R-Vision
At the root of your security

План курса

Модуль 1	Соответствие нормативным требованиям РФ в области ИБ
Модуль 2	**Управление активами ИБ и уязвимостями прикладного и общесистемного ПО**
Модуль 3	Техники компьютерных атак и методы противодействия
Модуль 4	Моделирование угроз и риск ориентированный подход в обеспечении ИБ

Лекции + практические занятия с использованием решений R-Vision + практические ДЗ

Григорий Ревенко

Руководитель отдела технической экспертизы R-Vision

grevenko@rvision.pro

О модуле

О чем?

Модуль посвящен двум процессам Управлению Активами и Управлению Уязвимостями

Цель

Основная цель – понять что такое процесс и научиться эффективно работать с активами и уязвимостями в контексте противодействия компьютерным инцидентам

Практика

Используя R-Vision, практически реализовать процессы управления активами и уязвимостями

План Модуля 2

09 октября

Вводная
в модуль лекция

16 октября

Лекция по блоку
Активы

Практика

23 октября

Лекция по блоку
Уязвимости

Практика

30 октября

Лекция по блоку
Автоматизация

Закрытие
хвостов / ответы
на вопросы

Определения

- Процесс – это совокупность последовательных действий для достижения какого-либо результата
- Актив – всё, что имеет ценность для организации.
- Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств
- ITAM – методология учёта ИТ-активов и управления ИТ-ресурсами на всём их жизненном цикле
- PCM – Ресурсно-сервисная модель конкретной услуги представляет собой перечень конфигурационных единиц/сервисных активов, т.е. всего того, что там необходимо для качественного оказания этой самой услуги, а также массив связей между конфигурационными единицами.
- Уязвимость – Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации
- Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность

