ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 7 марта 2026 г. № 246

МОСКВА

Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере науки

В соответствии со статьей 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 согласованные с Федеральной службой по техническому и экспортному контролю прилагаемые отраслевые особенности категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере науки.

Председатель Правительства Российской Федерации

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
00FFAD9E6A5A8FD915A579C5FC8623865A
Действителен с 26.06.2025 по 19.09.2026
Владелец: Правительство Российской Федерации

М.Мишустин

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 7 марта 2026 г. № 246

ОТРАСЛЕВЫЕ ОСОБЕННОСТИ

категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере науки

I. Общие положения

1. Настоящий документ определяет порядок установления соответствия объекта критической информационной инфраструктуры Российской Федерации в сфере науки (далее - объект критической информационной инфраструктуры) критериям значимости и показателям их значений в целях присвоения объекту критической информационной инфраструктуры одной из категорий значимости (далее - проведение категорирования) и порядок расчета значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры.

2. Субъектами критической информационной инфраструктуры в сфере науки являются государственные органы, государственные учреждения, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере науки, и государственные органы, государственные учреждения, которые обеспечивают взаимодействие указанных систем или сетей (далее - субъекты критической информационной инфраструктуры).

3. При проведении категорирования объектов критической информационной инфраструктуры следует учитывать отраслевую специфику объектов критической информационной инфраструктуры, а также перечни типовых отраслевых объектов критической информационной инфраструктуры, установленные в соответствии с пунктом 4 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

(далее - перечни типовых отраслевых объектов критической информационной инфраструктуры).

4. Проведение категорирования объектов критической информационной инфраструктуры осуществляется в соответствии со статьей 7 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации и перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденными постановлением 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" (далее - перечень показателей критериев значимости).

5. Понятия "компьютерный инцидент" и "компьютерная атака" используются в настоящем документе в значениях, определенных Федеральным законом "О безопасности критической информационной инфраструктуры Российской Федерации".

II. Порядок проведения категорирования объектов критической информационной инфраструктуры

6. Проведение категорирования объектов критической информационной инфраструктуры включает в себя:

а) выявление информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, соответствующих типовым объектам критической информационной инфраструктуры, включенным в перечень типовых отраслевых объектов критической информационной инфраструктуры;

б) оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

в) присвоение каждому объекту критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения ему одной из категорий значимости.

7. В случае осуществления модернизации объектов критической информационной инфраструктуры решением субъекта критической информационной инфраструктуры объект критической информационной инфраструктуры может быть разделен на несколько отдельных объектов критической информационной инфраструктуры.

8. В случае выявления субъектом критической информационной инфраструктуры объекта критической информационной инфраструктуры, который не соответствует типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, включенных в перечни типовых отраслевых объектов критической информационной инфраструктуры, но масштаб возможных последствий возникновения компьютерных инцидентов на котором соответствует критериям значимости и показателям их значений, субъект критической информационной инфраструктуры присваивает объекту критической информационной инфраструктуры одну из категорий значимости, наиболее подходящих для выявления объекта критической информационной инфраструктуры, и направляет сведения об объекте критической информационной инфраструктуры, а также предложения о дополнении перечней типовых отраслевых объектов критической информационной инфраструктуры в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

Сведения об объекте критической информационной инфраструктуры, подлежащие направлению в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, установлены пунктом 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением 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".

9. При применении к объектам критической информационной инфраструктуры перечня показателей критериев значимости следует учитывать следующие особенности:

а) показатель, предусмотренный позицией 1 перечня показателей критериев значимости, применим в случае, если при выполнении

научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ предусматривается использование вредных веществ, в том числе опасных химических веществ;

б) показатель, предусмотренный позицией 7 перечня показателей критериев значимости, применим в случае, если субъект критической информационной инфраструктуры выполняет научно-исследовательские работы, опытно-конструкторские работы и (или) научно-исследовательские и опытно-конструкторские работы в рамках международного договора Российской Федерации;

в) показатель, предусмотренный позицией 9 перечня показателей критериев значимости, применим в случае, если субъект критической информационной инфраструктуры выполняет научно-исследовательские работы, опытно-конструкторские работы и (или) научно-исследовательские и опытно-конструкторские работы;

г) показатель, предусмотренный позицией 11 перечня показателей критериев значимости, применим в случае, если при выполнении научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ предусматривается использование вредных веществ, в том числе опасных химических веществ;

д) показатель, предусмотренный позицией 13^1 перечня показателей критериев значимости, применим в случае выполнения субъектом критической информационной инфраструктуры научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ в рамках государственного оборонного заказа.

