Вопросы обеспечения безопасности критической информационной инфраструктуры

г. Сургут
14 марта 2018 г.

ФЗ от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (вступил в силу с 1 января 2018 г.)

1. Нормативная база и основные понятия
2. Обязанности субъектов КИИ
3. Категорирование КИИ
4. Требования к созданию систем безопасности КИИ
5. Требования по ОБИ значимых объектов КИИ
6. Государственный контроль
7. Ответственность за нарушения

Кто попадает под действие закона

Субъекты КИИ

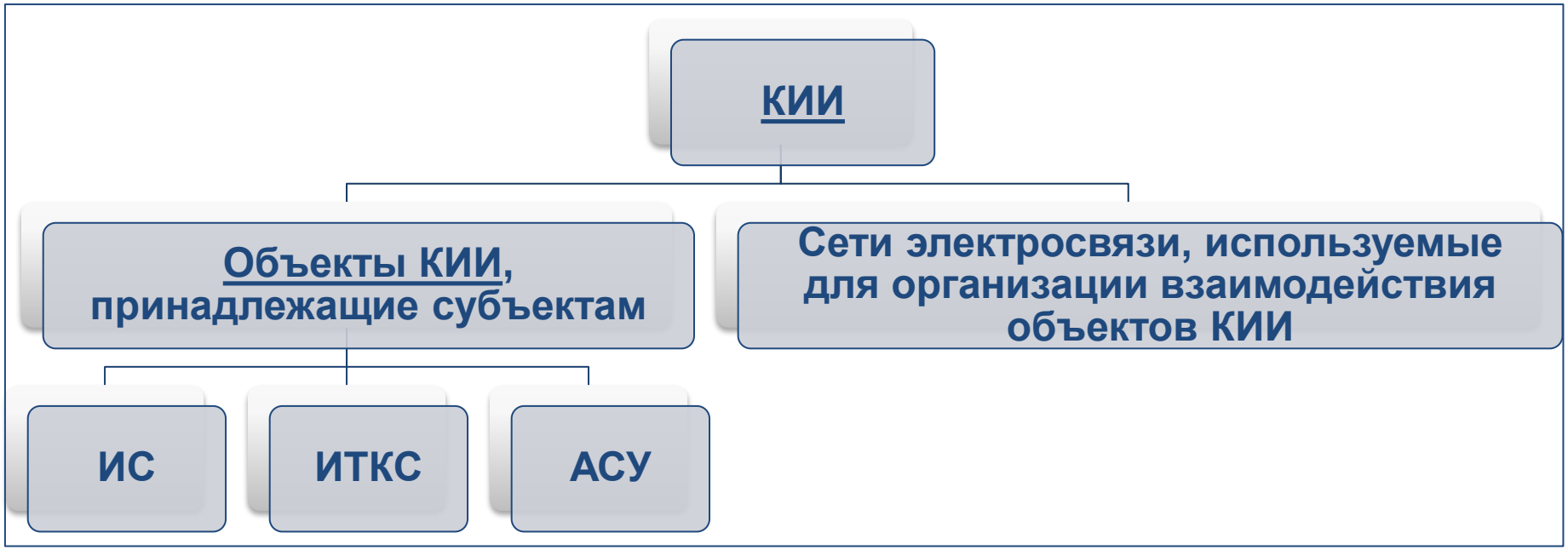
- **Госорганы**
- **Госучреждения**
- **российские ЮЛ и (или) ИП**
- **российские ЮЛ и (или) ИП, обеспечивающие взаимодействие объектов КИИ**

Владеющие на праве собственности, аренды или на ином законном основании объектами КИИ, функционирующими в сферах:

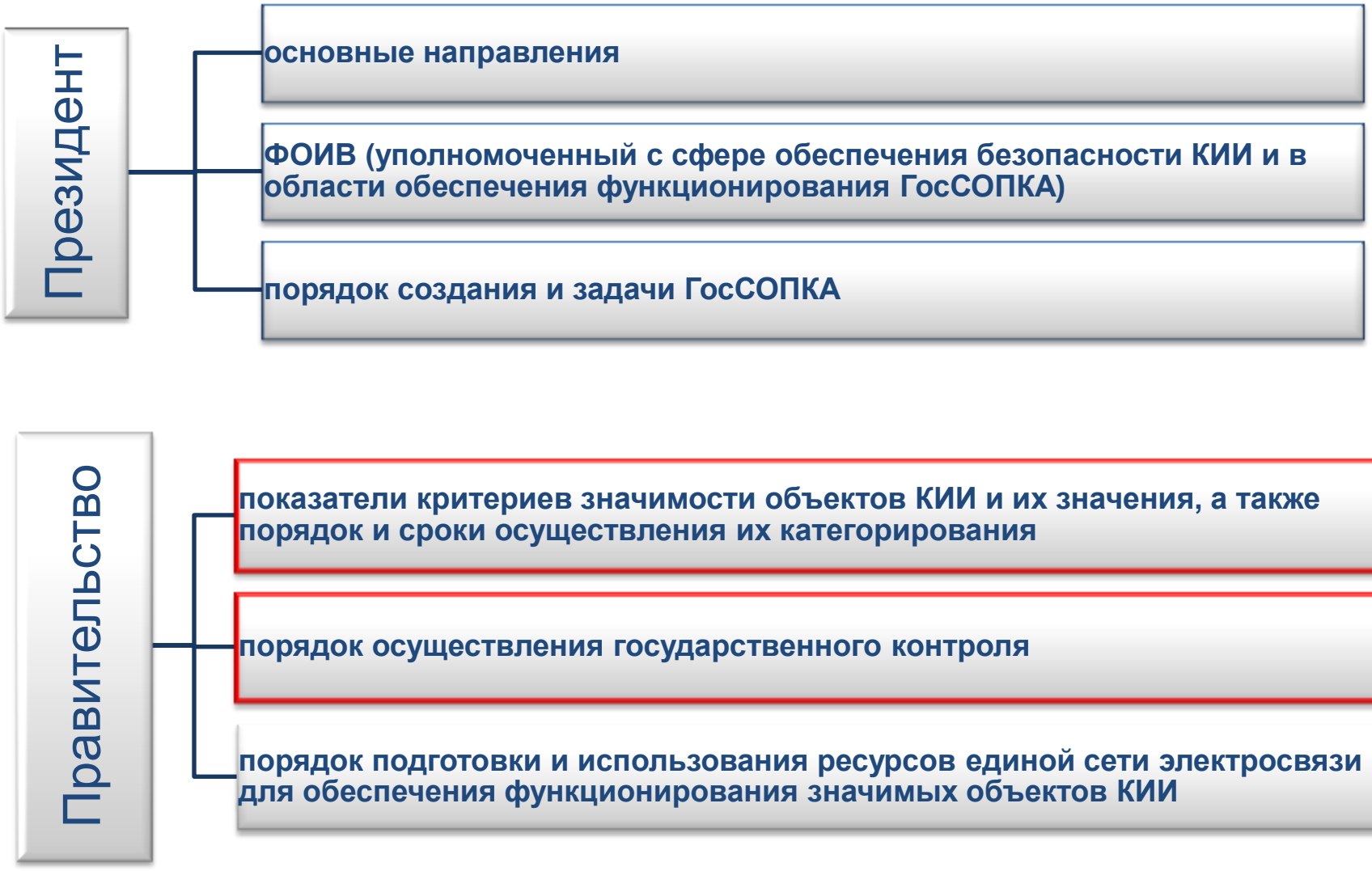
Здравоохранение	Наука	Транспорт	Связь	Энергетика

Банковская сфера и иные сферы финансового рынка	ТЭК	Атомная энергия	Промышленность (оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая)

Критическая информационная инфраструктура



Регулирование



Регулирование

ФСТЭК России

- ведет реестр значимых объектов КИИ
- устанавливает требования к созданию систем безопасности и по обеспечению безопасности значимых объектов КИИ
- осуществляет государственный контроль в области обеспечения безопасности значимых объектов КИИ

ФСБ России

- создает национальный координационный центр по компьютерным инцидентам
- утверждает порядок информирования о компьютерных инцидентах, реагирования на них, определяет состав передаваемой информации
- координирует деятельность по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак, в том числе порядок обмена информацией
- Обеспечивает установку средств ГосСОПКА, определяет требования к ним
- проводит оценку безопасности КИИ

Обязанности субъектов КИИ

Общие обязанности субъектов КИИ:

- **категорировать объекты КИИ которыми они владеют**
- незамедлительно **информировать** о компьютерных инцидентах ФСБ
- оказывать содействие должностным лицам в деятельности, связанной с предупреждением, обнаружением и ликвидацией последствий инцидентов.
- обеспечивать выполнение порядка, технических условий установки и эксплуатации технических средств ГосСОПКА (в случае установки на объектах КИИ)

Владельцы значимых объектов КИИ:

- **создать систему безопасности** в соответствии с требованиями к созданию безопасности и обеспечению их функционирования
- **соблюдать требования по обеспечению безопасности** значимых объектов КИИ;
- обеспечивать беспрепятственный доступ должностным лица ФСТЭК к значимым объектам КИИ при осуществлении государственного контроля и выполнять предписания об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ;
- **реагировать на компьютерные инциденты**, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ;

Основные моменты категорирования объектов КИИ

Осуществляется субъектами КИИ на основании порядка и критериев категорирования определенных ПП РФ от 8 февраля 2018 г. № 127.