Минутка ЧСВ

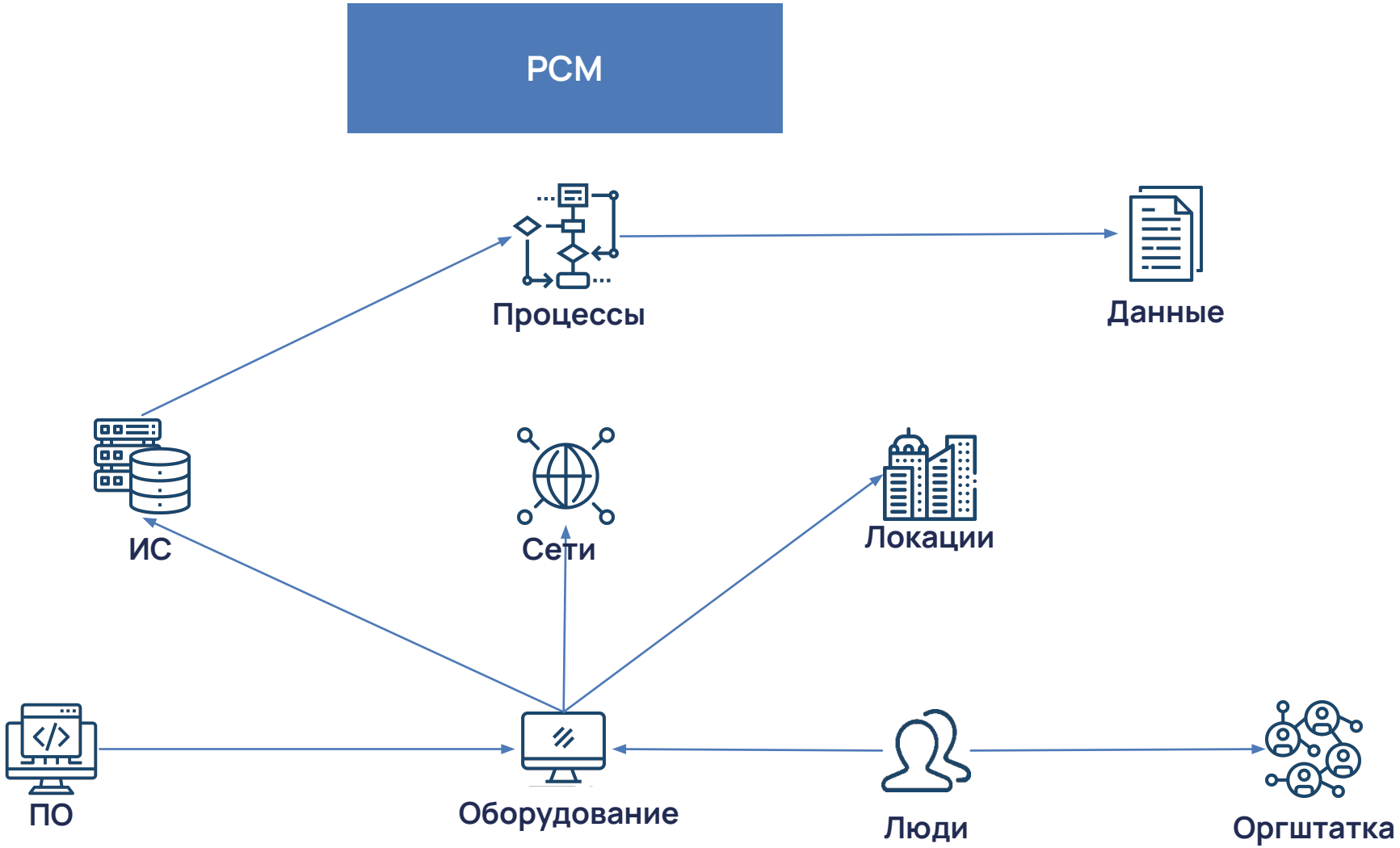
Олимпийские игры в Соч

Универсиада в Красноярске

РСМ для ПФР

Построено несколько SOC

Знать «Себя»


PCM
Процессы
Данные
ИС
Сети
Локации
ПО
Оборудование
Люди
Оргштатка

01

ITAM

Из IT в ИБ

ITAM. Объекты управления ИТ-активами

Аппаратное обеспечение (АО)

любое ИТ-оборудование, для которого требуется организации физической поставки, складирования, установки, обслуживания и возможной утилизации по завершению эксплуатации.

Программное обеспечение (ПО)

дистрибутивы ПО, лицензии, патчи, работоспособность которых должна обеспечивать предоставление соответствующих ИТ-сервисов.

Комплексные активы

ИТ-системы и ИТ-услуги, которые, с одной стороны, понимает бизнес и какую функциональность ИТ дает для решения бизнес-задач, а с другой стороны понимает ИТ, которые базируются и работают на основании сконфигурированного соответствующим образом оборудования и ПО.

ITAM. Подходы и практики

Учёт и контроль ИТ-активов

- Планирование закупки необходимого оборудования и ПО;
- Закупка, складирование;
- Инсталляция;
- Эксплуатация (поддержка);
- Вывод из эксплуатации или утилизация.

Управление активами ПО

- Учет и контроль дистрибутивов ПО;
- Получение и обновление лицензий;
- Управление распределением лицензий;
- Контроль используемых лицензий;
- Отслеживание патчей и обновлений.

Управление комплексными активами

- Ведение реестра ИТ-систем;
- Ведение каталога сервисов;
- Определение Сервисно-ресурсной модели;
- Определение Финансово-ресурсной модели;
- Заключение Соглашений об уровне сервисов (SLA).

Управление финансами

- Финансовое планирование;
- Финансовые расчеты по закупке и по эксплуатации ИТ-активов;
- Обеспечение контроля и оплаты счетов;
- Управление финансовыми расчетами за предоставление ИТ-услуг согласно SLA;
- Расчёт совокупной стоимости владения ИТ-активов (TCO);
- Расчёт возврата инвестиций (ROI).

Управление контрактами

- Учёт контрактов по всем ИТ-активам;
- Учёт поставщиков;
- Согласование стоимости предполагаемой закупки ИТ-активов;
- Взаимодействие с поставщиками;
- Отслеживание контрактных обязательств;
- Контроль качества по контрактам.

Ценного из ITAM

Учёт и контроль ИТ-активов

• Эксплуатация (поддержка);
• Вывод из эксплуатации или утилизация.

Управление активами ПО

• Отслеживание патчей и обновлений.

