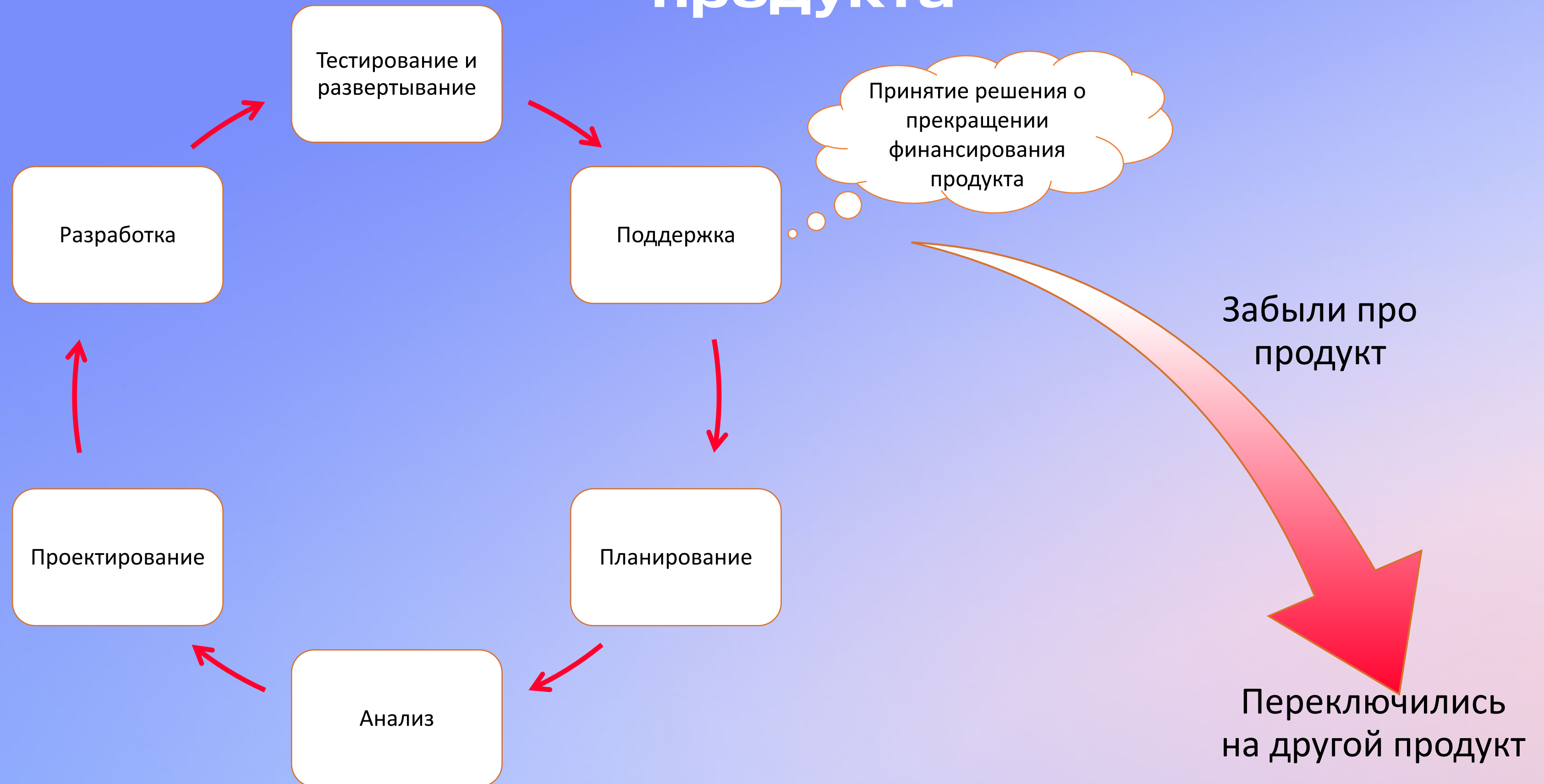
Общий жизненный цикл продукта



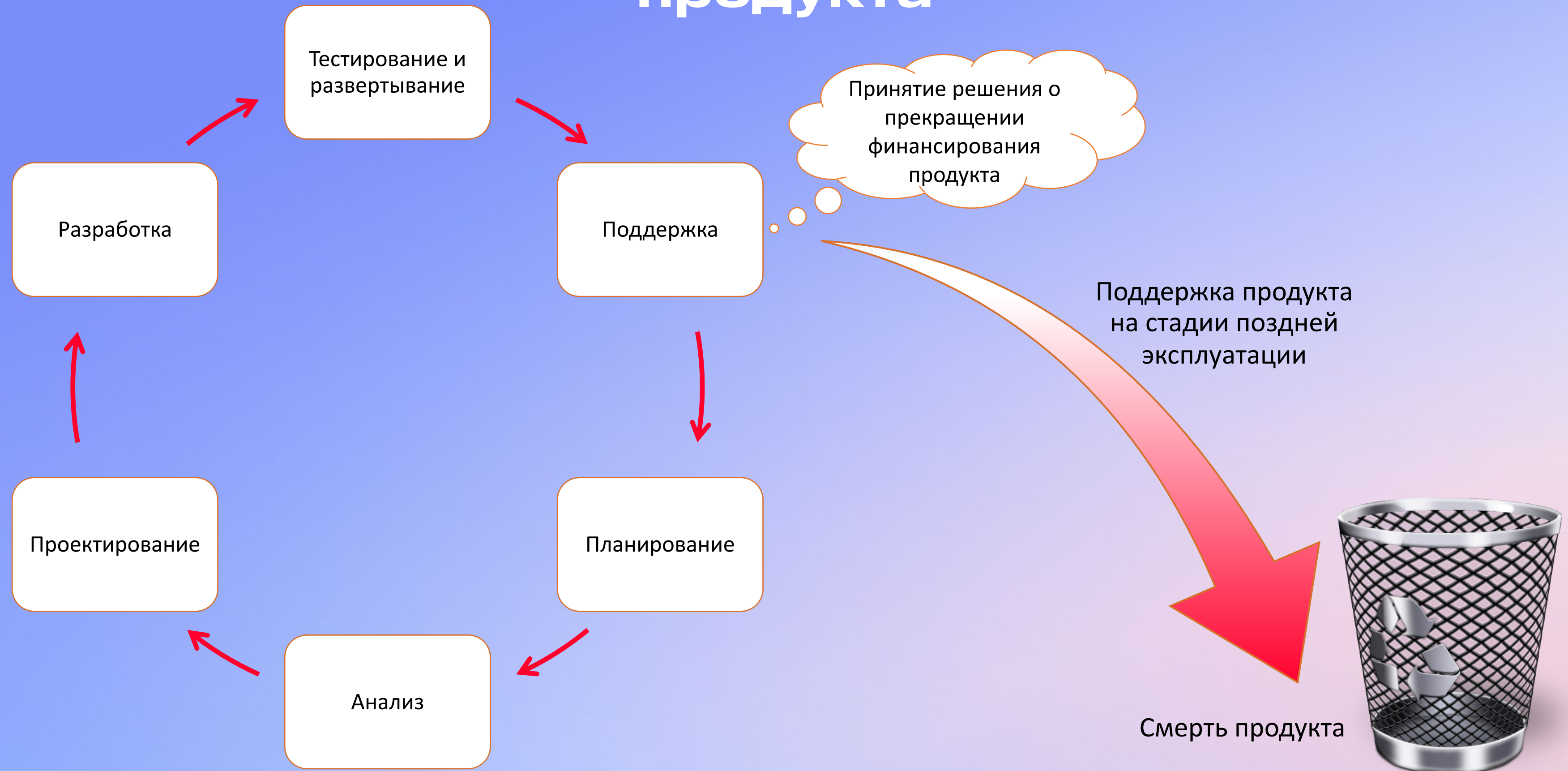
Общий жизненный цикл продукта



Общий жизненный цикл продукта



Общий жизненный цикл продукта

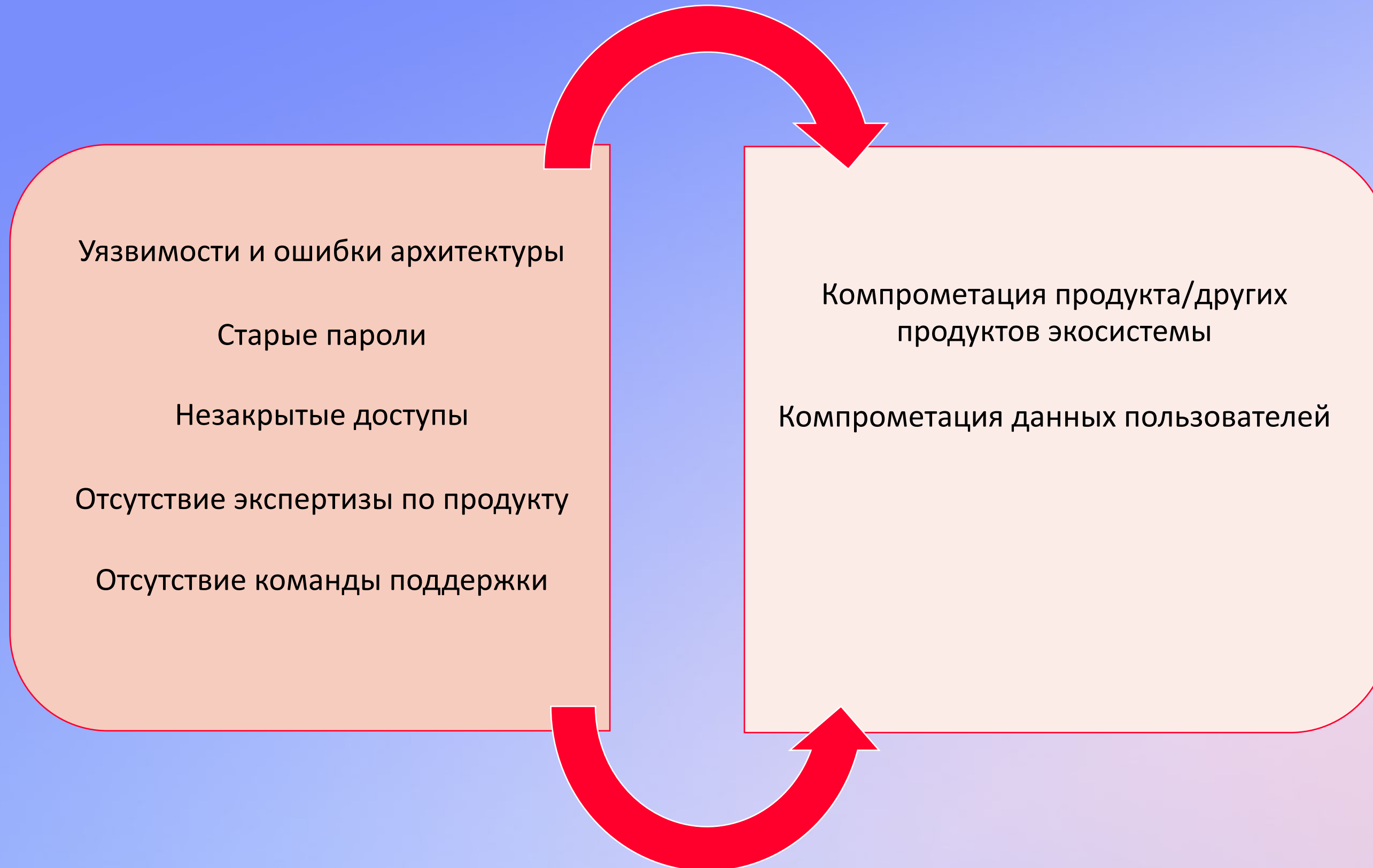


Поддержка продуктов



Поддержка продуктов





1. Предсмертие

Инвентаризация продукта

1

Актуализация информационных потоков

2

Актуализация сетевой архитектуры

3

Пересмотр чувствительных данных

4

Актуализация комплаенса ИБ

Инвентаризация продукта

1

Актуализация информационных потоков

2

Актуализация сетевой архитектуры

3

Пересмотр чувствительных данных

4

Актуализация комплаенса ИБ

1

2

3

4



Инвентаризация продукта

1

Актуализация информационных потоков

2

Актуализация сетевой архитектуры

3

Пересмотр чувствительных данных

4

Актуализация комплаенса ИБ

Инвентаризация продукта

1

Актуализация информационных потоков

2

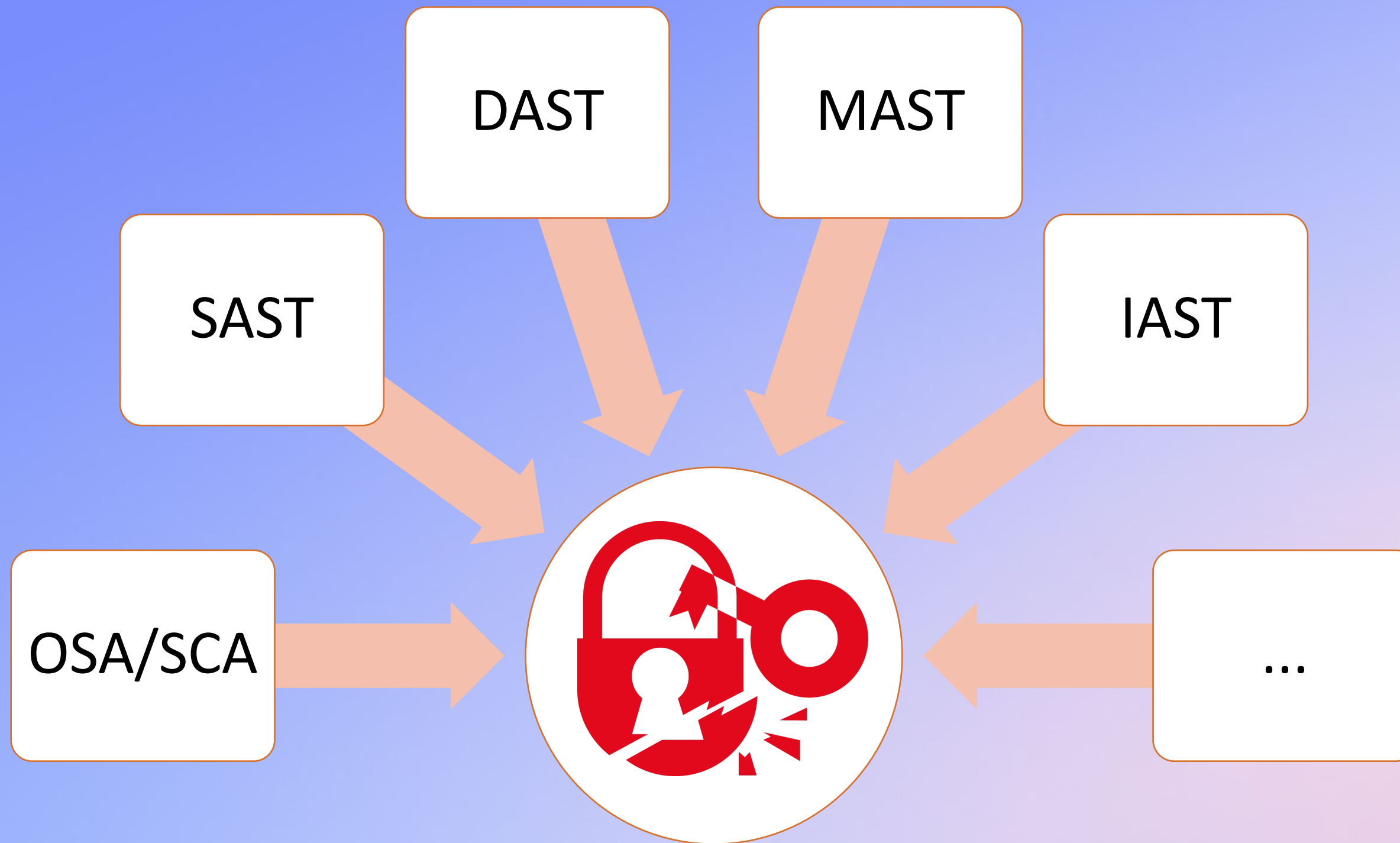
Актуализация сетевой архитектуры

3

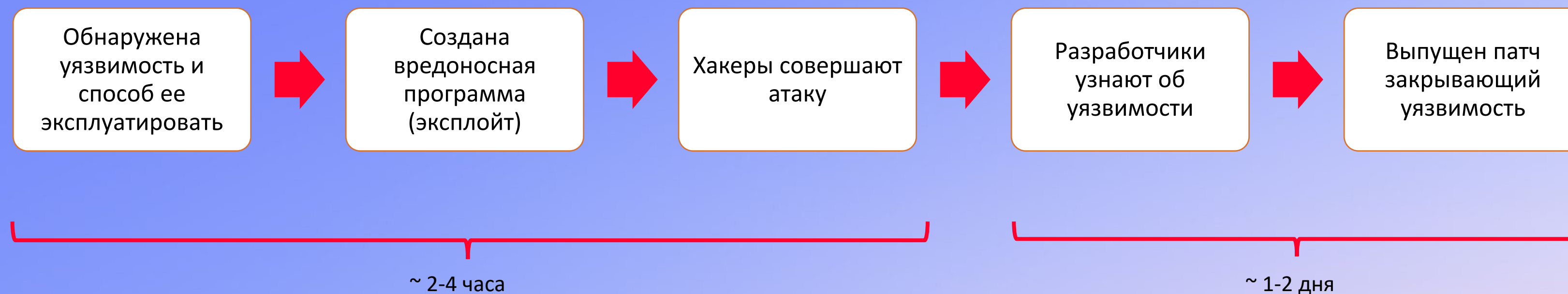
Пересмотр чувствительных данных

4

Актуализация комплаенса ИБ



Patch management



Жизненный цикл уязвимости нулевого дня

