Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от «___» _____ № ____

МОСКВА

Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры в сфере оборонной промышленности

В соответствии со статьей 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» Правительство Российской Федерации **п о с т а н о в л я е т**:

1. Утвердить прилагаемые отраслевые особенности категорирования объектов критической информационной инфраструктуры в сфере оборонной промышленности.

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 М. Мишустин

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

ОТРАСЛЕВЫЕ ОСОБЕННОСТИ
категорирования объектов критической информационной инфраструктуры в сфере оборонной промышленности

I. Общие положения

1. Настоящие отраслевые особенности категорирования объектов критической информационной инфраструктуры в сфере оборонной промышленности регламентируют особенности категорирования объектов критической информационной инфраструктуры в сфере оборонной промышленности (далее – объекты критической информационной инфраструктуры), определяют порядок определения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, которые на праве собственности, аренды или на ином законном основании принадлежат субъекту критической информационной инфраструктуры (далее – категорирование объекта критической информационной инфраструктуры), порядок оценки в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры, а также включают в себя отраслевые признаки значимости объектов критической информационной инфраструктуры, соответствующие критериям значимости и показателям их значений.

2. Настоящие отраслевые особенности предназначены для проведения процедуры категорирования объектов критической информационной инфраструктуры государственными органами, государственными учреждениями, российскими юридическими лицами, функционирующими в сфере оборонной промышленности, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также государственными органами, государственными учреждениями, российскими юридическими лицами, которые обеспечивают взаимодействие указанных систем или сетей (далее – субъекты критической информационной инфраструктуры).

3. Функционирование субъектов критической информационной инфраструктуры в сфере оборонной промышленности определяется наличием одного из следующих условий:

а) осуществление субъектом критической информационной инфраструктуры, в том числе входящими в его состав представительствами и филиалами, деятельности по разработке, производству, ремонту и утилизации вооружения, военной и специальной техники, а также производству товаров, используемых в составе такой продукции;

б) наличия у субъекта критической информационной инфраструктуры лицензий, сертификатов и иных разрешительных документов на виды деятельности в сфере оборонной промышленности;

в) наличия сведений о субъекте критической информационной инфраструктуры в сводном реестре организаций оборонно-промышленного комплекса, сформированном в соответствии с постановлением Правительства Российской Федерации от 20 февраля 2004 года № 96 «О сводном реестре организаций оборонно-промышленного комплекса»;

г) выполнение работ (оказание услуг) субъектом критической информационной инфраструктуры, в том числе входящими в его состав представительствами и филиалами, в рамках государственного оборонного заказа.

4. Настоящие отраслевые особенности определяют процедуру категорирования объектов критической информационной инфраструктуры, соответствующих типов информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, предусмотренных пунктом 4 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

5. В случае осуществления субъектом критической информационной инфраструктуры деятельности в сфере оборонной промышленности при проведении процедуры категорирования объектов критической информационной инфраструктуры в форме направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утверждаемой в соответствии с пунктом 2 части 3 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», в графе, касающейся сферы (области) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» указывается оборонная промышленность, при этом категорирование может осуществляться с учетом отраслевых особенностей категорирования объектов критической информационной инфраструктуры иных сфер, предусмотренных

пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

6. Процедура категорирования объектов критической информационной инфраструктуры осуществляется в соответствии со статьей 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации и перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденными постановлением Правительства Российской Федерации от 8 августа 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации , а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (далее соответственно – Правила, Перечень), в соответствии с пунктом 4 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», а также настоящими отраслевыми особенностями.

7. С целью осуществления процедуры категорирования объектов критической информационной инфраструктуры приказом руководителя субъекта критической информационной инфраструктуры создается постоянно действующая комиссия по категорированию (далее – комиссия по категорированию), в состав которой включаются:

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

б) работники субъекта критической информационной инфраструктуры, осуществляющие деятельность по направлению, соответствующему основному виду деятельности ОКВЭД2 субъекта критической информационной инфраструктуры, в области информационных технологий и связи, 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 объектов критической информационной инфраструктуры;

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

д) работники субъекта критической информационной инфраструктуры, 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;

е) работники финансово-экономического подразделения субъекта критической информационной инфраструктуры.

