Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

П О С Т А Н О В Л Е Н И Е

от «___» _____ 2025 г. № ____

МОСКВА

Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере науки

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 по согласованию с Федеральной службой по техническому и экспортному контролю прилагаемые отраслевые особенности категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере науки.

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 Российской Федерации в сфере науки

I. Общие положения

1. Настоящие Отраслевые особенности категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере науки (далее соответственно – Отраслевые особенности,) определяют порядок установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений в целях присвоения ему одной из категорий значимости (далее – категорирование) 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. Отраслевые особенности предназначены для использования в процессе проведения категорирования объектов критической информационной инфраструктуры государственными органами, государственными учреждениями, российскими юридическими лицами, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере науки, а также российскими юридическими лицами, которые обеспечивают взаимодействие указанных систем или сетей (далее – субъекты критической информационной инфраструктуры).

3. 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. 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).

5. Понятия и термины, используемые в настоящих отраслевых особенностях категорирования, применяются в том значении, в котором они используются в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации».

6. Категорирование в сфере науки 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 сферы науки;

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.

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

7. В случае отсутствия информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления, соответствующих объектам критической информационной инфраструктуры, включенным в перечень типовых отраслевых объектов критической информационной инфраструктуры сферы науки, субъектом критической

информационной инфраструктуры принимается решение об отсутствии объектов критической информационной инфраструктуры, подлежащих категорированию.

8. В случае выявления субъектом критической информационной инфраструктуры принадлежащих на праве собственности, аренды или на ином законном основании информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, функционирующих в иных сферах, установленных пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», субъекту критической информационной инфраструктуры необходимо руководствоваться перечнями типовых отраслевых объектов критической информационной инфраструктуры в иных сферах.

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

10. В случае выявления субъектом критической информационной инфраструктуры принадлежащих на праве собственности, аренды или на ином законном основании информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, функционирующих в сфере науки, но не соответствующих типам информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, включенных в перечень типовых отраслевых объектов критической информационной инфраструктуры сферы науки, субъекту критической информационной инфраструктуры необходимо провести категорирование выявленного объекта критической информационной инфраструктуры, а также направить в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, предложения о дополнении перечней типовых отраслевых объектов критической информационной инфраструктуры.

11. К объектам критической информационной инфраструктуры, подлежащим категорированию, также относятся объекты критической информационной инфраструктуры субъекта критической информационной инфраструктуры, имеющего филиалы, представительства.

12. К объектам критической информационной инфраструктуры в сфере науки применимы следующие показатели критериев значимости Перечня:

а) причинение ущерба жизни и здоровью людей – в случае если при проведении научно-исследовательской работы (далее – НИР), опытно-конструкторской работы (далее – ОКР) или научно-исследовательской опытно-

конструкторской работы (далее – НИОКР) предусматривается использование вредных веществ, в том числе опасных химических веществ;

б) нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации – применим в случае, если субъект критической информационной инфраструктуры выполняет НИР, ОКР или НИОКР в рамках международного договора;

в) возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период) – применим в случае, если субъект критической информационной инфраструктуры является: государственной корпорацией; государственным унитарным предприятием; государственной компанией; стратегическим акционерным обществом, включенным в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. № 1009; стратегическим предприятием, включенным в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. № 1009;

г) возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период) – применим в случае, если субъект критической информационной инфраструктуры является: государственным органом, государственным учреждением, российским юридическим лицом, индивидуальным предпринимателем;

д) вредные воздействия на окружающую среду – применим, в случае если при проведении НИР, ОКР или НИОКР предусматривается использование вредных веществ, в том числе опасных химических веществ;

е) снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры – применим в случае выполнения субъектом критической информационной

инфраструктуры НИР, ОКР или НИОКР в рамках государственного оборонного заказа.

13. При оценке объекта критической информационной инфраструктуры необходимо определить масштаб возможных последствий в результате возникновения компьютерных инцидентов, основываясь на выявленных возможных угрозах безопасности информации, типах компьютерных атак, назначении объекта критической информационной инфраструктуры и автоматизируемого процесса. Для рассматриваемого объекта критической информационной инфраструктуры должны выбираться те типы последствий, которые могут стать следствием реализации вероятных угроз безопасности информации для данного объекта критической информационной инфраструктуры.

