Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

П О С Т А Н О В Л Е Н И Е

от «___» _____ № ____

МОСКВА

Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры в сфере транспорта

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 в сфере транспорта.

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 транспорта

I. Общие положения

1. Настоящие Отраслевые особенности категорирования объектов критической информационной инфраструктуры в сфере транспорта (далее – Отраслевые особенности) регламентируют особенности категорирования объектов критической информационной инфраструктуры в сфере транспорта (далее – объекты критической информационной инфраструктуры) и определяют порядок установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений в целях присвоения ему одной из категорий значимости (далее – категорирование объекта критической информационной инфраструктуры) и включают в себя отраслевые признаки значимости объектов критической информационной инфраструктуры, соответствующие критериям значимости и показателям их значений, а также порядок расчета значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры.

2. Настоящие Отраслевые особенности предназначены для использования в процессе проведения категорирования объектов критической информационной инфраструктуры государственными органами, выполняющими функции (полномочия) в сфере транспорта, государственными учреждениями, выполняющими функции (полномочия) или осуществляющими виды деятельности в сфере транспорта, российскими юридическими лицами, осуществляющими деятельность в сфере транспорта, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере транспорта, а также российскими юридическими лицами, которые обеспечивают взаимодействие указанных систем или сетей (далее – субъекты критической информационной инфраструктуры).

3. Настоящие Отраслевые особенности определяют процедуру категорирования объектов критической информационной инфраструктуры,

соответствующих типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, включенных в перечни типовых отраслевых объектов критической информационной инфраструктуры, предусмотренных пунктом 4 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

4. 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 в соответствии с пунктом 1 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее соответственно – Правила, Перечень).

5. Категорирование объектов критической информационной инфраструктуры включает в себя:

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

б) оценку в соответствии с Перечнем масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

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

6. С целью осуществления категорирования объектов критической информационной инфраструктуры, решением руководителя субъекта критической информационной инфраструктуры создается постоянно действующая комиссия по категорированию.

Комиссия по категорированию создается локальным нормативным актом (приказом или распоряжением) руководителя субъекта критической информационной инфраструктуры. Локальный нормативный акт о создании комиссии по категорированию оформляется в соответствии с правилами документооборота, принятыми в субъекте критической информационной инфраструктуры.

Локальный нормативный акт о создании комиссии по категорированию определяет (утверждает):

состав комиссии по категорированию, в том числе председателя комиссии по категорированию, заместителя председателя комиссии по категорированию, секретаря комиссии по категорированию;

порядок (положение) работы комиссии по категорированию.

В состав комиссии по категорированию включаются:

руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо;

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;

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

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

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.

7. По решению руководителя субъекта критической информационной инфраструктуры в состав комиссии могут быть включены работники, не указанные в пункте 6 настоящих Отраслевых особенностей подразделений, в том числе финансово-экономического подразделения.

8. По решению руководителя субъекта критической информационной инфраструктуры, имеющего филиалы, представительства, могут создаваться отдельные комиссии по категорированию объектов критической информационной инфраструктуры в этих филиалах, представительствах.

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

10. 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 сфере транспорта, по согласованию с такими государственными органами и российскими юридическими лицами.

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

12. Комиссия по категорированию в ходе своей работы:

а) выявляет объекты критической информационной инфраструктуры, соответствующие перечню типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта;

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 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.

13. Комиссия по категорированию подлежит расформированию в следующих случаях:

а) прекращение субъектом критической информационной инфраструктуры выполнения функций (полномочий) или осуществления видов деятельности в сфере транспорта;

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

14. Заседания комиссии по категорированию оформляются протоколами.

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.

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

15. 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, обрабатывающие информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляющие управление, контроль или мониторинг критических процессов, подлежащие категорированию, а также выявлены процессы, нарушение или прекращение которых может привести к компьютерным атакам и компьютерным инцидентам.

16. Определение объектов критической информационной инфраструктуры, подлежащих категорированию, 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 в сфере транспорта к соответствующим типовым отраслевым объектам критической информационной инфраструктуры, функционирующих в сфере транспорта.

17. В случае выявления при осуществлении деятельности одного субъекта критической информационной инфраструктуры взаимозависимости информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления решением субъекта информационной инфраструктуры такие системы могут быть включены в состав одного объекта критической информационной инфраструктуры.

18. В случае отсутствия информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления, относящихся к соответствующим типовым отраслевым объектам критической информационной инфраструктуры, функционирующих в сфере транспорта, комиссией по категорированию принимается решение об отсутствии объектов критической информационной инфраструктуры, подлежащих категорированию.

19. В случае осуществления модернизации объектов критической информационной инфраструктуры в сфере транспорта, решением субъекта критической информационной инфраструктуры объект критической информационной инфраструктуры, состоявший из нескольких систем, может быть разделен на несколько отдельных объектов критической информационной инфраструктуры.

