БЕЗОПАСНОСТЬ КИИ
И ТРЕБОВАНИЯ 187-ФЗ

УЦСБ

СУБЪЕКТЫ И ОБЪЕКТЫ КИИ

Серия вебинаров посвящена вопросам соблюдения требований законодательства в области обеспечения безопасности критической информационной инфраструктуры РФ в соответствии с Федеральным законом 187-ФЗ и его подзаконными актами. Рассматриваются как юридические, так и технические аспекты.

USSC.RU

ВЕДУЩИЙ

Алексей Комаров
Менеджер по развитию решений, УЦСБ

26.09.2018
11:00-12:00 (МСК)

УЧАСТИЕ БЕСПЛАТНОЕ

УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

Субъекты и объекты КИИ

Серия: Безопасность КИИ и требования 187-ФЗ

Главные определения, их смысловое наполнение, практические нюансы отнесения объектов и субъектов к КИИ

Вебинар,
26 сентября 2018 года

Алексей Комаров
Менеджер по развитию решений
Уральский Центр Систем Безопасности
akomarov@USSC.ru
https://ZLONOV.ru/

Серия: Безопасность КИИ и требования 187-ФЗ

- Законодательство о Безопасности КИИ
- **Субъекты и объекты КИИ**
- Дорожная карта по выполнению требований 187-ФЗ
- Практика категорирования объектов КИИ
- ГосСОПКА
- Построение системы безопасности значимых объектов КИИ
- Реализация требований по обеспечению безопасности значимых объектов КИИ в промышленности

https://www.ussc.ru/events https://youtube.com/usscpublic

Определения

$$p(x) = \sum_{i=0}^{n} a_i x^i$$

- 187-ФЗ (КИИ)
- 149-ФЗ (И, ИТ и ЗИ)

Критическая информационная инфраструктура

6) критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

- **КИИ** - **объекты КИИ**, а также **сети электросвязи**, используемые для организации **взаимодействия** таких объектов (ст. 2, 187-ФЗ)

Неправомерное воздействие на КИИ РФ

194-ФЗ

- 1. Создание, **распространение** и (или) **использование** ПО или иной компьютерной информации для неправомерного воздействия на КИИ:
  - принудительные работы до 5 лет / лишение свободы до 5 лет / штраф до 1 млн руб
- 2. **Неправомерный доступ** к информации КИИ, если он повлёк вред:
  - принудительные работы до 5 лет / лишение свободы до 6 лет / штраф до 1 млн руб
- 3. **Нарушение правил эксплуатации средств** хранения, обработки или передачи охраняемой законом информации КИИ либо правил доступа, если оно повлекло причинение вреда для КИИ:
  - принудительные работы до 5 лет / лишение свободы до 6 лет / запрет занимать должности до 3 лет

УК РФ Статья 274.1

Усиление ответственности

194-ФЗ

- 4. Группой лиц или
  с использованием служебного положения:
  - лишение свободы до 8 лет / запрет занимать должности до 3 лет
- 5. Если повлекло тяжкие последствия:
  - лишение свободы до 10 лет / запрет занимать должности до 5 лет

УК РФ Статья 274.1

Объекты КИИ

7) объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

- **Объекты КИИ** - ИС, ИТКС, АСУ субъектов КИИ (ст. 2, 187-ФЗ)

Субъекты КИИ

8) субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

- **Субъекты КИИ** - **госорганы**, **госучреждения**, российские **юрлица** и (или) **ИП**, которым на праве собственности, аренды или на ином законном основании **принадлежат ИС**, **ИТКС**, **АСУ**, функционирующие в [**перечень сфер**], российские **юрлица** и (или) **ИП**, которые **обеспечивают взаимодействие** указанных систем или сетей (ст. 2, 187-ФЗ)

Итоговое определение 1/3

- КИИ - **объекты КИИ**, а также сети электросвязи, используемые для организации их взаимодействия

Итоговое определение 2/3

- КИИ - ИС, ИТКС, АСУ **субъектов КИИ**, а также сети электросвязи, используемые для организации их взаимодействия

Итоговое определение 3/3

- КИИ - ИС, ИТКС, АСУ госорганов, госучреждений, российских юрлиц и (или) ИП, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в [перечень сфер], российских юрлиц и (или) ИП, которые обеспечивают взаимодействие указанных систем или сетей, а также сети электросвязи, используемые для организации их взаимодействия

Субъекты и объекты КИИ

СУБЪЕКТЫ*	ФОРМА ВЛАДЕНИЯ	ОБЪЕКТЫ КИИ: ЧТО ПРИНАДЛЕЖИТ	ФУНКЦИОНИРУЮЩИЕ В СФЕРЕ/ОБЛАСТИ		
ГОС. ОРГАНЫ	АРЕНДА	ИНФОРМАЦИОННЫЕ СИСТЕМЫ	ЗДРАВООХРАНЕНИЕ	ЭНЕРГЕТИКА	ПРОМЫШЛЕННОСТЬ: ОБОРОННАЯ
ГОС. УЧРЕЖДЕНИЯ	ПРАВО СОБСТВЕННОСТИ	ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ	НАУКА	БАНКОВСКАЯ И ИНЫЕ СФЕРЫ ФИН. РЫНКА	РАКЕТНО-КОСМИЧЕСКАЯ
РОС. ЮРЛИЦА			ТРАНСПОРТ	ТЭК	ГОРНО-ДОБЫВАЮЩАЯ
ИП	ИНОЕ ЗАКОННОЕ ОСНОВАНИЕ	АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ	СВЯЗЬ	АТОМНАЯ ЭНЕРГИЯ	МЕТАЛЛУРГИЧЕСКАЯ; ХИМИЧЕСКАЯ