Сколько времени займет реагирование
на стороне продукта и команды сопровождения?

Пересмотр и актуализация требований ИБ

1

Пересмотр парольных политик

2

Интеграция с новыми СЗИ

3

**Обновление используемых алгоритмов
шифрования**

4

**Пересмотр используемых протоколов
взаимодействия**

Пересмотр и актуализация требований ИБ

1

Пересмотр парольных политик

2

Интеграция с новыми СЗИ

3

**Обновление используемых алгоритмов
шифрования**

4

**Пересмотр используемых протоколов
взаимодействия**

Пересмотр и актуализация требований ИБ

1

Пересмотр парольных политик

2

Интеграция с новыми СЗИ

3

**Обновление используемых алгоритмов
шифрования**

4

**Пересмотр используемых протоколов
взаимодействия**

Пересмотр и актуализация требований ИБ

1

Пересмотр парольных политик

2

Интеграция с новыми СЗИ

3

**Обновление используемых алгоритмов
шифрования**

4

**Пересмотр используемых протоколов
взаимодействия**



Продуктовая
команда*



ИБ

*возможна сторонняя команда поддержки/разработки

2.Смерть продукта

Предварительные работы



Этап 0. Ресурсы

0

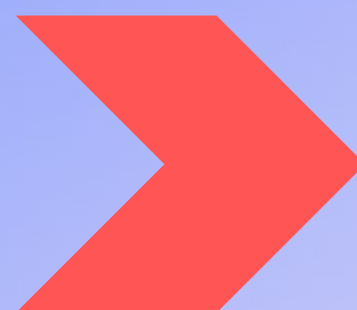