14. При оценке масштаба возможных последствий в случае возникновения компьютерных инцидентов при проведении компьютерных атак на объект критической информационной инфраструктуры необходимо:

а) рассматривать наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты критической информационной инфраструктуры, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба;

б) учитывать зависимость процессов от осуществления иных процессов, выполняемых субъектом критической информационной инфраструктуры;

в) учитывать зависимость функционирования одного объекта критической информационной инфраструктуры от функционирования другого объекта критической информационной инфраструктуры;

г) оценить возможность реализации угроз безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

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

15. Определение категории значимости объектов критической информационной инфраструктуры осуществляется субъектом критической информационной инфраструктуры исходя из возможности возникновения компьютерных атак и компьютерного инцидента (при проведении НИР и (или) ОКР не ниже седьмого уровня готовности технологии, определяемого в соответствии с пунктом 3^1 Положения о единой государственной информационной системе учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения,

утвержденного постановлением Правительства Российской Федерации от 12 апреля 2013 г. № 327 «О единой государственной информационной системе учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения») и зависит от:

а) количества людей, которым может быть причинен ущерб жизни и здоровью;

б) наличия заключенного международного договора Российской Федерации, возможности срыва переговоров или подписания планируемого к заключению международного договора Российской Федерации;

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;

г) ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры;

д) возникновения вредных воздействий на окружающую среду;

е) наличия государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры.

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

16. До начала расчета показателей критериев значимости субъектом критической информационной инфраструктуры определяется применимость критериев значимости для оценки значимости информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

17. Для показателей критериев значимости объекта критической информационной инфраструктуры, по которым обоснована их неприменимость, расчет показателей критериев значимости субъектом критической информационной инфраструктуры не проводится.

18. В целях определения категории значимости объекта критической информационной инфраструктуры:

а) в части показателя «Причинение ущерба жизни и здоровью людей» значение показателя определяется субъектом критической информационной инфраструктуры исходя из:

штатного расписания;

количества лиц, задействованных во взаимодействии с объектом (процессом) производства

количества лиц, задействованных при испытаниях и (или) измерениях объектов производства;

количества лиц, задействованных при проведении научных исследований исследований объектов (процессов) производства и осуществлении экспериментальных разработок, а также обеспечении безопасности производственных процессов;

б) в части показателя «Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации» показатель ущерба определяется субъектом критической информационной инфраструктуры с учетом нарушения условий международного договора за счет снижения количества завершенных испытаний (опытов, экспериментов, измерений) за определенный промежуток времени, снижения точности (правильности, прецизионности) результатов изменений при проведении испытаний (опытов, экспериментов, измерений) или целостности, доступности информации, полученной в ходе НИР, ОКР, НИОКР, наступающих в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры;

в) в части показателя «Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности» показатель ущерба субъекту критической информационной инфраструктуры определяется снижением уровня дохода субъекта критической информационной инфраструктуры, наступающим в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры;

г) в части показателя «Возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры» показатель ущерба бюджетам определяется снижением субъектом критической информационной инфраструктуры налоговых выплат (отчислений) в бюджеты Российской Федерации, наступающим в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры;

д) в части показателя «Вредные воздействия на окружающую среду» значение показателя определяется исходя из:

штатного расписания;

количества лиц, задействованных во взаимодействии с объектом (процессом) производства;

количества лиц, задействованных при испытаниях и (или) измерениях объектов производства;

количества лиц, задействованных при проведении научных исследований, исследований объектов (процессов) производства и осуществлении экспериментальных разработок, а также обеспечении безопасности производственных процессов;

е) в части показателя «Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое» показатель ущерба определяется снижением количества завершенных испытаний (опытов, экспериментов, измерений) за определенный промежуток времени, снижением точности (правильности, прецизионности) результатов изменений при проведении испытаний (опытов, экспериментов, измерений) или целостностью, доступностью информации, полученной в ходе НИР, ОКР, НИОКР, наступающих в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры.

19. При расчете значений показателей критериев значимости субъекту критической информационной инфраструктуры необходимо определить масштаб возможных последствий в результате возникновения компьютерных инцидентов, основываясь на выявленных возможных угрозах безопасности информации, типах компьютерных атак, назначении объекта критической информационной инфраструктуры и автоматизируемого процесса. Для рассматриваемого объекта критической информационной инфраструктуры должны выбираться те типы последствий, которые могут стать следствием реализации вероятных угроз безопасности информации для данного объекта критической информационной инфраструктуры.

