Управление ФСТЭК России по Сибирскому федеральному округу

ЩЕКЛАЧЕВ
Иван Владимирович

«Система нормативных правовых актов по вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации»

Система нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры

Федеральный закон от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Нормативные правовые акты Президента Российской Федерации

- Указ Президента РФ от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085»
- Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
- Указ Президента РФ от 2 марта 2018 г. № 98 «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203»

Нормативные правовые акты Правительства Российской Федерации

- Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»
- Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»
- Проект постановления Правительства РФ «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ»

Нормативные правовые акты федеральных органов исполнительной власти

- Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ» (зарегистрирован Минюстом России 22 февраля 2018 г., рег. № 50118)
- Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости» (зарегистрирован Минюстом России 13 апреля 2018 г., рег. № 50753)
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ» (зарегистрирован Минюстом России 26 марта 2018 г., рег. № 50524)
- Приказ ФСТЭК России от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки» (зарегистрирован Минюстом России 28 декабря 2017 г., рег. № 49500)
- Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов КИИ» (зарегистрирован Минюстом России 8 февраля 2018 г., рег. № 49966)

- Приказ ФСБ России от 24 июля 2018 г. № 366 «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам»
- Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»
- Приказ ФСБ России «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах и реагирования на них»
- Приказ ФСБ России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»
- Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении порядка об обмене информации о компьютерных инцидентах между субъектами КИИ»
- Приказ Минкомсвязи России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи»
- Приказ ФСБ России «Об утверждении требований к средствам обнаружения, предупреждения и ликвидации компьютерных атак»

Указ
Президента Российской Федерации
«О Доктрине информационной безопасности Российской Федерации»
от 5 декабря 2016 г. № 646

Доктрина развивает положения Стратегии национальной безопасности в информационной сфере и определяет:

ОСНОВНЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ

- Усиление деятельности организаций, осуществляющих техническую разведку
- Возрастание масштабов компьютерной преступности в кредитно-финансовой сфере, увеличение числа преступлений, связанных с нарушений прав, свобод человека и гражданина, в том числе в части, неприкосновенности частной жизни
- Увеличение масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях
- **Рост компьютерных атак на объекты критической информационной инфраструктуры**
- Недостаточный уровень развития отечественных информационных технологий
- Недостаточное кадровое обеспечение в области информационной безопасности
- Стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Области

- Оборона страны
- Государственная и общественная безопасность
- Экономическая сфера
- Наука, технологии и образование
- Стратегическая стабильность и равноправное стратегическое партнерство

-стратегическое сдерживание и предотвращение военных конфликтов;
-совершенствование системы обеспечения информационной безопасности ВС РФ, включающей в себя силы и средства информационного противоборства;
-прогнозирование, обнаружение и оценка информационных угроз в информационной сфере;
-содействие обеспечению защиты союзников;
-нейтрализация информационно-психологического, воздействия, в том числе подрыва исторических и патриотических традиций

-противодействие использованию информационных технологий для пропаганды экстремисткой идеологии;
-пресечение деятельности, наносящей ущерб национальной безопасности, осуществляемой с использование технических средств и информационных технологий спецслужбами и организациями иностранных государств;
-повышение защищенности критической информационной инфраструктуры и устойчивого её функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидация последствий их проявления;
-повышения безопасности функционирования объектов информационной инфраструктуры,
-обеспечение защиты информации ограниченного доступа;
-нейтрализация информационных воздействий

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

26 июля 2017 г. ***№ 187-ФЗ***

О безопасности критической информационной инфраструктуры Российской Федерации

Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак

Основные понятия, используемые в 187-ФЗ:

Критическая информационная инфраструктура	объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов
Безопасность критической информационной инфраструктуры	состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак
Значимый объект критической информационной инфраструктуры	объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры

Основные понятия, используемые в 187-ФЗ:

Компьютерная атака	целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации
Компьютерный инцидент	факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки
Объекты критической информационной инфраструктуры	информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры
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,……..,российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Сферы функционирования субъектов КИИ

здравоохранение 

наука 

транспорт 

связь 

энергетика 

топливно-энергетический комплекс 

атомная энергетика 

оборонная область 

ракетно-космическая промышленность 

горнодобывающая промышленность 

металлургическая промышленность 

химическая промышленность 

банковская и иные сферы финансового рынка 

Объекты критической информационной инфраструктуры	информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года **№ 149-ФЗ**

Информационная система	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информационно-телекоммуникационная сеть	технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № **187-ФЗ**

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

Президент Российской Федерации определяет

основные направления государственной политики в области обеспечения безопасности КИИ

федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ

федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ

порядок создания и задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ

Правительство Российской Федерации устанавливает

показатели критериев значимости объектов КИИ и их значения, а также порядок и сроки осуществления их категорирования

порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ

порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Указом Президента РФ от 25 ноября 2017 г. № 569 определена **ФСТЭК России**

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности КИИ;
2) утверждает порядок ведения реестра значимых объектов КИИ;
3) утверждает форму направления сведений о результатах присвоения объектам КИИ одной из категорий значимости;
4) устанавливает требования по обеспечению безопасности значимых объектов КИИ;
5) осуществляет государственный контроль в области обеспечения безопасности значимых объектов КИИ, а также утверждает форму акта проверки

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Указом Президента РФ от 15 января 2013 г. № 31с с учетом изменений, внесенных Указом от 22 декабря 2017 г. № 620 определена **ФСБ России**

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности КИИ;
2) создает национальный координационный центр по компьютерным инцидентам;
3) координирует деятельность субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак;
4) организует и проводи оценку безопасности КИИ;
5) определяет перечень информации, представляемой в ГосСОПКУ, и порядок её представления;
6) утверждает порядок информирования о компьютерных инцидентах;
7) утверждает порядок обмена информацией о компьютерных инцидентах;
8) организует установку на значимых объектах КИИ средств ГосСОПКА;
9) устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак;
10) утверждает порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак

Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи

Федеральным законом «О связи» с учетом изменений, внесенных 193-ФЗ от 26 июля 2017 г., определена **Минкомсвязь России**

-утверждает по согласованию с ФСБ России порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации Взаимодействия объектов критической информационной инфраструктуры

Центральный Банк Российской Федерации
(в соответствии в 187-ФЗ)

-согласовывает порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятии мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ в банковской сфере и в иных сферах финансового рынка

Категорирование объекта критической информационной инфраструктуры представляет собой **установление соответствия** объекта критической информационной инфраструктуры **критериям значимости и показателям** их значений, **присвоение ему одной из категорий значимости**, **проверку сведений** о результатах ее присвоения

