



Григорий Ревенко

Руководитель отдела
технической экспертизы R-Vision
grevenko@rvision.pro

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

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
- ИТАМ – методология учёта ИТ-активов и управления ИТ-ресурсами на всём их жизненном цикле
- РСМ – 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



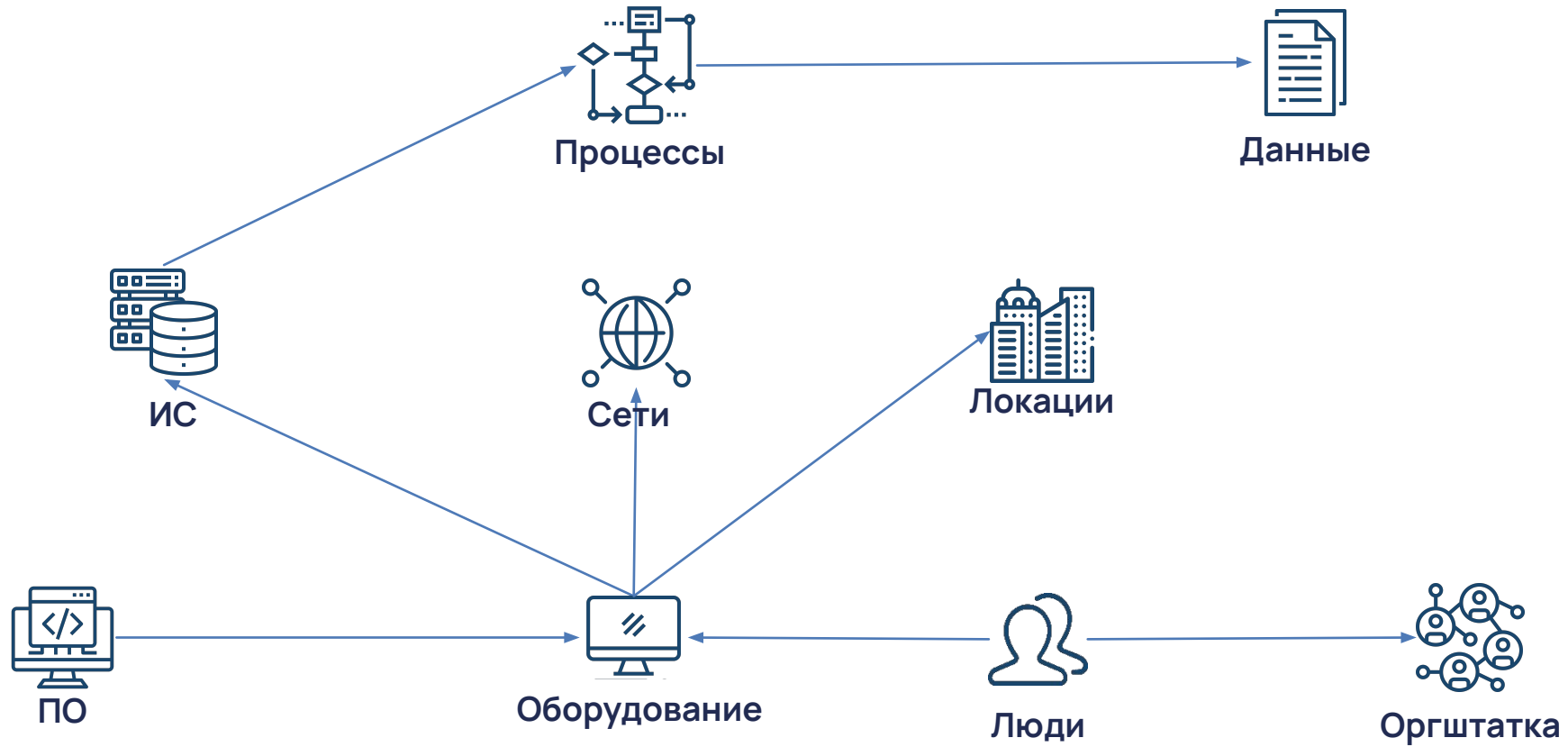
Построено
несколько SOC





Знать «Себя»

PCM



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



CYBERSECURITY

Управление комплексными активами

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

Учёт и контроль ИТ-активов

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

Управление активами ПО

- Отслеживание патчей и обновлений.

