



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.)

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)

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, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

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) определение процессов, указанных в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее - критические процессы);

в) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

г) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее - перечень объектов);

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.

В случае если ни один из показателей критериев значимости неприменим для объекта критической информационной инфраструктуры или объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, категория значимости не присваивается.

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 о критических процессах субъекта критической информационной инфраструктуры.

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 или индивидуальными предпринимателями, 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 или индивидуальными предпринимателями.

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) процессы, указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

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);

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.

11. Для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается постоянно действующая комиссия по категорированию, в состав которой включаются:

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 в состав комиссии могут быть включены работники не указанных в пункте 11 настоящих Правил подразделений, в том числе финансово-экономического подразделения.

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.

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.

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) определяет процессы, указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры;

в) выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, готовит предложения для включения в перечень объектов, а также оценивает необходимость категорирования вновь создаваемых информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей;

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;

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

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 является прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба.

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 функционирования вследствие компьютерной атаки объекта критической информационной инфраструктуры, от которого зависит оцениваемый объект.

14.3. В случае если осуществление критического процесса зависит от осуществления иных критических процессов, предусмотренная подпунктом «е» пункта 14 настоящих Правил оценка проводится исходя из совокупного масштаба возможных последствий от нарушения или прекращения функционирования всех выполняемых критических процессов.

15. 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.

По мере необходимости указанный перечень может быть изменен в порядке, предусмотренном для его разработки и утверждения.

Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений).

Перечень объектов в течение 10 рабочих дней после утверждения направляется в печатном и электронном виде в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

В перечень объектов в том числе включаются объекты критической информационной инфраструктуры филиалов, представительств субъекта критической информационной инфраструктуры.

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.

Допускается оформление единого акта по результатам категорирования нескольких объектов критической информационной инфраструктуры,

принадлежащих одному субъекту критической информационной инфраструктуры.

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:

- 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;

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

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.

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» пункта 17 настоящих Правил, в течение 10 рабочих дней после ввода объекта критической информационной инфраструктуры в эксплуатацию (принятия на снабжение).

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".

19¹. В случае изменения сведений, указанных в подпунктах "а" — "е" пункта 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.

19². 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 подпунктах "а" - "е" пункта 17 настоящих Правил.

Мониторинг осуществляется регулярно путем запроса и оценки информации о сроках представления, актуальности и достоверности сведений, указанных в подпунктах "а" - "е" пункта 17 настоящих Правил.

При выявлении по результатам мониторинга нарушения сроков работ по категорированию, представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, неактуальных либо недостоверных сведений государственные органы и российские юридические лица, указанные в абзаце первом настоящего пункта, направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о выявленных нарушениях.

19³. К мониторингу, указанному в пункте 19² 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 подпунктах "а" - "е" пункта 17 настоящих Правил.

Организации, привлекаемые к оценке актуальности и достоверности сведений, указанных в подпунктах "а" - "е" пункта 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.

Состав организаций, привлекаемых к оценке актуальности и достоверности сведений, указанных в подпунктах "а" - "е" пункта 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.

Перечни организаций, привлекаемые к оценке актуальности и достоверности сведений, указанных в подпунктах "а" - "е" пункта 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».

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 подпунктах "а" - "е" пункта 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.

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, а также в случае изменения показателей критериев значимости объектов критической информационной инфраструктуры или их значений осуществляет пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий 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.

_____ УТВЕРЖДЕН
постановлением
Правительства
Российской Федерации
от 8 февраля 2018 г. № 127
(в ред. постановления Правительства
Российской Федерации
от 13 апреля 2019 г. № 452)

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, оцениваемые:			

	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	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, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 2, но менее 1 000	более или равно 1 000, но менее 5 000	более или равно 5 000
4.	Прекращение ¹⁾ или нарушение функционирования ²⁾ сети связи, оцениваемое 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
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого	менее или равно 24, но более 12	менее или равно 12, но более 6	менее или равно 6

	государственная услуга может быть недоступна для получателей такой услуги (часов)			
II. Политическая значимость				
6.	Прекращение ¹⁾ или нарушение функционирования ²⁾ государственного органа в части невыполнения возложенной на него функции (полномочия)	Прекращение ¹⁾ или нарушение функционирования ²⁾ органа государственной власти субъекта Российской Федерации или города федерального значения	Прекращение ¹⁾ или нарушение функционирования ²⁾ федерального органа государственной власти	Прекращение ¹⁾ или нарушение функционирования ²⁾ Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации

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 критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, 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)	более или равно 1, но менее или равно 10	более 10, но менее или равно 20	более 20

9.	Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый трехлетний период)	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
10.	Прекращение ¹⁾ или нарушение ²⁾ проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц)	более 3, но менее или равно 70	более 70, но менее или равно 120	более 120

	(расчет осуществляется по итогам года, а для создаваемых объектов – на основе прогнозных значений)			
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, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры	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, с выходом вредных воздействий за пределы территории субъекта критической	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры

			информационной 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 значения	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 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 выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	более 0, но менее или равно 10	более 10, но менее или равно 40	более 40
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	менее или равно 4, но более 2	менее или равно 2, но более 1	менее или равно 1

	система может быть недоступна пользователю (часов)			
--	---	--	--	--

¹⁾ Полное прекращение выполнения критического процесса.

²⁾ Отклонение значений параметров критического процесса, в том числе временных параметров и параметров надежности, от проектных (штатных) режимов функционирования.

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. № 1009.

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

⁶⁾ Не распространяется на системы технических средств для обеспечения функций оперативно-розыскных мероприятий.».
