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 Российской Федерации в сфере связи

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 Российской Федерации в сфере связи.

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 Российской Федерации.

3. Субъектам критической информационной инфраструктуры Российской Федерации в сфере связи в течение 6 месяцев со дня вступления в силу настоящего постановления осуществить категорирование объектов критической информационной инфраструктуры в соответствии с отраслевыми особенностями, устанавливаемыми настоящим постановлением.

4. Субъекты критической информационной инфраструктуры Российской Федерации в сфере связи вправе использовать на значимых объектах критической информационной инфраструктуры Российской Федерации программы для электронных вычислительных машин и базы данных, входящие в состав программно-аппаратных комплексов, сведения о которых не включены в единый реестр российских программ для электронных вычислительных машин и баз данных, предусмотренный статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации», до окончания срока

полезного использования (срока амортизации) указанных программно-аппаратных комплексов.

Председатель Правительства
Российской Федерации М.Мишустин

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

ОТРАСЛЕВЫЕ ОСОБЕННОСТИ
категорирования объектов критической информационной инфраструктуры в сфере связи

I. Общие положения

1. Настоящие Отраслевые особенности категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере связи (далее соответственно – Отраслевые особенности, критическая информационная инфраструктура) регламентируют особенности категорирования объектов критической информационной инфраструктуры в сфере связи (далее – объекты критической информационной инфраструктуры), 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 при категорировании объектов критической информационной инфраструктуры государственными органами, выполняющими функции (полномочия) в сфере связи, государственными учреждениями, выполняющими функции (полномочия) или осуществляющими виды деятельности в сфере связи, российскими юридическими лицами, осуществляющими деятельность в сфере связи, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере связи, а также российскими юридическими лицами, которые обеспечивают взаимодействие указанных систем или сетей (далее – субъекты 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 «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), и настоящими Отраслевыми особенностями.

4. Категорирование объектов критической информационной включает в себя:

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

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.

5. С целью категорирования объектов критической информационной инфраструктуры решением руководителя субъекта критической информационной инфраструктуры создается постоянно действующая комиссия по категорированию, в состав которой включаются:

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

б) работники субъекта критической информационной инфраструктуры, обеспечивающих эксплуатацию и функционирование информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, относящихся к сфере связи;

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

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

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

е) для операторов универсального обслуживания и федеральной службы почтовой связи – представители федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере электросвязи и почтовой связи, по согласованию с таким государственным органом;

ж) для подведомственных федеральным органам в сфере связи органов и организаций – представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в сфере связи, по согласованию с такими государственными органами и российскими юридическими лицами.

6. По решению руководителя субъекта критической информационной инфраструктуры в состав комиссии могут быть включены работники не указанных в пункте 5 настоящих Отраслевых особенностей подразделений, в том числе финансово-экономического подразделения.

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

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

9. 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 связи, по согласованию с такими государственными органами и российскими юридическими лицами.

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

11. Комиссия по категорированию в ходе своей работы:

а) выявляет объекты критической информационной инфраструктуры, соответствующие перечням 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 в соответствии с Перечнем 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.

12. Комиссия по категорированию подлежит расформированию в следующих случаях:

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

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

13. 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.

14. Субъект критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта, указанного в пункте 13 настоящих Отраслевых особенностей, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий в порядке, установленном пунктом 22 Правил.

15. Формирование перечня 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 связи к соответствующим типовым отраслевым объектам критической информационной инфраструктуры в сфере связи.

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

16. С целью установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений субъектом критической информационной инфраструктуры должен быть сформирован перечень объектов, подлежащих категорированию, а также выявлены процессы, которые в результате компьютерной атаки могут привести к аварийным ситуациям и

компьютерным инцидентам у субъекта критической информационной инфраструктуры.

17. В случае выявления технологической и (или) технической взаимной зависимости двух и более 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 комиссией по категорированию принимается решение об отсутствии объектов критической информационной инфраструктуры, подлежащих категорированию. Решение комиссии по категорированию оформляется актом в соответствии с пунктом 13 настоящих Отраслевых особенностей.

19. При осуществлении модернизации объектов критической информационной инфраструктуры объект критической информационной инфраструктуры, состоящий из нескольких информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления, решением комиссии по категорированию может быть разделен на несколько отдельных объектов критической информационной инфраструктуры в случае, если после такой модернизации технологическая и (или) техническая зависимость прекращается. Решение комиссии по категорированию оформляется актом.

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 перечни типовых отраслевых объектов критической информационной инфраструктуры, но масштаб возможных последствий в случае возникновения компьютерных инцидентов соответствует показателям критериев значимости и их значениям, субъект критической информационной инфраструктуры присваивает указанному объекту одну из категорий значимости и направляет 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 направляет предложения о дополнении перечней типовых отраслевых объектов критической информационной инфраструктуры.

