УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

#КИИ #категорирование #187-ФЗ

ИБ АСУ ТП КВО

КОНФЕРЕНЦИЯ
Информационная безопасность
АСУ ТП КВО

Москва,
27 февраля 2018 года

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

УЦСБ и ИБ АСУ ТП

- Разработка корпоративных стандартов
- **Аудиты** действующих АСУ ТП
- Проектирование, ввод в эксплуатацию и поддержка систем обеспечения ИБ АСУ ТП
- Разработка собственного решения - **DATAPK**
- **Вебинары**, семинары, курсы
- **Категорирование** объектов КИИ по 187-ФЗ

История появления 187-ФЗ

- Федеральный закон от 21.07.2011 г. №256-ФЗ «О безопасности объектов ТЭК»
- Приказ ФСТЭК России №31 от 14.03.2014 г. «Об утверждении Требований к обеспечению защиты информации в АСУ П и ТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
- «Доктрина ИБ РФ» (Утв. Указ Президента РФ от 05.12.2016 г. № 646)
- **Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности КИИ РФ»**

История появления 187-ФЗ

Безопасность КИИ. Мифы и страхи

- Информация о КИИ - **гостайна**
- **Уголовная** ответственность
- **Сроки** категорирования:
  - Перечень объектов - ~~полгода~~ сразу
  - Категорирование - год
  - Пересмотр - раз в пять лет
- ГосСОПКА - **все** обязаны установить

Отнесение к гостайне

193-ФЗ

- Перечень сведений, составляющих государственную тайну дополнить пунктом:
  - о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак

Ответственность за нарушения

194-ФЗ

- 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
- **Неправомерный доступ** к информации КИИ, если он повлёк вред:
  - принудительные работы до 5 лет / лишение свободы до 6 лет / штраф до 1 млн руб
- **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

Ответственность за нарушения - усиление

194-ФЗ

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

Кодекс РФ об административных правонарушениях

- **Статья 19.5**. **ч.1** Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего госнадзор (контроль) [...] об устранении нарушений законодательства влечет наложение административного штрафа
- на граждан в размере от 300 до 500 руб.
- на должностных лиц - от 1 000 до 2 000 руб. или дисквалификацию на срок до 3 лет
- на юрлиц - от 10 000 до 20 000 руб.

№ 187-ФЗ «О безопасности КИИ РФ» от 26.07.2017

- **критическая информационная инфраструктура** (КИИ) - **объекты КИИ**, а также сети электросвязи, используемые для организации взаимодействия таких объектов
- **объекты КИИ** - информационные **системы** (ИС), информационно-телекоммуникационные сети (ИТС), автоматизированные системы управления (АСУ) **субъектов КИИ**
- **субъектов КИИ** - госорганы, госучреждения, юрлица и (или) ИП, **которым** […] **принадлежат ИС, ИТС, АСУ, функционирующие в сфере** здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, ТЭК, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, юрлица и (или) ИП, которые обеспечивают взаимодействие указанных систем или сетей

№ 187-ФЗ «О безопасности КИИ РФ» от 26.07.2017

- **КИИ** - это информационные системы (**ИС**), информационно-телекоммуникационные сети (**ИТС**), автоматизированные системы управления (**АСУ**) **госорганов**, **госучреждений**, **юрлиц** и (или) **ИП**, **которым принадлежат ИС, ИТС, АСУ, функционирующие в сфере** здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, ТЭК, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, **юрлиц** и (или) **ИП**, которые обеспечивают взаимодействие указанных систем или сетей

