ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 8 февраля 2018 г. № 127

МОСКВА

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

(с изменениями от 13 апреля 2019 г., 24 декабря 2021 г., 19 августа 2022 г. 20 декабря 2022 г., 19 сентября 2024 г., 7 ноября 2025 г.)

В соответствии с пунктом 1 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**:

1. Утвердить прилагаемые:

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации;

перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений.

2. Финансирование расходов, связанных с реализацией настоящего постановления государственными органами и государственными учреждениями, осуществляется за счет и в пределах бюджетных ассигнований, предусмотренных соответствующим бюджетом на обеспечение деятельности субъектов критической информационной инфраструктуры.

Председатель
Правительства
Российской Федерации Д.Медведев

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. № 127
(в ред. постановлений
Правительства
Российской Федерации
от 13 апреля 2019 г. № 452,
от 24 декабря 2021 г. № 2431,
от 19 августа 2022 г. № 1463,
от 20 декабря 2022 г. № 2360,
от 19 сентября 2024 г. № 1281,
от 7 ноября 2025 г. № 1762)

ПРАВИЛА
категорирования объектов критической информационной инфраструктуры Российской Федерации

1. Настоящие Правила устанавливают порядок и сроки категорирования объектов критической информационной инфраструктуры Российской Федерации (далее соответственно - критическая информационная инфраструктура, категорирование).

2. Категорирование осуществляется субъектами критической информационной инфраструктуры в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры.

3. Категорированию подлежат объекты критической информационной инфраструктуры, соответствующие типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, включенным в перечни типовых отраслевых объектов критической информационной инфраструктуры, предусмотренные пунктом 4 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее - перечни типовых отраслевых объектов критической информационной инфраструктуры).
(п. 3 в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

4. Определение категорий значимости объектов критической информационной инфраструктуры (далее - категория значимости) осуществляется

на основании показателей критериев значимости объектов критической информационной инфраструктуры и их значений, предусмотренных перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденным 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 соответственно - перечень показателей критериев значимости, показатели критериев значимости).

5. Категорирование включает в себя:

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

(пп. «а» в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

б) - в) утратили силу. - Постановление Правительства РФ от 07.11.2025 № 1762;

г) утратил силу. - Постановление Правительства РФ от 19 сентября 2024 г. № 1281;

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

е) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

6. Объекту критической информационной инфраструктуры по результатам категорирования присваивается в соответствии с перечнем показателей критериев значимости категория значимости с наивысшим значением.

Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (территория, количество людей), оценка производится по каждому из значений показателя критериев значимости, а категория значимости присваивается по наивысшему значению такого показателя.

В случае если объект критической информационной инфраструктуры по одному из показателей критериев значимости отнесен к первой категории, расчет по остальным показателям критериев значимости не проводится.

(абзац введен Постановлением Правительства РФ от 13.04.2019 № 452)

В случае если объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, категория значимости не присваивается.
(в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

6.1. Установление соответствия 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 осуществляются в соответствии с настоящими Правилами и отраслевыми особенностями категорирования объектов критической информационной инфраструктуры, предусмотренными пунктом 5 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее - отраслевые особенности категорирования).
(п. 6.1 введен Постановлением Правительства РФ от 07.11.2025 № 1762)

7. Устанавливаются 3 категории значимости. Самая высокая категория - первая, самая низкая - третья.

8. В отношении создаваемого объекта критической информационной инфраструктуры, в том числе в рамках создания объекта капитального строительства, категория значимости определяется при формировании заказчиком, техническим заказчиком или застройщиком требований к объекту критической информационной инфраструктуры с учетом имеющихся исходных данных.
(в ред. Постановлений Правительства РФ от 13.04.2019 № 452, от 07.11.2025 № 1762)

Для создаваемого объекта критической информационной инфраструктуры, указанного в абзаце первом настоящего пункта, категория значимости может быть уточнена в ходе его проектирования.

9. Для объектов, принадлежащих одному субъекту критической информационной инфраструктуры, но используемых для целей контроля и управления технологическим и (или) производственным оборудованием, принадлежащим другому субъекту критической информационной инфраструктуры, категорирование осуществляется на основе исходных данных, представляемых субъектом критической информационной инфраструктуры, которому принадлежит технологическое и (или) производственное оборудование.