21. Субъект критической информационной инфраструктуры 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. Сведения, указанные в пункте 21 настоящих Отраслевых особенностей, и их содержание направляются в печатном и электронном виде по форме, утверждаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

23. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, проверяет сведения об объекте критической информационной инфраструктуры, указанные в пункте 21 настоящих Отраслевых особенностей, и в течение 30 дней со дня получения таких сведений принимает решение о дополнении перечня типовых отраслевых объектов критической информационной инфраструктуры в сфере связи либо об отказе в дополнении.

24. Выявление процессов, которые в результате компьютерной атаки могут привести к аварийным ситуациям и компьютерным инцидентам, осуществляется комиссией по категорированию посредством сопоставления процессов, реализуемых объектом критической информационной инфраструктуры, с показателями критериев значимости Перечня.

25. К субъектам критической информационной инфраструктуры применимы следующие показатели Перечня:

а) «прекращение или нарушение функционирования сети связи, оцениваемое по количеству абонентов, для которых могут быть недоступны услуги связи» для всех субъектов критической информационной инфраструктуры;

б) «прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» для субъектов критической информационной инфраструктуры, заключивших государственный контракт с органом государственной власти, в соответствии с которым в условиях отсутствия связи (по перечню услуг) и (или) доступа в информационно-телекоммуникационную сеть «Интернет» орган государственной власти не сможет осуществлять государственные функции и (или) полномочия;

в) «нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации» для субъектов критической информационной инфраструктуры, заключивших договор об оказании услуг связи, предусматривающий международные обязательства Российской Федерации;

г) «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 сфере связи 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;

д) «возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет» в случае, если расчетные показатели, приведенные в пункте 36 Отраслевых особенностей для субъекта критической информационной инфраструктуры сопоставимы со значениями показателя критерия значимости из Перечня.

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

26. Определение категории значимости объектов критической информационной инфраструктуры осуществляется субъектом критической информационной инфраструктуры исходя из возможности возникновения в результате компьютерной атаки аварийных ситуаций и компьютерных инцидентов и зависит от:

а) количества абонентов, для которых могут быть недоступны услуги связи;

б) нарушения и (или) прекращения функционирования сети связи в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

в) ущерба субъекту критической информационной инфраструктуры, являющимся 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) наличия заключенного между субъектом критической информационной инфраструктуры и органом государственной власти государственного контракта на оказание услуг связи, в соответствии с которым в условиях отсутствия связи (по перечню услуг) и (или) доступа в информационно-телекоммуникационную сеть «Интернет» орган государственной власти не сможет осуществлять государственные функции и (или) полномочия.

27. В целях определения категории значимости объектов критической информационной инфраструктуры для каждого объекта критической информационной инфраструктуры комиссией по категорированию:

а) оценивается масштаб последствий возникновения компьютерных инцидентов в виде нарушения и (или) прекращения функционирования сети связи;

б) оценивается количество обслуживаемых абонентов;

в) сопоставляется количество абонентов со значениями, приведенными для показателя Перечня «прекращение или нарушение функционирования сети связи».

28. Оценка проводится по каждому из значений показателя Перечня, указанных в пункте 25 настоящих Отраслевых особенностей, а категория значимости присваивается объекту критической информационной инфраструктуры по наивысшему значению одного из этих показателей Перечня.

29. При оценке масштаба последствий возникновения компьютерных инцидентов в виде нарушения и (или) прекращения функционирования сети связи субъект критической информационной инфраструктуры:

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

б) определяет технологическую и (или) техническую взаимную зависимость двух и более объектов критической информационной инфраструктуры.

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

30. Для показателя Перечня «прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи» в целях определения количества абонентов, для которых могут быть недоступны услуги связи, используются следующие расчетные методы в зависимости от вида оказываемых услуг связи

а) для операторов связи, оказывающих услуги электросвязи на основании договоров, заключаемых в соответствии с правилами оказания услуг связи с абонентами, – определяется количество абонентов, с которыми такими операторами связи заключены договоры об оказании услуг связи и оказание услуг связи которым осуществляется с использованием категорируемого объекта критической информационной инфраструктуры;

б) для операторов связи, оказывающих услуги электросвязи пользователям услугами связи без выделения для этих целей абонентского номера или уникального кода идентификации, – определяется численность домохозяйств, оказание услуг электросвязи которым осуществляется с использованием категорируемого объекта критической информационной инфраструктуры;

в) для собственников или иных владельцев точек обмена трафиком – определяется наивысшая категория значимости объектов критической информационной инфраструктуры пользователей услуг таких точек обмена трафиком, непосредственно подключенных к точке обменом трафиком и указанных в договорах на оказание услуг, с указанием их категории значимости;

г) для иных организаций связи, объекты критической информационной инфраструктуры которых непосредственно влияют на пропуск и (или) маршрутизацию трафика в сети связи общего пользования, – определяется количество абонентов, на доступность услуг электросвязи которым влияет функционирование категорируемого объекта критической информационной инфраструктуры.

В случае использования категорируемого объекта критической информационной инфраструктуры в оказании нескольких услуг (групп услуг) в сфере связи, расчет показателя осуществляется в отношении каждой такой услуги (групп услуг). Категория значимости категорируемого объекта критической информационной инфраструктуры определяется равной наивысшей категории значимости, из числа таких значений, полученных в результате выполнения настоящего пункта.