Выделение человеческих ресурсов
Поиск экспертизы



Этап 1. Анализ и ревизия ИС

Что нужно собрать

- ☐ Подробная информация о стендах
 - ☐ Список ресурсов/сервисов
 - ☐ Перечень БД и данных
 - ☐ Внешние интерфейсы
- ☐ Взаимодействия с другими ИС
- ☐ Кто имеет доступ к системе?
- ☐ Цифровой след продукта в инфраструктуре компании и корпоративных сервисах



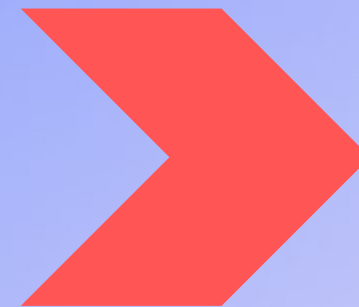
Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных, хранящихся и обрабатываемых в БД
 - + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты
- ☐ Схема информационных потоков
 - + аутентификационные данные для доступа в другие продукты
 - + доступы из других продуктов
- ☐ Список сотрудников и способ их аутентификации
- ☐ *Зависит от компании*

Этап 1. Анализ и ревизия ИС

Что нужно собрать

- ☐ **Подробная информация о стендах**
 - ☐ **Список ресурсов/сервисов**
 - ☐ **Перечень БД и данных**
 - ☐ **Внешние интерфейсы**
- ☐ **Взаимодействия с другими ИС**
- ☐ **Кто имеет доступ к системе?**
- ☐ **Цифровой след продукта в инфраструктуре компании и корпоративных сервисах**



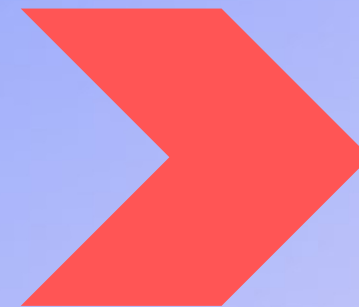
Артефакты