Управление финансами

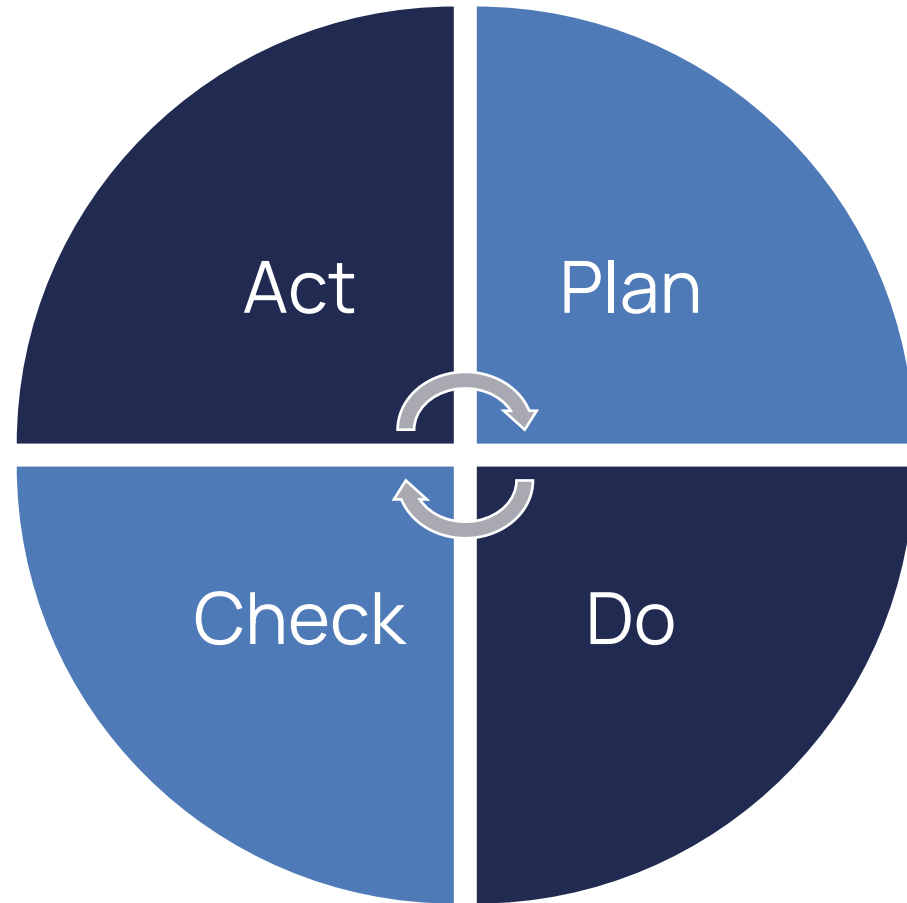
Управление контрактами

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

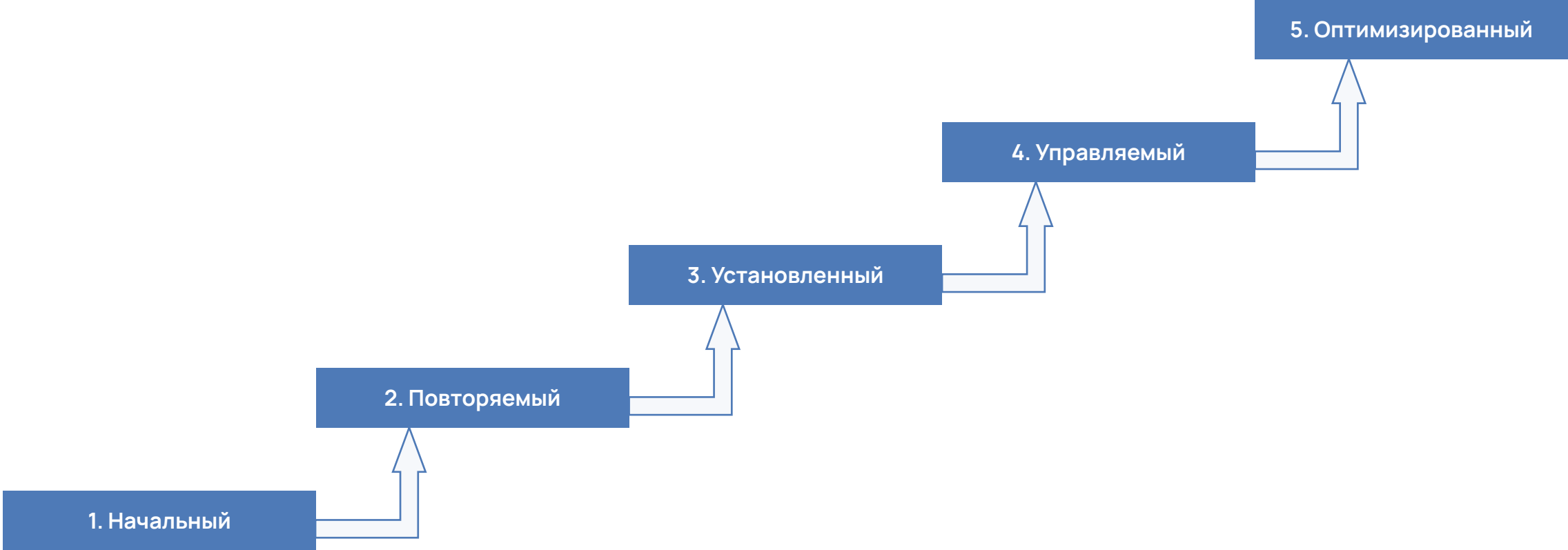
02

Процесс

Цикл Деминга-Шухарта



Capability Maturity Model (CMM)



03

Пример

Откуда взялся файл?

РVision < Активы Инциденты Уязвимости Меры защиты Аудит и контроль Риски Задачи Документы Отчеты На admin

Подразделение / Организация Помещения Оборудование Группы ИТ-активов Бизнес-процессы Информация ПО Сети Персонал Домены Учет СКЗИ

Все устройства ERP CRM АСУ ТП

Внеш...	Имя устройства	IP-адрес	Тип узла	Источники данных	S:AV	S:FW	S:UPD	S:USB
	iredmail	172.16.101.6 (00:0c:29:c5:22:48)	Почтовый сервер	Collector, Nessus, Qualys, Почтовая си...	●	●	●	✗
	WIN7EN32	172.16.101.188 (00:0c:29:43:fa:be), 172.16.101.138 (00:0c:29:43:fa:be)	Рабочая станция Windows	Collector, Nessus, Почтовая система	●	●	●	✗
	WIN7RU32	172.16.101.241 (00:0c:29:20:da:d2)	Рабочая станция Windows	Collector, MaxPatrol SIEM, Nessus, Qu...	●	●	●	✗
	WIN2000EN	172.16.101.246 (00:0c:29:27:fb:0a)	Сервер Windows	Collector, Nessus	●	●	●	✗