Управление комплексными активами

• Ведение реестра ИТ-систем;
• Ведение каталога сервисов;
• Определение Сервисно-ресурсной модели;
• Определение Финансово-ресурсной модели;

Управление финансами

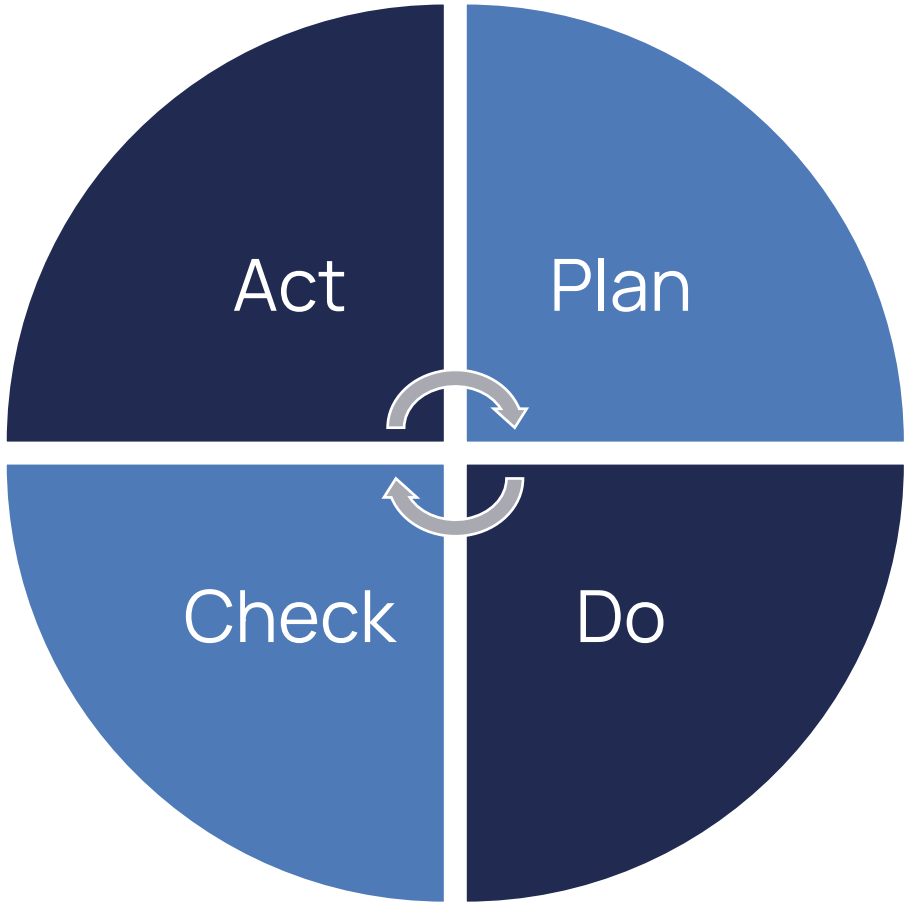
Управление контрактами

• Учёт контрактов по всем ИТ-активам;
• Контроль качества по контрактам.

