Приложение № 1

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 здравоохранения

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 здравоохранения.

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 здравоохранения

I. Общие положения

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

2. Отраслевые особенности предназначены для проведения категорирования объектов критической информационной инфраструктуры государственными органами в сфере здравоохранения, государственными учреждениями, осуществляющими деятельность в сфере здравоохранения, российскими юридическими лицами, осуществляющими медицинскую деятельность и фармацевтическую деятельность, Федеральным фондом обязательного медицинского страхования, территориальными фондами Федерального фонда обязательного медицинского страхования, которым на праве собственности, аренды или ином законном основании принадлежат информационные системы, автоматизированные системы управления, функционирующие в сфере здравоохранения, а также российскими юридическими

лицами, которые обеспечивают взаимодействие указанных систем (далее – субъекты критической информационной инфраструктуры).

3. Отраслевые особенности определяют процедуру категорирования объектов критической информационной инфраструктуры в сфере здравоохранения, в соответствии с перечнем типовых отраслевых объектов критической информационной инфраструктуры, утвержденным постановлением Правительства Российской Федерации от «____» _____ 2025 г. № _____.

4. Категорирование объектов критической информационной инфраструктуры в сфере здравоохранения 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, с учетом отраслевых особенностей категорирования объектов критической информационной инфраструктуры в сфере здравоохранения, утвержденных настоящим постановлением (далее соответственно – Правила, Перечень).

5. Категорирование объектов критической информационной инфраструктуры в сфере здравоохранения включает в себя:

а) определение информационных систем, автоматизированных систем управления, соответствующих типовым объектам критической информационной инфраструктуры, включенных в перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере здравоохранения;

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

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

6. Для проведения категорирования объектов критической информационной инфраструктуры в сфере здравоохранения в соответствии с Правилами решением руководителя субъекта критической информационной инфраструктуры создается постоянно действующая комиссия по категорированию.

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

7. Сфера здравоохранения имеет отраслевые признаки значимости:

а) субъект критической информационной инфраструктуры, являющийся медицинской организацией, осуществляет оказание специализированной, в том числе высокотехнологичной, медицинской помощи, скорой, в том числе скорой специализированной, медицинской помощи;

б) субъект критической информационной инфраструктуры, являющийся организацией оптовой торговли лекарственными средствами и (или) аптечной организацией, осуществляет оптовую торговлю и (или) розничную торговлю лекарственными средствами с выручкой не менее 5 миллиардов рублей и численностью сотрудников не менее 250 человек.

8. Определение категории значимости объектов критической информационной инфраструктуры осуществляется субъектом критической информационной инфраструктуры исходя из возможности возникновения компьютерных атак и компьютерных инцидентов.

9. 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 показателей Перечня.

10. При оценке масштаба последствий возникновения компьютерных атак и компьютерных инцидентов в виде прекращения или нарушения функционирования объектов критической информационной инфраструктуры в сфере здравоохранения:

а) рассматриваются наихудшие сценарии последствий проведения компьютерных атак и компьютерных инцидентов на объекты критической информационной инфраструктуры в сфере здравоохранения, результатом которых является прекращение или нарушение функционирования объектов критической информационной инфраструктуры сферы здравоохранения;

б) определяется зависимость функционирования одного объекта критической информационной инфраструктуры в сфере здравоохранения от функционирования другого объекта критической информационной инфраструктуры;

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

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

11. С целью установления соответствия объекта критической информационной инфраструктуры в сфере здравоохранения критериям значимости и показателям их значений, субъектом критической информационной инфраструктуры определяются объекты критической информационной инфраструктуры в сфере здравоохранения, обрабатывающие информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляющие управление, контроль или мониторинг критических процессов, подлежащие категорированию, а также выявляются процессы, нарушение или прекращение которых может привести к компьютерным атакам и компьютерным инцидентам.

12. Определение объектов критической информационной инфраструктуры в сфере здравоохранения, подлежащих категорированию, осуществляется посредством отнесения принадлежащих субъекту критической информационной инфраструктуры на праве собственности, аренды или на ином законном основании информационных систем, автоматизированных систем управления в сфере здравоохранения к соответствующим типовым отраслевым объектам критической информационной инфраструктуры, функционирующим в сфере здравоохранения.

13. В случае выявления при осуществлении деятельности одного субъекта критической информационной инфраструктуры взаимозависимости информационных систем или автоматизированных систем управления, решением субъекта информационной инфраструктуры такие системы могут быть включены в состав одного объекта критической информационной инфраструктуры в сфере здравоохранения.