	win10enten86	172.16.100.185 (00:0c:29:c6:cb:10)	Рабочая станция Windows	Microsoft SCCM	●	●	●	✗
	dc4	172.16.101.46 (00:0c:29:88:2b:58)	Контроллер домена Active...	Collector, Kaspersky	●	●	●	✗
	REDCHECK	172.16.101.173 (00:0c:29:e9:e2:05)	Сервер базы данных	Collector, Nessus	●	●	●	✗
	172.16.101.110	172.16.101.110 (00:0c:29:3e:fc:ad)	Сервер Linux / Unix	Collector, Nessus	●	●	●	✗
	WINXPEN32RED	172.16.101.102 (00:0c:29:77:6a:21)	Рабочая станция Windows	Collector, Nessus	●	●	●	✗
	win8en64	172.16.101.235 (00:0c:29:7b:27:c8), 10.10.5.3 (00:0c:29:7b:27:d0), 172.17.0.2	Рабочая станция Windows	ArcSight ESM, Collector, Kaspersky SC...	●	●	●	✗
	win8en64	192.168.56.1	Рабочая станция Windows	ArcSight ESM, Collector, Kaspersky SC...	●	●	●	✗
	win8en64	172.16.101.236	Рабочая станция Windows	ArcSight ESM, Collector, Kaspersky SC...	●	●	●	✗
	win8en64	172.16.101.243 (00:0c:29:88:5e:0c)	Рабочая станция Windows	Collector, Kaspersky SC, MaxPatrol SIE...	●	●	●	✗
	win8en64	172.16.101.245	Рабочая станция Windows	Collector, Kaspersky SC, MaxPatrol SIE...	●	●	●	✗