10. При оценке масштаба возможных последствий в случае возникновения компьютерных инцидентов при проведении компьютерных атак на объекты критической информационной инфраструктуры необходимо:

а) рассматривать наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты критической информационной инфраструктуры, следствием которых являются прекращение или нарушение проектного или штатного функционирования объектов критической информационной инфраструктуры и нанесение максимально возможного ущерба (отсутствие организационных, технических и иных мер безопасности, реализованных на объектах

критической информационной инфраструктуры и в субъекте критической информационной инфраструктуры в целом, дублирование процесса аналоговыми приборами или переход на бумажные носители информации);

б) учитывать зависимость технологических процессов от осуществления иных процессов, выполняемых субъектом критической информационной инфраструктуры;

в) учитывать зависимость функционирования одного объекта критической информационной инфраструктуры от функционирования другого объекта критической информационной инфраструктуры;

г) оценивать возможность реализации угрозы безопасности информации для объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

11. Проведение категорирования объектов критической информационной инфраструктуры осуществляется субъектом критической информационной инфраструктуры исходя из возможности возникновения компьютерных атак и компьютерных инцидентов (при выполнении научно-исследовательских работ и (или) опытно-конструкторских работ не ниже седьмого уровня готовности разрабатываемых или разработанных технологий, а также получении научных и (или) научно-технических результатов не ниже седьмого уровня готовности разрабатываемых или разработанных технологий, определяемых в соответствии с порядком определения уровней готовности разрабатываемых или разработанных технологий, а также научных и (или) научно-технических результатов, соответствующих каждому уровню готовности технологий, утверждаемым в соответствии с пунктом 3^1 Положения о единой государственной информационной системе учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения, утвержденного постановлением Правительства Российской Федерации от 12 апреля 2013 г. № 327 "О единой государственной информационной системе учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения") и зависит от показателей критериев значимости перечня показателей критериев значимости, указанных в пункте 9 настоящего документа.

III. Порядок расчета значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры

12. До начала расчета значений показателей критериев значимости субъектом критической информационной инфраструктуры определяется применимость критериев значимости для оценки значимости информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

13. В случае неприменимости показателей критериев значимости к объекту критической информационной инфраструктуры расчет значений показателей критериев значимости субъектом критической информационной инфраструктуры не проводится.

14. В целях определения категории значимости объекта критической информационной инфраструктуры:

а) при расчете значения показателя, указанного в подпункте "а" пункта 9 настоящего документа, субъектом критической информационной инфраструктуры учитываются:

количество лиц, задействованных в обеспечении функционирования объекта критической информационной инфраструктуры при проведении испытаний, научных исследований, осуществлении экспериментальных разработок;

количество работников подразделений субъекта критической информационной инфраструктуры в соответствии со штатным расписанием, которые могут находиться в зоне поражения при возникновении чрезвычайной ситуации;

б) при расчете значения показателя, указанного в подпункте "б" пункта 9 настоящего документа, субъектом критической информационной инфраструктуры учитывается снижение количества завершенных испытаний (опытов, экспериментов, измерений) за определенный промежуток времени, снижение точности (правильности, прецизионности) результатов измерений при проведении испытаний (опытов, экспериментов, измерений) или целостности, доступности информации, полученной в ходе выполнения научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ, которое может произойти в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры. Значение указанного показателя

оценивается исходя из уровня международного договора Российской Федерации;