20. При оценке масштаба возможных последствий в случае возникновения компьютерных инцидентов при проведении компьютерных атак на объект критической информационной инфраструктуры субъекту критической информационной инфраструктуры необходимо:

а) рассмотреть наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты критической информационной инфраструктуры, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба;

б) учесть зависимость процессов от осуществления иных процессов, выполняемых субъектом критической информационной инфраструктуры;

в) учесть зависимость функционирования одного объекта критической информационной инфраструктуры от функционирования другого объекта критической информационной инфраструктуры;

г) оценить возможность реализации угроз безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

21. Оценка возможных последствий в результате возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры проводится субъектом критической информационной инфраструктуры в соответствии с показателем:

а) причинение ущерба жизни и здоровью людей.

Оценивается возможность причинения ущерба жизни и здоровью людей при проведении НИР, ОКР, НИОКР, наступающим в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры. При этом должны рассматриваться следующие сценарии развития компьютерных инцидентов:

инциденты, из-за которых возможно возникновение техногенных катастроф на производстве (взрывы, утечки и разливы опасных веществ), связанных с нарушением управления, с нарушением работы объекта (в том числе нарушение параметров техпроцесса, нарушение работы или состояния исполнительных механизмов);

инциденты, из-за которых возможен ущерб потребителям продукции или услуг (в том числе производство медицинских препаратов, использование медицинского оборудования, пищевая продукция, бытовая химическая продукция, транспортные средства, топливо), связанный с нарушением технологического процесса.

Масштаб возможного ущерба рассчитывается исходя из следующих значений:

число человек, которые могут потенциально находиться в зоне поражения при возникновении аварии или техногенной катастрофы;

число человек, находящихся в зоне, потенциально подверженной воздействию последствий техногенной катастрофы;

число потенциальных потребителей продукции, которая может нанести вред здоровью людей до выявления нарушений;

б) нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации.

Показатель применим к объектам критической информационной инфраструктуры, от работоспособности которых зависит реализация соответствующих договорных обязательств или выполнение предварительных условий, требуемых для выполнения (заключения) соответствующих международных договоров.

Рассматриваются инциденты, из-за которых возможно прекращение или нарушение работы объекта критической информационной инфраструктуры, а также нарушение доступности или целостности информации, полученной в ходе НИР, ОКР, НИОКР, наступающих в результате совершения компьютерной атаки на категорируемый объект критической информационной инфраструктуры, влекущие нарушение требований международных договоров.

Масштаб возможного ущерба оценивается на основании сведений о типе международного договора, выполнение которого зависит от рассматриваемого объекта критической информационной инфраструктуры:

договор межведомственного характера;

межправительственный договор;

межгосударственный договор;

в) 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.

Рассматривается возможность снижения уровня дохода соответствующего субъекта (государственной корпорации, государственного унитарного предприятия, государственной компании, стратегического акционерного общества, включенного в перечень стратегических предприятий и стратегических акционерных обществ, утвержденного Указом Президента Российской Федерации от 4 августа 2004 г. № 1009, стратегического предприятия, включенного в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. № 1009) в случае прекращения или нарушения функционирования рассматриваемого объекта критической информационной инфраструктуры.

Данный показатель применим к объектам критической информационной инфраструктуры, которые реализуют процессы, связанные с производством продукции или предоставлением услуг, являющимися источниками дохода субъекта критической информационной инфраструктуры.

Рассматриваются инциденты, из-за которых возможно прекращение или нарушение работы объекта критической информационной инфраструктуры, влекущие нарушение производственных процессов или процессов предоставления услуг. При оценке рассматриваются такие последствия как:

нарушение производства/предоставления услуг субъекта критической информационной инфраструктуры;

изменение качества, скорости, объема выпускаемой продукции, которые способны повлечь нарушение договорных обязательств, штрафные санкции и (или) разрыв договорных отношений.

Ущерб оценивается как прогнозируемые потери за ожидаемый период нарушения объекта критической информационной инфраструктуры в процентах от среднегодового дохода за прошедший 5-летний период:

выполняется оценка максимальной оценочной длительности разового нарушения работоспособности объекта критической информационной инфраструктуры с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления;

оценивается какие процессы будут нарушены из-за нарушения работоспособности объекта критической информационной инфраструктуры и связанные с ними усредненные дневные потери дохода субъекта: суммарный доход, связанный с рассматриваемым процессом за прошедший 5-летний период;

для оценки влияния объекта критической информационной инфраструктуры на доход субъекта критической информационной инфраструктуры рекомендуется строить дерево процессов, отражающее взаимосвязь процессов с указанием зависимости (полная, частичная). В случае, если автоматизируемый процесс не является непосредственным источником дохода, то необходимо рассмотреть процессы, на которые он оказывает влияние и выполнение которых будет невозможно или усложнится в случае нарушения данного процесса. В случае, если объект критической информационной инфраструктуры оказывает влияние на несколько процессов, являющихся самостоятельными источниками дохода, расчет потерь должен выполняться для каждого подобного процесса;

рассчитывается итоговый ущерб посредством умножения максимальной оценочной длительности нарушения работоспособности объекта критической информационной инфраструктуры на суммарные дневные потери от нарушения

работоспособности данного объекта критической информационной инфраструктуры;

г) возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры.