КРИТЕРИИ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ

- социальная значимость
- политическая значимость
- экономическая значимость
- экологическая значимость
- значимость для обеспечения обороны страны, безопасности государства и правопорядка

3

категории значимости объектов КИИ

Основания для изменения присвоенной категории значимости объекта КИИ

по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ РФ, принятому **по результатам проверки**, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ

изменения значимого объекта КИИ, в результате которого такой объект **перестал соответствовать критериям значимост**и и показателям их значений, на основании которых ему была присвоена определенная категория значимости

ликвидация, реорганизация субъекта КИИ и (или) изменение его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта КИИ

Права субъектов КИИ

1) получать информацию, необходимую для обеспечения безопасности значимых объектов КИИ

2) получать информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения

3) за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

4) разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта КИИ

Субъекты КИИ обязаны:

1) незамедлительно информировать о компьютерных инцидентах

2) оказывать содействие должностным лицам в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов

3) в случае установки на объектах КИИ средств, предназначенных для ОПЛКА и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность

Субъекты КИИ имеющие значимые объекты КИИ также обязаны:

1) соблюдать требования по обеспечению безопасности значимых объектов КИИ

2) выполнять предписания должностных лиц, об устранении нарушений требований по обеспечению безопасности значимого объекта КИИ

3) реагировать на компьютерные инциденты, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ

4) обеспечивать беспрепятственный доступ должностным лицам к значимым объектам КИИ при реализации этими лицами полномочий

Субъект КИИ создает систему безопасности значимого объекта КИИ

ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ

предотвращение неправомерного **доступа к информации**, обрабатываемой значимым объектом КИИ, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации

недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта КИИ

восстановление функционирования значимого объекта КИИ

непрерывное взаимодействие с государственной системой ОПЛКА на информационные ресурсы Российской Федерации

Требования по обеспечению безопасности значимых объектов КИИ (в зависимости от категории значимости)

утверждает

ФОИВ, уполномоченный в области обеспечения безопасности КИИ РФ

Требования предусматривают

- планирование, разработку, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности
- принятие организационных и технических мер для обеспечения безопасности
- установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности

Субъекты КИИ

данные от установленных средств ОПЛКА

информация от субъектов КИИ

ФОИВ, уполномоченный в области ОБКИИ РФ

информация в соответствии с перечнем и порядком предоставления

сведения по итогам госконтроля

Результаты оценки безопасности

Иные организации, в том числе: иностранные и международные

информация в соответствии с перечнем и порядком предоставления

Проводит оценку ФОИВ, уполномоченный в области ОПЛКА на ИР РФ на основе анализа

Изменения в законодательных актах в связи с принятием ФЗ-187

УК РФ → Введена ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

УПК РФ → Определена подследственность по уголовным делам за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации – ФСБ России

«Закон о гостайне» → Определено, что сведения о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак составляют государственную тайну

ФЗ-294 → Определено, что порядок установленный настоящим Федеральным законом, в части организации и проведения проверок, не применяется при осуществлении государственного контроля в области ОБ КИИ

ФЗ «О связи» → Определено, что:

-порядок подготовки и использования ресурсов единой сети электросвязи для обеспечения функционирования значимых объектов КИИ утверждается Правительством РФ;

-операторы связи в случае установки в сети электросвязи, используемой для организации взаимодействия объектов КИИ, средств, предназначенных для поиска признаков компьютерных атак обязаны обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств и их сохранность

Постановление
Правительства Российской Федерации
от 8 февраля 2018 г. № 127

«Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

Подготовлено в соответствии с пунктом 1 части 2 статьи 6 Федерального закона № 187-ФЗ

Утверждает:

- Правила категорирования объектов КИИ РФ
- Перечень показателей критериев значимости объектов КИИ РФ и их значения

Правила категорирования объектов КИИ РФ

Категорирование объектов КИИ – осуществляется субъектами КИИ в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов КИИ функционирующих в соответствующих сферах

Кто является субъектом КИИ?

Общероссийский классификатор видов экономической деятельности

Лицензии и иные разрешительные документы на различные виды деятельности

Уставы , положения организаций (государственных органов)

……

Приказ Росстандарта от 31.01.2014 №14-ст

Федеральные законы,Законы: 99-ФЗ, 170-ФЗ, 395-1, 325-ФЗ, 39-ФЗ, 1565-ФЗ, 75-ФЗ, 5663-1, 35-ФЗ, 2395-1, 323-ФЗ

Правила категорирования объектов КИИ РФ

Правила категорирования объектов КИИ РФ

Комиссия по категорированию

Создается решением руководителя субъекта КИИ

руководитель субъекта КИИ или уполномоченное им лицо

работники субъекта КИИ, являющиеся специалистами в области выполняемых функций, осуществляемых видов деятельности, в области информационных технологий и связи, по эксплуатации основного технологического оборудования, работники субъекта КИИ, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов КИИ

работники субъекта КИИ, на которых возложены функции обеспечения безопасности объектов КИИ

работники подразделения по защите государственной тайны субъекта КИИ

работники структурного подразделения по ГО и ЧС или работники, уполномоченные на решение задач в этой области

В состав <u>могут</u> включаться представители гос. органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, <u>по согласованию с ними</u>.

