Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от «___» _____ № ____

МОСКВА

Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры в сферах топливно-энергетического комплекса и энергетики

В соответствии с пунктом 5 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» Правительство Российской Федерации **п о с т а н о в л я е т**:

Утвердить прилагаемые Отраслевые особенности категорирования объектов критической информационной инфраструктуры в сферах топливно-энергетического комплекса и энергетики.

Председатель Правительства
Российской Федерации М.Мишустин

Утверждены
постановлением Правительства
Российской Федерации
от «__» _____ 2025 г. № _____

ОТРАСЛЕВЫЕ ОСОБЕННОСТИ

категорирования объектов критической информационной инфраструктуры в сферах топливно-энергетического комплекса и энергетики

I. Общие положения

1. Настоящие Отраслевые особенности категорирования объектов критической информационной инфраструктуры в сферах топливно-энергетического комплекса и энергетики (далее – Отраслевые особенности) регламентируют особенности категорирования объектов критической информационной инфраструктуры в сферах топливно-энергетического комплекса и энергетики (далее – объекты критической информационной инфраструктуры) и определяют порядок установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений в целях присвоения ему одной из категорий значимости (далее – категорирование объекта критической информационной инфраструктуры) и включают в себя отраслевые признаки значимости объектов критической информационной инфраструктуры, соответствующие критериям значимости и показателям их значений, а также порядок расчета значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры.

2. Категорирование объектов критической информационной инфраструктуры осуществляется субъектами критической информационной инфраструктуры в соответствии со статьей 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденными постановлением Правительства Российской Федерации от 08 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» (далее соответственно – Правила, Перечень).

II. Признаки значимости объектов критической информационной инфраструктуры

3. Категорированию подлежат объекты критической информационной инфраструктуры:

а) соответствующие типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, включенных в перечни типовых отраслевых объектов критической информационной инфраструктуры, предусмотренных пунктом 4 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

б) не соответствующие типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, включенных в перечни типовых отраслевых объектов критической информационной инфраструктуры, предусмотренных пунктом 4 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», при условии, что масштаб возможных последствий в случае возникновения компьютерных инцидентов на которых соответствует показателям критериев значимости и их значениям, если такие объекты функционируют на объекте топливно-энергетического комплекса, которому в соответствии с Федеральным законом «О безопасности объектов топливно-энергетического комплекса» присвоена одна из категорий опасности (высокая, средняя или низкая).

III. Порядок установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений

4. Субъект критической информационной инфраструктуры устанавливает соответствие объекта критической информационной инфраструктуры критериям значимости и показателям их значений. Расчет значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры и присвоение ему одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения такой категории осуществляется субъектом критической информационной инфраструктуры в соответствии с Перечнем и настоящими Отраслевыми особенностями.

5. Руководствуясь Перечнем и в порядке, предусмотренном Правилами, субъектом критической информационной инфраструктуры в ходе установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений рассматриваются показатель 1, подпункты «а», «б» показателя 2, показатели 8, 9, подпункты «а», «б» показателя 11, подпункты «а», «б» показателя 13 Перечня.

Иные показатели Перечня рассматриваются субъектом критической информационной инфраструктуры с учетом данных об особенностях и специфике функционирования принадлежащих ему объектов критической информационной инфраструктуры, а также в случаях, предусмотренных пунктом 14^2 Правил.

6. В целях установления соответствия, а также обоснования применимости критериев значимости и показателей их значений к объектам критической информационной инфраструктуры в случае возникновения на них компьютерных инцидентов, помимо исходных данных, предусмотренных пунктом 10 Правил, субъектом критической информационной инфраструктуры рассматриваются:

а) сведения о возможном ущербе жизни и здоровью людей, территории (тип населенного пункта), на которой возможно прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, включая количество людей, условия жизнедеятельности которых могут быть нарушены, а также сведения о территории и количестве людей, которые могут быть подвержены вредным воздействиям, содержащиеся в декларации промышленной безопасности опасного производственного объекта, декларации безопасности гидротехнического сооружения, паспорте безопасности объекта топливно-энергетического комплекса, а также планах по локализации и ликвидации последствий аварий на опасных производственных объектах (если разработка указанных документов предусмотрена законодательством Российской Федерации) и (или) иных документах, разработанных в отношении объекта топливно-энергетического комплекса и энергетики, на котором функционирует объект критической информационной инфраструктуры;

б) сведения об отсутствии альтернативных источников тепловой (электрической) энергии (мощности) на территории, в пределах которой возможно прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения в результате компьютерного инцидента, а также сведения о количестве людей (потребителей), условия жизнедеятельности которых могут быть нарушены в случае отключения теплоснабжения и (или) электроснабжения на период, превышающий допустимые нормы, установленные законодательством Российской Федерации;

в) сведения о наличии у субъекта критической информационной инфраструктуры заключенного договора на оказание услуг энергоснабжения с потребителями электрической энергии, условия жизнедеятельности которых могут