Категорирование объектов критической информационной инфраструктуры, в составе которых используются программные и (или) программно-аппаратные средства, принадлежащие и эксплуатируемые иными государственными органами, государственными учреждениями, российскими юридическими лицами,

осуществляется субъектом критической информационной инфраструктуры с учетом данных о последствиях нарушения или прекращения функционирования указанных программных и (или) программно-аппаратных средств, представляемых этими государственными органами, государственными учреждениями, российскими юридическими лицами.

(абзац введен Постановлением Правительства РФ от 13.04.2019 № 452; в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

10. Исходными данными для категорирования являются:

а) сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

б) утратил силу. - Постановление Правительства РФ от 07.11.2025 № 1762;

в) состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;

г) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт безопасности объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной инфраструктуры (если разработка указанных деклараций и паспорта безопасности предусмотрена законодательством Российской Федерации);

(в ред. Постановления Правительства РФ от 13.04.2019 № 452)

д) сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объекта критической информационной инфраструктуры от других таких объектов;

е) угрозы безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа**;**

ж) перечни типовых отраслевых объектов критической информационной инфраструктуры;

(пп. «ж» в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

з) иные данные, определенные отраслевыми особенностями категорирования.

(пп. «з» введен Постановлением Правительства РФ от 07.11.2025 № 1762)

11. Для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается постоянно действующая комиссия по категорированию, в состав которой включаются:
(в ред. Постановления Правительства РФ от 13.04.2019 № 452)

а) руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо;

б) работники субъекта критической информационной инфраструктуры, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности, и в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов;

в) работники субъекта критической информационной инфраструктуры, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры;

г) работники подразделения по защите государственной тайны субъекта критической информационной инфраструктуры (в случае, если объект критической информационной инфраструктуры обрабатывает информацию, составляющую государственную тайну);

д) работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций.

11.1. По решению руководителя субъекта критической информационной инфраструктуры и в соответствии с отраслевыми особенностями категорирования в состав комиссии могут быть включены иные лица, не указанные в пункте 11 настоящих Правил.
(п. 11.1 в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

11.2. По решению руководителя субъекта критической информационной инфраструктуры, имеющего филиалы, представительства, могут создаваться отдельные комиссии для категорирования объектов критической информационной инфраструктуры в этих филиалах, представительствах.

Координацию и контроль деятельности комиссий по категорированию в филиалах, представительствах осуществляет комиссия по категорированию субъекта критической информационной инфраструктуры.
(п. 11.2 введен Постановлением Правительства РФ от 13.04.2019 № 452)

11.3. Комиссия по категорированию подлежит расформированию в следующих случаях:

а) прекращение субъектом критической информационной инфраструктуры выполнения функций (полномочий) или осуществления видов деятельности в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

б) ликвидация, реорганизация субъекта критической информационной инфраструктуры и (или) изменения его организационно-правовой формы, в результате которых были утрачены признаки субъекта критической информационной инфраструктуры.

(п. 11.3 введен Постановлением Правительства РФ от 13.04.2019 № 452)

12. В состав комиссии по категорированию могут включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с государственными органами и российскими юридическими лицами.

13. Комиссию по категорированию возглавляет руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо.

14. Комиссия по категорированию в ходе своей работы:

а) выявляет объекты критической информационной инфраструктуры, соответствующие типовым объектам, включенным в перечни типовых отраслевых объектов критической информационной инфраструктуры;

(пп. «а» в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

б) - в) утратили силу. - Постановление Правительства РФ от 07.11.2025 № 1762;

г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

д) анализирует угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

(в ред. Постановления Правительства РФ от 13.04.2019 № 452)

е) оценивает в соответствии с перечнем показателей критериев значимости и с учетом отраслевых особенностей категорирования масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры, определяет значения каждого из показателей критериев значимости или обосновывает их неприменимость;

(в ред. Постановлений Правительства РФ от 13.04.2019 № 452, от 07.11.2025 № 1762)

ж) устанавливает каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.