Правила категорирования объектов КИИ РФ

Правила категорирования объектов КИИ РФ

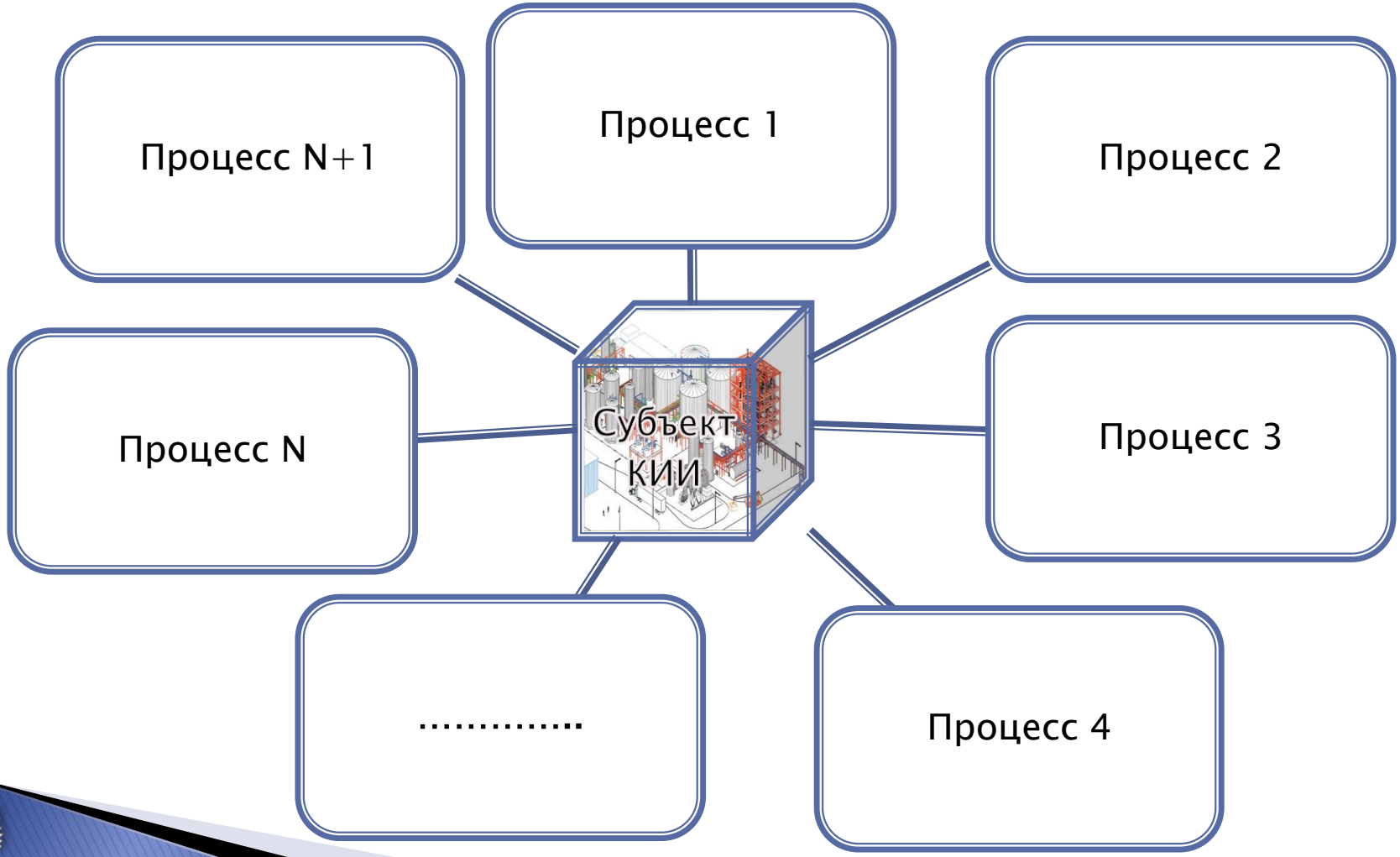
Исходные данные для категорирования:	сведения об объекте КИИ
	процессы в рамках выполнения функций субъекта КИИ
	состав информации, обрабатываемой объектами КИИ, сервисы предоставляемые объектами КИИ
	декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения, паспорт объекта ТЭК, на которых функционирует объект КИИ, *если их разработка предусмотрена законодательством Российской Федерации*
	сведения о взаимодействии объекта КИИ с другими объектами КИИ
	угрозы безопасности информации, а также данные о компьютерных инцидентах, произошедших ранее на объектах КИИ данного типа

Правила категорирования объектов КИИ РФ

Категорированию подлежат объекты КИИ, обеспечивающие процессы

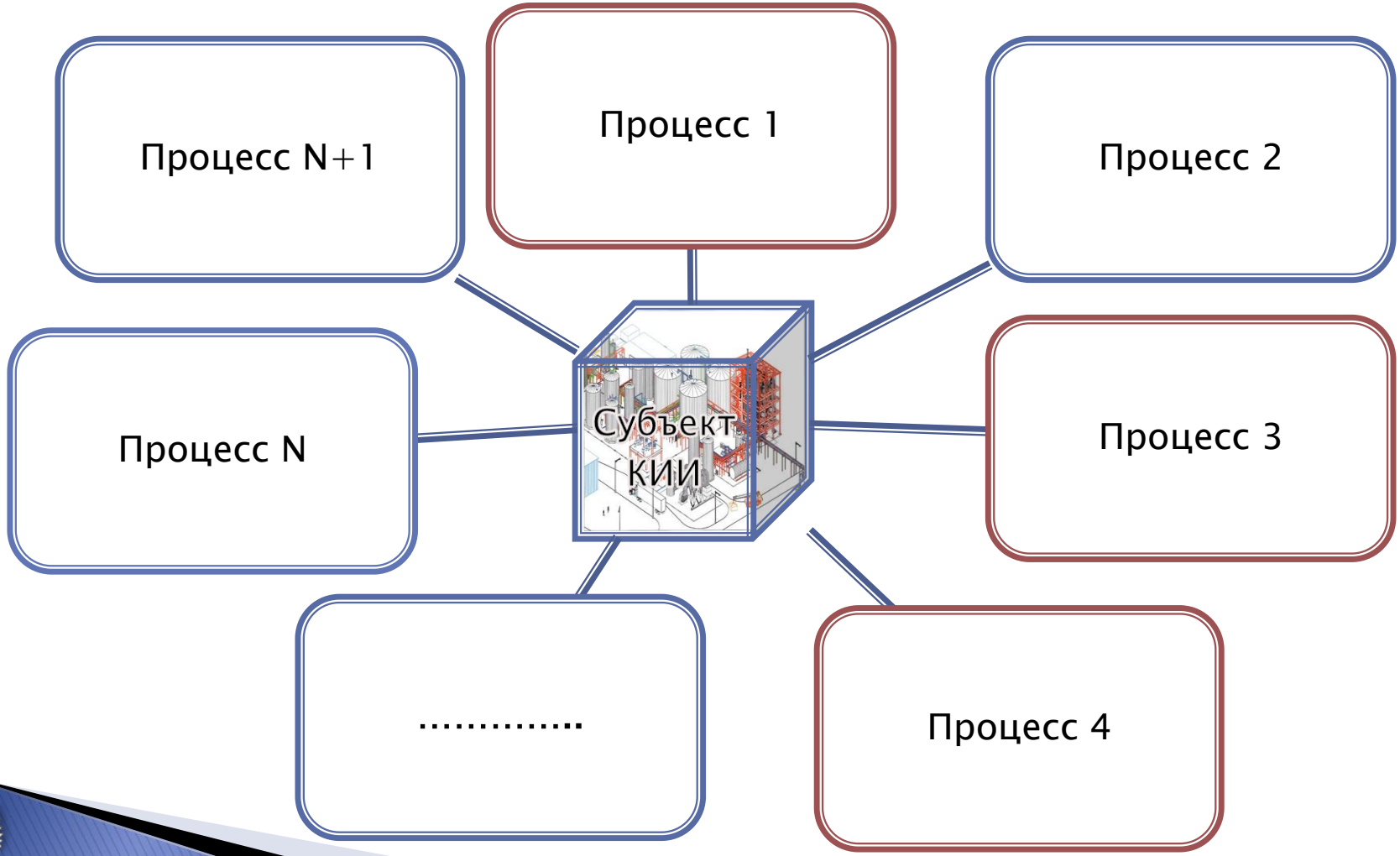
Правила категорирования объектов КИИ РФ

определение <u>всех</u> процессов в рамках выполнения функций (полномочий), осуществления видов деятельности субъекта КИИ