быть нарушены в результате компьютерного инцидента на объект критической информационной инфраструктуры, обеспечивающий работу соответствующего оборудования;

г) сведения о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры, повлекших причинение ущерба жизни и здоровью людей, наступление экологических последствий, а также механические повреждения и (или) разрушения технологического и (или) производственного оборудования;

д) угрозы безопасности информации в отношении объекта критической информационной инфраструктуры, наступление которой повлечет нарушение в работе противоаварийных средств защиты и (или) систем противоаварийной автоматики, реализованных с использованием средств вычислительной техники;

е) сведения о выполнении субъектом критической информационной инфраструктуры работ в рамках исполнения государственного оборонного заказа;

ж) сведения о наличии резервирования (технологического (функционального) и (или) аппаратного) работы элементов энергосистемы, обеспечивающего сохранение ее надежности и способности выполнять функции по производству, передаче электрической энергии и электроснабжению потребителей (если это предусмотрено законодательством Российской Федерации);

з) сведения об отсутствии управляющих функций у объекта критической информационной инфраструктуры, оказывающих влияние на технологическое и (или) производственное оборудование объекта;

и) наличие и надежность[1] аварийного пульта управления, обеспечивающего оперативное отключение технологического и (или) производственного оборудования объекта, а также возможность оперативного перевода объекта на ручное управление или резервное оборудование в случае возникновения нештатных и аварийных ситуаций в результате возникновения компьютерных инцидентов;

к) сведения о наличии противоаварийных средств защиты реализованных без использования средств вычислительной техники;

л) сведения о наличии независимого (выделенного) канала связи с диспетчерским пунктом.

7. Последствия от прекращения или нарушения функционирования объекта критической информационной инфраструктуры могут приниматься равными последствиям от аварии, предусмотренными в декларации промышленной безопасности опасного производственного объекта, декларации безопасности гидротехнического сооружения, паспорте безопасности объекта топливно-энергетического комплекса, а также планах по локализации и ликвидации последствий

[1] Питание аварийного пульта управления обеспечивается от независимых источников

аварий на опасных производственных объектах и (или) иных документах, разработанных в отношении объекта, на котором функционирует объект критической информационной инфраструктуры, в случаях если в указанных документах рассмотрены сценарии развития (возникновения) аварийных ситуаций вследствие возникновения компьютерного инцидента.

8. В случае наличия в указанных документах сценариев аварий вследствие возникновения компьютерных инцидентов на объекте критической инфраструктуры оценка масштаба возможных последствий, предусмотренная подпунктом «е» пункта 14 Правил (далее – оценка масштаба возможных последствий), осуществляется комиссией по категорированию путем анализа причин возникновения угроз безопасности информации (действий нарушителей), исходя из функциональных возможностей объекта критической информационной инфраструктуры, в том числе сведений о существующих уязвимостях используемого программного обеспечения, входящего в состав объекта критической информационной инфраструктуры.

9. При отсутствии в документах, указанных в пункте 7 настоящих Отраслевых особенностей, сценариев аварий, которые могут быть вызваны компьютерными инцидентами в отношении объекта критической информационной инфраструктуры, оценка масштаба возможных последствий осуществляется комиссией по категорированию путем проведения соответствующей экспертной оценки, содержащей обоснования применимости и (или) неприменимости показателей критериев значимости к объектам критической информационной инфраструктуры, решение которой оформляется актом в соответствии с пунктом 16 Правил.

10. По результатам анализа исходных данных в соответствии с пунктом 6 настоящих Отраслевых особенностей, комиссией по категорированию в целях оценки масштаба возможных последствий, которые могут возникнуть в результате проведения в отношении объекта критической информационной инфраструктуры компьютерного инцидента, проводится расчет показателей критериев значимости объекта критической информационной инфраструктуры.

11. Субъектом критической информационной инфраструктуры должен быть рассмотрен наихудший сценарий последствий проведения компьютерных атак на объекты критической информационной инфраструктуры, результатом которого является прекращение или нарушение проектного (штатного) функционирования объектов критической инфраструктуры, а также максимально возможный ущерб субъекту критической информационной инфраструктуры.

IV. Порядок расчета (оценки) значений показателей критериев значимости с учетом особенностей функционирования объектов критической информационной инфраструктуры

13. Для расчета субъектом критической информационной инфраструктуры последствий социальной значимости, определенных показателем 1, подпунктами «а» и «б» показателя 2 Перечня, учитываются:

а) количество людей, жизни и здоровью которых может быть нанесен вред в случае возникновения на объекте критической информационной инфраструктуры компьютерного инцидента;

Commented [a1]: устойчивое выражение "вред здоровью"
ст. 1084, 1085 ГК РФ
ст. 118 УК РФ

б) масштаб последствий возникновения на объекте критической информационной инфраструктуры компьютерного инцидента (муниципальный (межмуниципальный), региональный (межрегиональный), влекущего за собой прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения;

в) количество людей, условия жизнедеятельности которых могут быть нарушены в случае возникновения на объекте критической информационной инфраструктуры компьютерного инцидента.