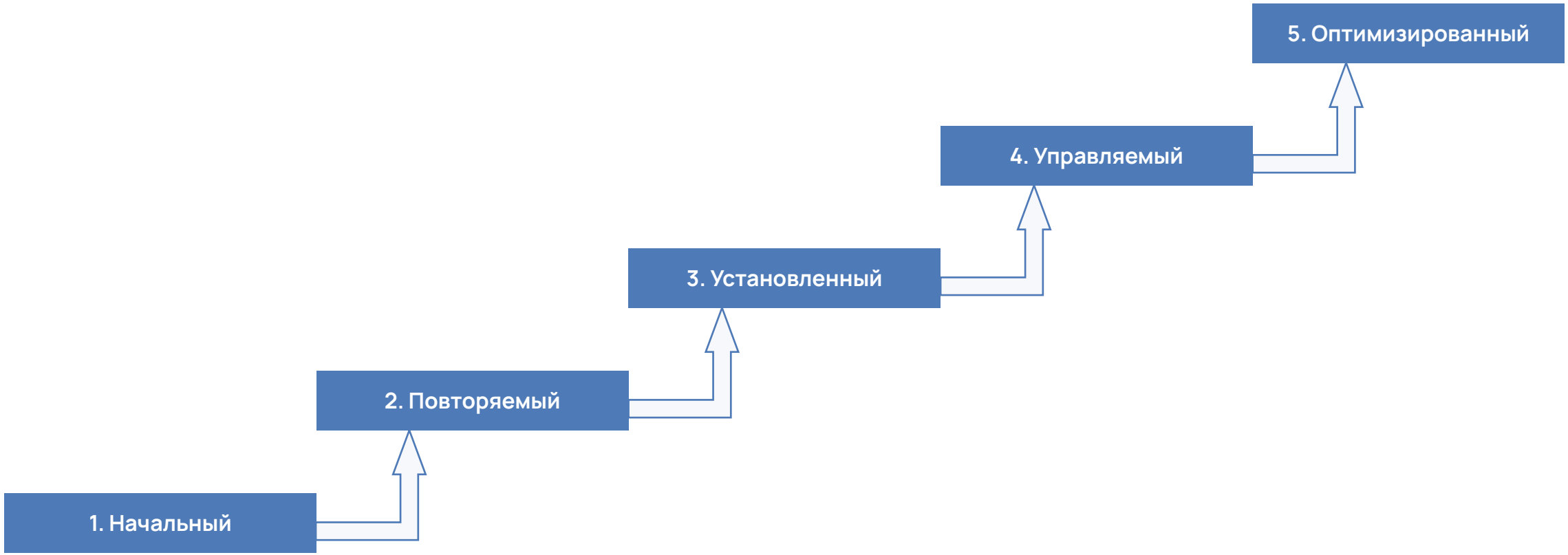
02

Процесс

Цикл Деминга-Шухарта



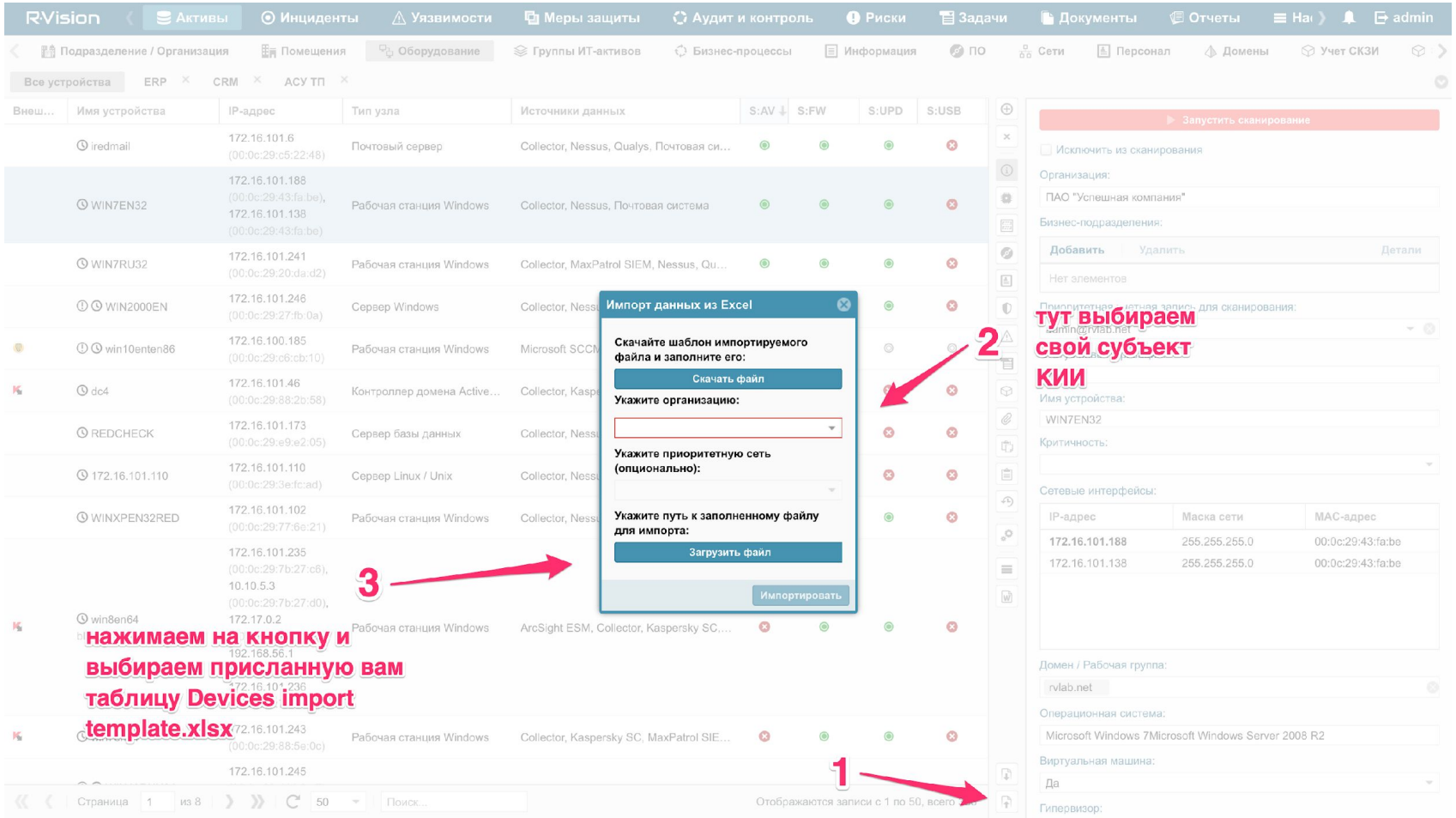
Capability Maturity Model (CMM)