31. В случае невозможности применения одного из расчетных методов, указанных в пункте 30 настоящих Отраслевых особенностей, расчет значения показателя осуществляется исходя из определения площади территории, на которой могут быть недоступны услуги связи:

– в пределах территории одного муниципального образования (численностью от 3 тыс. человек) или одной внутригородской территории города федерального значения, что соответствует 3 категории значимости;

- выход за пределы территории одного муниципального образования (численностью от 3 тыс. человек) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения, что соответствует 2 категории значимости;

- выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения, что соответствует 1 категории значимости.

32. В случае использования нескольких расчетных методов при осуществлении расчета значения показателя Перечня в соответствии с пунктом 30 настоящих Отраслевых особенностей, объекту критической информационной инфраструктуры присваивается категория значимости с наивысшим значением из всех полученных расчетных значений.

33. Показатель Перечня «прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» применяется для субъекта критической информационной инфраструктуры, имеющего действующий государственный контракт на оказание услуг связи органу государственной власти, в соответствии с которым в условиях отсутствия связи (по перечню услуг) и (или) доступа в информационно-телекоммуникационную сеть «Интернет» орган государственной власти не сможет осуществлять государственные функции и (или) полномочия.

В случае отсутствия таких сведений в государственном контракте, субъект критической информационной инфраструктуры обязан принять исчерпывающие меры по получению информации о наличии влияния на функционирование значимых объектов критической информационной инфраструктуры, включая сведения о наивысшей категории значимости объектов критической информационной инфраструктуры такого получателя, на которых оказывается такое влияние. В случае отсутствия такой информации по результатам принятия субъектом критической информационной инфраструктуры указанных мер объекту критической информационной инфраструктуры присваивается категория значимости на основании имеющихся у субъекта критической информационной инфраструктуры данных.

Расчет показателя Перечня «прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» производится в отношении информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, функционирование которых способно повлиять на нарушение условий государственного контракта, в соответствии с которым в условиях отсутствия связи (по перечню услуг) и (или) доступа в информационно-телекоммуникационную сеть «Интернет» орган государственной власти не сможет осуществлять государственные функции и (или) полномочия.

Полученные значения сопоставляются со значениями, приведенными для показателя Перечня «прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)».

34. Для показателя Перечня «нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации» оценивается наличие у субъекта критической информационной инфраструктуры заключенных договоров, предусматривающих обязательства Российской Федерации.

Расчет показателя Перечня «нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации» производится в отношении информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, функционирование которых способно повлиять на нарушение условий международных договоров Российской Федерации, срыв переговоров или срыв подписания планируемого к заключению международного договора Российской Федерации.

Полученные значения сопоставляются со значениями показателя Перечня «нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации».

35. 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 используются:

– 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 сетей 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 дней.

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».

36. Для показателя Перечня «возникновение ущерба бюджету Российской Федерации» рассчитываются значения потенциально возможного ущерба бюджету Российской Федерации в следующем порядке.

Определяется усредненный годовой доход федерального бюджета на основании данных, установленных федеральным законом о федеральном бюджете на текущий календарный год и на плановый период, включающий два последующих календарных года.

Определяется годовой размер выплачиваемых субъектом критической информационной инфраструктуры налогов в бюджет Российской Федерации, исходя из данных, предоставляемых в Федеральную налоговую службу Российской Федерации, как налог на прибыль организации от деятельности в сфере связи, зачисляемой в федеральный бюджет и определяемый по ставке, установленной абзацем вторым части 1 статьи 284 Налогового кодекса Российской Федерации. Размер такого налога определяется организацией связи по данным раздельного учета, либо пропорционально объему выручки от осуществляемых видов деятельности, в том числе с учетом данных форм федерального статистического наблюдения.

При определении указанного размера налога учитываются в полном объеме следующие затраты:

а) затраты на ликвидацию и устранение последствий компьютерных атак и компьютерных инцидентов;

б) затраты на оплату труда персонала и условно-постоянные расходы за время простоя и (или) деградации процесса;

в) затраты на оплату труда персонала, привлекаемого сверхурочно, для ликвидации последствий нарушений, вызванных простоем и (или) деградацией процесса;

г) потери от выплаты штрафных санкций за невыполнение условий договоров в результате простоя и (или) деградации процесса.

В случае, если значение налога на прибыль, рассчитанное в соответствии с абзацем третьим настоящего пункта, меньше наименьшего значения показателя Перечня, то определение категории значимости объектам критической информационной инфраструктуры по данному показателю не производится.

Определяется максимально возможный период прекращения оказания услуг в сфере связи в результате нарушения и (или) прекращения функционирования категорируемого объекта критической информационной инфраструктуры и оценивается максимально возможное снижение прибыли организации от оказания услуг в сфере связи с использованием категорируемого объекта критической информационной инфраструктуры в течение такого периода. Полученные значения сопоставляются со значениями (диапазонами значений) для показателя Перечня «возникновение ущерба бюджету Российской Федерации» для каждого объекта критической информационной инфраструктуры.

_____