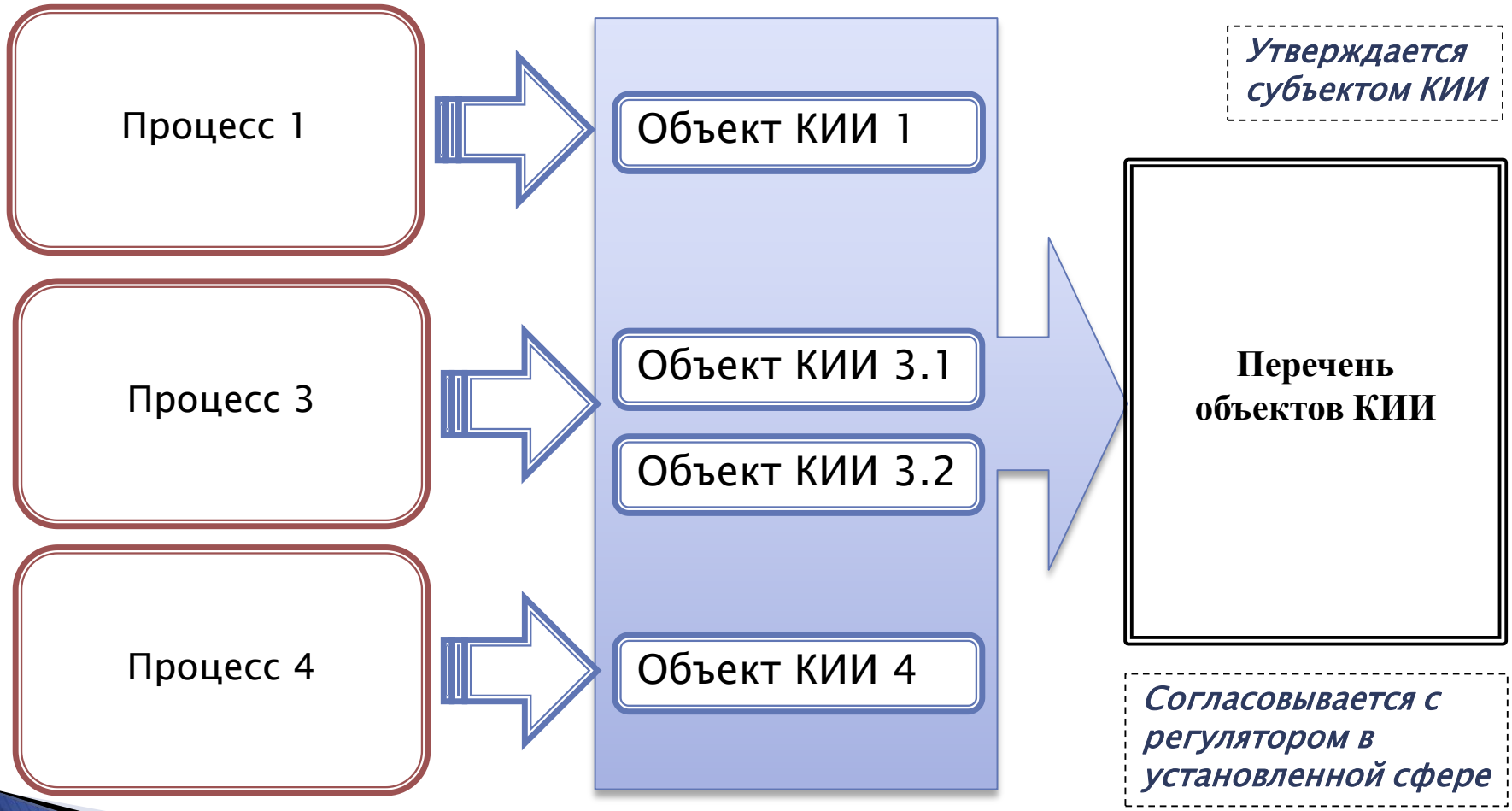
Правила категорирования объектов КИИ РФ

выявление критических процессов

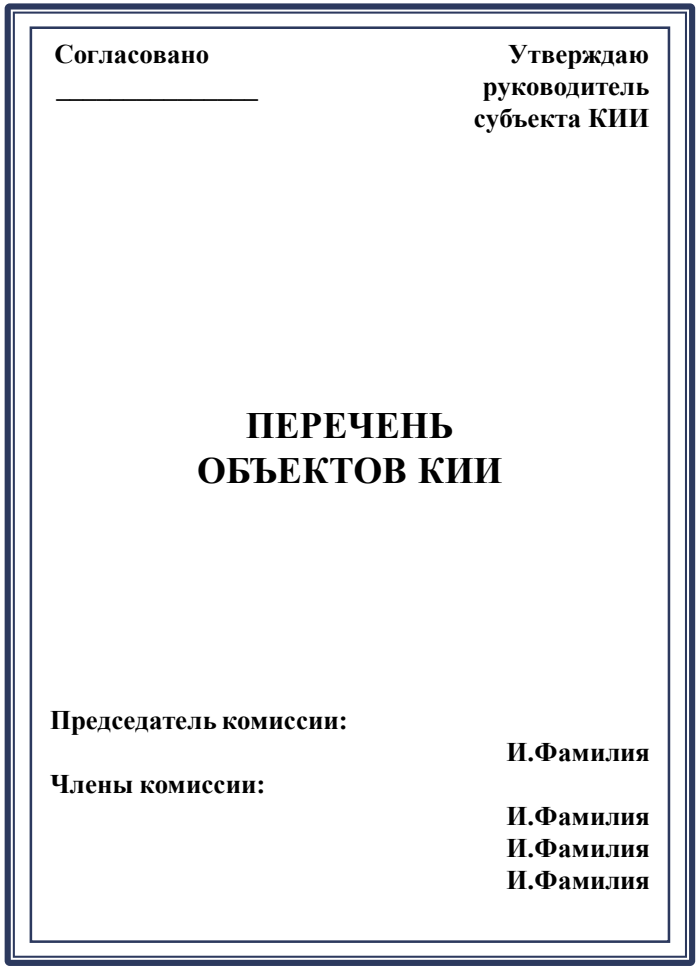


Правила категорирования объектов КИИ РФ

определение объектов КИИ, связанных с критическими процессами



Правила категорирования объектов КИИ РФ



Согласовано
_____

Утверждаю
руководитель
субъекта КИИ

ПЕРЕЧЕНЬ
ОБЪЕКТОВ КИИ

Председатель комиссии:
И.Фамилия

Члены комиссии:
И.Фамилия
И.Фамилия
И.Фамилия

п. 15 постановления Правительства РФ № 127

- перечень объектов утверждается субъектом критической информационной инфраструктуры