Субъекты 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

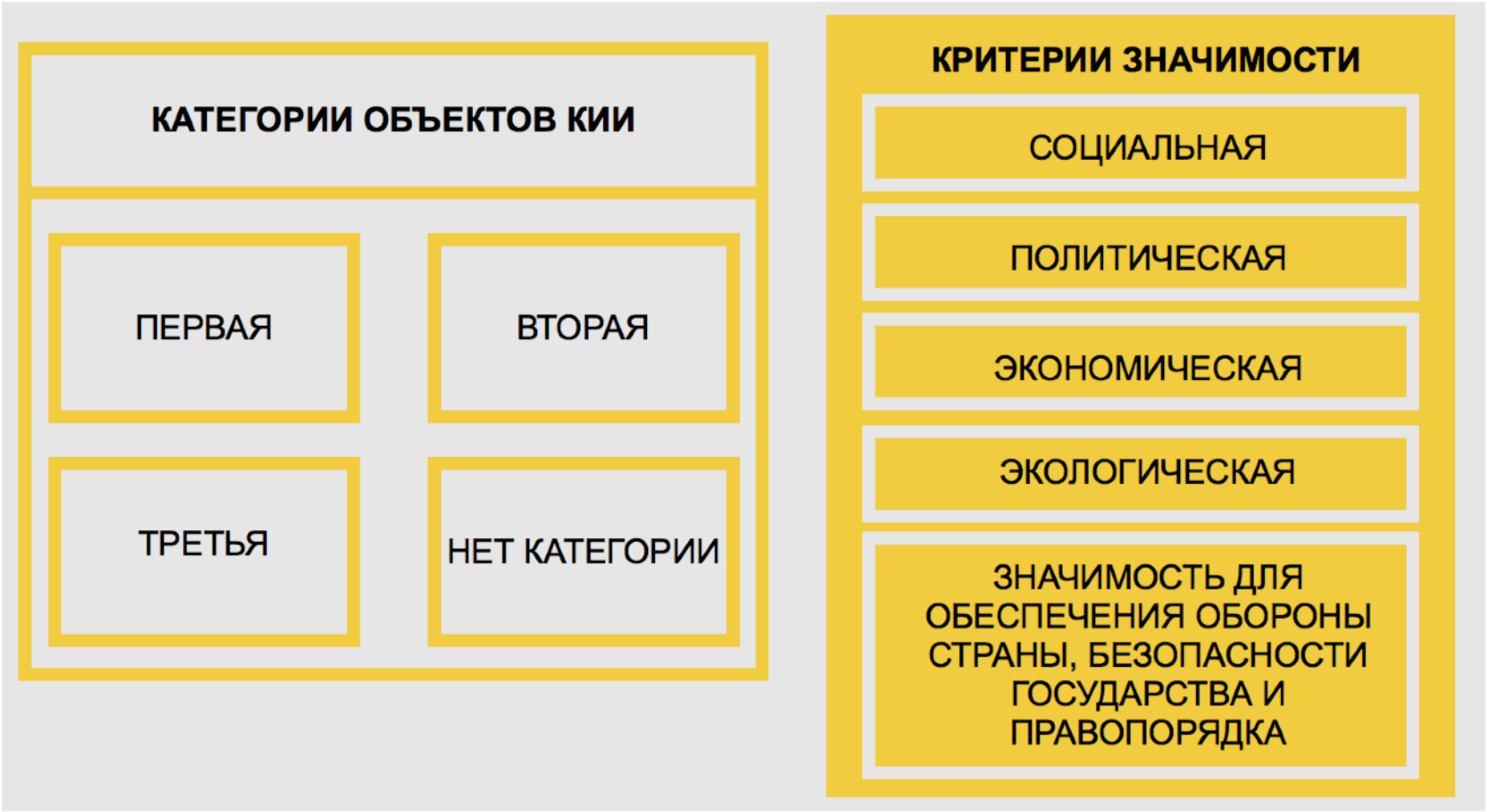
* А ТАКЖЕ РОС. ЮРЛИЦА И (ИЛИ) ИП, КОТОРЫЕ ОБЕСПЕЧИВАЮТ ВЗАИМОДЕЙСТВИЕ УКАЗАННЫХ СИСТЕМ ИЛИ СЕТЕЙ

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

Что нужно категорировать?

- Категорированию подлежат объекты КИИ, которые обеспечивают **управленческие**, **технологические**, **производственные**, **финансово-экономические** и (или) **иные процессы** в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры.
  - Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

Категорирование объектов КИИ



III категория Экономической значимости 1/3

- Возникновение ущерба субъекту КИИ, который является **госкорпорацией**, **ГУП**, **МУП**, **госкомпанией**, организацией с участием **государства** и (или) **стратегическим акционерным обществом**, **стратегическим предприятием**:

  - **5% <** снижение уровня дохода (с учетом НДС, акцизов и иных обязательных платежей) по всем видам деятельности в процентах прогнозируемого объема годового дохода по всем видам деятельности **⩽ 10%**

III категория Экономической значимости 2/3

- **Прекращение** или **нарушение** проведения клиентами **операций по банковским счетам** и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ, являющимся в соответствии с законодательством РФ системно значимой **кредитной организацией**, **оператором услуг платежной инфраструктуры** системно и (или) социально значимых платежных систем или системно значимой **инфраструктурной организацией финансового рынка**:

  - **3 млн <** среднедневное (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) **⩽ 70 млн**
  - Расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений

III категория Экономической значимости 3/3

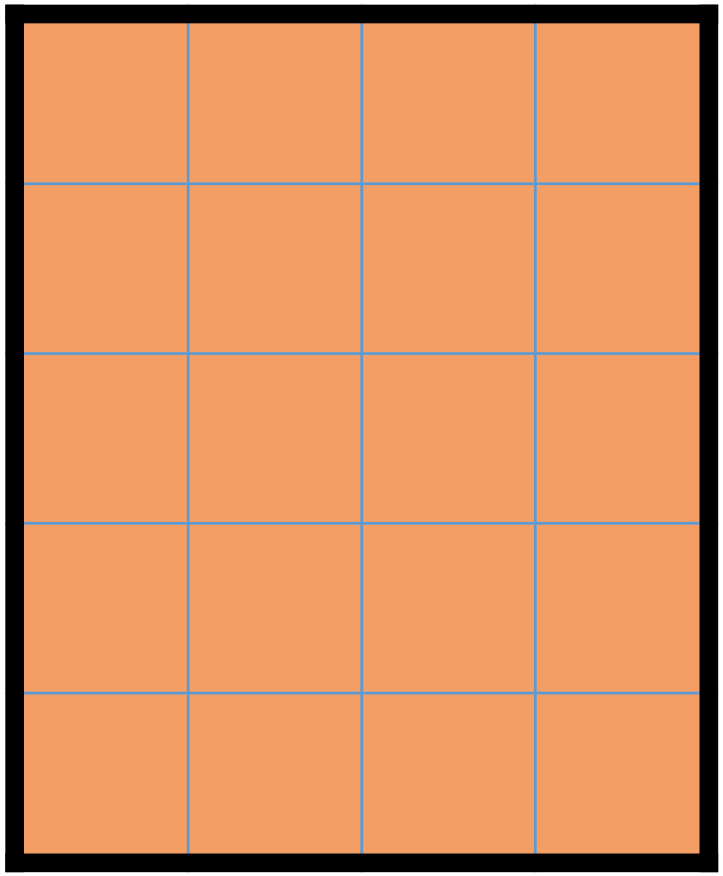
- Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении доходов (в % от прогнозируемого годового дохода бюджета)
  - 0,001% < федерального бюджета ⩽ 0,05%
  - **0,001% < бюджета субъекта Российской Федерации ⩽ 0,05%**
  - 0,01% < бюджеты государственных внебюджетных фондов ⩽ 0,5%

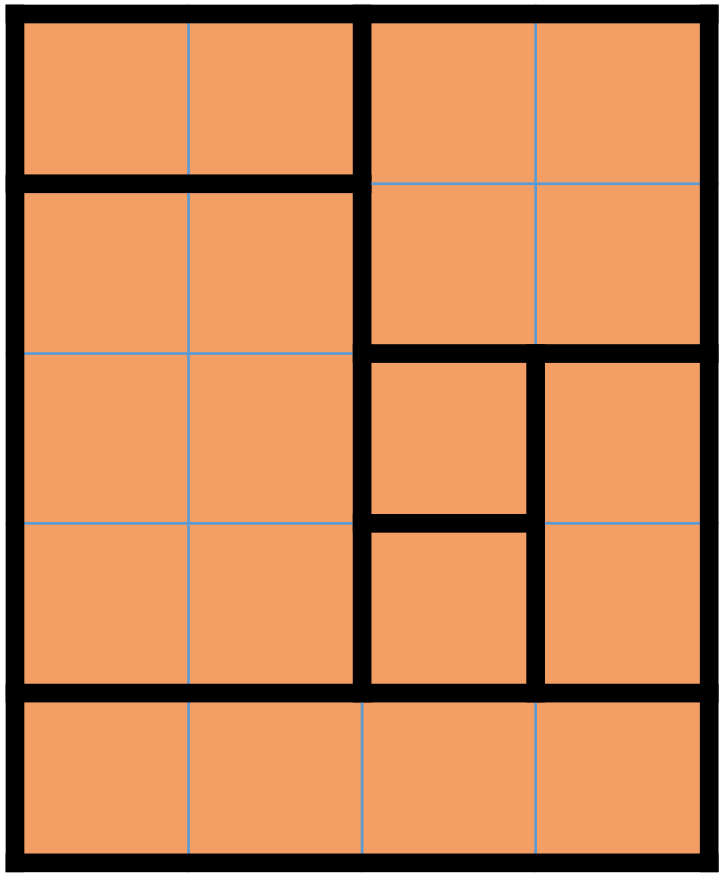
III категория Экономической значимости 3/3

- Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении доходов (в % от прогнозируемого годового дохода бюджета)
  - 0,001% < федерального бюджета ⩽ 0,05%
  - **0,001% < бюджета субъекта Российской Федерации ⩽ 0,05%**
  - 0,01% < бюджеты государственных внебюджетных фондов ⩽ 0,5%

Бюджет Свердловской области: ₽213,7 млрд	Бюджет Челябинской области: ₽119,2 млрд	Бюджет ХМАО-Югры: ₽176,79 млрд	Бюджет Пермского края: ₽115,6 млрд	Бюджет Московской области: ₽469 млрд	Бюджет Москвы: ₽2103,6 млрд

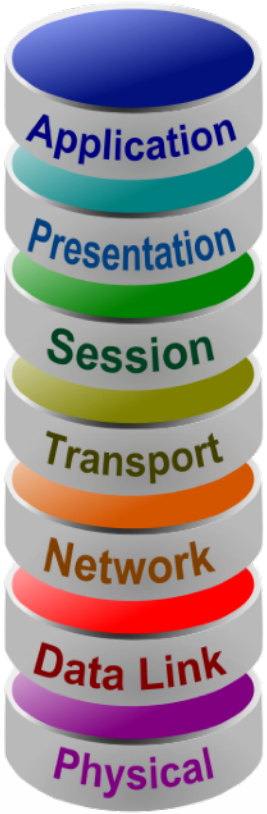
Дробление объектов КИИ - снижение категории



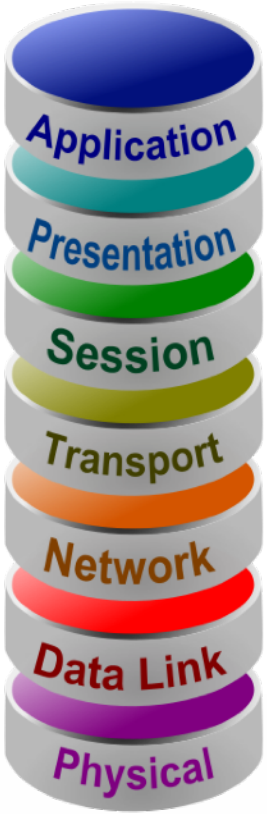


Граница между объектам КИИ

Объект 1



Объект 2

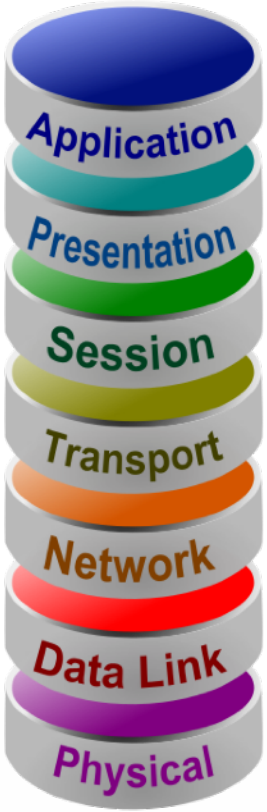


Объект 3

Граница между объектам КИИ

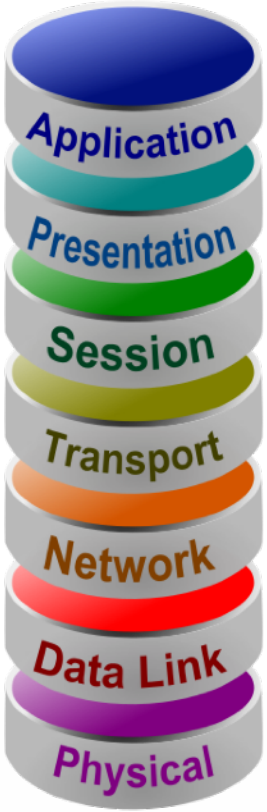
Объект 1

Организационный уровень



Объект 2

Организационный уровень



Объект 3

Организационный уровень

Два базовых сценария

- **Самостоятельное построение системы обеспечения ИБ**
  - Выбор средств и методов (и сроков реализации)
  - Объекты КИИ с низкой категорией значимости
  - Оптимизация стоимости, управление бюджетом
  - Последующая упрощённая процедура соблюдения требований