* А ТАКЖЕ РОС. ЮРЛИЦА И (ИЛИ) ИП, КОТОРЫЕ ОБЕСПЕЧИВАЮТ ВЗАИМОДЕЙСТВИЕ УКАЗАННЫХ СИСТЕМ ИЛИ СЕТЕЙ

Все ИС, ИТС и АСУ субъекта КИИ - это объекты КИИ

Субъекты и объекты КИИ

СУБЪЕКТЫ*	ФОРМА ВЛАДЕНИЯ	ОБЪЕКТЫ КИИ: ЧТО ПРИНАДЛЕЖИТ	ФУНКЦИОНИРУЮЩИЕ В СФЕРЕ/ОБЛАСТИ		
ГОС. ОРГАНЫ	АРЕНДА	ИНФОРМАЦИОННЫЕ СИСТЕМЫ	ЗДРАВООХРАНЕНИЕ	ЭНЕРГЕТИКА	ПРОМЫШЛЕННОСТЬ: ОБОРОННАЯ
ГОС. УЧРЕЖДЕНИЯ	ПРАВО СОБСТВЕННОСТИ	ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ	НАУКА	БАНКОВСКАЯ И ИНЫЕ СФЕРЫ ФИН. РЫНКА	РАКЕТНО-КОСМИЧЕСКАЯ
РОС. ЮРЛИЦА			ТРАНСПОРТ	ТЭК	ГОРНО-ДОБЫВАЮЩАЯ
ИП	ИНОЕ ЗАКОННОЕ ОСНОВАНИЕ	АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ	СВЯЗЬ	АТОМНАЯ ЭНЕРГИЯ	МЕТАЛЛУРГИЧЕСКАЯ
					ХИМИЧЕСКАЯ

* А ТАКЖЕ РОС. ЮРЛИЦА И (ИЛИ) ИП, КОТОРЫЕ ОБЕСПЕЧИВАЮТ ВЗАИМОДЕЙСТВИЕ УКАЗАННЫХ СИСТЕМ ИЛИ СЕТЕЙ

Позиция ФСТЭК

Что такое «принадлежащих на … ином законном основании»?

Статья 209 Гражданского кодекса РФ «Содержание права собственности»

Основание	**это документ, в котором определено, что пользователь получил от владельца объекта право на его использование в течении определенного периода на условиях, установленных собственником**
Пример	**договор пользования, договор на право хозяйственного ведения, договор на право оперативного управления и т.п.**

- Собственник вправе […] другим лицам, передавать […] права владения, пользования и распоряжения имуществом. (п.2, ст.209, ГК)
- Собственник может передать свое имущество в доверительное управление другому лицу (доверительному управляющему) (п.4, ст.209, ГК)

Субъекты и объекты КИИ

СУБЪЕКТЫ*	ФОРМА ВЛАДЕНИЯ	ОБЪЕКТЫ КИИ: ЧТО ПРИНАДЛЕЖИТ	ФУНКЦИОНИРУЮЩИЕ В СФЕРЕ/ОБЛАСТИ		
ГОС. ОРГАНЫ	АРЕНДА	ИНФОРМАЦИОННЫЕ СИСТЕМЫ	ЗДРАВООХРАНЕНИЕ	ЭНЕРГЕТИКА	ПРОМЫШЛЕННОСТЬ: ОБОРОННАЯ
ГОС. УЧРЕЖДЕНИЯ	ПРАВО СОБСТВЕННОСТИ	ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ	НАУКА	БАНКОВСКАЯ И ИНЫЕ СФЕРЫ ФИН. РЫНКА	РАКЕТНО-КОСМИЧЕСКАЯ
РОС. ЮРЛИЦА			ТРАНСПОРТ	ТЭК	ГОРНО-ДОБЫВАЮЩАЯ
ИП	ИНОЕ ЗАКОННОЕ ОСНОВАНИЕ	АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ	СВЯЗЬ	АТОМНАЯ ЭНЕРГИЯ	МЕТАЛЛУРГИЧЕСКАЯ
					ХИМИЧЕСКАЯ

* А ТАКЖЕ РОС. ЮРЛИЦА И (ИЛИ) ИП, КОТОРЫЕ ОБЕСПЕЧИВАЮТ ВЗАИМОДЕЙСТВИЕ УКАЗАННЫХ СИСТЕМ ИЛИ СЕТЕЙ

АСУ

1) автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

- **АСУ** - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами (ст. 2, 187-ФЗ)

ИС и ИТКС

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

- **ИТ** - **процессы**, **методы** поиска, сбора, хранения, обработки, предоставления, распространения информации и **способы** осуществления таких процессов и методов;
- **ИС** - совокупность содержащейся в БД **информации** и обеспечивающих ее обработку **ИТ** и **техсредств**;
- **ИТКС** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. (ст.2, 149-ФЗ)

Кодекс РФ об административных правонарушениях

- **Статья 13.12**. **ч.6** Нарушение требований о защите информации (за исключением информации, составляющей гостайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ [...] влечет наложение административного штрафа
- на граждан в размере от 500 до 1 000 руб.
- на должностных лиц - от 1 000 до 2 000 руб.
- на юридических лиц - от 10 000 до 15 000 руб.