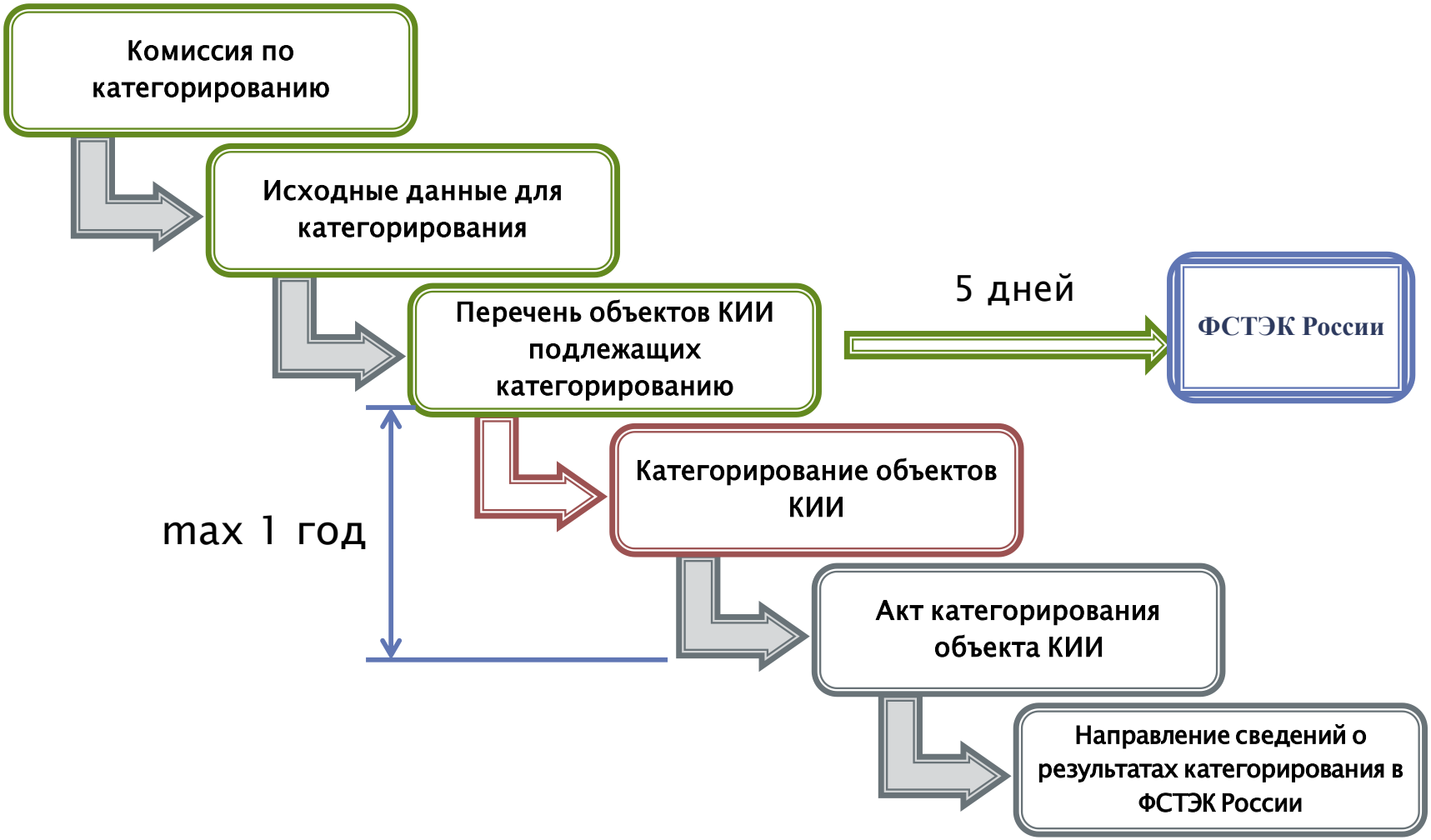
- перечень объектов подлежит согласованию с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере в части подведомственных им субъектов критической информационной инфраструктуры.

Перечень объектов критической информационной инфраструктуры

№ п.п.	Наименование объекта	Тип объекта	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)
1	2	3	4	5	6
1.	Локально информационно-вычислительная сеть ПАО «Метрика»	Информационная система	оборонно-промышленный комплекс	ноябрь 2018 г.	Ведущий инженер Сидоров Александр Александрович, тел. (910) 100-22-22 (доб. 4040) metrika@metrika.ru
2.	Корпоративные сервисы и информационные системы семейства 1С (Бухгалтерия, Зарплата и управление ERP–Управление производственным предприятием, Битрикс);	Информационная система	оборонно-промышленный комплекс	ноябрь 2018 г.	
3.	Корпоративные сервисы и информационные системы семейства Microsoft (AD, Exchange, SharePoint, СХД).	Информационная система	оборонно-промышленный комплекс	декабрь 2018 г.	