- ☐ **LLD для всех стендов**
 - + список сервис:назначение**
 - + структура БД, перечень данных, хранящихся и обрабатываемых в БД**
 - + внешние интерфейсы:** IP, доступы, взаимодействия, домены и сертификаты
- ☐ **Схема информационных потоков**
 - + аутентификационные данные для доступа в другие продукты**
 - + доступы из других продуктов**
- ☐ **Список сотрудников и способ их аутентификации**
- ☐ *Зависит от компании*

Этап 1. Анализ и ревизия ИС

Что нужно собрать

- ☐ Подробная информация о всех стендах
 - ☐ Список ресурсов/сервисов
 - ☐ Перечень БД и данных
 - ☐ Внешние интерфейсы
- ☐ **Взаимодействия с другими ИС**
- ☐ Кто имеет доступ к системе?
- ☐ Цифровой след продукта в инфраструктуре компании и корпоративных сервисах



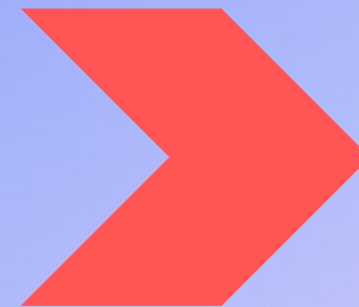
Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных, хранящихся и обрабатываемых в БД
 - + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты
- ☐ **Схема информационных потоков**
 - + аутентификационные данные для доступа в другие продукты
 - + доступы из других продуктов
- ☐ Список сотрудников и способ их аутентификации
- ☐ *Зависит от компании*