Представляет собой установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение одной из категорий значимости, проверку сведений о результатах ее присвоения

Установлено 3 категории значимости объекта КИИ (1-3, 1 - максимальная) или принимается решение «об отсутствии необходимости присвоения ему одной из таких категорий»

Субъект сообщает во ФСТЭК о всех объектах КИИ.

Сведения о значимых объектах КИИ ФСТЭК вносит в реестр.

В случае непредставления субъектом КИИ сведений о результатах категорирования ФСТЭК направляет в адрес указанного субъекта требование о необходимости соблюдения положений ФЗ-187.

Что категорируем

Объекты КИИ (ИС, ИТКС, АСУ), обеспечивающие следующие процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ:

- управленческие
- технологические
- производственные
- финансово-экономические
- иные

Кто проводит категорирование

Создается **комиссия по категорированию**, в состав которой включаются:

- руководитель или уполномоченное им лицо
- работники, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности, и в области ИТ и связи
- специалисты по эксплуатации технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ
- работники, на которых возложены функции обеспечения безопасности (ИБ) объектов КИИ
- работники ПЗГТ (в случае, если объект КИИ обрабатывает информацию, составляющую ГТ)
- уполномоченные на решение задач в области ГО и ЧС

Порядок категорирования

Выявление критических процессов

Определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют **управление, контроль или мониторинг** критических процессов

Формирование перечня объектов КИИ

Оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ

Присвоение одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения категории значимости

Процесс категорирования объектов КИИ

Акт категорирования объектов КИИ

Содержание акта категорирования объекта КИИ

- **сведения об объекте КИИ**
- **результаты анализа угроз безопасности информации**
- **реализованные меры по обеспечению безопасности**
- **сведения о категории значимости**
- **сведения о необходимых мерах по обеспечению безопасности**

Сведения, направляемые во ФСТЭК

Состав

- об объекте КИИ;
- о субъекте КИИ;
- о взаимодействии объекта КИИ и сетей электросвязи;
- о лице, эксплуатирующем объект КИИ;
- о программных и программно-аппаратных средствах, в том числе средствах защиты информации и их сертификатах соответствия (при наличии);
- об угрозах безопасности информации и о категориях нарушителей либо об отсутствии таких угроз;
- возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ либо сведения об отсутствии таких последствий;
- о категории значимости, которая присвоена объекту КИИ, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;
- организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ, либо сведения об отсутствии необходимости применения указанных мер.

О показателях критериев значимости объектов КИИ

I. Социальная значимость	
1.	*Причинение ущерба жизни и здоровью людей (человек)*
2.	*Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения*
3.	*Прекращение или нарушение функционирования объектов транспортной инфраструктуры*
4.	*Прекращение или нарушение функционирования сети связи*
5.	*Отсутствие доступа к государственной услуге*
II. Политическая значимость	
6.	*Прекращение или нарушение функционирования госоргана*
7.	*Нарушение условий международного договора РФ, срыв переговоров или подписания договора*
III. Экономическая значимость	
8.	*Возникновение ущерба субъекту КИИ, который является госкорпорацией, ГУП, МУП, госкомпанией, организацией с участием государства и (или) стратегическим АО, стратегическим предприятием*
9.	*Возникновение ущерба бюджетам Российской Федерации*
10	*Прекращение или нарушение проведения клиентами операций по банковским счетам или операций, осуществляемых субъектом КИИ, являющимся системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка*
IV. Экологическая значимость	
11	*Вредные воздействия на окружающую среду*
V. Значимость для обеспечения обороны, безопасности государства и правопорядка	
12	*Прекращение или нарушение функционирования пункта управления (ситуационного центра)*
13	*Снижение показателей государственного оборонного заказа*
14	*Прекращение или нарушение функционирования ИС в области обеспечения обороны страны,*

Изменение/пересмотр установленной категории объектов КИИ

Изменение:

1) по мотивированному решению ФСТЭК, принятому по результатам проверки, проведенной в рамках гос. контроля;

2) объект КИИ перестал соответствовать критериям значимости и показателям их значений;

3) изменены или утрачены признаки субъекта КИИ (в связи с ликвидацией, реорганизацией субъекта КИИ и (или) изменением его организационно-правовой формы).