По решению руководителя субъекта критической информационной инфраструктуры в состав комиссии могут быть включены работники других подразделений, в том числе подразделения юридического сопровождения.

8. Работа постоянно действующей комиссии по категорированию регламентируется положением о постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры, которое вводится в действие приказом руководителя субъекта критической информационной инфраструктуры.

9. Приказом руководителя субъекта критической информационной инфраструктуры, имеющего филиалы или представительства, могут создаваться отдельные комиссии по категорированию объектов критической информационной инфраструктуры в этих филиалах, представительствах.

10. Координацию и контроль деятельности комиссий по категорированию в филиалах, представительствах осуществляет комиссия по категорированию субъекта критической информационной инфраструктуры.

11. В случае если субъект критической информационной инфраструктуры является головным юридическим лицом, имеющим в подчинении другие субъекты критической информационной инфраструктуры, являющиеся отдельными юридическими лицами, то в каждом отдельном субъекте критической информационной инфраструктуры создается отдельная комиссия по категорированию.

Координацию и контроль деятельности отдельно созданных в таком случае комиссий по категорированию, может осуществлять любая из созданных комиссий по категорированию, в соответствии с приказом руководителя головного субъекта критической информационной инфраструктуры.

12. В ходе процедуры категорирования объектов критической информационной инфраструктуры комиссия по категорированию:

а) определяет все информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, которые на праве собственности, аренды или на ином законном основании принадлежат субъекту критической информационной инфраструктуры;

б) оценивает в соответствии с Перечнем масштаб возможных последствий в случае возникновения компьютерных инцидентов на информационных системах,

информационно-телекоммуникационных сетях, автоматизированных системах управления, которые на праве собственности, аренды или на ином законном основании принадлежат субъекту критической информационной инфраструктуры;

в) на основании оценки, осуществляемой в подпункте «б» пункта 13 настоящих особенностей, определяет перечень объектов критической информационной инфраструктуры;

г) определяет актуальные угрозы, нарушителей безопасности для объектов критической информационной инфраструктуры;

д) определяет критические процессы, осуществляемые объектом критической информационной инфраструктуры;

е) принимает решение о присвоении каждому из объектов критической информационной инфраструктуры одной из категорий значимости, либо принимает решение об отсутствии необходимости присвоения им одной из категорий значимости (далее – категорирование).

13. Комиссия по категорированию подлежит расформированию в случаях:

а) прекращения соответствия государственного органа, государственного учреждения, российского юридического лица условиям, указанным в пункте 3 настоящих отраслевых особенностей;

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

в) ликвидация или реорганизация субъекта критической информационной инфраструктуры, в результате которых были утрачены признаки субъекта критической информационной инфраструктуры.

14. Итоги заседания комиссии по категорированию оформляются протоколами заседания, в которых фиксируются все принятые решения.

Допускается оформление решений комиссии по категорированию отдельными актами, которые подписываются членами комиссии по категорированию и утверждаются председателем комиссии по категорированию, с последующей фиксацией в протоколе заседания.

II. Порядок определения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, которые на праве собственности, аренды или на ином законном основании принадлежат субъекту критической информационной инфраструктуры

15. Комиссия по категорированию определяет перечень информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, являющихся объектами критической информационной инфраструктуры, на основе:

а) утвержденного Правительством Российской Федерации перечня типовых объектов критической информационной инфраструктуры в сфере оборонной промышленности;

б) результатов инвентаризации информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, используемых субъектом критической информационной инфраструктуры;

в) финансово-хозяйственных документов субъекта критической информационной инфраструктуры;

г) документов о вводе в эксплуатацию информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

16. В случае выявления при осуществлении деятельности одного субъекта критической информационной инфраструктуры взаимозависимости информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления решением комиссии по категорированию такие информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления могут быть включены в состав одного объекта критической информационной инфраструктуры.

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

III. Порядок оценки в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры

18. Комиссия по категорированию оценивает в соответствии с Перечнем масштаб возможных последствий в случае возникновения компьютерных атак и компьютерных инцидентов на всех объектах критической информационной инфраструктуры.