Субъекты и объекты КИИ

СУБЪЕКТЫ*	ФОРМА ВЛАДЕНИЯ	ОБЪЕКТЫ КИИ: ЧТО ПРИНАДЛЕЖИТ	ФУНКЦИОНИРУЮЩИЕ В СФЕРЕ/ОБЛАСТИ		
ГОС. ОРГАНЫ	АРЕНДА	ИНФОРМАЦИОННЫЕ СИСТЕМЫ	ЗДРАВООХРАНЕНИЕ	ЭНЕРГЕТИКА	ПРОМЫШЛЕННОСТЬ: ОБОРОННАЯ
ГОС. УЧРЕЖДЕНИЯ	ПРАВО СОБСТВЕННОСТИ	ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ	НАУКА	БАНКОВСКАЯ И ИНЫЕ СФЕРЫ ФИН. РЫНКА	РАКЕТНО-КОСМИЧЕСКАЯ
РОС. ЮРЛИЦА			ТРАНСПОРТ	ТЭК	ГОРНО-ДОБЫВАЮЩАЯ
ИП	ИНОЕ ЗАКОННОЕ ОСНОВАНИЕ	АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ	СВЯЗЬ	АТОМНАЯ ЭНЕРГИЯ	МЕТАЛЛУРГИЧЕСКАЯ
					ХИМИЧЕСКАЯ

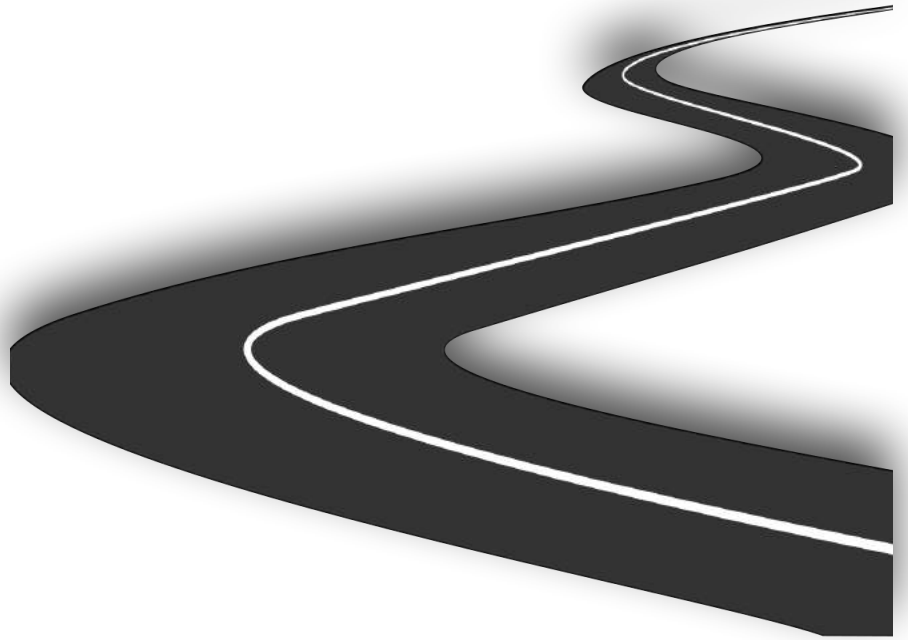
* А ТАКЖЕ РОС. ЮРЛИЦА И (ИЛИ) ИП, КОТОРЫЕ ОБЕСПЕЧИВАЮТ ВЗАИМОДЕЙСТВИЕ УКАЗАННЫХ СИСТЕМ ИЛИ СЕТЕЙ

Постановление Правительства РФ №447 от 12.04.2018

- Понятие “**информационные системы в сфере здравоохранения**” означает федеральные государственные информационные системы в сфере здравоохранения, информационные системы в сфере здравоохранения Федерального фонда обязательного медицинского страхования и территориальных фондов обязательного медицинского страхования, государственные информационные системы в сфере здравоохранения субъектов Российской Федерации, медицинские информационные системы медицинских организаций и информационные системы фармацевтических организаций.