Пересмотр:

не реже чем один раз в 5 лет

Система безопасности значимого объекта КИИ

Создается субъектом КИИ в отношении ВСЕХ значимых объектов КИИ в соответствии с требованиями, утвержденными приказом ФСТЭК России от 21.12.2017 № 235.

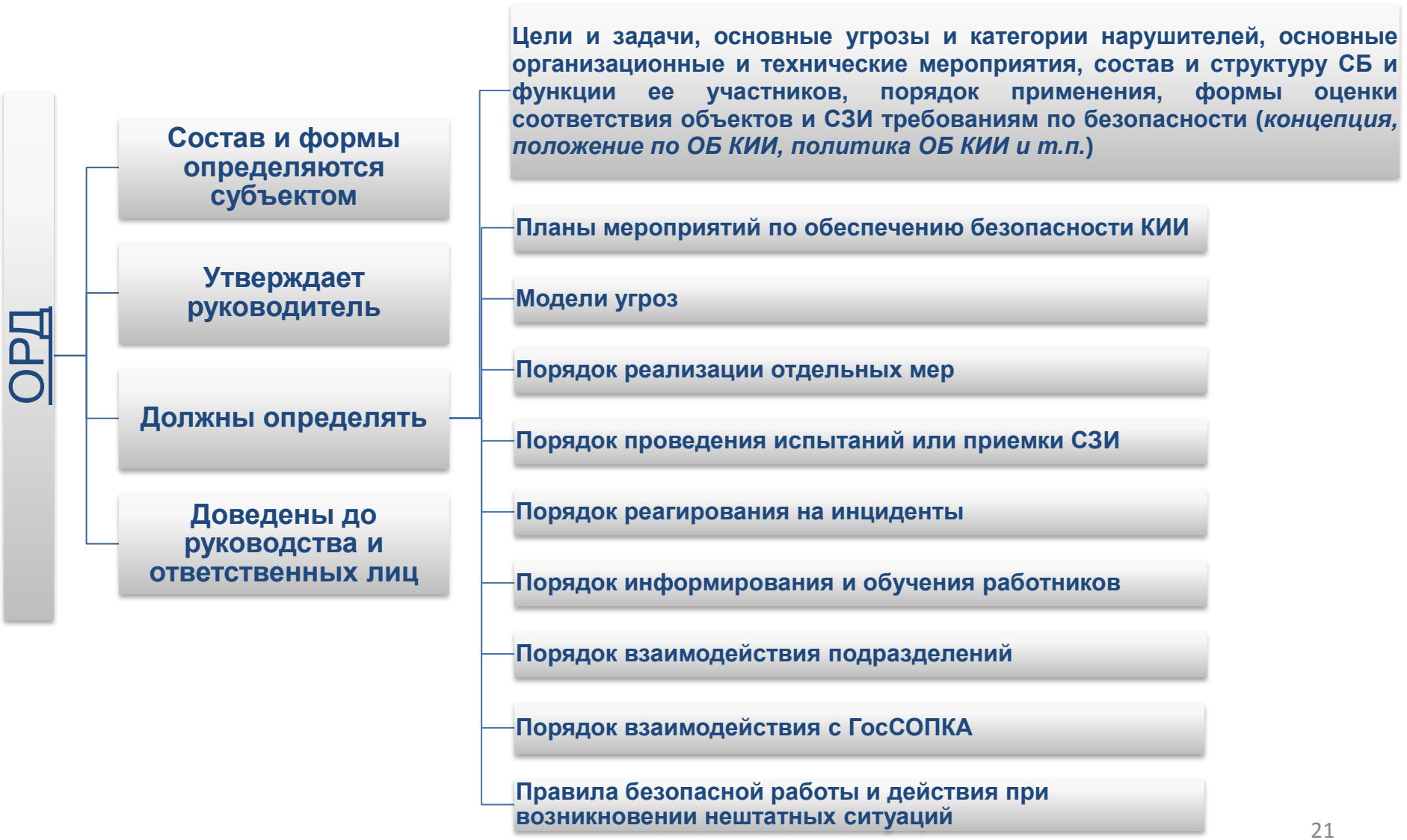
Система безопасности значимого объекта КИИ