Оценивается возможность снижения соответствующих выплат государственным органом, государственным учреждением, российским юридическим лицом в бюджет в случае нарушения функционирования рассматриваемого объекта критической информационной инфраструктуры.

Данный показатель применим к объектам критической информационной инфраструктуры, которые реализуют процессы, связанные в том числе с производством продукции или предоставлением услуг, являющимися источниками дохода субъекта, облагаемыми налогами, пошлинами, акцизами.

Рассматриваются инциденты, из-за которых возможно прекращение или нарушение работы объекта критической информационной инфраструктуры, влекущие нарушение производственных процессов или процессов предоставления услуг. При оценке рассматриваются такие последствия как:

нарушение производства/предоставления услуг субъекта;

изменение качества, скорости, объема выпускаемой продукции.

Ущерб оценивается как прогнозируемое снижение выплат в бюджет за ожидаемый период нарушения объекта критической информационной инфраструктуры в процентах от среднегодового дохода федерального бюджета за 3-летний период:

выполняется оценка максимальной оценочной длительности разового нарушения работоспособности объекта критической информационной инфраструктуры с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления;

рассчитываются средние выплаты субъекта критической информационной инфраструктуры. Рассматриваются исключительно выплаты, связанные с деятельностью субъекта критической информационной инфраструктуры (производство, оказание услуг);

оценивается влияние объекта критической информационной инфраструктуры на выплаты в бюджет. В случае, если автоматизируемый процесс не является непосредственным источником отчислений в бюджет, то необходимо рассмотреть процессы, на которые он оказывает влияние и выполнение которых будет невозможно или усложнится в случае нарушения данного процесса. В случае, если объект критической информационной инфраструктуры оказывает влияние

на несколько процессов, являющихся самостоятельными источниками отчислений в бюджет, расчет потерь должен выполняться для каждого подобного процесса;

рассчитывается итоговый ущерб посредством умножения максимальной оценочной длительности нарушения работоспособности объекта критической информационной инфраструктуры на усредненное дневное уменьшение выплат в бюджеты Российской Федерации, связанное с нарушением работоспособности объекта критической информационной инфраструктуры;

итоговый ущерб оценивается в процентном соотношении к прогнозируемому годовому доходу федерального бюджета, усредненному за планируемый 3-летний период;

д) вредные воздействия на окружающую среду.

Оценивается возможность возникновения выбросов/сбросов/разливов вредных и загрязняющих веществ в атмосферу/водоемы/почву из-за нарушения функционирования объекта критической информационной инфраструктуры, при проведении НИР, ОКР или НИОКР.

Данный показатель применим к системам управления соответствующими промышленными объектами, которые осуществляют управление процессами, связанными с производством, использованием, переработкой, утилизацией, транспортом вредных и загрязняющих веществ, а также мониторинг данных процессов (если на основании данных мониторинга могут приниматься управляющие решения).

Рассмотрению подлежит в том числе кратковременные/разовые факты выбросов/сбросов/разливов, достигающих соответствующего масштаба.

При этом рассматриваются следующие сценарии развития компьютерных инцидентов:

инциденты, из-за которых возможно возникновение техногенных катастроф на производстве (взрывы, утечки и разливы опасных веществ);

инциденты, связанные с нарушением работы объекта (в том числе нарушение параметров техпроцесса, нарушение работы или состояния исполнительных механизмов).

Масштаб возможного ущерба оценивается относительно:

территории, на которой окружающая среда может подвергнуться вредным воздействиям;

количества людей, которые могут быть подвержены вредным воздействиям;

е) снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры.

Оценивается возможность снижения объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции), а также увеличение времени изготовления единицы продукции с заданным объемом

(процентов установленного времени на изготовление единицы продукции) при прекращении и (или) нарушении функционирования объекта критической информационной инфраструктуры, в случае выполнения НИР, ОКР или НИОКР в рамках государственного оборонного заказа.

_____