Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры [критериям](http://ivo.garant.ru/#/document/71876120/entry/2000) значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения. [2]

Категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры. [1]

Первое, что нужно сделать – это составить для себя алгоритм категорирования объектов КИИ:

Отвечаем на вопрос, является ли наша организация субъектом КИИ (согласно № 187-ФЗ, см. выше, определены конкретные отрасли).

Определяем все процессы в нашей организации и составляем их полный перечень (процессы могут быть управленческие, технологические, финансово-экономические, производственные и т.д.).

Выявляем из всех процессов именно критические процессы.

Выделяем объекты, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов и (или) осуществляют управление, контроль или мониторинг критических процессов.

Смотрим [ПП №127](https://rtmtech.ru/wp-content/uploads/2018/09/PP-127-ot-08.02.2018.pdf) и оцениваем, исходя из перечня показателей критериев значимости и учитывая дополнительные исходные данные, к какой категории относятся объекты КИИ.

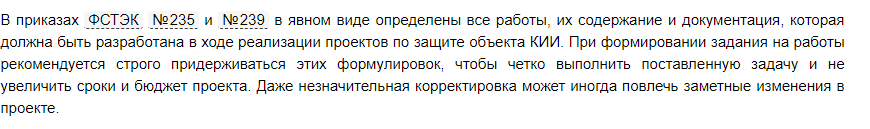
Готовим Акт категорирования объектов КИИ для отправки во ФСТЭК.

"При этом с учетом положений Федерального закона N 187-ФЗ [2] в качестве причины возникновения негативных последствий рассматривается только компьютерные инциденты вследствие компьютерных атак, т.е. не рассматриваются случаи, когда:

─ оператор связи прекращает и/или ограничивает оказание услуг электросвязи на основании Правил оказания услуг связи [9-11] или договора возмездного оказания услуг между абонентом и оператором связи;

─ прекращение и/или нарушение оказания услуг электросвязи вызвано техногенной аварией, природным явлением и/или стихийным бедствием;

─ прекращение и/или нарушение оказания услуг электросвязи вызвано непреднамеренными действиями оператора связи, пользователей услугами связи или третьих лиц (обрыв линий связи, создание аварийных ситуаций в отношении средств связи и т.п.)."



В соответствии с определением в 187-ФЗ, субъект КИИ — это:

государственный орган, государственное учреждение, российское юридическое лицо и (или) индивидуальный предприниматель, которому 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,

‒ атомной энергии, ‒ оборонной промышленности,

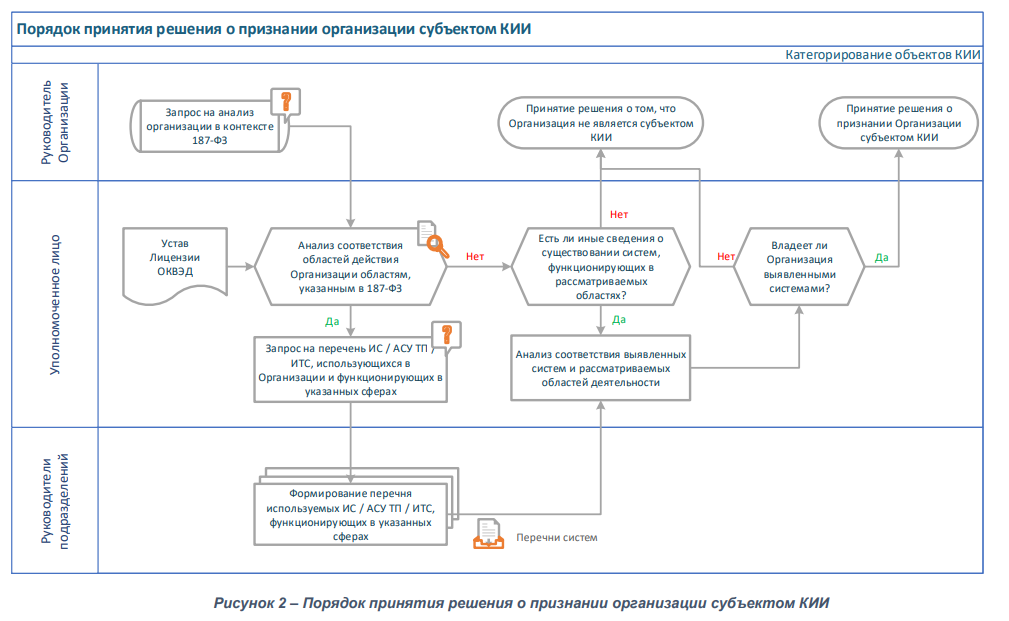
‒ ракетно-космической промышленности,

‒ горнодобывающей промышленности,

‒ металлургической промышленности,

‒ химической промышленности;

2) российское юридическое лицо и (или) индивидуальный предприниматель, который обеспечивает взаимодействие указанных систем или сетей.



[5]

В 187-ФЗ установлены 13 сфер (областей деятельности), которые подпадают под его область действия. При этом, по определению, к субъектам КИИ относятся те организации, которые владеют объектами, функционирующими в указанных сферах, а не организации, работающие в данных областях (ФЗ-187 Статья 2, п.8).

В соответствии с разъяснениями ФСТЭК России, достаточным фактом для признания организации субъектом является сочетание следующих факторов:

- организация работает в одной из указанных сфер;

- организация владеет какими-либо ИС, АСУ, ИТС. То есть предлагается отталкиваться от сферы работы организации, а не от области функционирования систем.

Библиография

Постановление правительства №127

Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

<https://zen.yandex.ru/media/id/5c7b7864fa818600ae3856a1/klub-liubitelei-kii-sostavliaem-perechen-obektov-podlejascih-kategorirovaniiu-5e289c87df944400bd8ad506> - полезное про процесс принятия КИИ

[https://www.tadviser.ru/index.php/Статья:Как\_выполнить\_требования\_закона\_187-ФЗ\_о\_безопасности\_критической\_информационной\_инфраструктуры\_Рекомендации\_«Стэп\_Лоджик»#cite\_note-0](https://www.tadviser.ru/index.php/Статья:Как_выполнить_требования_закона_187-ФЗ_о_безопасности_критической_информационной_инфраструктуры_Рекомендации_) – как выполнить требования 187 ФЗ обобщенная информация

<https://step.ru/upload/pdf/87877a75035badbaed3ab8f792ea0ca5.pdf> МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ Категорирование объектов критической информационной инфраструктуры - методичка, как выполнить 187 ФЗ