14.1. При проведении работ, предусмотренных подпунктами «г» и «д» пункта 14 настоящих Правил, должны быть рассмотрены наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты критической информационной инфраструктуры, результатом которых являются прекращение функционирования объектов критической информационной инфраструктуры или нарушение заданных параметров его проектного или штатного функционирования, которые могут быть определены отраслевыми особенностями категорирования, и нанесение максимально возможного ущерба.
(п. 14.1 введен Постановлением Правительства РФ от 13.04.2019 № 452; в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

14.2. В случае если функционирование одного объекта критической информационной инфраструктуры зависит от функционирования другого объекта критической информационной инфраструктуры, оценка масштаба возможных последствий, предусмотренная подпунктом «е» пункта 14 настоящих Правил, проводится исходя из предположения о прекращении или нарушении заданных параметров проектного или штатного функционирования вследствие компьютерной атаки объекта критической информационной инфраструктуры, от которого зависит оцениваемый объект.
(п. 14.2 введен Постановлением Правительства РФ от 13.04.2019 № 452; в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

14.3. Утратил силу. - Постановление Правительства РФ от 07.11.2025 № 1762.

15. Утратил силу. - Постановление Правительства РФ от 19.09.2024 № 1281.

16. Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.
(в ред. Постановления Правительства РФ от 13.04.2019 № 452)

Допускается оформление единого акта по результатам категорирования нескольких объектов критической информационной инфраструктуры, принадлежащих одному субъекту критической информационной инфраструктуры.
(абзац введен Постановлением Правительства РФ от 13.04.2019 № 452)

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры.

Субъект критической информационной инфраструктуры обеспечивает хранение акта до вывода из эксплуатации объекта критической информационной инфраструктуры или до изменения категории значимости.

17. Субъект критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта, указанного в пункте 16 настоящих Правил, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Указанные сведения включают:

(в ред. Постановления Правительства РФ от 13.04.2019 № 452)

а) сведения об объекте критической информационной инфраструктуры;

б) сведения о субъекте критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит объект критической информационной инфраструктуры;

в) сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи;

г) сведения о лице, эксплуатирующем объект критической информационной инфраструктуры;

д) сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры, в том числе средствах, используемых для обеспечения безопасности объекта критической информационной инфраструктуры и их сертификатах соответствия требованиям по безопасности информации (при наличии);

е) сведения об угрозах безопасности информации и о категориях нарушителей в отношении объекта критической информационной инфраструктуры либо об отсутствии таких угроз;

ж) возможные последствия в случае возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры либо сведения об отсутствии таких последствий;

з) категорию значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости, содержащие полученные значения по каждому из рассчитываемых показателей критериев значимости с обоснованием этих значений или информацию о неприменимости показателей к объекту с соответствующим обоснованием;

(в ред. Постановления Правительства РФ от 13.04.2019 № 452)

и) организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры, либо сведения об отсутствии необходимости применения указанных мер;

к) доменные имена и сетевые адреса объекта критической информационной инфраструктуры, взаимодействующего с сетями электросвязи общего пользования, в том числе с информационно-телекоммуникационной сетью «Интернет».

(пп. «к» введен Постановлением Правительства РФ от 07.11.2025 № 1762)

18. Сведения, указанные в пункте 17 настоящих Правил, и их содержание направляются в печатном и электронном виде по форме, утверждаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

(в ред. Постановления Правительства РФ от 13.04.2019 № 452)

По вновь создаваемым объектам критической информационной инфраструктуры сведения, указанные в подпунктах «а» - «в» и «з» пункта 17 настоящих Правил, направляются в течение 10 рабочих дней после утверждения требований к создаваемому объекту критической информационной инфраструктуры, а сведения, указанные в подпунктах «г» - «ж», «и» и «к» пункта 17 настоящих Правил, - в течение 10 рабочих дней после ввода объекта критической информационной инфраструктуры в эксплуатацию (принятия на снабжение).

