Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

П О С Т А Н О В Л Е Н И Е

от "___"_____ №_____

Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры, функционирующих в области ракетно-космической промышленности

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

1 Утвердить прилагаемые отраслевые особенности категорирования объектов критической информационной инфраструктуры, функционирующих в области ракетно-космической промышленности.

2. Настоящее постановление вступает в силу с 1 сентября 2025 г.

Председатель Правительства
Российской Федерации М. Мишустин

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от "___"_____ 2025 № _____

О Т Р А С Л Е В Ы Е О С О Б Е Н Н О С Т И
категорирования объектов критической информационной инфраструктуры, функционирующих в области ракетно-космической промышленности

I. Общие положения

1. Настоящие отраслевые особенности предназначены для проведения категорирования объектов критической информационной инфраструктуры, функционирующих в области ракетно-космической промышленности (далее - объекты критической информационной инфраструктуры) и являющихся информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления, принадлежащих на праве собственности, аренды или на ином законном основании субъектам критической информационной инфраструктуры.

2. Настоящие отраслевые особенности определяют процедуру категорирования объектов критической информационной инфраструктуры, соответствующих перечням типовых отраслевых объектов критической информационной инфраструктуры, предусмотренных пунктом 4 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - перечень типовых отраслевых объектов критической информационной инфраструктуры).

3. Категорирование 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 (далее соответственно - правила, перечень) и настоящими отраслевыми особенностями.

4. Категорирование объектов критической информационной инфраструктуры включает в себя:

а) выявление объектов критической информационной инфраструктуры, соответствующих перечню типовых отраслевых объектов критической информационной инфраструктуры;

б) оценку в соответствии с перечнем масштаба возможных последствий в случае нарушения или прекращения функционирования объектов критической информационной инфраструктуры;

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

5. С целью осуществления категорирования объектов критической информационной инфраструктуры решением руководителя субъекта критической информационной инфраструктуры создается постоянно действующая комиссия по категорированию объектов критической информационной инфраструктуры (далее - комиссия по категорированию), согласно пунктам 11 - 13 правил.

Комиссия по категорированию создается приказом руководителя субъекта критической информационной инфраструктуры.

Работа комиссии по категорированию регламентируется внутренним нормативным актом субъекта критической информационной инфраструктуры.

6. Комиссия по категорированию в ходе своей работы:

а) выявляет объекты критической информационной инфраструктуры, соответствующие перечню типовых отраслевых объектов критической информационной инфраструктуры;

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

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

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

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

7. 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 (уполномоченным заместителем руководителя) субъекта критической информационной инфраструктуры.

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

II. Порядок установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений в целях присвоения ему одной из категорий значимости

8. С целью установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений субъектом критической информационной инфраструктуры должны быть определены объекты критической информационной инфраструктуры, подлежащие категорированию, а также выявлены процессы, нарушение или прекращение которых может привести к прекращению или нарушению функционирования объектов критической информационной инфраструктуры.

Категорированию подлежат объекты критической информационной инфраструктуры, принадлежащие субъекту критической информационной инфраструктуры на праве собственности, аренды или на ином законном основании, соответствующие типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления отраслевых объектов критической информационной инфраструктуры, функционирующим в области ракетно-космической промышленности.

9. В случае выявления субъектом критической информационной инфраструктуры каналов взаимодействия различных информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления, решением субъекта критической информационной инфраструктуры такие системы могут быть объединены в один объект критической информационной инфраструктуры.

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

11. В случае выявления субъектом критической информационной инфраструктуры объектов критической информационной инфраструктуры, не соответствующих перечню типовых отраслевых объектов критической информационной инфраструктуры, но масштаб возможных последствий в случае нарушения или прекращения их функционирования, сбоев ключевых функций субъекта критической информационной инфраструктуры соответствуют показателям критериев значимости и их значениям, субъект критической информационной инфраструктуры обязан присвоить указанному объекту одну из категорий значимости и направить сведения о таком объекте в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, а также предложения о дополнении перечня типовых отраслевых объектов критической информационной инфраструктуры.