20. В случае выявления субъектом критической информационной инфраструктуры объектов критической информационной инфраструктуры, не соответствующих типам информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, включенных в перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта, но масштаб возможных последствий в случае возникновения компьютерных атак и компьютерных инцидентов соответствует показателям критериев значимости и их значениям, субъект критической информационной инфраструктуры вправе присвоить указанному

объекту одну из категорий значимости и направить сведения о таком объекте, указанные в пункте 21 настоящих Отраслевых особенностей, в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, а также направить предложения о дополнении перечней типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта.

21. Субъект критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта, указанного в пункте 14 настоящих Отраслевых особенностей, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, следующие сведения:

а) об объекте критической информационной инфраструктуры;

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

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

г) о лице, эксплуатирующем объект критической информационной инфраструктуры;

д) 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) 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 атак и 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;

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

22. Выявление процессов, нарушение или прекращение которых может привести к компьютерным атакам и компьютерным инцидентам, осуществляется

комиссией по категорированию посредством сопоставления процессов, реализуемых субъектом критической информационной инфраструктуры в рамках осуществления деятельности, с показателями критериев значимости Перечня.

23. К субъектам критической информационной инфраструктуры применимы нижеследующие показатели Перечня:

а) «причинение ущерба жизни и здоровью людей (человек)» - для всех субъектов критической информационной инфраструктуры;

б) «прекращение или нарушение функционирования объектов транспортной инфраструктуры, организаций, осуществляющих деятельность в области грузовых и пассажирских перевозок, транспортных средств, в том числе высокоавтоматизированных транспортных средств» - для всех субъектов критической информационной инфраструктуры;

в) «возникновение ущерба субъекту критической информационной инфраструктуры, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности» - для субъектов критической информационной инфраструктуры в случае, если они являются государственными корпорациями, государственными унитарными предприятиями, государственными компаниями, организациями с участием государства, стратегическими акционерными обществами, организациями оборонно-промышленного комплекса, стратегическими предприятиями;

г) «возникновение ущерба бюджету Российской Федерации», в случае, если расчетные параметры, приведенные в пункте 31 настоящих Отраслевых особенностей для субъекта критической информационной инфраструктуры сопоставимы со значениями показателя критерия значимости из Перечня.

д) «снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры» – для субъектов критической информационной инфраструктуры, заключивших договор, предусматривающий исполнение обязательств в рамках выполнения государственного оборонного заказа;

е) «прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка» – для субъектов критической информационной инфраструктуры, эксплуатирующих информационные системы, в области обеспечения обороны страны, безопасности государства и правопорядка.

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

24. Определение категории значимости объектов критической информационной инфраструктуры осуществляется субъектом критической информационной инфраструктуры исходя из возможности возникновения компьютерных атак и компьютерных инцидентов и зависит от:

а) оценивания масштаба возможных последствий в результате компьютерной атаки или компьютерного инцидента на объект критической информационной инфраструктуры и с учетом количества людей (человек), которым в результате воздействия компьютерной атаки и компьютерного инцидента на объект критической информационной инфраструктуры будет причинён или возможно будет причинен ущерб жизни или здоровью, а также с учетом того, что:

объекты критической информационной инфраструктуры относятся к опасным производственным объектам или к объектам транспортной инфраструктуры;

субъект критической информационной инфраструктуры имеет в своем составе подразделения транспортной инфраструктуры и объекты критической информационной инфраструктуры, задействованные в критических процессах субъекта критической информационной инфраструктуры, участвуют в обработке информации, необходимой для управления, контроля или мониторинга опасными производственными объектами или объектами транспортной инфраструктуры;

б) оценивания территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг, количества людей, для которых могут быть недоступны транспортные услуги, видов деятельности, осуществляемых субъектом критической информационной инфраструктуры, типа перевозок, типа грузов и категории объекта транспортной инфраструктуры;

в) ущерба субъекту критической информационной инфраструктуры, являющемуся 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 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) снижения показателей государственного оборонного заказа, оцениваемого в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции), а также увеличении времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции);

е) прекращения или нарушения функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, с учетом того, что субъект критической информационной инфраструктуры обеспечивает эксплуатацию объекта критической информационной инфраструктуры и критические процессы субъекта критической информационной инфраструктуры осуществляют управление, контроль или мониторинг объекта критической информационной инфраструктуры в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемые в максимально допустимом времени (часов), в течение которого объект критической информационной инфраструктуры может быть недоступна пользователю.