19. При оценке масштаба последствий возникновения компьютерных атак и компьютерных инцидентов в виде нарушения и (или) прекращения

функционирования объектов критической инфраструктуры комиссия по категорированию:

а) рассматривает наихудшие сценарии последствий проведения компьютерных атак и компьютерных инцидентов на объекты критической информационной инфраструктуры, результатом которых является нарушение и (или) прекращение функционирования объектов критической информационной инфраструктуры;

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

в) выявляет статистические данные о компьютерных атаках и компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

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

В случае если ни один из показателей Перечня не применим к объекту критической информационной инфраструктуры, или объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, то категория значимости такому объекту критической информационной инфраструктуры не присваивается.

21. Сфера оборонной промышленности имеет отраслевые признаки значимости:

а) субъектом критической информационной инфраструктуры осуществляется поставка товаров, выполнение работ, оказание услуг по договорам или контрактам в рамках государственного оборонного заказа, результатом которого является продукция, создаваемая и(или) поставляемая по технической документации, утвержденной или согласованной государственным заказчиком государственного оборонного заказа;

б) наличие у субъекта критической информационной инфраструктуры в отношении принадлежащих ему объектов критической информационной инфраструктуры декларации промышленной безопасности опасного производственного объекта в соответствии с Федеральным законом «О промышленной безопасности опасных производственных объектов»;

в) наличие информации о субъекте критической информационной инфраструктуры в перечне стратегических предприятий и стратегических акционерных обществ, утвержденном Указом Президента Российской Федерации от 4 августа 2004 г. № 1009 «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ»;

г) наличие информации о субъекте критической информационной инфраструктуры в сводном реестре организаций оборонно-промышленного комплекса, сформированном в соответствии с постановлением Правительства Российской Федерации от 20 февраля 2004 г. № 96 «О сводном реестре организаций оборонно-промышленного комплекса»;

д) поставка товаров, выполнение работ, оказание услуг субъектами критической информационной инфраструктуры по договорам или контрактам, контроль качества и приемка результатов работы которых сопровождается военными представительствами Министерства обороны Российской Федерации.

22. В соответствии с отраслевыми признаками значимости в сфере оборонной промышленности, учитывая отраслевые особенности, особое внимание необходимо уделить следующим показателям критериев значимости Перечня:

а) причинение ущерба жизни и здоровью людей (человек);

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 (процент от годового объема доходов, усредненного за прошедший 5-летний период);

в) возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процент прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период);

г) 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.

23. Для показателя Перечня «причинение ущерба жизни и здоровью людей (человек)» комиссии по категорированию необходимо провести оценку объекта критической информационной инфраструктуры на основании осмотра объекта критической информационной инфраструктуры, опроса персонала, работающего с объектом критической информационной инфраструктуры, и анализа документации (при наличии):

а) паспорт безопасности опасного производственного объекта;

б) декларации промышленной безопасности объекта;

в) проектная документация на объект критической информационной инфраструктуры;

г) эксплуатационная документация на объект критической информационной инфраструктуры;

д) планы по предупреждению и ликвидации чрезвычайных ситуаций природного и техногенного характера;

е) статистические данные по нештатным ситуациям в организации;

ж) иные документы, указывающие на потенциальную опасность объекта критической информационной инфраструктуры.

В ходе оценки необходимо определить:

а) наличие опасных факторов, источниками которых является производственное и(или) технологическое оборудование и(или) конструкции, обрабатываемое или хранимое в них сырье и(или) параметры (характеристики) и условия его обработки, в обеспечении функционирования которых участвует рассматриваемый объект критической информационной инфраструктуры;

б) расположение территориальных зон, защищаемых от опасных факторов объекта критической информационной инфраструктуры (жилые, общественно-деловые, производственные зоны, зоны инженерной и транспортной инфраструктуры, зоны сельскохозяйственного использования, зоны рекреационного назначения, зоны особо охраняемых территорий, зоны специального назначения, зоны размещения военных объектов и иные виды территориальных зон);

в) количество человек, потенциально находящихся в зоне поражения при возникновении чрезвычайной ситуации, или числа потенциальных потребителей продукции или услуг;

г) количество человек, потенциально находящихся в зоне поражения при возникновении чрезвычайной ситуации из числа персонала предприятия.