в) при расчете значения показателя, указанного в подпункте "в" пункта 9 настоящего документа, субъектом критической информационной инфраструктуры учитывается снижение налоговых выплат (отчислений) в бюджеты бюджетной системы Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры;

г) при расчете значения показателя, указанного в подпункте "г" пункта 9 настоящего документа, субъектом критической информационной инфраструктуры учитываются:

количество лиц, задействованных в обеспечении функционирования объекта критической информационной инфраструктуры при проведении испытаний, научных исследований, осуществлении экспериментальных разработок;

количество работников подразделений субъекта критической информационной инфраструктуры в соответствии со штатным расписанием, которые могут находиться в зоне поражения при возникновении чрезвычайной ситуации;

территория, на которой окружающая среда может подвергнуться вредным воздействиям. При определении границ территории воздействия учитываются количество вредных веществ, которые могут быть выброшены в результате аварии, наличие неровности поверхности земли, сила и направление ветра и иные факторы, влияющие на окружающую среду;

д) при расчете значения показателя, указанного в подпункте "д" пункта 9 настоящего документа, субъектом критической информационной инфраструктуры учитывается снижение количества завершенных испытаний (опытов, экспериментов, измерений) за определенный промежуток времени, снижение точности (правильности, прецизионности) результатов измерений при проведении испытаний (опытов, экспериментов, измерений) или целостности, доступности информации, полученной в ходе научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ, которое может произойти в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры. Значение указанного показателя оценивается исходя из статуса субъекта критической информационной инфраструктуры в кооперации головного исполнителя поставок продукции по государственному оборонному заказу.

15. При расчете значений показателей критериев значимости субъекту критической информационной инфраструктуры необходимо определить масштаб возможных последствий компьютерных инцидентов, основываясь на выявленных угрозах безопасности информации, типах компьютерных атак, назначении объекта критической информационной инфраструктуры и автоматизируемого процесса.

16. Оценка последствий, которые могут наступить в результате возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры, проводится субъектом критической информационной инфраструктуры в соответствии с показателями, указанными в пункте 9 настоящего документа.

17. По показателю, указанному в подпункте "а" пункта 9 настоящего документа, учитываются компьютерные инциденты, в случае наступления которых возможно возникновение:

а) техногенных катастроф (взрывов, утечек и разливов опасных веществ), связанных с нарушением управления и работы объекта критической информационной инфраструктуры (в том числе с нарушением параметров технологического процесса, нарушением работы или состояния исполнительных механизмов устройств);

б) негативных последствий при проведении научных исследований, исследований объектов (процессов) производства и осуществлении экспериментальных разработок (в том числе медицинских препаратов, медицинского оборудования, пищевой продукции, бытовой химической продукции, транспортных средств, топлива), связанных с нарушением технологического процесса при работе объекта критической информационной инфраструктуры.

18. По показателю, указанному в подпункте "б" пункта 9 настоящего документа, учитываются компьютерные инциденты, которые могут негативно повлиять на объект критической информационной инфраструктуры, от работоспособности которого зависит выполнение научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ, осуществляемых в рамках международного договора Российской Федерации.

19. По показателю, указанному в подпункте "в" пункта 9 настоящего документа, учитывается возможность снижения налоговых выплат (отчислений) субъектами критической информационной инфраструктуры в бюджеты бюджетной системы Российской Федерации

в случае нарушения функционирования объекта критической информационной инфраструктуры, который участвует в выполнении научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ.

20. По показателю, указанному в подпункте "г" пункта 9 настоящего документа, учитывается возможность возникновения выбросов (сбросов, разливов) вредных и загрязняющих веществ в атмосферу (водоемы, почву) в случае нарушения функционирования объекта критической информационной инфраструктуры при выполнении научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ.

21. По показателю, указанному в подпункте "д" пункта 9 настоящего документа, учитывается возможность снижения объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции), а также увеличения времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции) в случае нарушения функционирования объекта критической информационной инфраструктуры при выполнении научно-исследовательских работ, опытно-конструкторских работ и (или) научно-исследовательских и опытно-конструкторских работ в рамках государственного оборонного заказа.

_____