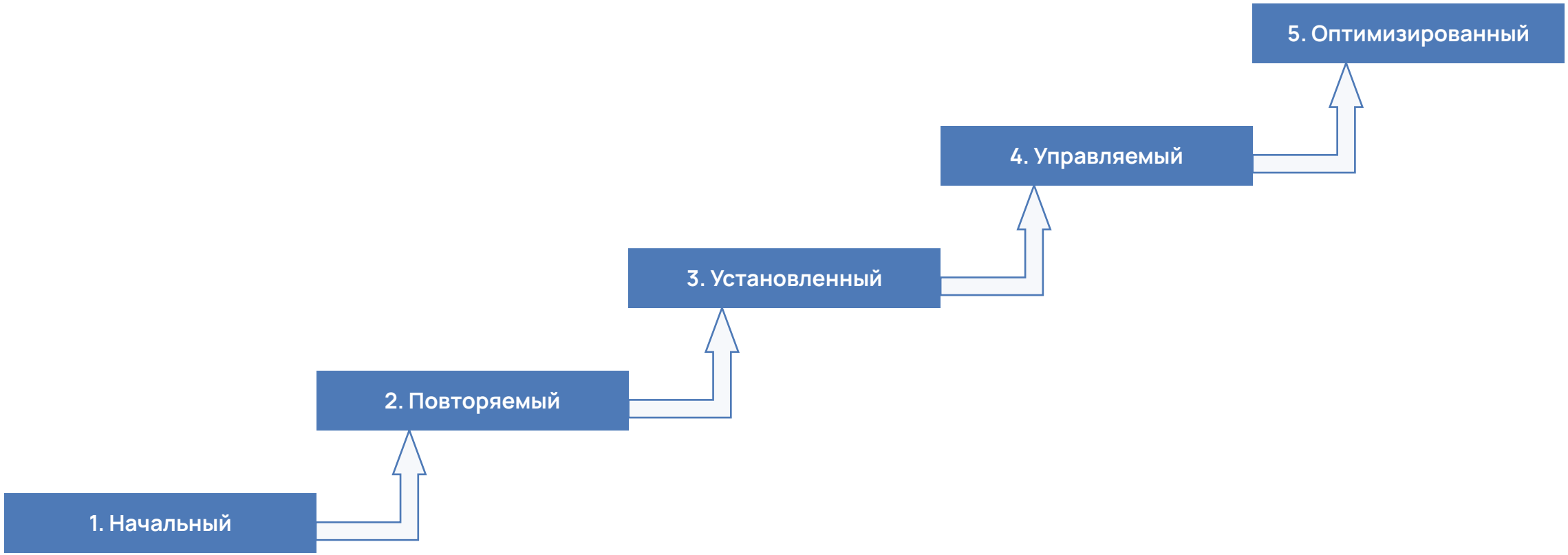
03

Пример

Откуда взялся файл?



Разбор примера



Список литературы

- ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
- ГОСТ Р 55.0.01-2014/ИСО 55000:2014 Управление активами. Национальная система стандартов. Общее представление, принципы и терминология
- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
- ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем
- CMMI® for Services, Version 1.3