Этап 1. Анализ и ревизия ИС

Что нужно собрать

- ☐ Подробная информация о всех стендах
 - ☐ Список ресурсов/сервисов
 - ☐ Перечень БД и данных
 - ☐ Внешние интерфейсы
- ☐ Взаимодействия с другими ИС
- ☐ **Кто имеет доступ к системе?**
- ☐ Цифровой след продукта в инфраструктуре компании и корпоративных сервисах



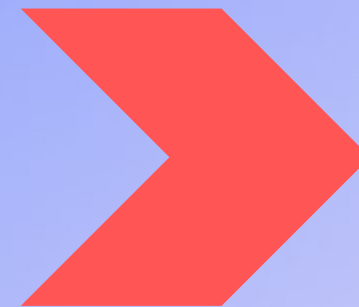
Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных, хранящихся и обрабатываемых в БД
 - + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты
- ☐ Схема информационных потоков
 - + аутентификационные данные для доступа в другие продукты
 - + доступы из других продуктов
- ☐ **Список сотрудников и способ их аутентификации**
- ☐ *Зависит от компании*

Этап 1. Анализ и ревизия ИС

Что нужно собрать

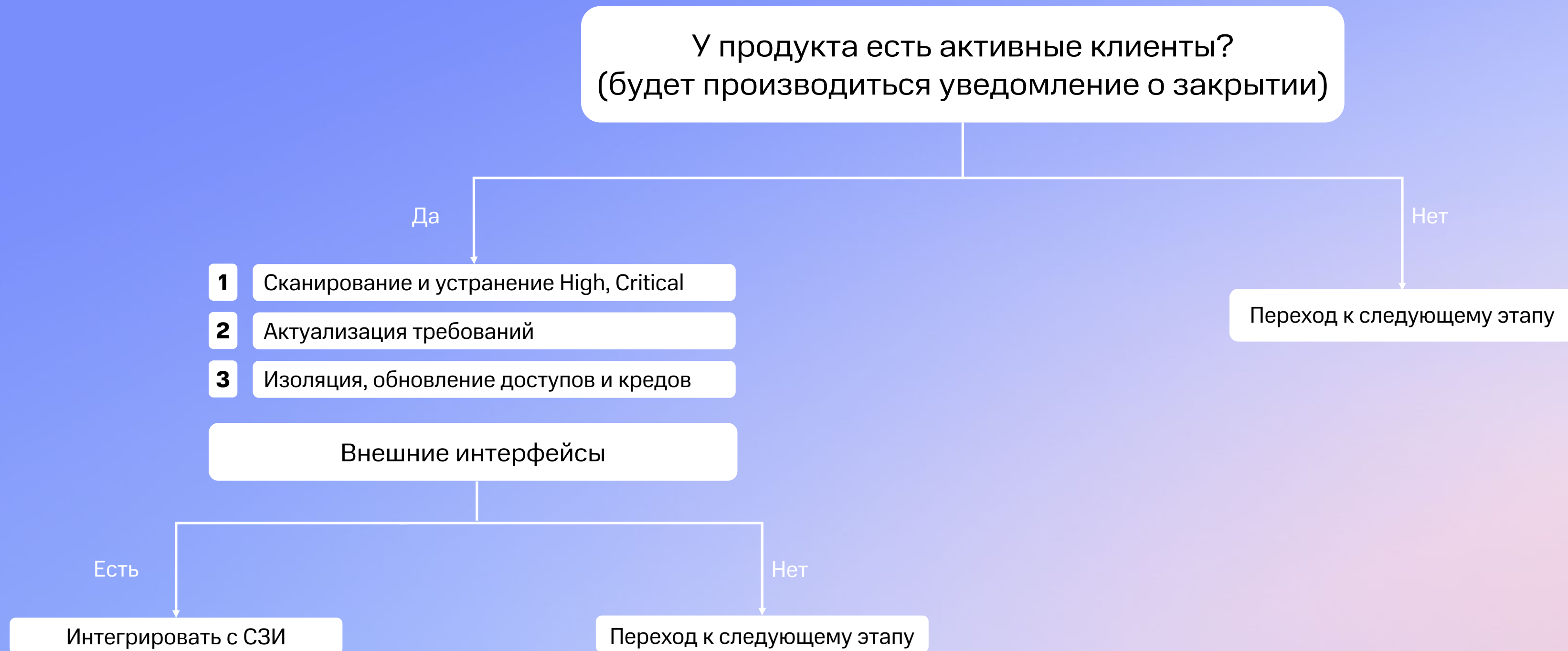
- ☐ Подробная информация о всех стендах
 - ☐ Список ресурсов/сервисов
 - ☐ Перечень БД и данных
 - ☐ Внешние интерфейсы
- ☐ Взаимодействия с другими ИС
- ☐ Кто имеет доступ к системе?
- ☐ **Цифровой след** продукта в инфраструктуре компании и корпоративных сервисах