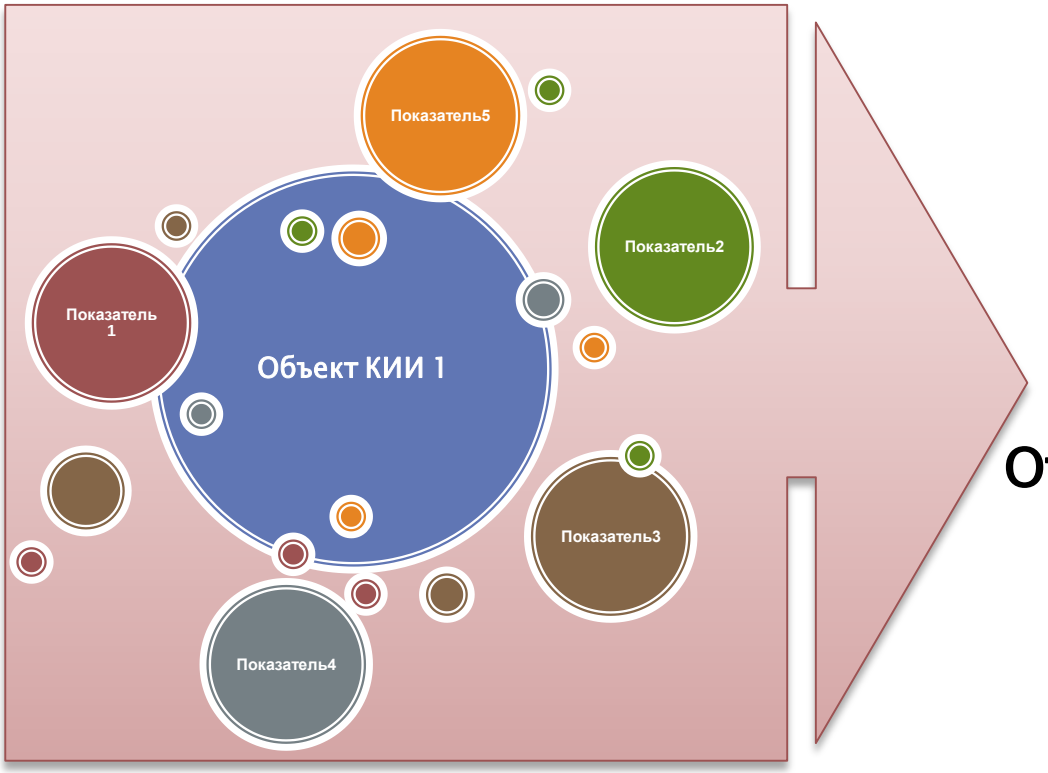
Правила категорирования объектов КИИ РФ

Правила категорирования объектов КИИ РФ



Правила категорирования объектов КИИ РФ

На основании оценки масштаба возможных последствий осуществляется присвоение одной из категорий значимости



Категория значимости объекта КИИ

или

Отсутствие необходимости присвоения категории

Перечень показателей критериев значимости объектов КИИ РФ и их значения

I Социальная значимость

1. | 2. а),б) | 3. а),б) | 4. а),б) | 5.

II Политическая значимость

6. | 7.

III Экономическая значимость

8. | 9. | 10.

IV Экологическая значимость

11. а), б)

V Значимость для обеспечения обороны страны, безопасности государства и правопорядка

12. | 13. а), б) | 14.

Оценка производится по каждому из значений показателя!

Категория присваивается по наивысшему значению показателя

Перечень показателей критериев значимости объектов КИИ РФ и их значения

ПЕРЕЧЕНЬ

показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения

Показатель		Значение показателя		
		III категория	II категория	I категория
I. Социальная значимость				
1.	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:			
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения

Перечень показателей критериев значимости объектов КИИ РФ и их значения

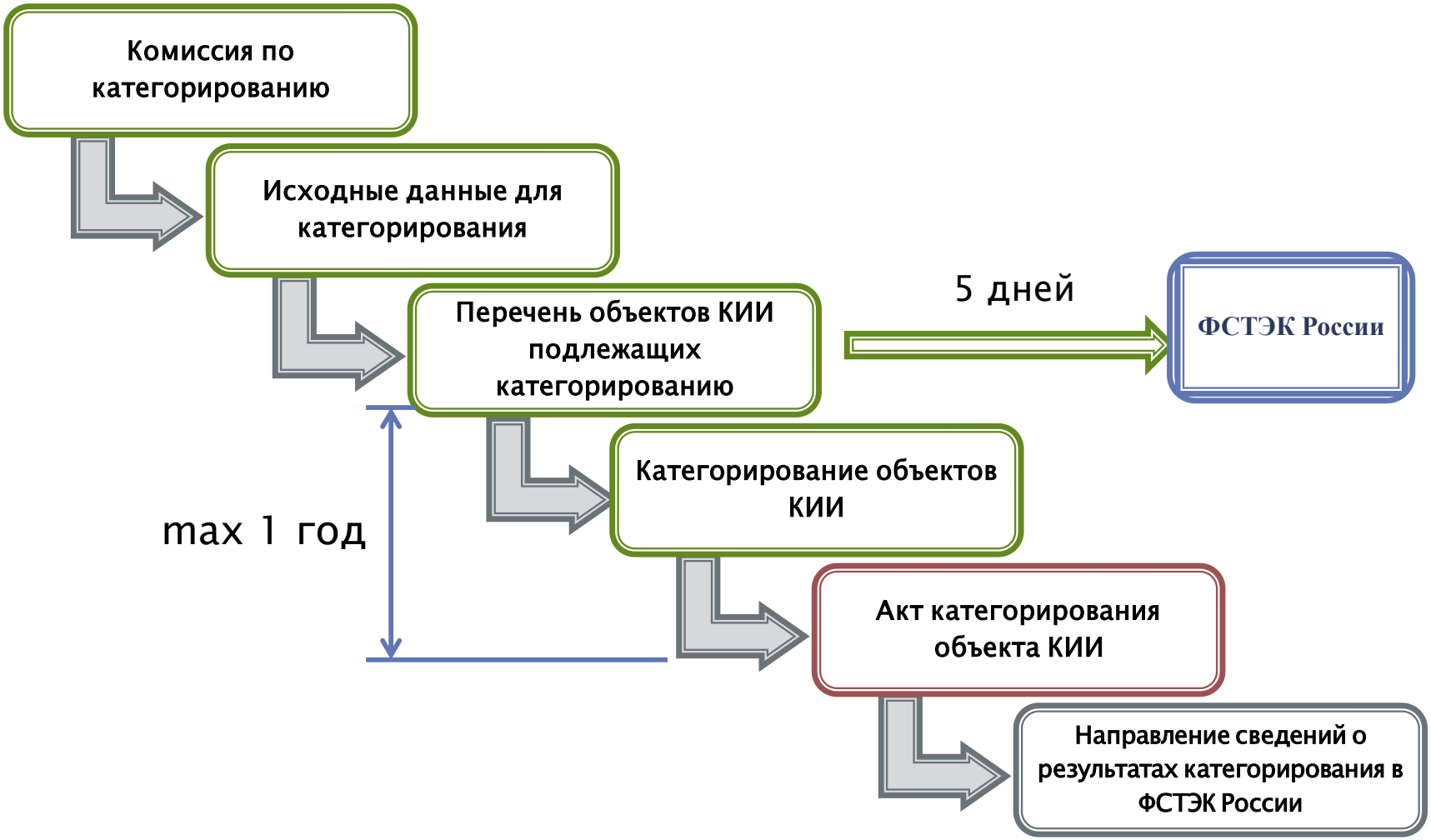
I. Социальная значимость

Показатель	Значение показателя		
	III категория	II категория	I категория
5. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течении которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12 но более 6	менее 6