12. Субъект критической информационной инфраструктуры направляет в Государственную корпорацию по космической деятельности "Роскосмос", следующие утвержденные документы:

а) перечень объектов критической информационной инфраструктуры, подлежащих категорированию;

б) протоколы заседаний комиссии по категорированию;

в) акты категорирования объектов критической информационной инфраструктуры;

г) сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, направляемые субъектом критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта категорирования в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

13. К субъектам критической информационной инфраструктуры применимы следующие показатели перечня:

а) "причинение ущерба жизни и здоровью людей";

б) "возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, 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 5-летний период)" - для субъектов критической информационной инфраструктуры, которые являются государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием;

в) "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)" - для субъектов критической информационной инфраструктуры, которые являются организацией, на которую в соответствии с Налоговым кодексом Российской Федерации возложена обязанность уплачивать соответственно налоги, сборы, страховые взносы;

г) "вредные воздействия на окружающую среду" - для субъектов критической информационной инфраструктуры, объекты критической

информационной инфраструктуры которых относятся к опасным производственным объектам в соответствии с законодательством Российской Федерации;

д) "снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры" - для субъектов критической информационной инфраструктуры являющихся головными исполнителями или исполнителями по государственному оборонному заказу и их объектов критической информационной инфраструктуры, задействованных в разработке, производстве, поставке продукции по государственному оборонному заказу;

е) "снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое по его статусу в кооперации головного исполнителя поставок продукции по государственному оборонному заказу".

III. Признаки значимости объектов критической информационной инфраструктуры, соответствующие критериям значимости и показателям их значений

14. Определение категории значимости объектов критической информационной инфраструктуры осуществляется субъектом критической информационной инфраструктуры исходя из возможности возникновения нарушения или прекращения функционирования объектов критической информационной инфраструктуры и зависит от:

а) участия объекта критической информационной инфраструктуры в осуществлении деятельности, полномочий и функций субъекта критической информационной инфраструктуры;

б) нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры в результате целенаправленного воздействия программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры;

в) ущерба субъекту критической информационной инфраструктуры, являющемуся государственной корпорацией, государственным унитарным предприятием, государственной компанией, акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности такого субъекта (процентов

от годового объема доходов, усредненного за прошедший пятилетний период);

г) 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 трехлетний период);

д) выполнения субъектом критической информационной инфраструктуры государственного оборонного заказа.

15. В целях определения категории значимости объектов критической информационной инфраструктуры для каждого объекта критической информационной инфраструктуры:

а) определяется выполнение объектом критической информационной инфраструктуры субъекта критической информационной инфраструктуры одного или нескольких его процессов, или участие объекта в выполнении такого процесса;

б) оценивается масштаб последствий при нарушении или прекращении функционирования объектов критической информационной инфраструктуры;

в) оценивается масштаб последствий при невыполнении поставленных задач, необходимой продукции или неисполнения государственного оборонного заказа объектом критической информационной инфраструктуры.

16. Оценка проводится по каждому из значений показателя перечня, категория значимости присваивается объекту критической информационной инфраструктуры по наивысшему значению одного из этих показателей перечня.

17. При оценке масштаба последствий при нарушении безопасности объектов критической информационной инфраструктуры субъект критической информационной инфраструктуры:

а) рассматривает наихудшие сценарии последствий нарушения или прекращения функционирования объектов критической информационной инфраструктуры, результатом которых является нарушение и (или) прекращение функционирования субъекта критической информационной инфраструктуры;

б) определяет зависимость функционирования одного объекта критической информационной инфраструктуры от функционирования

другого объекта критической информационной инфраструктуры внутри субъекта критической информационной инфраструктуры;

в) выявляет статистические данные о компьютерных атаках, компьютерных инцидентах, нарушению или полному прекращению функционирования объектов критической информационной инфраструктуры, произошедших ранее у субъекта критической информационной инфраструктуры.

IV. Порядок расчета значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры в области ракетно-космической промышленности

18. Для показателя перечня "причинение ущерба жизни и здоровью людей (человек)" комиссии по категорированию необходимо провести оценку объекта критической информационной инфраструктуры, анализ проектной и эксплуатационной документации на объект критической информационной инфраструктуры, статистические данные по нештатным ситуациям у субъекта критической информационной инфраструктуры, иных документов, указывающих на потенциальную опасность объекта критической информационной инфраструктуры.