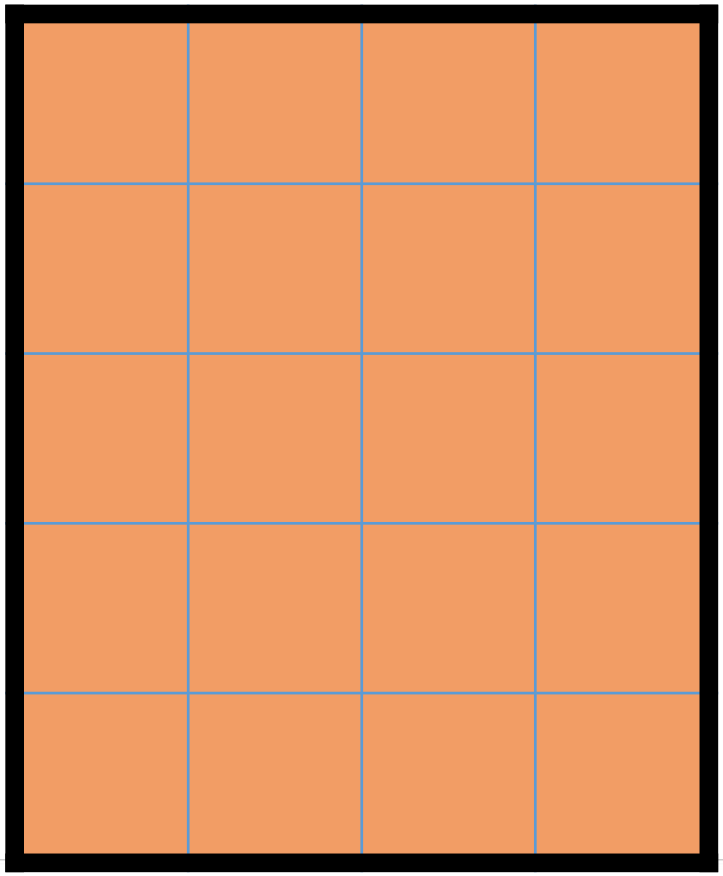
Позиция ФСТЭК

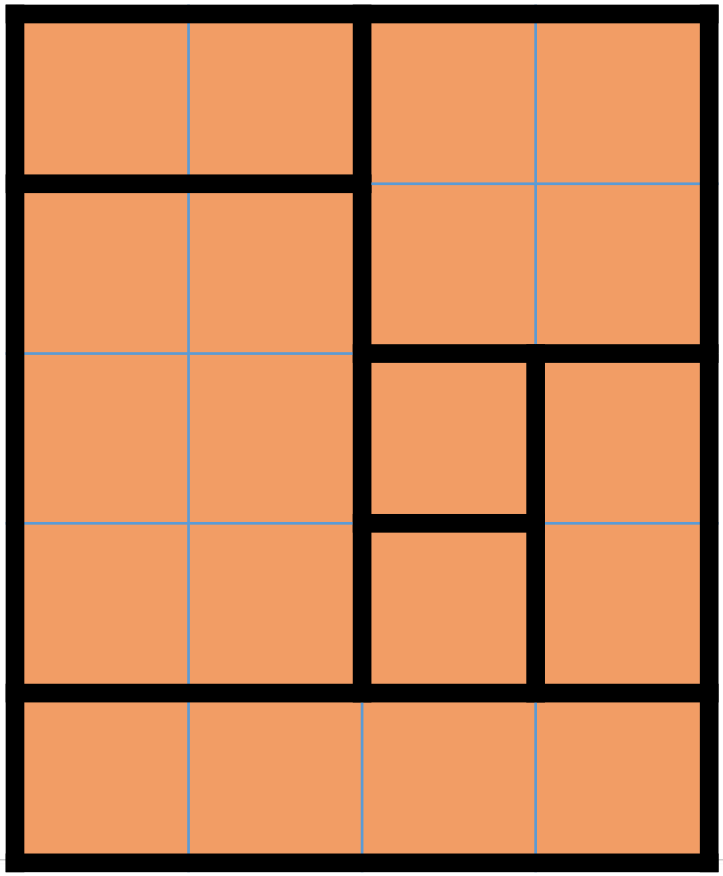
Примеры подходов



- Как бывает на практике?

Дробление объектов КИИ - снижение категории





Граница между объектам КИИ

Объект 1

Объект 2

Объект 3

Граница между объектам КИИ

Объект 1

Организационный уровень

Объект 2

Организационный уровень

Объект 3

Организационный уровень

Практика ФСТЭК - 5 сентября 2018

Перечни объектов КИИ, подлежащих категорированию, поступившие в ФСТЭК России

12

Поступило в ФСТЭК России:

- **перечни объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию, от 423 субъектов критической информационной инфраструктуры Российской Федерации**
  - **из них 7 субъектов (1,65 %) функционируют в сфере транспорта**
- **информация о 18 643 объектах критической информационной инфраструктуры Российской Федерации, подлежащих категорированию**
  - **из них 16 объектов (0,086 %) функционируют в сфере транспорта**

Практика ФСТЭК - 20 сентября 2018

Перечни объектов КИИ, подлежащих категорированию, поступившие в ФСТЭК России

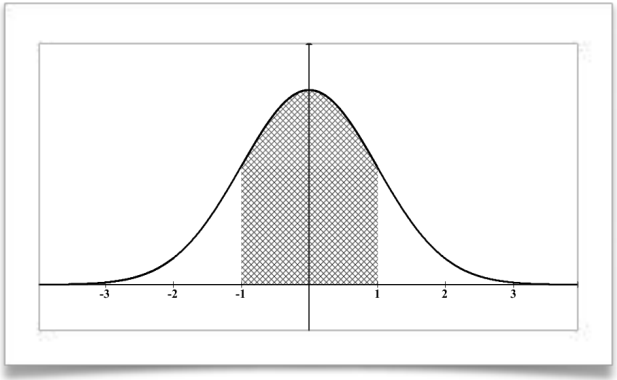
12

Поступили в ФСТЭК России:

- перечни объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию, от 482 субъектов критической информационной инфраструктуры Российской Федерации, из них
  - 6 субъектов (1,24 %) осуществляют деятельность в банковской сфере
  - 2 субъекта (0,41 %) осуществляет деятельность в иных сферах финансового рынка
- информация о 20 524 объектах критической информационной инфраструктуры Российской Федерации, подлежащих категорированию, из них
  - 47 объектов (0,229 %) функционируют в банковской сфере
  - 2 объекта (0,01 %) функционируют в иных сферах финансового рынка

Краткие статистические выводы

- 59 новых субъектов за ~2 недели
- В среднем у субъекта 43-44 объекта
  - Транспортная сфера: 2 объекта у субъекта
  - Финансовая сфера: 6 объектов у субъекта

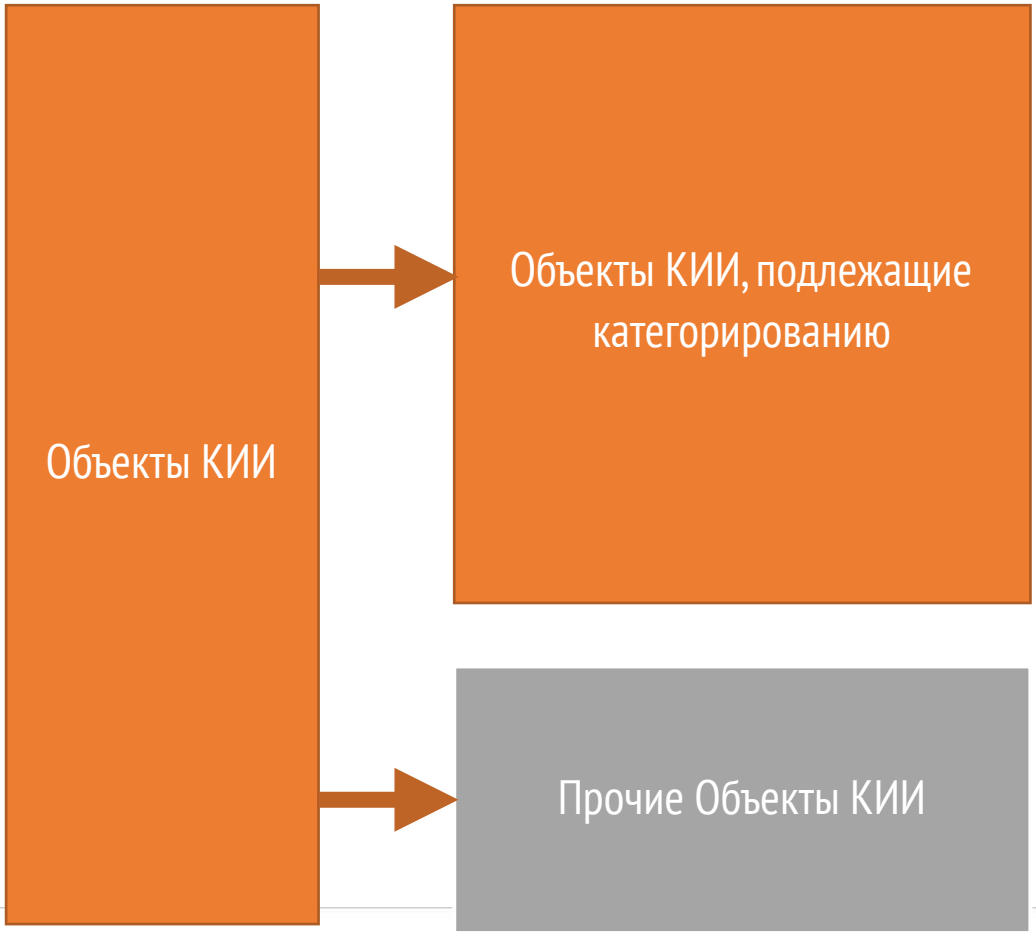


	По всем сферам			Транспорт			Банковская и фин.сферы		
Дата	Субъектов всего	Объектов всего	Объектов у субъекта	Субъектов всего	Объектов всего	Объектов у субъекта	Субъектов всего	Объектов всего	Объектов у субъекта
5/9/18	423	18 643	44	7	16	2			
20/9/18	482	20 524	43				8	49	6