После определения вышеуказанных факторов комиссия по категорированию принимает решение о присвоении категории значимости объекту критической информационной инфраструктуры в зависимости от количества людей (человек), потенциально попадающих в зону поражения опасного фактора, или неприменимости данного показателя.

24. Для показателя Перечня «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 (процент от годового объема доходов, усредненного за прошедший 5-летний период)» комиссии по категорированию необходимо провести расчет потенциального ущерба субъекту критической информационной инфраструктуры.

Расчет показателя производится по следующей формуле:

$$U_8 = \frac{U_{y8}}{R_{\text{год}}} * 100,$$

где U_8 – показатель ущерба критической информационной инфраструктуры;

U_{y8} – ущерб субъекту критической информационной инфраструктуры от компьютерной атаки и компьютерного инцидента;

$R_{год}$ – усредненный объем годового дохода за прошедший пятилетний период.

Объем годового дохода за прошедший пятилетний период рассчитывается по следующей формуле:

$$R_{\text{год}} = \frac{\sum_{i=n}^{n+4} D_i}{5},$$

где:

D_i – доход субъекта критической информационной инфраструктуры за i-й год исчисляется в рублях;

n – значение первого года в рассматриваемый пятилетний период.

Ущерб субъекту критической информационной инфраструктуры от компьютерной атаки, компьютерного инцидента (U_{y8}) рассчитывается по формуле:

$$U_{\text{у8}} = C + A + X,$$

где:

C – суммарные затраты на объект критической информационной инфраструктуры;

A – затраты на возмещение ущерба, причиненного жизни и (или) здоровью людей или имуществу третьих лиц, исчисляются в рублях (если прекращение или нарушение работоспособности объекта критической информационной инфраструктуры не влечет за собой никакого ущерба, то $A = 0$);

X – ущерб, зафиксированный субъектом критической информационной инфраструктуры, либо вышестоящей организацией в ходе уже произошедших компьютерных инцидентов по отношению к объекту критической информационной инфраструктуры, либо аналогичных объектов, за весь период существования (если данных ситуаций не зафиксировано, то $X = 0$);

Суммарные затраты на объект критической информационной инфраструктуры, рассчитываются по формуле:

$$C = C_{\text{о}} + C_{\text{п}} + C_{\text{и}},$$

где:

C_o – общая стоимость самого ОКИИ, исчисляется в рублях;

C_n – стоимость пусконаладочных работ, исчисляется в рублях;

C_u – иные затраты на объект (например, разработка программного обеспечения).

Затраты на возмещение ущерба, причиненного людям или имуществу третьих лиц, рассчитывается по формуле[1]:

$$A = \sum_{i=1}^{m} 3000000 + \sum_{i=1}^{p} 300000 + \sum_{i=1}^{t} 750000 + \sum_{i=1}^{u} 1000000,$$

где:

m – количество пострадавших, которым необходимо возмещение вреда, причиненного их жизни/здоровью;

p – количество пострадавших, которым необходимо возмещения вреда, причиненного в связи с нарушением условий жизнедеятельности;

t – количество пострадавших, которым необходимо возмещения вреда, причиненного имуществу;

u – количество юридических лиц, которым необходимо возмещения вреда, причиненного имуществу.

Количество рассчитывается на основе Декларации промышленной безопасности субъекта КИИ, либо экспертным методом на основе анализа возможных максимальных последствий.

Ущерб, зафиксированный субъектом критической информационной инфраструктуры, либо вышестоящей организацией в ходе уже произошедших компьютерных атак и компьютерных инцидентов по отношению к объекту критической информационной инфраструктуры, либо аналогичных объектов (*X)*, за весь период существования, фактически является суммой расходов, понесенных субъектом критической информационной инфраструктуры, либо вышестоящей организацией, полученной в ходе ликвидации последствий уже случившихся компьютерных атак и компьютерных инцидентов. Рассчитывается только в том случае если компьютерные атаки, компьютерные инциденты уже происходили и субъект критической информационной инфраструктуры, либо вышестоящая организация располагают данными о данных происшествиях.

Рассчитанный показатель возможного ущерба *(U_8)* субъекту критической информационной инфраструктуры сопоставляется с показателями, приведенными в пункте 8 Перечня, объекту критической информационной инфраструктуры Российской Федерации и их значений, и дается заключение о присвоении объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.