(абзац введен Постановлением Правительства РФ от 13.04.2019 № 452; в ред. Постановления Правительства РФ от 07.11.2025 № 1762)

19. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, проверяет сведения о результатах присвоения категорий значимости в порядке, предусмотренном частями 6 - 8 статьи 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

19.1. В случае изменения сведений, указанных в пункте 17 настоящих Правил, субъект критической информационной инфраструктуры направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, новые сведения в печатном и электронном виде не позднее 20 рабочих дней со дня их изменения по форме, предусмотренной пунктом 18 настоящих Правил.

(п. 19.1. введен Постановлением Правительства РФ от 24.12.2021 № 2431; в ред. Постановления Правительства РФ от 20.12.2022 № 2360)

19.2. Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, осуществляют мониторинг представления субъектами критической информационной инфраструктуры, выполняющими функции (полномочия) или осуществляющими виды деятельности в соответствующих областях (сферах), актуальных и достоверных сведений, указанных в пункте 17 настоящих Правил, с учетом перечней типовых отраслевых объектов критической информационной инфраструктуры и отраслевых особенностей категорирования.

(в ред. Постановлений Правительства РФ от 20.12.2022 № 2360, от 07.11.2025 № 1762)

В отношении субъектов критической информационной инфраструктуры, подведомственных государственным органам и российским юридическим лицам, указанным в абзаце первом настоящего пункта, мониторинг представления актуальных и достоверных сведений осуществляется этими государственными органами и российскими юридическими лицами.

(в ред. Постановления Правительства РФ от 20.12.2022 № 2360)

Мониторинг осуществляется регулярно путем запроса и оценки информации о сроках представления, актуальности и достоверности сведений, указанных в пункте 17 настоящих Правил. Актуальность и достоверность сведений может подтверждаться государственными органами и российскими юридическими лицами, указанными в абзаце первом настоящего пункта, путем ознакомления с объектами критической информационной инфраструктуры по месту их нахождения.

(в ред. Постановления Правительства РФ от 20.12.2022 № 2360)

Государственные органы и российские юридические лица, указанные в абзаце первом настоящего пункта, по результатам мониторинга не позднее 30 дней со дня выявления нарушений направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения:

о нарушении сроков работ по категорированию;

о нарушении отраслевых особенностей категорирования;

о представлении в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, неактуальных либо недостоверных сведений;

о выявлении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, которые соответствуют типовым объектам критической информационной инфраструктуры,

включенным в перечни типовых отраслевых объектов критической информационной инфраструктуры, и категорирование которых не проведено.
(в ред. Постановления Правительства РФ от 07.11.2025 № 1762)
(п. 19.2 введен Постановлением Правительства РФ от 24.12.2021 № 2431)

19.3. К мониторингу, указанному в пункте 19^2 настоящих Правил, государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, могут привлекать подведомственные им организации в части оценки актуальности и достоверности сведений, указанных в пункте 17 настоящих Правил.
(в ред. Постановления Правительства РФ от 20.12.2022 № 2360)

Организации, привлекаемые к оценке актуальности и достоверности сведений, указанных в пункте 17 настоящих Правил, должны иметь в соответствии с Законом Российской Федерации «О государственной тайне» лицензию на проведение работ с использованием сведений, составляющих государственную тайну, а также в соответствии с Федеральным законом «О лицензировании отдельных видов деятельности» лицензию на деятельность по технической защите конфиденциальной информации в части оказания услуг по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации и (или) услуг по мониторингу информационной безопасности средств и систем информатизации.
(в ред. Постановления Правительства РФ от 20.12.2022 № 2360)

Состав организаций, привлекаемых к оценке актуальности и достоверности сведений, указанных в пункте 17 настоящих Правил, определяется государственными органами и российскими юридическими лицами, выполняющими функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, в соответствии с критериями, определяемыми указанными органами и российскими юридическими лицами по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.
(в ред. Постановления Правительства РФ от 20.12.2022 № 2360)

Перечни организаций, привлекаемые к оценке актуальности и достоверности сведений, указанных в пункте 17 настоящих Правил, размещаются государственными органами и российскими юридическими лицами, выполняющими функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию

в установленной сфере деятельности, на их официальных сайтах в информационно-телекоммуникационной сети «Интернет».
(в ред. Постановления Правительства РФ от 20.12.2022 № 2360)