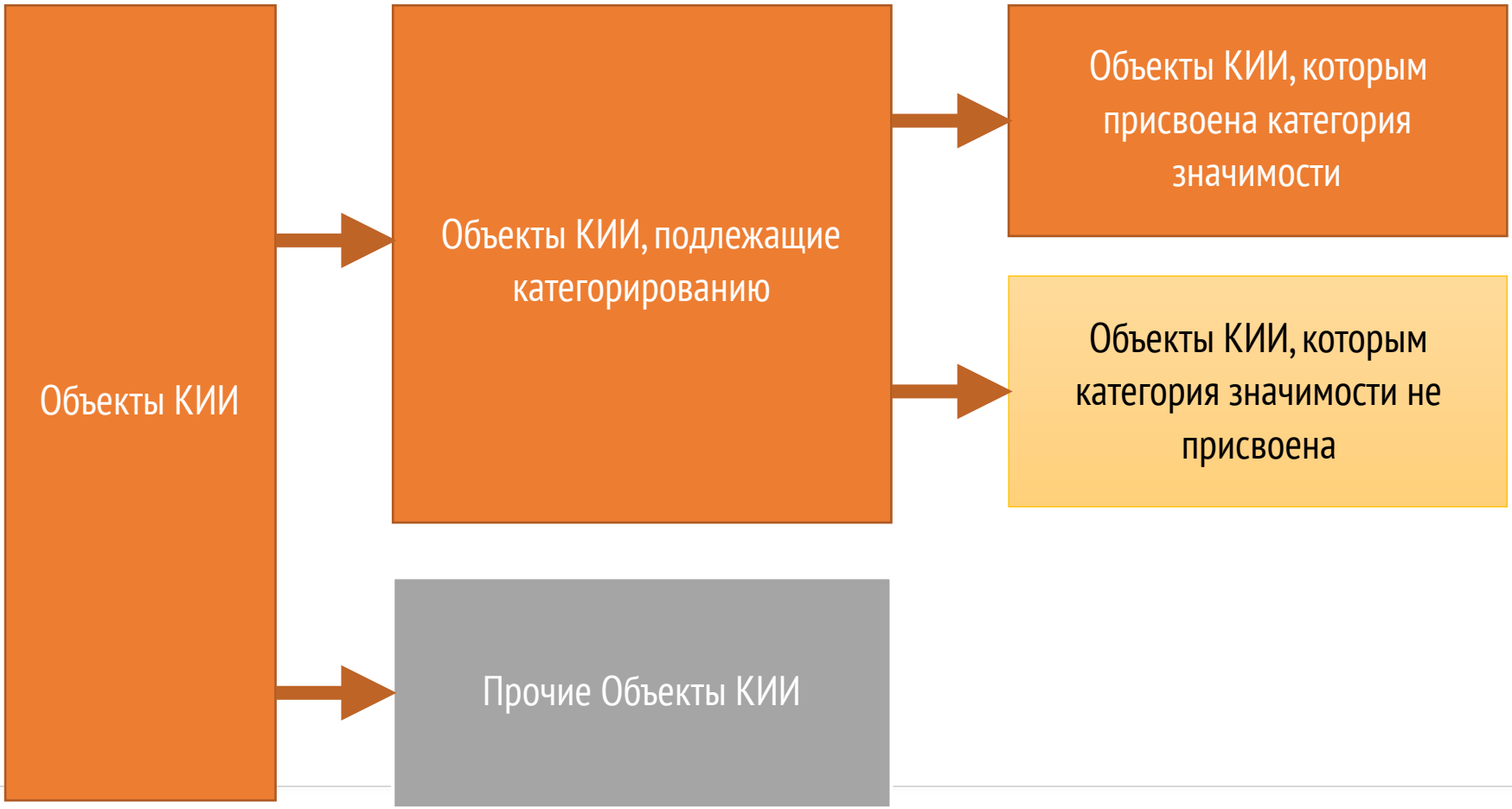
Разновидности объектов

Объекты КИИ

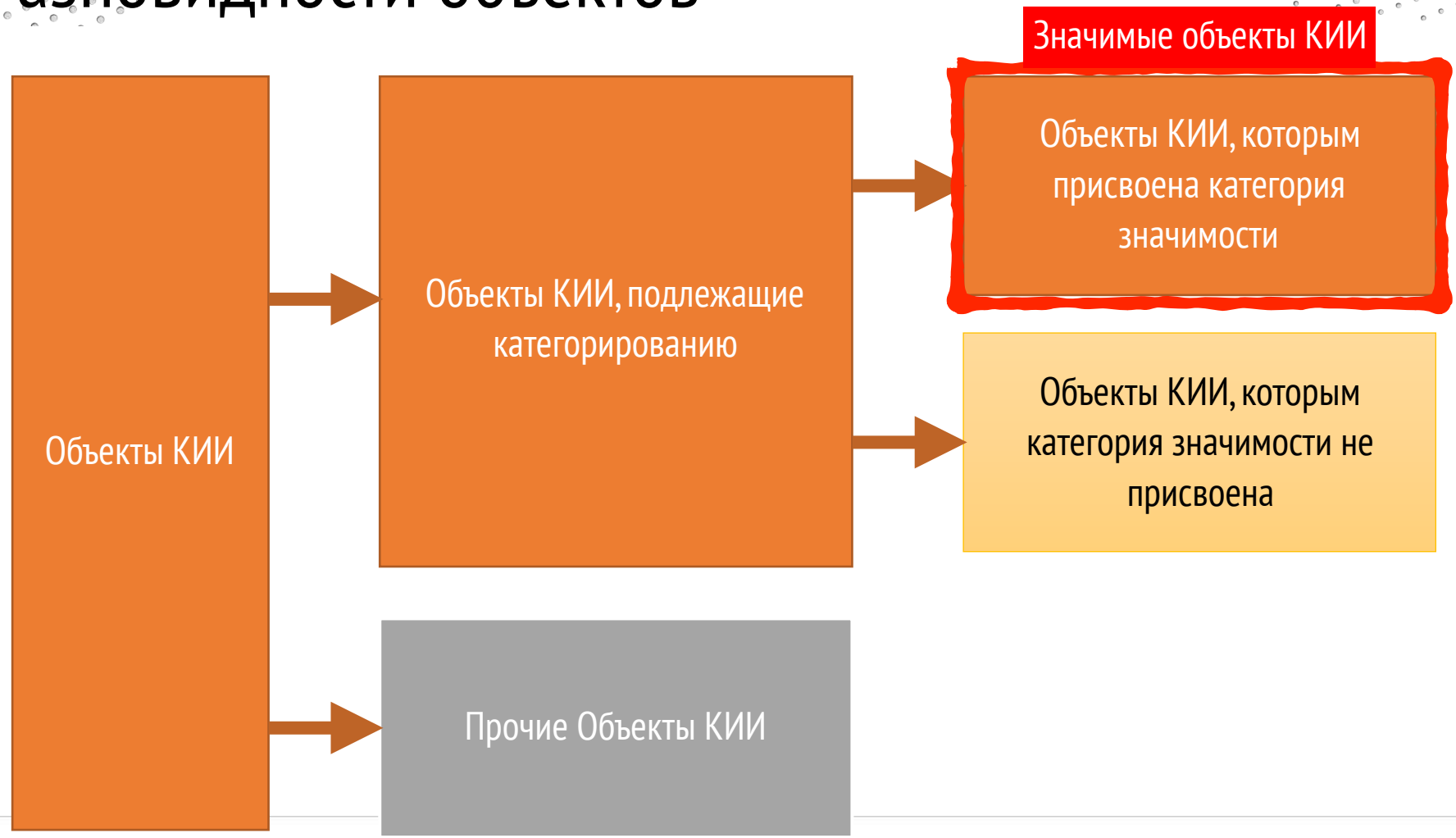
Разновидности объектов



Разновидности объектов



Разновидности объектов

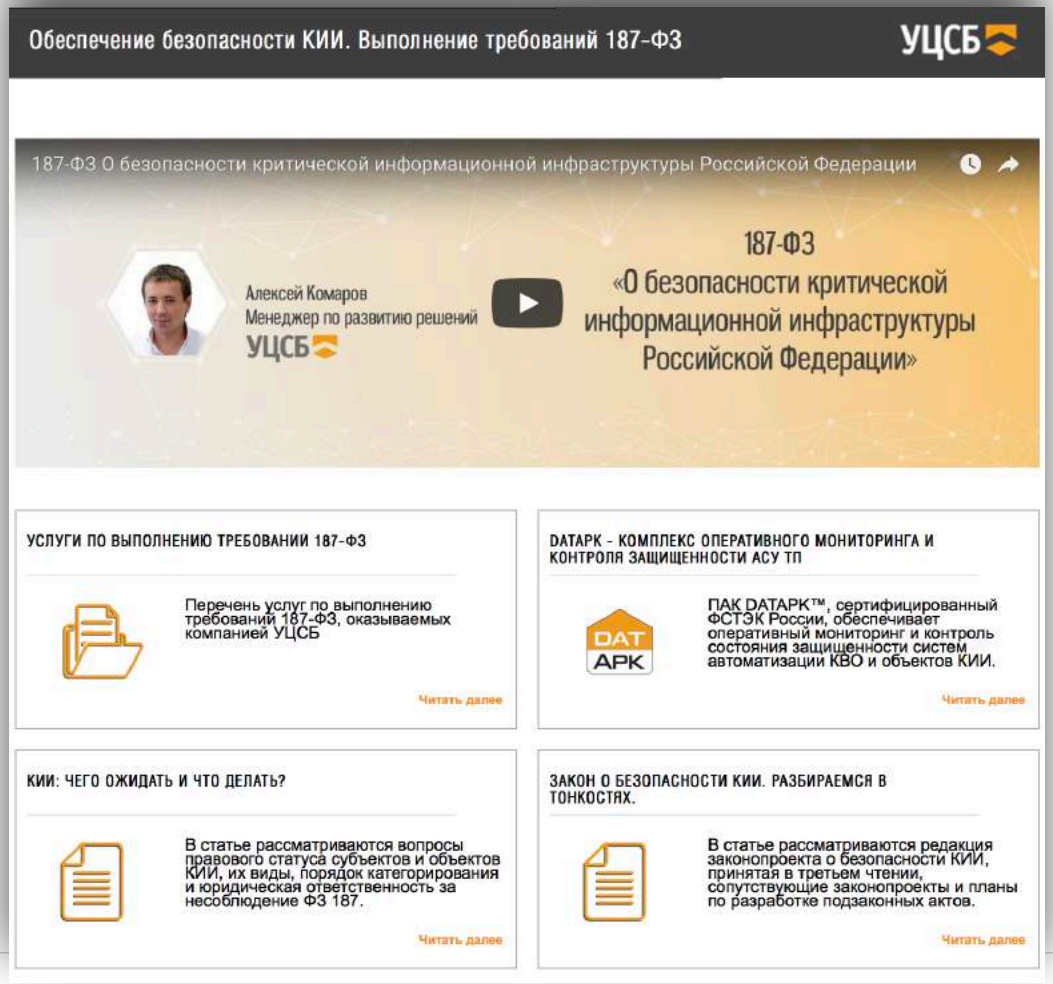


ФСТЭК: типовые ошибки

Основные источники информации

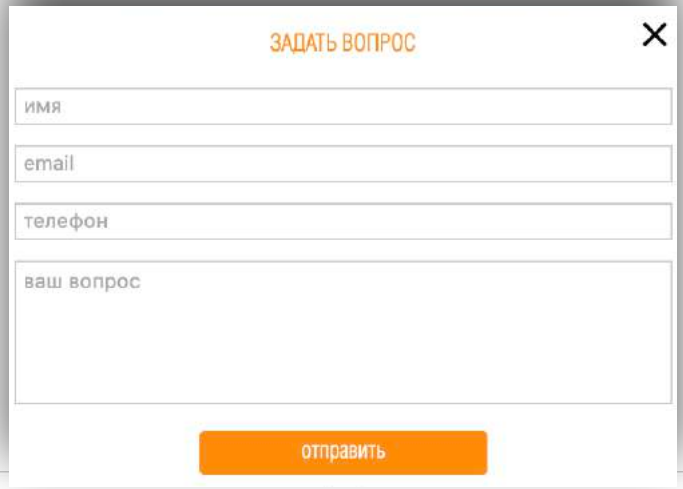
- Кого спросить?