Требования к системе безопасности значимого объекта КИИ

Требования к силам обеспечения безопасности значимого объекта КИИ

Требования к средствам обеспечения безопасности значимого объекта КИИ

Требования к организационно-распорядительным документам по безопасности значимого объекта КИИ



Требования к функционированию системы безопасности

Цикл Шухарта-Деминга (PDCA)

Особенности реализации требований по обеспечению безопасности значимых объектов КИИ

Обеспечение безопасности значимых объектов, в которых обрабатывается информация, составляющая государственную тайну

→ Законодательство РФ о государственной тайне

Обеспечение безопасности иных значимых объектов -

Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (проходит регистрацию)

- ГИС — **Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17**
- ИСПД — **Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119**
- ИТКС — **Нормативные правовые акты Минкомсвязи России**

Особенности обеспечения безопасности объектов КИИ

Анализ уязвимостей:

- на этапе ввода в эксплуатацию при анализе уязвимостей осуществляется в т.ч. **тестирование на проникновение** в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации
- допускается проведение анализа уязвимостей на макете (тестовая зона, виртуальная среда).

Форма оценки значимых объектов:

- **Аттестация** (ГИС или иные случаи в соответствии с законодательством или по решению субъекта)
- **Приемочные испытания** - комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности требованиям, а также ТЗ

Не допускаются(!):

наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе средствам зашиты информации, для обновления или управления со стороны лиц**, не являющихся работниками субъекта**

Мероприятия по обеспечению безопасности на стадиях жизненного цикла объектов КИИ

Задание требований к обеспечению безопасности

Разработка организационных и технических мер

Внедрение организационных и технических мер

Обеспечение безопасности значимого объекта в ходе его эксплуатации

Обеспечение безопасности значимого объекта при выводе его из эксплуатации

Организационные и технические меры

1) идентификация и аутентификация (ИАФ);
2) управление доступом (УПД);
3) ограничение программной среды (ОПС);
4) защита машинных носителей информации (ЗНИ);
5) аудит безопасности (АУД) – новая группа мер;
6) антивирусная защита (АВЗ);
7) предотвращение вторжений (компьютерных атак) (СОВ);
8) обеспечение целостности (ОЦЛ);
9) обеспечение доступности (ОДТ);
10) защита технических средств и систем (ЗТС);
11) защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
12) планирование мероприятий по обеспечению безопасности (ПЛН);
13) управление конфигурацией (УКФ);
14) управление обновлениями программного обеспечения (ОПО);
15) реагирование на инциденты информационной безопасности (ИНЦ);
16) обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС);
17) информирование и обучение персонала (ИПО).

Нет АНЗ, ЗСВ, РСБ.

Государственный контроль

Порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ (ПП РФ от 17 февраля 2018 г. № 162);

Плановый

- **Истечение 3 лет со дня внесения сведений об объекте КИИ в Реестр**
- **Истечение 3 лет со дня осуществления последней плановой проверки**

Внеплановый

- **Истечение срока выполнения субъектом КИИ предписания об устранении выявленного нарушения**
- **Возникновение компьютерного инцидента, повлекшего негативные последствия**
- **Поручение Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора**

Ответственность за нарушения

Статья 274.1. УК: Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Нарушение	Ответственность
Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ	принудительные работы до 5 лет / **лишение свободы до 5 лет** / штраф до 1 млн руб
Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации	принудительные работы до 5 лет / **лишение свободы до 6 лет** / штраф до 1 млн руб
Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ, или объектов КИИ, либо правил доступа к указанным информации, объектам КИИ, если оно повлекло причинение вреда КИИ	принудительные работы до 5 лет / **лишение свободы до 6 лет** / запрет занимать должности до 3 лет
Все вышеперечисленное по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения	**лишение свободы на срок от 3 до 8 лет** / лишение права занимать должности до 3 лет.
Если повлекли тяжкие последствия	**лишение свободы на срок от 5 до 10 лет** / лишение права занимать должности до 5 лет

Ответственность за нарушения

Статья 19.5. ч.1. **Кодекс РФ об административных правонарушениях**

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.

Спасибо за внимание!

ООО «Радиоэлектронные системы»

Белогородский Алексей Юрьевич, ктн
Заместитель руководителя ОСП в г. Ханты-Мансийске

+7 909 037 65 75

302@irsural.ru