- **Принудительное выполнение требований**
  - Навязываемые подходы, состав и набор средств
  - На момент категорирования - высокая категория объектов КИИ
  - Рост стоимости из-за роста требований и цейтнота
  - Риски ответственности за несоблюдение законодательства

Требования законодательства как мотивация

Безопасность КИИ и 187-ФЗ

Нормативные документы о безопасности КИИ

- Верхнеуровневые концептуальные документы
- Федеральное законодательство
- Подзаконные нормативные акты
- Методические документы

Проекты подзаконных нормативных актов о безопасности КИИ

- Проекты документов ФСТЭК России
- Проекты документов ФСБ России
- Проекты документов Минкомсвязи России
- Готовящиеся проекты

Статьи, вебинары, ссылки

- [Статья] Закон о безопасности КИИ: разбираемся в тонкостях
- [Вебинар] Проект Федерального закона о безопасности КИИ (187-ФЗ)
- Группы и сообщества по теме Безопасности КИИ

Частые вопросы

- Частые вопросы про безопасность КИИ и 187-ФЗ

https://zlonov.ru/kii/

Спасибо! Вопросы?

Алексей Комаров
Менеджер по развитию решений
Уральский Центр Систем Безопасности

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

Категорирование, задачи 1/2

- Создаётся комиссия, возглавляемая руководителем субъекта КИИ или уполномоченным лицом, которая:
  - а) **определяет** управленческие, технологические, производственные, финансово-экономические и (или) иные **процессы** в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ;
  - б) **выявляет** наличие **критических процессов** (КрПр) у субъекта КИИ (**КрПр** - **процессы**, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка);
  - в) **выявляет объекты КИИ**, которые обрабатывают информацию, необходимую для **обеспечения выполнения КрПр**, и (или) осуществляют **управление**, **контроль** или **мониторинг КрПр**, а также готовит предложения для включения в **перечень объектов** (**ПерОб** - перечень объектов КИИ, подлежащих категорированию);

Категорирование (проект), задачи 2/2

- Создаётся комиссия, возглавляемая руководителем субъекта КИИ или уполномоченным лицом, которая:
  - г) **рассматривает** возможные **действия нарушителей** в отношении объектов КИИ инфраструктуры, а также иные **источники угроз** безопасности информации;
  - д) **анализирует угрозы безопасности** информации и **уязвимости**, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;
  - е) **оценивает масштаб возможных последствий** в случае возникновения компьютерных инцидентов на объектах КИИ;
  - ж) **устанавливает** каждому из объектов КИИ одну из **категорий значимости** либо принимает решение об **отсутствии необходимости присвоения** им категорий значимости.

История появления 187-ФЗ

Обязанности субъектов КИИ

НЕЗАМЕДЛИТЕЛЬНО ИНФОРМИРОВАТЬ О КОМПЬЮТЕРНЫХ ИНЦИДЕНТАХ

ОКАЗЫВАТЬ СОДЕЙСТВИЕ ДОЛЖНОСТНЫМ ЛИЦАМ ФСБ В ОБНАРУЖЕНИИ, ПРЕДУПРЕЖДЕНИИ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК, УСТАНОВЛЕНИИ ПРИЧИН И УСЛОВИЙ ВОЗНИКНОВЕНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

СОБЛЮДАТЬ ПРАВИЛА ЭКСПЛУАТАЦИИ ГОССОПКА (ПРИ УСТАНОВКЕ)

ВЛАДЕЛЬЦЫ ЗНАЧИМЫХ ОБЪЕКТОВ (ЗО) КИИ

СОБЛЮДАТЬ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОТ ФСТЭК

ВЫПОЛНЯТЬ ПРЕДПИСАНИЯ ДОЛЖНОСТНЫХ ЛИЦ ФСТЭК ОБ УСТРАНЕНИИ НАРУШЕНИЙ

РЕАГИРОВАТЬ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ В ПОРЯДКЕ, УТВЕРЖДЕННОМ ФСБ

ПРИНИМАТЬ МЕРЫ ПО ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК, ПРОВЕДЕННЫХ В ОТНОШЕНИИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