25. Для показателя Перечня «возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процент прогнозируемого годового дохода федерального бюджета, усредненного

[1] Суммы возмещения ущерба основаны на размерах страховых выплат, установленных в Федеральном законе «Об обязательном страховании гражданской ответственности владельца опасного объекта за причинение вреда в результате аварии на опасном объекте»

за планируемый 3-летний период)» комиссии по категорированию необходимо провести расчет потенциального ущерба бюджету Российской Федерации.

Расчет показателя производится по следующей формуле:

$$U_9 = \frac{U_{y9}}{N_{\text{уср}}} * 100,$$

где:

U_9 – показатель ущерба бюджетам Российской Федерации;

U_{y9} – снижение выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры, которое может быть следствием прекращения или нарушения критических процессов, исчисляется в рублях;

$N_{уср}$ – усредненный размер прогнозируемого годового дохода федерального бюджета за прошедший трехлетний период (прогнозируемый годовой доход федерального бюджета, усредненный за планируемый трехлетний период с учетом действующего федерального закона о федеральном бюджете на очередной финансовый год и плановый период.

Объем дохода федерального бюджета за прошедший трехлетний период, рассчитывается по следующей формуле:

$$N_{\text{уср}} = \frac{\sum_{i=n}^{n+2} N_i}{3},$$

где:

N_i – прогнозируемый доход федерального бюджета, за i-й год, исчисляется в рублях;

n – значение первого года в рассматриваемый трехлетний период.

Перед тем как рассчитывать U_{y9} для каждого объекта критической информационной инфраструктуры рекомендуется рассчитать ущерб бюджетам Российской Федерации относительно всего субъекта критической информационной инфраструктуры. Для этого необходимо прировнять весь усредненный годовой размер выплачиваемых субъектом критической информационной инфраструктуры в бюджеты Российской Федерации в соответствии с Налоговым кодексом Российской Федерации налогов за предыдущий трехлетний период (R_c) к снижению выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры, исчисляется в рублях (U_{y9}) и воспользоваться формулой, то есть необходимо принять что:

$$U_{y9} = R_c,$$

где:

R_c – усредненный годовой размер выплачиваемых субъектом критической информационной инфраструктуры в бюджеты Российской Федерации

в соответствии с Налоговым Кодексом Российской Федерации налогов за предыдущий трехлетний период[2].

Если всего объема годовых выплат субъекта критической информационной инфраструктуры недостаточно для нанесения ущерба, соответствующего минимально установленному значению для присвоения объекту третьей категории значимости, то данный расчет проводится один раз, для всех объектов критической информационной инфраструктуры.

В случае, если всего объема годовых выплат субъекта критической информационной инфраструктуры в бюджеты Российской Федерации окажется достаточно для нанесения ущерба, соответствующего минимально установленному значению для присвоения объекту третьей категории значимости, то расчет снижения выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры, которое может быть следствием прекращения или нарушения критических процессов (U_{y9}), проводится для каждого объекта критической информационной инфраструктуры и рассчитывается по формуле:

$$U_{\text{у9}} = U_{y8} * K_{\text{н}},$$

где:

$K_н$ – коэффициент выплат (отчислений) субъекта критической информационной инфраструктуры в бюджеты Российской Федерации, осуществленных за предыдущий трехлетний период.

U_{y8} – ущерб субъекту КИИ от компьютерной атаки, компьютерного инцидента.

Ущерб субъекту критической информационной инфраструктуры (U_{y8}) рассчитывается по формуле, приведенной в пункте 27 настоящих отраслевых особенностей.

Коэффициент выплат (отчислений) субъекта критической информационной инфраструктуры в бюджеты Российской Федерации, осуществленных за предыдущий трехлетний период ($K_{нп}$), рассчитывается по следующей формуле:

$$K_{\text{нп}} = \frac{R_c}{D}$$

где:

D – усредненный годовой доход субъекта критической информационной инфраструктуры за предыдущий трехлетний период, исчисляется в рублях.