Порядок проведения в отношении субъектов критической информационной инфраструктуры, осуществляющих деятельность в каждой из областей (сфер), приведенных в пункте 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», оценки актуальности и достоверности сведений, указанных в пункте 17 настоящих Правил, определяется государственными органами и российскими юридическими лицами, выполняющими функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности.
(в ред. Постановления Правительства РФ от 20.12.2022 № 2360)
(п. 19.3 введен Постановлением Правительства РФ от 19.08.2022 № 1463)

20. Категория значимости может быть изменена в порядке, предусмотренном для категорирования, в случаях, предусмотренных частью 12 статьи 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

21. Субъект критической информационной инфраструктуры не реже чем один раз в 5 лет, если иные сроки не установлены отраслевыми особенностями категорирования, а также в случае изменения показателей критериев значимости объектов критической информационной инфраструктуры или их значений, отраслевых особенностей категорирования осуществляет пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий (в части внесенных изменений) в соответствии с настоящими Правилами. В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются в федеральный орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.
(в ред. Постановлений Правительства РФ от 13.04.2019 № 452, от 07.11.2025 № 1762)

22. В случае выявления субъектом критической информационной инфраструктуры вновь создаваемых объектов критической информационной инфраструктуры, которые не соответствуют типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, включенных в перечни типовых отраслевых объектов критической информационной инфраструктуры, но масштаб возможных последствий в случае возникновения компьютерных инцидентов на которых соответствует показателям критериев значимости и их значениям, субъект критической информационной

инфраструктуры присваивает указанному объекту одну из категорий значимости, направляет сведения о таком объекте, указанные в пункте 17 настоящих Правил, 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.

(п. 22 введен Постановлением Правительства РФ от 07.11.2025 № 1762)

УТВЕРЖДЕН
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. № 127
(в ред. постановлений
Правительства Российской
Федерации
от 13 апреля 2019 г. № 452,
от 20 декабря 2022 г. № 2360,
от 7 ноября 2025 г. № 1762)

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[1)] или нарушение функционирования[2)] объектов обеспечения жизнедеятельности населения[3)], оцениваемые:			

	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	в пределах территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования (численностью от 2 тыс. чел.) 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
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 2, но менее 1 000	более или равно 1 000, но менее 5 000	более или равно 5 000
3.	Прекращение[1)] или нарушение функционирования[2)] объектов транспортной инфраструктуры, организаций, осуществляющих деятельность в области грузовых и пассажирских перевозок, транспортных средств, в том числе			

	высокоавтоматизированных транспортных средств, оцениваемые:			
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг (пассажирских и грузовых перевозок)	в пределах территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования (численностью от 2 тыс. человек) 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
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 2, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
	в) по типам нарушенных перевозок и грузов	мультимодальные и интермодальные перевозки	перевозка, погрузка, разгрузка, хранение опасных грузов, на	перевозка, погрузка, разгрузка, хранение опасных грузов, на

			перевозку которых требуется специальное разрешение, и (или) грузов повышенной опасности в пределах территории одного субъекта Российской Федерации	перевозку которых требуется специальное разрешение, и (или) грузов повышенной опасности в пределах территорий 2 и более субъектов Российской Федерации
	г) по категорированию объектов транспортной инфраструктуры[7)]	объект транспортной инфраструктуры 3-й или 4-й категории	объект транспортной инфраструктуры 2-й категории	объект транспортной инфраструктуры 1-й категории
4.	Прекращение[1)] или нарушение[2)] функционирования сети связи, оцениваемые:			
	а) по количеству абонентов, для которых могут быть недоступны услуги связи (тыс. человек)	более или равно 3, но менее 1 000	более или равно 1 000, но менее 5 000	более или равно 5 000
	б) по уровню органа государственной	орган	федеральный орган	Администрация