ОБЕСПЕЧИВАТЬ БЕСПРЕПЯТСТВЕННЫЙ ДОСТУП ДОЛЖНОСТНЫМ ЛИЦАМ ФСТЭК ПРИ ПРОВЕДЕНИИ ГОСКОНТРОЛЯ

Система безопасности значимого объекта (ЗО) КИИ

СОЗДАЕТ И ОБЕСПЕЧИВАЕТ ФУНКЦИОНИРОВАНИЕ СУБЪЕКТ КИИ

- ПРЕДОТВРАЩЕНИЕ НЕПРАВОМЕРНОГО ДОСТУПА К ИНФОРМАЦИИ, УНИЧТОЖЕНИЯ МОДИФИЦИРОВАНИЯ, БЛОКИРОВАНИЯ, КОПИРОВАНИЯ, ПРЕДОСТАВЛЕНИЯ И РАСПРОСТРАНЕНИЯ, А ТАКЖЕ ИНЫХ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ
- НЕДОПУЩЕНИЕ ВОЗДЕЙСТВИЯ НА ТЕХНИЧЕСКИЕ СРЕДСТВА ОБРАБОТКИ ИНФОРМАЦИИ, В РЕЗУЛЬТАТЕ КОТОРОГО МОЖЕТ БЫТЬ НАРУШЕНО И (ИЛИ) ПРЕКРАЩЕНО ФУНКЦИОНИРОВАНИЕ ЗО КИИ
- ВОССТАНОВЛЕНИЕ ФУНКЦИОНИРОВАНИЯ ЗО КИИ, ОБЕСПЕЧИВАЕМОГО В ТОМ ЧИСЛЕ ЗА СЧЕТ СОЗДАНИЯ И ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ НЕОБХОДИМОЙ ДЛЯ ЭТОГО ИНФОРМАЦИИ
- НЕПРЕРЫВНОЕ ВЗАИМОДЕЙСТВИЕ С ГОСУДАРСТВЕННОЙ СИСТЕМОЙ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система безопасности значимого объекта (ЗО) КИИ

СОЗДАЕТ И ОБЕСПЕЧИВАЕТ ФУНКЦИОНИРОВАНИЕ СУБЪЕКТ КИИ

ПРЕДОТВРАЩЕНИЕ НЕПРАВОМЕРНОГО ДОСТУПА К ИНФОРМАЦИИ, УНИЧТОЖЕНИЯ МОДИФИЦИРОВАНИЯ, БЛОКИРОВАНИЯ, КОПИРОВАНИЯ, ПРЕДОСТАВЛЕНИЯ И РАСПРОСТРАНЕНИЯ, А ТАКЖЕ ИНЫХ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ	НЕДОПУЩЕНИЕ ВОЗДЕЙСТВИЯ НА ТЕХНИЧЕСКИЕ СРЕДСТВА ОБРАБОТКИ ИНФОРМАЦИИ, В РЕЗУЛЬТАТЕ КОТОРОГО МОЖЕТ БЫТЬ НАРУШЕНО И (ИЛИ) ПРЕКРАЩЕНО ФУНКЦИОНИРОВАНИЕ ЗО КИИ	ВОССТАНОВЛЕНИЕ ФУНКЦИОНИРОВАНИЯ ЗО КИИ, ОБЕСПЕЧИВАЕМОГО В ТОМ ЧИСЛЕ ЗА СЧЕТ СОЗДАНИЯ И ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ НЕОБХОДИМОЙ ДЛЯ ЭТОГО ИНФОРМАЦИИ	НЕПРЕРЫВНОЕ ВЗАИМОДЕЙСТВИЕ С ГОСУДАРСТВЕННОЙ СИСТЕМОЙ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
СЗИ ОТ НСД	ШТАТНЫЕ	BACKUP	ГОССОПКА

Требования по обеспечению безопасности ЗО КИИ

ФСТЭК

УСТАНАВЛИВАЕТ ФСТЭК

ЗАВИСЯТ ОТ КАТЕГОРИИ ЗНАЧИМОСТИ

ПЛАНИРОВАНИЕ, РАЗРАБОТКА, СОВЕРШЕНСТВОВАНИЕ И ОСУЩЕСТВЛЕНИЕ ВНЕДРЕНИЯ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗО КИИ

ПРИНЯТИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗО КИИ

УСТАНОВЛЕНИЕ ПАРАМЕТРОВ И ХАРАКТЕРИСТИК ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗО КИИ