Полученные значения потенциального ущерба субъекту критической информационной инфраструктуры от компьютерной атаки и компьютерного инцидента сопоставляются со значениями показателей Перечня «причинение ущерба жизни и здоровью людей (человек), прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения» для каждого объекта критической информационной инфраструктуры.

14. Для расчета субъектом критической информационной инфраструктуры последствий экономической значимости, определенных показателем 8 Перечня, учитываются:

а) усредненный суммарный годовой размер выплачиваемых субъектом критической информационной инфраструктуры налогов в бюджет Российской Федерации, определенный на основании налоговой отчетности и предоставляемых в Федеральную налоговую службу декларациях за предыдущий пятилетний период;

б) усредненный размер годового дохода, определенный на основании сведений управленческого и бухгалтерского учета за предыдущий пятилетний период;

Полученные значения потенциального ущерба субъекту критической информационной инфраструктуры от компьютерной атаки и компьютерного инцидента сопоставляются с показателем усредненного размера годового дохода. Указанное соотношение (в процентах от усредненного размера годового дохода) сопоставляется с значением показателя 8 Перечня.

15. Для расчета субъектом критической информационной инфраструктуры последствий экономической значимости, определенных показателем 9 Перечня, учитываются:

а) прогнозируемый годовой доход федерального бюджета, пополняемый за счет отчислений субъекта критической информационной инфраструктуры, усредненный за трехлетний период;

б) виды отчислений субъекта критической информационной инфраструктуры выплачиваемых в федеральный бюджет Российской Федерации;

в) потенциальная сумма ущерба, которая может возникнуть в результате реализации компьютерных инцидентов на объекте критической информационной инфраструктуры и повлиять на снижение выплат (отчислений) в федеральный бюджет Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры.

Полученные значения потенциального ущерба субъекту критической информационной инфраструктуры от компьютерной атаки и компьютерного инцидента сопоставляются с показателем усредненного размера годового дохода федерального бюджета, пополняемого за счет отчислений субъекта критической информационной инфраструктуры. Указанное соотношение (в процентах от усредненного размера годового дохода) сопоставляется с значением показателя 9 Перечня.

16. Для расчета субъектом критической информационной инфраструктуры последствий экологической значимости, определенных подпунктами «а» и «б» показателя 11 Перечня, учитываются:

а) масштаб последствий возникновения на объекте критической информационной инфраструктуры компьютерного инцидента (муниципальный (межмуниципальный), региональный (межрегиональный), влекущий за собой вредное воздействие на окружающую среду;

б) количество людей, которые могут быть подвержены вредным воздействиям в случае возникновения на объекте критической информационной инфраструктуры компьютерного инцидента, влекущего за собой вредное воздействие на окружающую среду.

Полученные значения потенциального ущерба субъекту критической информационной инфраструктуры от компьютерной атаки и компьютерного инцидента сопоставляются со значениями показателя Перечня «вредные воздействия на окружающую среду» для каждого объекта критической информационной инфраструктуры.

17. Для расчета субъектом критической информационной инфраструктуры последствий значимости для обеспечения обороны страны, безопасности государства и правопорядка, определенных подпунктами «а» и «б» показателя 13 Перечня, учитываются:

а) прогнозируемые риски срыва исполнения государственного оборонного заказа (отдельного этапа исполнения государственного контракта (контрактов),

Commented [a2]: может стоит дополнить: "пополняемый за счет отчислений субъекта КИИ".

Commented [a3]: может стоит дополнить: "пополняемого за счет отчислений субъекта КИИ".

Commented [a4]: Маштаб..., влекущИЙ за собой вредное воздействие?

которые могут возникнуть в результате компьютерного инцидента, выраженные в снижении объемов продукции (работ, услуг) поставляемых в срок, установленный условиями государственного контракта (контрактов);

б) прогнозируемые риски срыва исполнения государственного оборонного заказа (отдельного этапа исполнения государственного контракта (контрактов), которые могут возникнуть в результате компьютерного инцидента, выраженные в увеличении времени на изготовление единицы продукции (работ, услуг), поставляемой в целях исполнения государственного контракта (контрактов).

Commented [a5]: Может стоит дополнить: "..., которые могут возникнуть в результате компьютерного инцидента".

Полученные значения потенциального ущерба субъекту критической информационной инфраструктуры от компьютерной атаки и компьютерного инцидента сопоставляются с условиями государственного контракта (контрактов), выполняемых субъектом критической информационной инфраструктуры. Указанное соотношение (в процентах от объема продукции (работ, услуг) и от времени на ее изготовление) сопоставляется с значением показателя 13 Перечня.