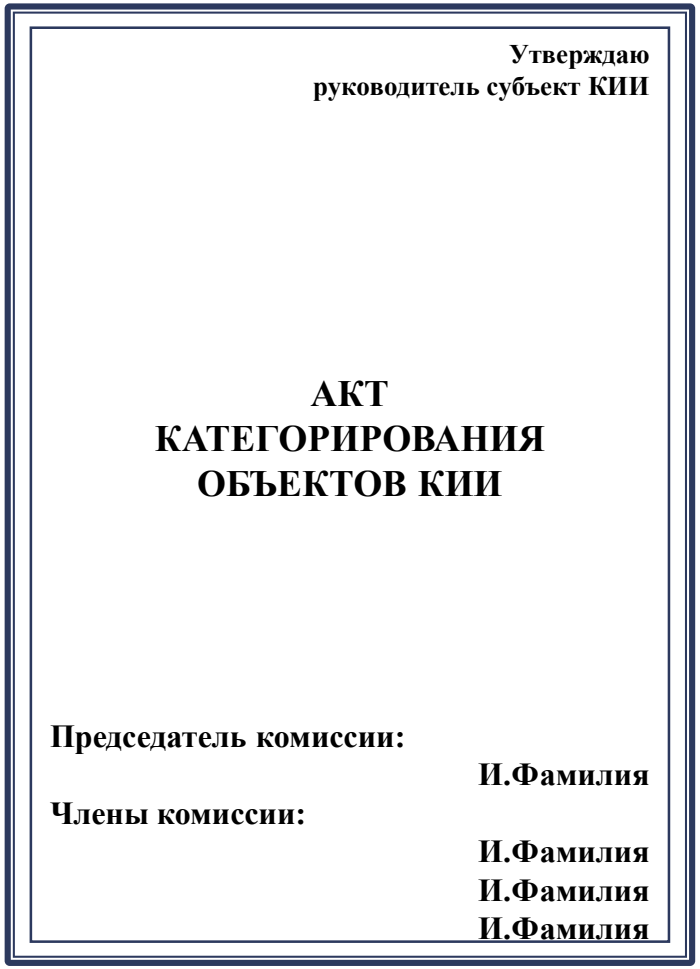
Перечень показателей критериев значимости объектов КИИ РФ и их значения

Категории значимости объектов КИИ

Правила категорирования объектов КИИ РФ



Правила категорирования объектов КИИ РФ



Утверждаю
руководитель субъект КИИ

АКТ
КАТЕГОРИРОВАНИЯ
ОБЪЕКТОВ КИИ

Председатель комиссии:
И.Фамилия

Члены комиссии:
И.Фамилия
И.Фамилия
И.Фамилия

должен содержать

Сведения об объекте КИИ, в т.ч.:

-наименовании;
-обеспечивающих критических процессах и (или) функциях управления и контроля;
-архитектуре;
-взаимодействии с сетями связи;
-программных и программно-аппаратных средствах

Результаты анализа угроз безопасности информации с учетом категорий нарушителей

Возможные последствия в случае возникновения компьютерного инцидента

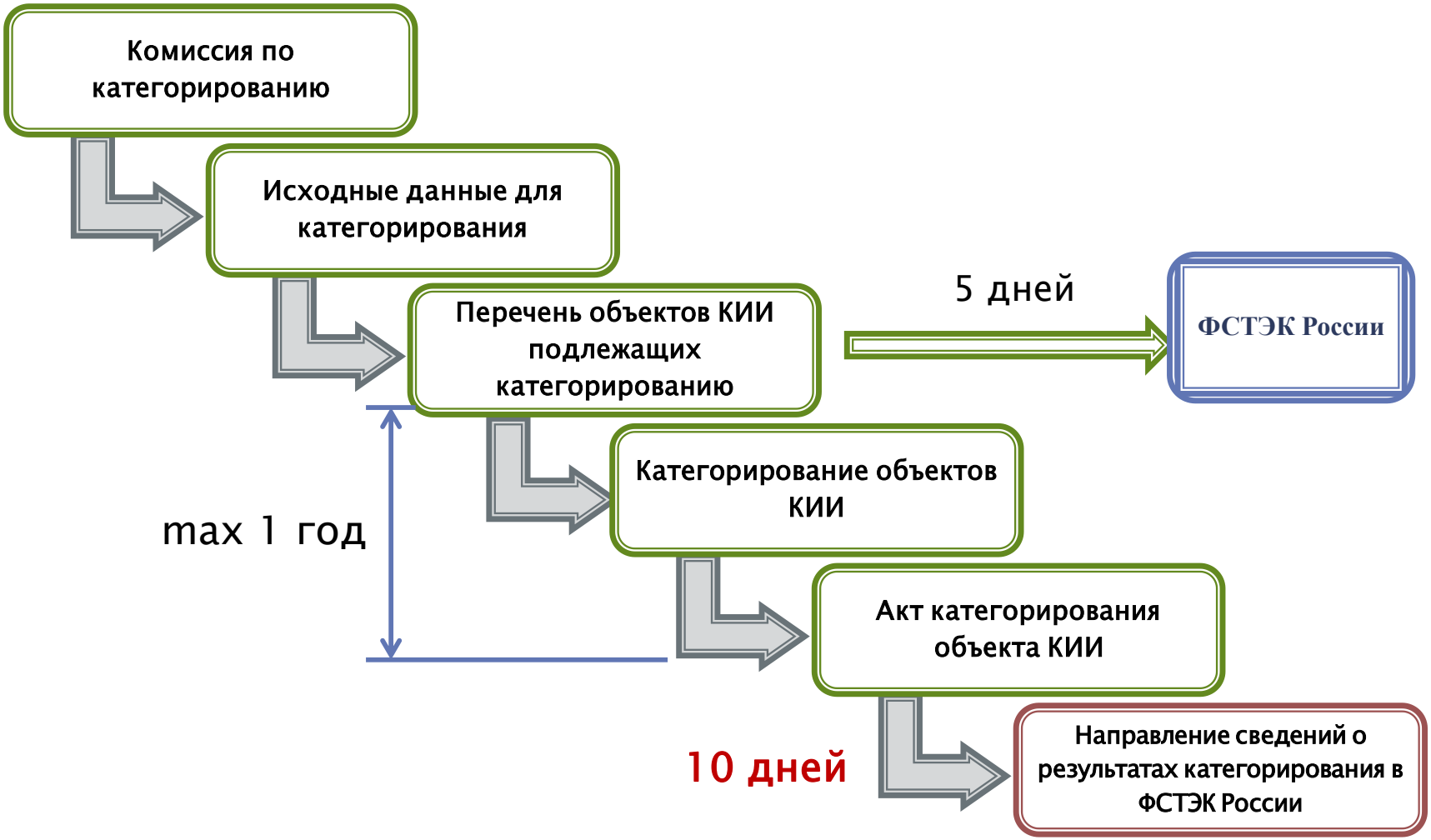
Реализованные меры по обеспечению безопасности объекта КИИ