По результатам оценки объекта критической информационной инфраструктуры и документов на него комиссией по категорированию определяется наличие факторов влияющих на жизнь и здоровье людей в случае изменения параметров функционирования объекта критической информационной инфраструктуры, а также учитывается количество человек, потенциально находящихся в зоне поражения при возникновении чрезвычайной ситуации.

Полученные данные сравниваются с показателями, приведенными в соответствующем показателе критериев значимости перечня.

19. Расчет показателя "возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, 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 5-летний период)" проводится на основании:

а) налоговой отчетности и деклараций за предыдущий пятилетний период, определяется усредненный суммарный годовой размер выплачиваемых субъектом критической информационной инфраструктуры в бюджеты Российской Федерации в соответствии с Налоговым кодексом Российской Федерации налогов (R_{Σ});

б) сведений управленческого и бухгалтерского учета за прошлый пятилетний период определяется усредненный размер годового дохода ($R_{год}$);

в) регламентов проведения профилактических работ объектов критической информационной инфраструктуры определяет максимально допустимый период простоя ($t_{доп}$);

г) эксплуатационных, технических, договорных и (или) иных документов определяется время, требуемое для устранения последствий компьютерной атаки ($t_{устр}$), при отсутствии таких документов используются статистические данные за прошлый пятилетний период, а в случае отсутствия статистических данных за прошлый пятилетний период принимается $t_{устр} = 10$ суток;

д) ущерб субъекта критической информационной инфраструктуры от компьютерной атаки (U) рассчитывается по формуле:

$$U = [(R_{год}+R_{\Sigma})/ 365] \times (t_{устр} - t_{доп})$$

Полученный возможный ущерб субъекта критической информационной инфраструктуры от компьютерной атаки сопоставляется с показателем усредненного размера годового дохода и определяется показатель возможного ущерба по формуле:

$$U_{\%}=U/R_{год}* 100$$

Полученные данные сравниваются с показателями, приведенными в соответствующем показателе критериев значимости перечня.

20. Расчет показателя "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)" проводится на основании:

а) налоговой отчетности и деклараций за предыдущий пятилетний период определяется усредненный суммарный годовой размер выплачиваемых субъектом критической информационной инфраструктуры

в бюджеты Российской Федерации в соответствии с Налоговым кодексом Российской Федерации налогов (R_{Σ});

б) сведений управленческого и бухгалтерского учета за прошлый пятилетний период определяется усредненный размер годового дохода ($R_{год}$);

в) регламентов проведения профилактических работ объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры, определяет максимально допустимый период простоя ($t_{доп}$);

г) эксплуатационных, технических, договорных и (или) иных документов определяется время, требуемое для устранения последствий компьютерной атаки ($t_{устр}$), при отсутствии таких документов используются статистические данные за прошлый пятилетний период, а в случае отсутствия статистических данных за прошлый пятилетний период принимается $t_{устр} = 10$ суток;

д) ущерб бюджету Российской Федерации от компьютерной атаки (U) рассчитывается по формуле:

$$U = [(R_{год}+R_{\Sigma})/ 365] \times (t_{устр} - t_{доп})$$

Полученный возможный ущерб бюджету Российской Федерации от компьютерной атаки сопоставляется с показателем усредненного размера годового дохода и определяется показатель возможного ущерба по формуле:

$$U_{\%}=U/R_{год}* 100$$

Полученные данные сравниваются с показателями, приведенными в пункте 9 перечня.

21. Расчет показателя "вредные воздействия на окружающую среду" рассчитывается на основании:

а) объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры, которые относятся к опасным производственным объектам в соответствии с законодательством Российской Федерации;

б) объектов критической информационной инфраструктуры, имеющихся у субъекта критической информационной инфраструктуры, задействованных в процессах и участвующих в обработке информации, необходимой для управления, контроля или мониторинга опасными производственными объектами;

в) данных о территории, на которой окружающая среда может подвергнуться вредным воздействиям, сравниваются с показателями, приведенными в подпункте "а" пункта 11 перечня, в соответствии с чем определяется категория значимости такого объекта критической информационной инфраструктуры;

г) данных по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек), сравниваются с показателями, приведенными в подпункте "б" пункта 11 перечня, на основании которых и определяется категория значимости такого объекта критической информационной инфраструктуры.