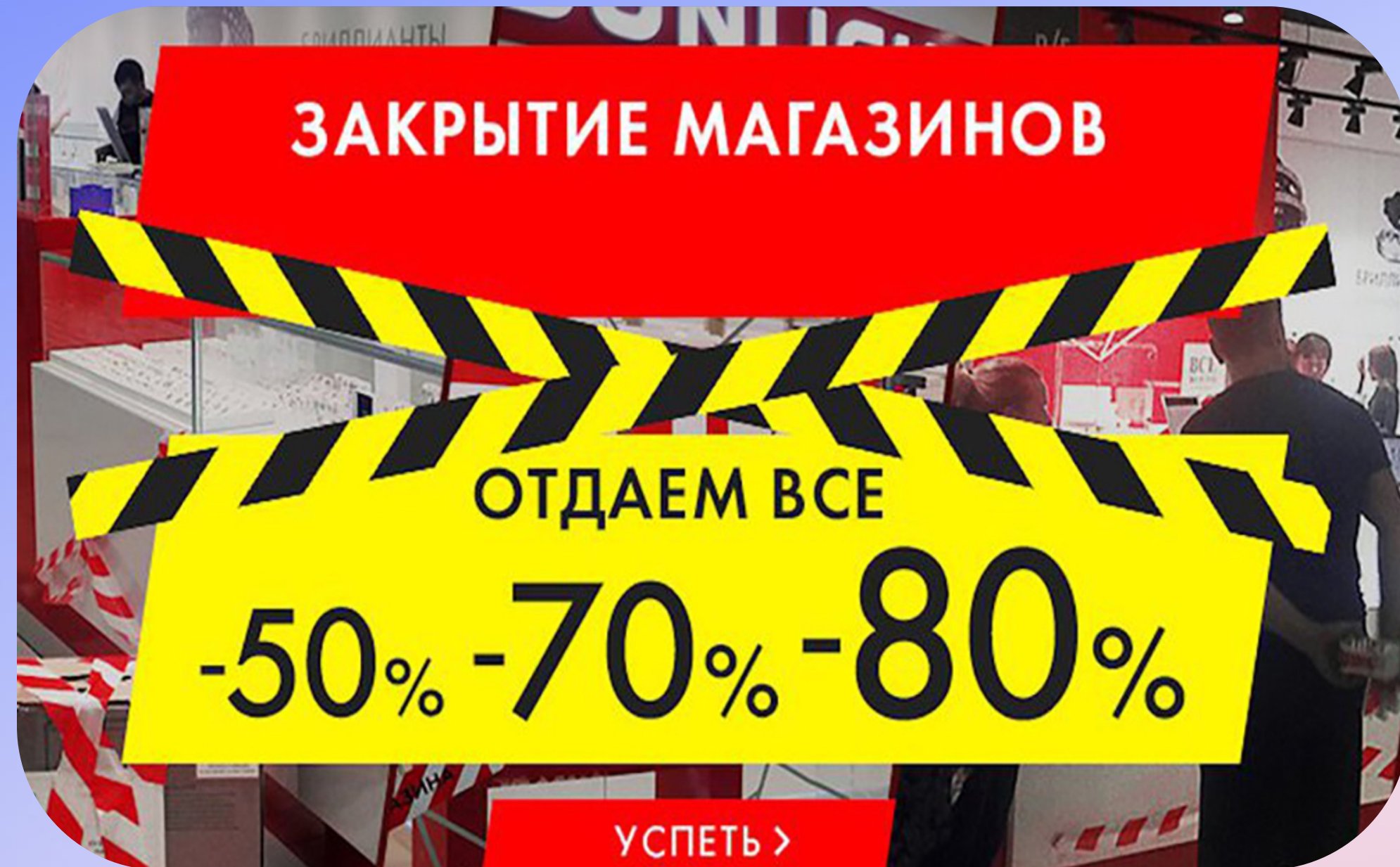
Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных, хранящихся и обрабатываемых в БД
 - + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты
- ☐ Схема информационных потоков
 - + аутентификационные данные для доступа в другие продукты
 - + доступы из других продуктов
- ☐ Список сотрудников и способ их аутентификации
- ☐ **Зависит от компании**

Этап 2. «Предсмертие интенсив» (подготовительный этап)



Предупреждение о закрытии



Этап 3. Предупреждение и закрытие

1

Разработка информационных страниц

2

Уведомление клиентов об окончании клиентов

3

Проработка выгрузки данных или миграции

Этап 3. Предупреждение и закрытие

1

Разработка информационных страниц

2

Уведомление клиентов об окончании поддержки

3

Проработка выгрузки данных или миграции

Этап 3. Предупреждение и закрытие

1

Разработка информационных страниц

2

Уведомление клиентов об окончании клиентов

3

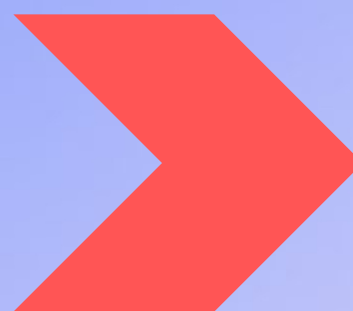
Проработка выгрузки данных или миграции

«Отключение рубильника»



Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных, хранящихся и обрабатывающихся в БД
 - + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты
- ☐ Схема информационных потоков
 - + аутентификационные данные для доступа в другие продукты
 - + доступы из других продуктов
- ☐ Список сотрудников и способ их аутентификации
- ☐ *Зависит от компании*



Что нужно сделать

- ☐ Сброс до заводских настроек VM, сервисов и железа
- ☐ Удаление данных
- ☐ Удаление «кредов» и закрытие доступов в продуктах, с которыми была интеграция
- ☐ Удаление «кредов» сотрудников
- ☐ Специфичное для ИС и компании:
 - ☐ *доступы на FW/СЗИ/DNS/корп. сервисах, сертификаты и токены*

Артефакты

☐ LLD для всех стендов

+ список сервис:назначение

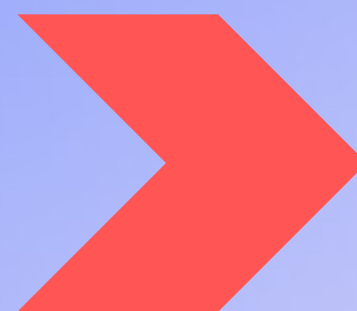
- + структура БД, перечень данных, хранящихся и обрабатывающихся в БД
- + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты

☐ Схема информационных потоков

- + аутентификационные данные для доступа в другие продукты
- + доступы из других продуктов

☐ Список сотрудников и способ их аутентификации

☐ Зависит от компании



Что нужно сделать

☐ Сброс до заводских настроек VM, сервисов и железа

☐ Удаление данных

☐ Удаление «кредов» и закрытие доступов в продуктах, с которыми была интеграция

☐ Удаление «кредов» сотрудников

☐ Специфичное для ИС и компании:

- ☐ *доступы на FW/СЗИ/DNS/корп. сервисах, сертификаты и токены*

Артефакты

☐ LLD для всех стендов

+ список сервис:назначение

+ структура БД, перечень данных, хранящихся и обрабатывающихся в БД

+ внешние интерфейсы, доступы, взаимодействия, домены и сертификаты

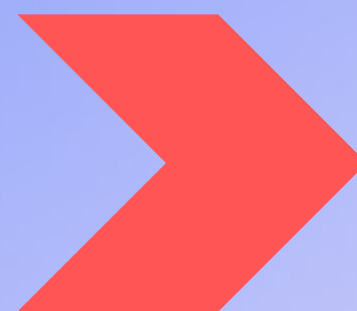
☐ Схема информационных потоков

+ аутентификационные данные для доступа в другие продукты

+ доступы из других продуктов

☐ Список сотрудников и способ их аутентификации

☐ Зависит от компании



Что нужно сделать

☐ Сброс до заводских настроек VM, сервисов и железа

☐ Удаление данных

☐ Удаление «кредов» и закрытие доступов в продуктах, с которыми была интеграция

☐ Удаление «кредов» сотрудников

☐ Специфичное для ИС и компании:

☐ *доступы на FW/СЗИ/DNS/корп. сервисах, сертификаты и токены*

Артефакты

☐ LLD для всех стендов

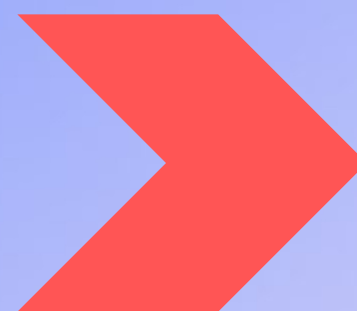
- + список сервис:назначение
- + структура БД, перечень данных, хранящихся и обрабатывающихся в БД
- + **внешние интерфейсы, доступы, взаимодействия, домены и сертификаты**

☐ Схема информационных потоков

- + аутентификационные данные для доступа в другие продукты
- + доступы из других продуктов

☐ Список сотрудников и способ их аутентификации

☐ Зависит от компании

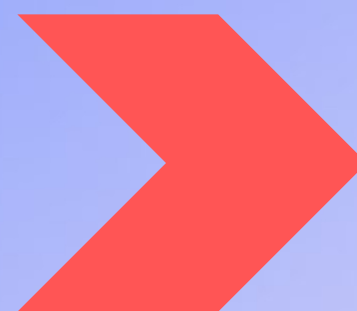


Что нужно сделать

- ☐ Сброс до заводских настроек VM, сервисов и железа
- ☐ Удаление данных
- ☐ **Удаление «кредов» и закрытие доступов в продуктах, с которыми была интеграция**
- ☐ Удаление «кредов» сотрудников
- ☐ Специфичное для ИС и компании:
 - ☐ *доступы на FW/СЗИ/DNS/корп. сервисах, сертификаты и токены*

Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных, хранящихся и обрабатывающихся в БД
 - + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты
- ☐ Схема информационных потоков
 - + аутентификационные данные для доступа в другие продукты
 - + доступы из других продуктов
- ☐ **Список сотрудников и способ их аутентификации**
- ☐ *Зависит от компании*

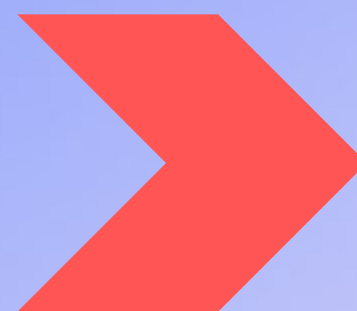


Что нужно сделать

- ☐ Сброс до заводских настроек VM, сервисов и железа
- ☐ Удаление данных
- ☐ Удаление «кредов» и закрытие доступов в продуктах, с которыми была интеграция
- ☐ **Удаление «кредов» сотрудников**
- ☐ Специфичное для ИС и компании:
 - ☐ *доступы на FW/СЗИ/DNS/корп. сервисах, сертификаты и токены*

Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных, хранящихся и обрабатывающихся в БД
 - + внешние интерфейсы, доступы, взаимодействия, домены и сертификаты
- ☐ Схема информационных потоков
 - + аутентификационные данные для доступа в другие продукты
 - + доступы из других продуктов
- ☐ Список сотрудников и способ их аутентификации
- ☐ **Зависит от компании**



Что нужно сделать

- ☐ Сброс до заводских настроек VM, сервисов и железа
- ☐ Удаление данных
- ☐ Удаление «кредов» и закрытие доступов в продуктах, с которыми была интеграция
- ☐ Удаление «кредов» сотрудников
- ☐ **Специфичное для ИС и компании:**
 - ☐ *доступы на FW/СЗИ/DNS/корп. сервисах, сертификаты и токены*

Артефакты

- ☐ LLD для всех стендов
 - + список сервис:назначение
 - + структура БД, перечень данных хранящихся и обрабатывающих
 - + внешние интерфейсы, доступы, взаимодействия, домены и сервисы
- ☐ Схема информационных потоков
 - + аутентификационные данные, доступы в другие продукты
 - + доступы из других продуктов
- ☐ Список сотрудников и способы аутентификации
- ☐ **Зависит от компании**