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

а) оценивается территория, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг (пассажирских и грузовых перевозок);

б) оценивается количество людей, для которых могут быть недоступны транспортные услуги;

в) оцениваются типы перевозок и грузов;

г) учитывается категория объектов транспортной инфраструктуры;

д) оценивается масштаб последствий возникновения компьютерных атак и компьютерных инцидентов в виде прекращения или нарушения функционирования объектов транспортной инфраструктуры, организаций, осуществляющих деятельность в области грузовых и пассажирских перевозок, транспортных средств, в том числе высокоавтоматизированных транспортных средств.

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

27. При оценке масштаба последствий возникновения компьютерных атак и компьютерных инцидентов в виде прекращения или нарушения функционирования объектов транспортной инфраструктуры, организаций, осуществляющих деятельность в области грузовых и пассажирских перевозок, транспортных средств, в том числе высокоавтоматизированных транспортных средств, субъект критической информационной инфраструктуры:

а) рассматривает наихудшие сценарии последствий проведения компьютерных атак и компьютерных инцидентов на объекты критической информационной инфраструктуры, результатом которых является прекращения или нарушения функционирования объектов транспортной инфраструктуры, организаций, осуществляющих деятельность в области грузовых и пассажирских перевозок, транспортных средств, в том числе высокоавтоматизированных транспортных средств;

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.

IV. Порядок расчета значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры в сфере транспорта

28. Для показателя Перечня «причинение ущерба жизни и здоровью людей (человек)» при расчете учитывается максимально возможное количество человек, пострадавших в результате компьютерной атаки, компьютерного инцидента.

Полученные значения сопоставляются со значениями показателя Перечня «причинение ущерба жизни и здоровью людей (человек)» для каждого объекта критической информационной инфраструктуры.

29. Для показателя Перечня «прекращение или нарушение функционирования объектов транспортной инфраструктуры, организаций, осуществляющих деятельность в области грузовых и пассажирских перевозок, транспортных средств, в том числе высокоавтоматизированных транспортных средств» используются следующие расчетные методы:

а) при определении территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг учитывается территория:

в пределах территории одного муниципального образования (численностью от 2 тысяч человек) или одной внутригородской территории города федерального значения;

за пределами территории одного муниципального образования (численностью от 2 тысяч человек) или одной внутригородской территории города федерального значения, но не за пределами территории одного субъекта Российской;

за пределами территории одного субъекта Российской Федерации или территории города федерального значения;

б) при определении количества людей, для которых могут быть недоступны транспортные услуги, учитываются следующие значения:

количество людей, более или равно 2000, но менее 1000 000 человек;

количество людей, более или равно 1000 000, но менее 5 000 000 человек;

количество людей, более или равно 5 000 000 человек;

в) при определении типов перевозок и грузов учитываются следующие параметры:

осуществление субъектом критической информационной инфраструктуры Мультимодальных и Интермодальных перевозок;

осуществление субъектом критической информационной инфраструктуры перевозки, погрузки, разгрузки, хранения опасных грузов, на перевозку которых

требуется специальное разрешение, и (или) грузов повышенной опасности в пределах территории одного субъекта Российской Федерации;

осуществление субъектом критической информационной инфраструктуры перевозки, погрузки, разгрузки, хранения опасных грузов, на перевозку которых требуется специальное разрешение, и (или) грузов повышенной опасности в пределах территории двух и более субъектов Российской Федерации.

При этом, если информационные системы, обрабатывают данные, связанные с перевозкой и хранением опасных грузов в пределах одного или нескольких субъектов Российской Федерации, и не зависимо от обстоятельства перемещаются опасные грузы за пределы одного субъекта Российской Федерации или нет, но в информационной системе происходит обработка таких видов перевозок грузов по двум и более субъектам Российской Федерации, то информационная система категорируется по наивысшему значению указанного показателя.

г) при учете категории объектов транспортной инфраструктуры, определенной субъектом критической информационной инфраструктуры в соответствии с Федеральным законом «О транспортной безопасности» расчет производится:

если объекту транспортной инфраструктуры присвоены 4 и 3 категории;

если объекту транспортной инфраструктуры присвоена 2 категория;

если объекту транспортной инфраструктуры присвоена 1 категория.

Полученные значения сопоставляются со значениями показателя Перечня «прекращение или нарушение функционирования объектов транспортной инфраструктуры, организаций, осуществляющих деятельность в области грузовых и пассажирских перевозок, транспортных средств, в том числе высокоавтоматизированных транспортных средств» для каждого объекта критической информационной инфраструктуры.

30. Показатель 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» применим в случае, если субъект критической информационной инфраструктуры является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией с участием государства, стратегическим акционерным обществом, организацией оборонно-промышленного комплекса, стратегическим предприятием.