По результатам полученных показателей готовится заключение о присвоении объекту критической информационной инфраструктуры наивысшей категории значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий, исходя из реализации наихудшего сценария одной целенаправленной компьютерной атаки.

22. Расчет показателя "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), должен оцениваться для прогнозируемого нарушения, которое может повлечь снижение объема соответствующей продукции;

алгоритм расчета показателя критерия:

на основании эксплуатационных, технических, договорных и (или) иных документов определяется время, требуемое для устранения последствий компьютерной атаки ($t_{устр}$), при отсутствии таких документов используются статистические данные за прошлый пятилетний период, а в случае отсутствия статистических данных за прошлый пятилетний период принимается $t_{устр} = 10$ суток;

на основании регламентов проведения профилактических работ объектов критической информационной инфраструктуры определяется максимально допустимый период простоя ($t_{доп}$);

количество дней, заложенных в государственном оборонном заказе, выполняемым (обеспечиваемым) субъектом критической информационной инфраструктуры (предлагается использовать срок реализации государственного оборонного заказа, например: 365 дней);

выполняется оценка максимальной оценочной длительности разового нарушения работоспособности объекта критической

информационной инфраструктуры с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления. Увеличение времени выполнения государственного оборонного заказа (T_{max}):

$$T_{max} = (t_{устр} - t_{доп})$$

снижение объемов продукции (работ, услуг) осуществляется в процентах от заданного объема продукции ($V_{пр.}$):

$$V_{пр.} = (T_{max} / 365) * 100$$

В случае, если рассматриваемый объект критической информационной инфраструктуры не является непосредственно производственным объектом, то необходимо рассмотреть объекты критической информационной инфраструктуры, на которые он оказывает влияние и выполнение которых будет невозможно или усложнится в случае нарушения данного процесса. В случае, если объект критической информационной инфраструктуры оказывает влияние на несколько производственных объектов, реализующих продукцию или услуги по государственному оборонному заказу, расчет потерь должен выполняться для каждого подобного объекта и суммироваться.

Полученные данные сравниваются с показателями, приведенными в соответствующем показателе критериев значимости перечня.

б) в увеличении времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции) алгоритм расчета показателя критерия:

на основании эксплуатационных, технических, договорных и (или) иных документов определяется время, требуемое для устранения последствий компьютерной атаки ($t_{устр}$), при отсутствии таких документов используются статистические данные за прошлый пятилетний период, а в случае отсутствия статистических данных за прошлый пятилетний период принимается $t_{устр}$ = 10 суток;

на основании регламентов проведения профилактических работ объекта критической информационной инфраструктуры определяется максимально допустимый период простоя ($t_{доп}$);

количество дней, заложенных в государственном оборонном заказе, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры (например: 365 дней);

объем изготовления продукции, заложенных в государственном оборонном заказе ($V_{об.}$);

увеличения времени выполнения государственного оборонного заказа с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления ($K_{ед.пр}$);

$$K_{ед.пр} = (t_{устр} - t_{доп}) / V_{об.}$$

снижении объемов продукции (работ, услуг) ($V_{пр.}$)

$$V_{пр.} = (K_{ед.пр} / 365) * 100$$

Полученные данные сравниваются с показателями, приведенными в соответствующем показателе критериев значимости перечня.

В случае, если объект критической информационной инфраструктуры оказывает влияние на иные объекты, реализующие продукцию или услуги по государственному оборонному заказу, то расчет потерь должен выполняться либо для каждого подобного объекта, либо за основу необходимо брать минимальное время выпуска заказа;

23. Для показателя перечня "снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое по его статусу в кооперации головного исполнителя поставок продукции по государственному оборонному заказу" комиссии по категорированию необходимо провести оценку контрактов, выполняемых с помощью объекта критической информационной инфраструктуры.

По результатам экспертного анализа контрактов, комиссия по категорированию, принимает решение о категории объекта критической информационной инфраструктуры в зависимости от статуса субъекта критической информационной инфраструктуры в кооперации головного исполнителя поставок продукции по государственному оборонному заказу.

_____