Обеспечение безопасности КИИ. Выполнение требований 187-ФЗ

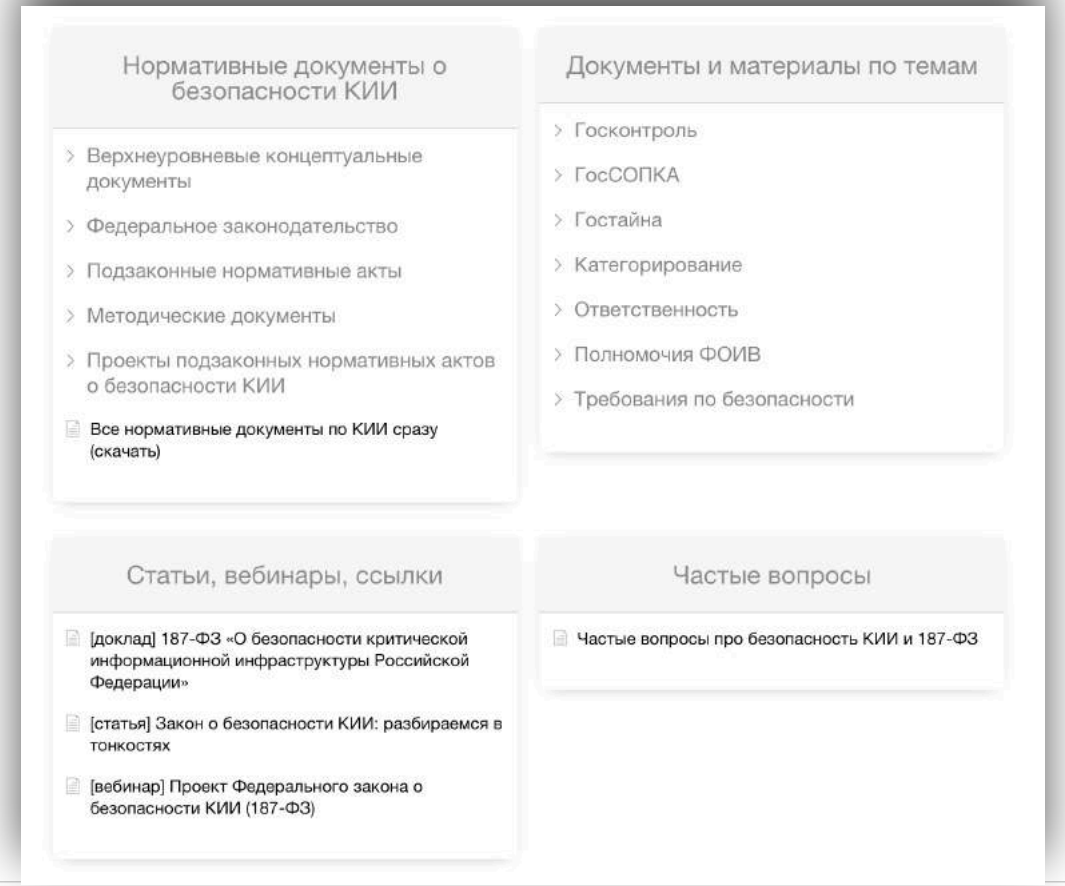


http://187.USSC.ru

http://187.УЦСБ.РФ



Раздел на сайте ZLONOV.ru



http://ZLONOV.ru/kii

Безопасность КИИ 187-ФЗ

- Обсуждение вопросов, связанных с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
  - Telegram-чат КИИ 187-ФЗ https://t.me/kii187fz
  - группа Facebook https://facebook.com/groups/kii187fz
  - группа ВКонтакте https://vk.com/kii187fz
  - Twitter https://twitter.com/kii187fz
- Форум Кибербезопасность++
  - Общение интересующихся ИБ, КБ, ЗИ и смежными темами
  - https://forum.zlonov.ru/c/kii

Спасибо! Вопросы?

Алексей Комаров
Менеджер по развитию решений
Уральский Центр Систем Безопасности

akomarov@USSC.ru
https://ZLONOV.ru