При расчете учитывается:

усредненный суммарный годовой размер выплачиваемых субъектом критической информационной инфраструктуры налогов в бюджет Российской Федерации, определенный на основании налоговой отчетности и предоставляемых в Федеральную налоговую службу декларациях за предыдущий пятилетний период;

усредненный размер годового дохода, определенный на основании сведений управленческого и бухгалтерского учета за предыдущий пятилетний период;

максимально допустимый период простоя, определенный на основании регламентов проведения профилактических работ информационных систем, автоматизированных систем управления, информационно-телекоммуникационных систем субъекта критической информационной инфраструктуры;

время, требуемое для устранения последствий компьютерной атаки, определяемое на основании эксплуатационных, технических, договорных и (или) иных документов, а при отсутствии таких документов используются статистические данные за предыдущий пятилетний период, в случае отсутствия статистических данных за предыдущий пятилетний период принимается значение – 10 суток.

Полученный возможный ущерб субъекта критической информационной инфраструктуры от компьютерной атаки и компьютерного инцидента сопоставляется с показателем усредненного размера годового дохода и определяется показатель возможного ущерба.

Полученные значения сопоставляются со значениями 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» для каждого объекта критической информационной инфраструктуры.

31. Для показателя Перечня «возникновение ущерба бюджету Российской Федерации» рассчитываются значения потенциально возможного ущерба бюджету Российской Федерации субъектом критической информационной инфраструктуры, на которого в соответствии с Налоговым кодексом Российской Федерации возложена обязанность уплачивать соответствующие налоги, сборы, страховые взносы.

Определяется актуальный годовой размер выплачиваемых субъектом критической информационной инфраструктуры налогов в бюджет Российской Федерации, исходя из данных, предоставляемых в Федеральную налоговую службу.

Исходными данными для расчета численного значения показателя ущерба бюджету Российской Федерации могут являться:

величины затрат и потерь субъекта критической информационной инфраструктуры, которые могут быть вызваны прекращением или нарушением критических процессов, обеспечиваемых объектом критической информационной инфраструктуры;

значения возможного времени нарушения выполнения (невыполнения) рассматриваемых критических процессов;

прогнозируемые годовые доходы федерального бюджета Российской Федерации по годам за планируемый трехлетний период;

объем выплат (отчислений) субъекта критической информационной инфраструктуры в бюджет Российской Федерации в виде налога на прибыль, осуществленных за прошедший год;

величина прибыли субъекта критической информационной инфраструктуры за прошедший год;

доля акций компании, принадлежащая Российской Федерации и (или) субъекту Российской Федерации;

доля от прибыли субъекта критической информационной инфраструктуры за прошедший год, выплаченная в качестве дивидендов;

объем налоговых выплат (отчислений) от дивидендов, осуществленных субъектом критической информационной инфраструктуры за прошедший год;

объем выплат (отчислений) дивидендов, осуществленных субъектом критической информационной инфраструктуры за прошедший год;

размер снижения выплат (отчислений) сторонних организаций в бюджет Российской Федерации вследствие прекращения или нарушения функционирования рассматриваемого объекта критической информационной инфраструктуры;

размер снижения сборов в бюджет Российской Федерации в случае прекращения или нарушения функционирования объекта критической информационной инфраструктуры, предназначенного для организации сборов в бюджет Российской Федерации.

Величины затрат и потерь, которые могут быть вызваны прекращением или нарушением критических процессов субъекта критической информационной инфраструктуры, оцениваются экспертным методом на основе анализа возможных максимальных экономических ущербов от прекращения или нарушения всех критических процессов, обеспечиваемых объектом критической информационной инфраструктуры, причиной которых могут являться компьютерные атаки и компьютерные инциденты.

Полученные значения сопоставляются со значениями для показателя Перечня «возникновение ущерба бюджету Российской Федерации» для каждого объекта критической информационной инфраструктуры.

32. Для показателя Перечня «снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры» расчет производится в части:

снижения объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);

увеличении времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции).

Показатель Перечня «снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры» рассчитывается в том случае, если субъект критической информационной инфраструктуры обеспечивает эксплуатацию объекта критической информационной инфраструктуры и критические процессы субъекта критической информационной инфраструктуры осуществляют управление, контроль или мониторинг объекта критической информационной инфраструктуры, задействованного в процессе выполнения государственного оборонного заказа и влияющего на снижение объемов продукции (работ, услуг) в заданный период времени.

Полученные значения сопоставляются со значениями для показателя Перечня «снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры» для каждого объекта критической информационной инфраструктуры.

33. Для показателя Перечня «прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка» расчет производится в том случае, если субъект критической информационной инфраструктуры обеспечивает эксплуатацию объекта критической информационной инфраструктуры и критические процессы субъекта критической информационной инфраструктуры осуществляют управление, контроль или мониторинг объекта критической информационной инфраструктуры в области обеспечения обороны страны, безопасности государства и правопорядка.

При этом учитывается максимально допустимое время, в течение которого информационная система может быть недоступна пользователю.

Полученные значения сопоставляются со значениями для показателя Перечня «прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка» для каждого объекта критической информационной инфраструктуры.

_____