Сведения о присвоении категории значимости либо отсутствия необходимости присвоения одной из таких категорий

Сведения о необходимых мерах по обеспечению безопасности значимых объектов КИИ, установленных ФСТЭК России

Субъект КИИ обеспечивает хранения акта до вывода из эксплуатации объекта КИИ или до изменения категории значимости

Правила категорирования объектов КИИ РФ



Правила категорирования объектов КИИ РФ

Направление сведений о результатах категорирования в ФСТЭК России

ФСТЭК России
ПРИКАЗ
от 22 декабря 2017 г. № 236

Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Реестр значимых объектов критической информационной инфраструктуры Российской Федерации

ФСТЭК России
ПРИКАЗ
от 6 декабря 2017 г. № 227

Об утверждении
Порядка ведения реестра
значимых объектов критической
информационной инфраструктуры
Российской Федерации

Структура НПА ФСТЭК России

ФСТЭК России
ПРИКАЗ
от 21 декабря 2017 г. № 235

Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования

I. Общие положения

II. Требования к силам обеспечения безопасности значимых объектов КИИ

III. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ

IV. Требования к организационно-распорядительным документам по безопасности значимых объектов

V. Требования к функционированию систем безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ

Структура НПА ФСТЭК России

ФСТЭК России
ПРИКАЗ
от 25 декабря 2017 г. № 239

Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

I. Общие положения

II. Требования к обеспечению безопасности значимых объектов в ходе их создания, эксплуатации и вывода из эксплуатации значимых объектов

III. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

Приложение. Состав мер по обеспечению безопасности и их базовые наборы для соответствующей категории значимого объекта критической информационной инфраструктуры

Структура НПА ФСТЭК России

ФСТЭК России
ПРИКАЗ
от 11 декабря 2017 г. № 229

Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Закон
«О государственной тайне»

Федеральный закон
«Об информации, информационных технологиях и о защите информации»

Федеральный закон
«О персональных данных»

Федеральный закон
«О безопасности критической информационной инфраструктуры Российской Федерации»

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

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

Законодательство РФ о государственной тайне

Обеспечение безопасности значимых объектов, являющихся государственными информационными системами

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

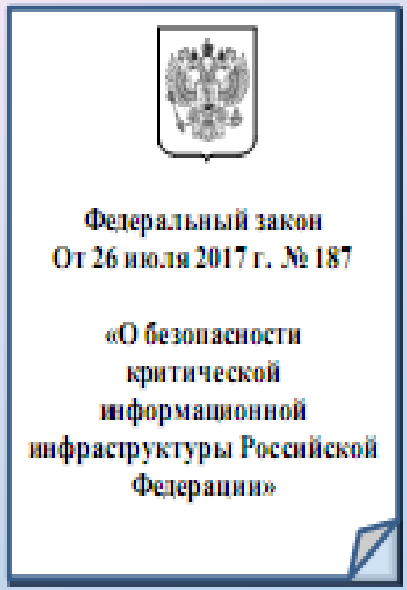
Обеспечение безопасности значимых объектов, являющихся информационными системами персональных данных

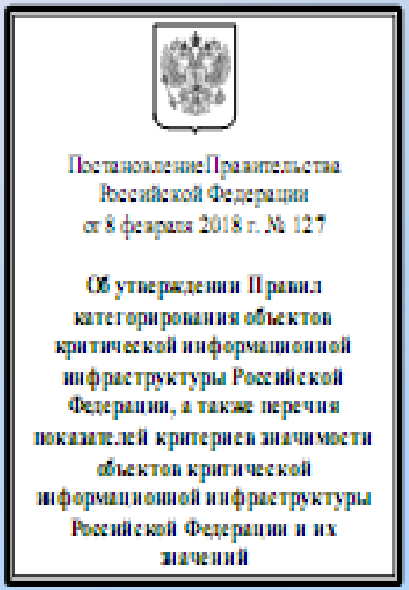
Постановление Правительства РФ от 1 ноября 2012 г. № 1119

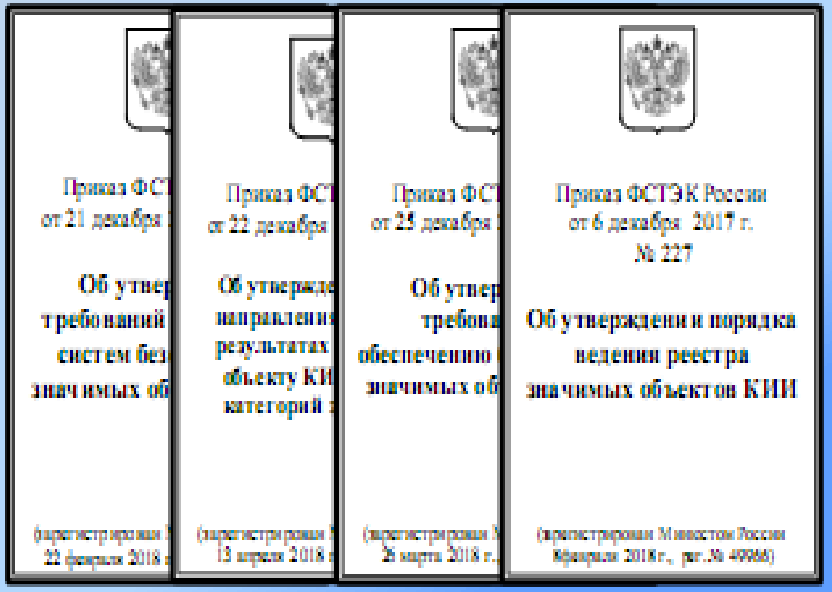
Обеспечения безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями

Нормативные правовые акты Минкомсвязи России

ПЕРВООЧЕРЕДНЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ







- Категорирование объектов КИИ
- Создание систем безопасности значимых объектов
- Реализация требований по обеспечению безопасности значимых объектов
- Обеспечение взаимодействия с ГосСОПКА

СПАСИБО ЗА ВНИМАНИЕ!