Объем дохода субъекта критической информационной инфраструктуры за прошедший трехлетний период, рассчитывается по следующей формуле:

$$D = \frac{\sum_{i=n}^{n+2} D_i}{3},$$

[2] Например, налог на прибыль (в Федеральный бюджет, в бюджет субъекта Российской Федерации), налог на добавленную стоимость, налоги, сборы и регулярные платежи за пользование природными ресурсами, социальные налоги.

где:

D_i – прогнозируемый доход субъекта критической информационной инфраструктуры, за i-й год, исчисляется в рублях;

n – значение первого года в рассматриваемый трехлетний период.

Рассчитанный показатель возможного ущерба (U_9) бюджетам Российской Федерации сопоставляется с показателями, приведенными в пункте 9 Перечня, и дается заключение о присвоении объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.

26. 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.

После 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.

IV. Порядок определения объектов критической информационной инфраструктуры, подлежащих категорированию

27. Формирование перечня объектов критической информационной инфраструктуры, осуществляется посредством отнесения принадлежащих субъекту критической информационной инфраструктуры на праве собственности, аренды или на ином законном основании информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления к соответствующим типовым отраслевым объектам критической информационной инфраструктуры в сфере горнодобывающей промышленности.

28. В перечень объектов критической информационной инфраструктуры также включаются:

а) объекты критической информационной инфраструктуры, осуществляющие выполнение критических процессов, указанных в перечне типовых отраслевых объектов критической информационной инфраструктуры**;**

б) объекты критической информационной инфраструктуры, масштаб возможных последствий в случае возникновения компьютерных атак

и компьютерных инцидентов соответствует одному из значений показателей критериев значимости, достаточному для присвоения категории значимости.

29. В случае если объект критической информационной инфраструктуры, не подпадает под действие пунктов 27 и 28 настоящих отраслевых особенностей, комиссией по категорированию принимается решение об отсутствии необходимости включения данного объекта критической информационной инфраструктуры в перечень объектов критической информационной инфраструктуры.

V. Порядок определения актуальных угроз, нарушителей безопасности для объектов критической информационной инфраструктуры

30. Комиссия по категорированию определяет актуальные угрозы, нарушителей безопасности, типы компьютерных инцидентов нарушителей для объектов, содержащихся в перечне объектов критической информационной инфраструктуры.

31. Для объектов критической информационной инфраструктуры, которые в ходе оценки масштаба возможных последствий в случае возникновения компьютерных инцидентов или проведения компьютерных атак и компьютерных инцидентов на объект критической информационной инфраструктуры получили значение в каком-либо критерии значимости, соответствующее одной из категорий значимости, необходимо при определении актуальных угроз, нарушителей безопасности для объектов критической информационной инфраструктуры руководствоваться методическими документами, разрабатываемыми Федеральной службой по техническому и экспортному контролю в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного постановлением Правительства Российской Федерации от 16 августа 2004 г. № 1085, для иных объектов критической информационной инфраструктуры для определения актуальных угроз, нарушителей безопасности применяется экспертный метод.

VI. Порядок присвоения каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятия решения об отсутствии необходимости присвоения им одной из категорий значимости

32. Комиссия по категорированию присваивает каждому из объектов критической информационной инфраструктуры, включенному в перечень объектов критической информационной инфраструктуры, одну из категорий значимости либо принимает решения об отсутствии необходимости присвоения ему одной

из категорий значимости, на основе оценки масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры.

33. 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.

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

35. Субъект критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта направляет в Федеральную службу по техническому и экспортному контролю сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, в соответствие с пунктом 17 Правил.

36. В случае выявления субъектом критической информационной инфраструктуры объектов критической информационной инфраструктуры, не соответствующих типам объектам критической информационной инфраструктуры, включенных в перечни типовых отраслевых объектов критической информационной инфраструктуры, но включенных в перечень объектов критической информационной инфраструктуры, субъект критической информационной инфраструктуры должен направить сведения о таком объекте критической информационной инфраструктуры, указанные в пункте 17 Правил, в Федеральную службу по техническому и экспортному контролю, а также направить предложения о дополнении перечней типовых отраслевых объектов критической информационной инфраструктуры в государственный орган формирующий перечни типовых отраслевых объектов

критической информационной инфраструктуры в сфере оборонной промышленности.

_____