	власти (количеству органов) или организации, для которых могут быть нарушены или недоступны услуги связи	государственной власти субъекта Российской Федерации	государственной власти, государственная корпорация, Центральный банк Российской Федерации, 2 и более органа государственной власти субъекта Российской Федерации	Президента Российской Федерации, Правительство Российской Федерации, Федеральное Собрание Российской Федерации, Совет Безопасности Российской Федерации, Верховный Суд Российской Федерации, Конституционный Суд Российской Федерации, 2 и более федеральных органа государственной власти
5.	Отсутствие доступа к государственной услуге, оцениваемое			
	а) в максимальном допустимом времени, в	менее или равно 24,	менее или равно 12,	менее или равно 6

	течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	но более 12	но более 6	
	б) во времени с момента приема запроса о предоставлении государственной услуги органом, предоставляющим государственную услугу, или подведомственной государственному органу организацией, участвующей в предоставлении государственной услуги в течение которого государственная услуга не может быть оказана (в процентах от времени предоставления услуги, предусмотренного административным регламентом)	менее или равно 30	более 30, но менее или равно 70	более 70
II. Политическая значимость				
6.	Прекращение[1)] или нарушение[2)] функционирования государственного органа или организации, созданной на основании федерального закона, в части невыполнения возложенной на них функции (полномочия)	Прекращение[1)] или нарушение[2)] функционирования органа государственной власти субъекта Российской Федерации	Прекращение[1)] или нарушение[2)] функционирования федерального органа государственной власти, государственной корпорации, Центрального банка Российской Федерации, 2 и более органов	Прекращение[1)] или нарушение[2)] функционирования Администрации Президента Российской Федерации, Правительства Российской Федерации,

			государственной власти субъекта Российской Федерации	Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации, 2 и более федеральных органов государственной власти
7.	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	нарушение условий договора межведомственного характера (срыв переговоров или подписания)	нарушение условий межправительственного договора (срыв переговоров или подписания)	нарушение условий межгосударственного договора (срыв переговоров или подписания)
III. Экономическая значимость				
8.	Возникновение ущерба субъекту	более или равно 1,	более 10, но менее	более 20

	критической информационной инфраструктуры, который является государственной корпорацией**,** государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом[4)], стратегическим предприятием[4)], оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший пятилетний период)	но менее или равно 10	или равно 20	
9.	Возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)	более 0,0003, но менее или равно 0,0006	более 0,0006, но менее или равно 0,001	более 0,001
10.	Прекращение[1)] или нарушение[2)] проведения клиентами операций по осуществлению перевода денежных средств,	менее или равно 70	более 70, но менее или равно 120	более 120

	осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации оператором платформы цифрового рубля, системно значимой кредитной организацией, кредитной организацией, выполняющей функции оператора услуг платежной инфраструктуры системно и социально значимых платежных систем, кредитной организацией, значимой на рынке платежных услуг, оператором услуг платежной инфраструктуры, оказывающим услуги платежной инфраструктуры в рамках системно значимых платежных систем, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)			
10.1	Прекращение[1)] или нарушение[2)] проведения операций по исполнению обязательств, осуществляемых субъектом критической информационной инфраструктуры, являющимся центральным контрагентом,	менее 1	более или равно 1, но менее 10	более или равно 10

	среднедневной размер обязательств которого по передаче денежных средств в валюте Российской Федерации по итогам клиринга за последние 12 месяцев (трлн. рублей)			
10.2	Прекращение[1)] или нарушение[2)] проведения учетно-расчетных операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся центральным депозитарием и регистратором финансовых транзакций, среднедневное количество ценных бумаг (ISIN) российских эмитентов, которые учитывались на счетах в центральном депозитарии (оцениваемые за последние 12 месяцев в тыс. штук)	менее 10	более или равно 10, но менее 25	более или равно 25
10.3	Прекращение[1)] или нарушение[2)] проведения операций по выплатам, передаче и размещению денежных средств, осуществляемых субъектом критической информационной инфраструктуры, являющимся негосударственным пенсионным фондом, которые оцениваются объемом активов (суммой пенсионных накоплений и пенсионных резервов) негосударственного пенсионного фонда	более или равно 50, но менее 1000	более или равно 1000, но менее 2000	более или равно 2000