14. В случае отсутствия информационных систем, автоматизированных систем управления, относящихся к соответствующим типовым отраслевым объектам критической информационной инфраструктуры, функционирующим в сфере здравоохранения, комиссией по категорированию принимается решение об отсутствии объектов критической информационной инфраструктуры в сфере здравоохранения, подлежащих категорированию.

15. В случае осуществления модернизации объектов критической информационной инфраструктуры в сфере здравоохранения, решением субъекта критической информационной инфраструктуры объект критической информационной инфраструктуры в сфере здравоохранения, состоявший

из нескольких систем, может быть разделен на несколько отдельных объектов критической информационной инфраструктуры в сфере здравоохранения.

16. В случае выявления субъектом критической информационной инфраструктуры объектов критической информационной инфраструктуры в сфере здравоохранения, не соответствующих типам информационных систем, автоматизированных систем управления, включенных в перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере здравоохранения, 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 в Федеральную службу по техническому и экспортному контролю.

17. Субъект критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта, указанного в пункте 16 Правил, направляет в Федеральную службу по техническому и экспортному контролю, сведения, предусмотренные пунктом 17 Правил.

18. 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.

19. В целях категорирования объектов критической информационной инфраструктуры в сфере здравоохранения применяются следующие показатели критериев значимости:

а) социальная значимость:

причинение ущерба жизни и здоровью людей (человека) – для всех субъектов критической информационной инфраструктуры.

В целях применения настоящих Отраслевых особенностей под причинением ущерба жизни и здоровью людей понимается причинение тяжкого и среднего вреда здоровью.

отсутствие доступа к государственной услуге – для субъектов критической информационной инфраструктуры, которые оказывают государственные услуги и субъектов критической информационной инфраструктуры, обеспечивающих эксплуатацию информационных систем, автоматизированных систем управления, задействованных в процессе оказания государственной услуги;

б) политическая значимость:

прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия) – для субъектов

критической информационной инфраструктуры являющихся федеральными органами исполнительной власти в сфере здравоохранения, территориальными органами и исполнительными органами субъектов Российской Федерации в сфере здравоохранения, Федерального фонда обязательного медицинского страхования, территориальных фондов Федерального фонда обязательного медицинского страхования;

в) экономическая значимость:

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).

г) экологическая значимость:

вредные воздействия на окружающую среду – для субъектов критической информационной инфраструктуры, использующих в своей деятельности источники ионизирующего излучения.

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

20. Для показателя «причинение ущерба жизни и здоровью людей (человека)» при расчете значения 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 (человека)» для каждого объекта критической информационной инфраструктуры в сфере здравоохранения.

21. Для показателя «отсутствие доступа к государственной услуге» при расчете оценивается максимальное допустимое время, в течение которого государственная услуга может быть недоступной в результате компьютерной атаки и компьютерного инцидента, а также во времени с момента приема запроса о предоставлении государственной услуги субъектом критической информационной инфраструктуры в сфере здравоохранения в течение которого государственная услуга не может быть оказана в результате компьютерной атаки и компьютерного инцидента.

Полученные значения сопоставляются со значениями Перечня «отсутствие доступа к государственной услуге» для каждого объекта критической информационной инфраструктуры в сфере здравоохранения.

22. Для показателя «прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» при расчете оценивается уровень государственного органа власти и делается заключение о присвоении объекту критической информационной инфраструктуры в сфере здравоохранения одной из категорий значимости для возможного события (инцидента), которое может возникнуть в результате компьютерной атаки и компьютерного инцидента.

Полученные значения сопоставляются со значениями Перечня «прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» для каждого объекта критической информационной инфраструктуры в сфере здравоохранения.

23. Для показателя «возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период)» учитываются при расчете следующие критерии:

а) 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;

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

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

г) 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 (процентов от годового объема доходов, усредненного за прошедший 5-летний период)» для каждого объекта критической информационной инфраструктуры в сфере здравоохранения.

24. Для показателя «вредные воздействия на окружающую среду» учитываются при расчете следующие критерии:

а) сведения из Единого государственного реестра недвижимости о границе между субъектами Российской Федерации, границе населённого пункта, декларации промышленной безопасности субъекта критической информационной инфраструктуры, использующей источники ионизирующего излучения, анализа действия поражающих факторов для наиболее опасных по последствиям и вероятных сценариев аварий и определяется граница и территория опасной зоны, на которой возможны вредные воздействия на окружающую среду;

б) данные статистических органов о численности населения на начало и конец периода (года) в границах опасной зоны и определяется среднеарифметическая численность населения в границах опасной зоны.

Полученные значения сопоставляются со значениями показателя Перечня «вредные воздействия на окружающую среду» для каждого объекта критической информационной инфраструктуры.