* Архивирование кода и документации
** Изменение статуса продукта в корп. сервисах

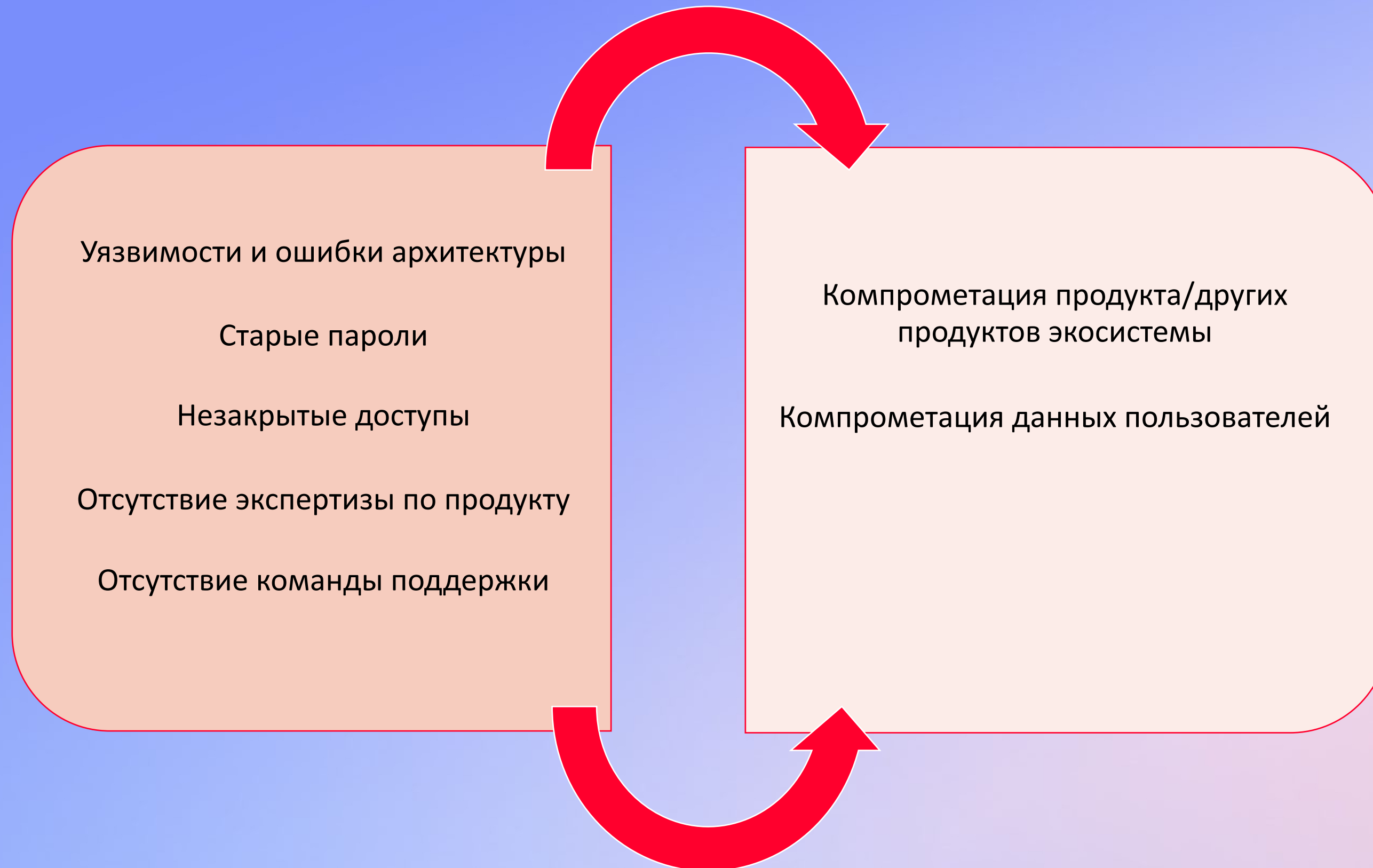
Что нужно сделать

...до заводских настроек VM,
...ов и железа
...ие данных
...е «кредов» и закрытие
...в продуктах, с которыми
...еграция
...е «кредов» сотрудников
...фичное для ИС и
...пании:
...доступы на FW/СЗИ/DNS/корп.
сервисах, сертификаты и токены

Уходя,
выключайте
~~СВЕТ~~

доступы





Уязвимости и ошибки архитектуры

Старые пароли

Незакрытые доступы

Отсутствие экспертизы по продукту

Отсутствие команды поддержки

Предсмертие:

1. Поддержка SSDLC
2. Поддержка SSDLC
3. Поддержка SSDLC
4. Поддержка SSDLC
5. Поддержка SSDLC

~~Компрометация продукта/других
продуктов экосистемы~~

~~Компрометация данных пользователей~~

Смерть:

1. Удалили данные
2. Удалили продукт
3. Удалили креды
4. Удалили доступы
5. Удалили архитектуру

Уязвимости и ошибки архитектуры

Старые пароли

Незакрытые доступы

Отсутствие экспертизы по продукту

Отсутствие команды поддержки

Предсмертие:

1. Инвентаризация продукта
2. Сканирования ИБ
3. Patch management
4. Актуализация требований ИБ

5. Планирование ресурсов

~~Компрометация продукта/других
продуктов экосистемы~~

~~Компрометация данных пользователей~~

Смерть:

1. Очистить БД
2. Сброс до заводских настроек
3. Отозвать/удалить кредиты
4. Закрыть доступы

5. Планирование ресурсов

Как обезопасить смерть продукта?

МТС: архитектура ИБ



Холод Денис
@dekholod



Молоденова Александра
@solinenarany