	(млрд. рублей)			
10.4	Прекращение[1)] или нарушение[2)] проведения операций по выплатам, перестрахованию, инвестициям, осуществляемых субъектом критической информационной инфраструктуры, являющимся страховой организацией, которые оцениваются объемом активов страховой организации (млрд. рублей)	более или равно 100, но менее 1500	более или равно 1500, но менее 5000	более или равно 5000
10.5	Прекращение[1)] или нарушение[2)] выполнения функций по переводу денежных средств, осуществляемых субъектом критической информационной инфраструктуры, являющимся оператором услуг информационного обмена (некредитной организацией), который оценивается количеством заключенных договоров с кредитными организациями	более или равно 25, но менее 100	более или равно 100, но менее 150	более или равно 150
10.6	Прекращение[1)] или нарушение[2)] выполнения деятельности по предоставлению потребительских займов субъектом критической информационной инфраструктуры, являющимся микрофинансовой компанией, которые оцениваются суммой микрозаймов, выданных за годовой отчетный период	более или равно 100, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000

	(млрд. рублей)			
10.7	Прекращение[1)] или нарушение[2)] предоставления пользователям кредитных историй и субъектам кредитных историй услуг, предусмотренных Федеральным законом «О кредитных историях», субъектом критической информационной инфраструктуры, являющимся бюро кредитных историй, которые оцениваются количеством кредитных историй, хранящихся в бюро кредитных историй (млн. единиц)	более или равно 30, но менее 200	более или равно 200, но менее 500	более или равно 500
IV. Экологическая значимость				
11.	Вредные воздействия на окружающую среду[5)], оцениваемые:			
	а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	в пределах территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города федерального значения,	выход за пределы территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города федерального значения, но не за пределы	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной

		с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры	территории одного субъекта Российской Федерации или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры	инфраструктуры
	б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	более или равно 2, но менее 1 000	более или равно 1 000, но менее 5 000	более или равно 5 000
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
12.	Прекращение[1)] или нарушение функционирования[2)] (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	прекращение[1)] или нарушение функционирования[2)] пункта управления или ситуационного центра органа государственной власти субъекта Российской Федерации или города федерального	прекращение[1)] или нарушение функционирования[2)] пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации	прекращение[1)] или нарушение функционирования[2)] пункта управления государством или ситуационного центра Администрации Президента Российской Федерации, Правительства Российской

		значения		Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации
13.	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое:			
	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	более 0, но менее или равно 10	более 10, но менее или равно 15	более 15
	б) в увеличении времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции)	более 0, но менее или равно 10	более 10, но менее или равно 40	более 40
13.1	Снижение показателей государственного	соисполнитель,	исполнитель контракта	головной исполнитель

	оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое по его статусу в кооперации головного исполнителя поставок продукции по государственному оборонному заказу	субподрядчик или поставщик части продукции, работ и услуг в рамках контракта по государственному оборонному заказу совместно с исполнителем, заключившим контракт с головным исполнителем государственного оборонного заказа	по государственному оборонному заказу, заключивший контракт с головным исполнителем государственного оборонного заказа	поставок продукции, работ и услуг по государственному оборонному заказу
14.	Прекращение[1)] или нарушение функционирования[2)] (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка[6)], оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	менее или равно 4, но более 2	менее или равно 2, но более 1	менее или равно 1

[1)] Полное прекращение процессов (функций), выполняемых (контролируемых) объектом. Состояние такого прекращения может быть определено в отраслевых особенностях категорирования объектов критической информационной инфраструктуры.

[2)] Отклонение значений процессов (функций), выполняемых (контролируемых и (или) обеспечиваемых) объектом, от заданных параметров, в том числе временных параметров и параметров надежности, от проектных или штатных режимов функционирования. Состояние такого нарушения может

быть определено в отраслевых особенностях категорирования объектов критической информационной инфраструктуры.

[3)] Объекты, обеспечивающие водо-, тепло-, газо- и электроснабжение населения.

[4)] Включен в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. N 1009 «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ»

[5)] Ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия.

[6)] Не распространяется на системы технических средств для обеспечения оперативно-разыскных мероприятий.

[7)] В соответствии с требованиями Федерального закона «О транспортной безопасности».