Импорт данных из Excel

Скачайте шаблон импортируемого файла и заполните его:

Скачать файл

Укажите организацию:

Укажите приоритетную сеть (опционально):

Укажите путь к заполненному файлу для импорта:

Загрузить файл

Импортировать

3

2

1

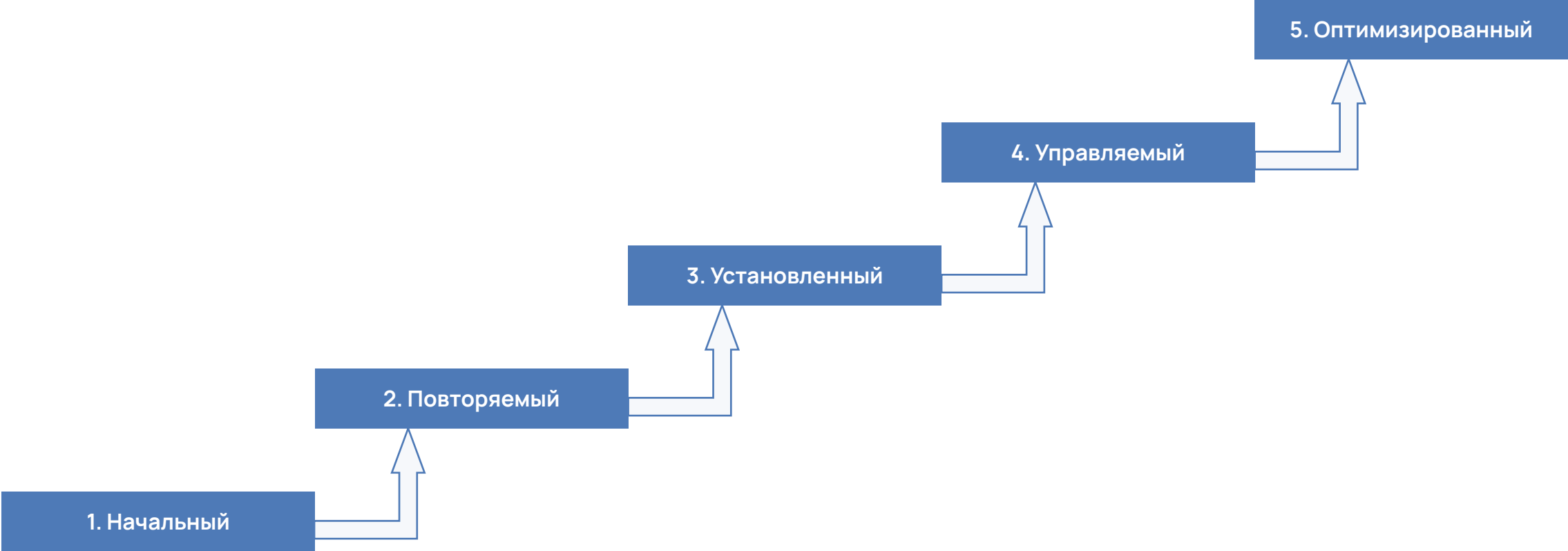
тут выбираем свой субъект КИИ

нажимаем на кнопку и выбираем присланную вам таблицу Devices import template.xlsx

нажимаем на кнопку и выбираем присланную вам таблицу Devices import template.xlsx

Отображаются записи с 1 по 50, всего 50 записей

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](#)