

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ
от 6 июля 2015 г. N 676

О ТРЕБОВАНИЯХ К ПОРЯДКУ СОЗДАНИЯ, РАЗВИТИЯ, ВВОДА В ЭКСПЛУАТАЦИЮ, ЭКСПЛУАТАЦИИ И ВЫВОДА ИЗ ЭКСПЛУАТАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ДАЛЬНЕЙШЕГО ХРАНЕНИЯ СОДЕРЖАЩЕЙСЯ В ИХ БАЗАХ ДАННЫХ ИНФОРМАЦИИ

В соответствии с частью 6 статьи 14 Федерального закона "Об информации, информационных технологиях и о защите информации" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемые требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации.
2. Установить, что мероприятия, предусмотренные требованиями, утвержденными настоящим постановлением, осуществляются федеральными органами исполнительной власти в пределах бюджетных ассигнований, предусмотренных федеральным законом о федеральном бюджете на соответствующий финансовый год и плановый период на руководство и управление в сфере установленных функций.
3. Рекомендовать иным государственным органам, помимо федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также органам управления государственными внебюджетными фондами, органам местного самоуправления руководствоваться в своей деятельности требованиями, утвержденными настоящим постановлением.

Председатель Правительства
Российской Федерации
Д.МЕДВЕДЕВ

Утверждены

ТРЕБОВАНИЯ

К ПОРЯДКУ СОЗДАНИЯ, РАЗВИТИЯ, ВВОДА В ЭКСПЛУАТАЦИЮ, ЭКСПЛУАТАЦИИ И ВЫВОДА ИЗ ЭКСПЛУАТАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ДАЛЬНЕЙШЕГО ХРАНЕНИЯ СОДЕРЖАЩЕЙСЯ В ИХ БАЗАХ ДАННЫХ ИНФОРМАЦИИ

I. Общие положения

1. Настоящий документ определяет требования к порядку реализации мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем (далее - система) и дальнейшему хранению содержащейся в их базах данных информации, осуществляемых федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации (далее - органы исполнительной власти) в целях повышения эффективности реализации полномочий органов исполнительной власти в результате использования информационно-коммуникационных технологий либо органами исполнительной власти, выступающими от имени публичных партнеров, и частными партнерами в соответствии с соглашениями о государственно-частном партнерстве (далее - частный партнер) в целях реализации указанных соглашений либо органами исполнительной власти, выступающими от имени концедентов, и концессионерами в соответствии с концессионными соглашениями (далее - концессионер) в целях реализации указанных соглашений.

1(1). При реализации органами исполнительной власти, частными партнерами либо концессионерами мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации систем и дальнейшему хранению содержащейся в их базах данных информации должны выполняться:

а) требования о защите информации, содержащейся в системах, устанавливаемые федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия

техническим разведкам и технической защите информации, в пределах их полномочий;

б) требования к организации и мерам защиты информации, содержащейся в системе;

в) требования о защите персональных данных, предусмотренные частью 3 статьи 19 Федерального закона "О персональных данных" (в случае наличия в системе персональных данных).

1(2). В целях выполнения требований о защите информации, предусмотренных пунктом 1(1) настоящего документа (далее - требования о защите информации), органы исполнительной власти определяют требования к защите информации, содержащейся в системе органа исполнительной власти, для чего осуществляют:

а) определение информации, подлежащей защите от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации;

б) анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать система;

в) классификацию системы в соответствии с требованиями о защите информации;

г) определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в системе, и разработку на их основе модели угроз безопасности информации;

д) определение требований к информационной системе (подсистеме) защиты информации, содержащейся в системе.

II. Требования к порядку создания системы

2. Основанием для создания системы является:

а) обязанность органа исполнительной власти по созданию системы, предусмотренная нормативными правовыми актами;

б) решение органа исполнительной власти о создании системы с целью

обеспечения реализации возложенных на него полномочий;

в) решение Правительства Российской Федерации о реализации проекта государственно-частного партнерства;

г) решение высшего исполнительного органа государственной власти субъекта Российской Федерации о реализации проекта государственно-частного партнерства, если публичным партнером является субъект Российской Федерации либо планируется проведение совместного конкурса с участием субъекта Российской Федерации (за исключением случаев проведения совместного конкурса с участием Российской Федерации);

д) решение Правительства Российской Федерации о заключении концессионного соглашения;

е) решение высшего исполнительного органа государственной власти субъекта Российской Федерации о заключении концессионного соглашения, если концедентом является субъект Российской Федерации.

2(1). Проекты правовых актов, указанных в пункте 2 настоящего документа, являющихся основанием для создания системы, разрабатываются с учетом концепции создания системы (далее - концепция), включающей в себя технико-экономическое обоснование реализации системы. Концепция является документом технической документации на систему и содержит обоснование вариантов построения системы, условия и мероприятия по ее созданию, на основе которых принимается решение о необходимости и целесообразности создания системы, формируются требования к ней, а также обеспечиваются единый контекст и взаимосвязь результатов реализации требований к системе на последующих этапах ее жизненного цикла, в том числе при разработке технического задания на систему. В концепции приводятся в том числе:

а) результаты анализа нормативных правовых актов, методических документов, международных и национальных стандартов Российской Федерации, в соответствии с которыми разрабатывается система;

б) классификация системы в соответствии с требованиями о защите информации;

в) описание выявленных проблем, решение которых возможно средствами системы, описание требований к системе, включая определение требований к информационной системе (подсистеме) защиты информации и допустимых затрат на разработку, ввод в действие и эксплуатацию системы, описание эффекта, ожидаемого от создания системы, условий создания и функционирования системы;

г) цели и задачи создания системы, архитектура системы, включая состав, выполняемые функции и взаимосвязи компонентов системы, состав сведений, подлежащих размещению в системе, обоснование выбранного варианта построения системы;

д) показатели степени автоматизации процессов и их значений, которые должны быть достигнуты в результате создания системы, а также критерии оценки достижения целей создания системы;

е) оценка финансовых, трудовых и материальных ресурсов, необходимых для реализации требований, указанных в подпункте "в" настоящего пункта (технико-экономическое обоснование), включая оценку указанных ресурсов для создания системы, ввода ее в эксплуатацию, эксплуатации и в случае, если установлен срок эксплуатации системы, оценку необходимых ресурсов для вывода системы из эксплуатации и дальнейшего хранения содержащейся в ее базах данных информации.

3. Создание системы осуществляется в соответствии с разрабатываемым согласно концепции техническим заданием с учетом модели угроз безопасности информации, предусмотренной подпунктом "г" пункта 1(2) настоящего документа, а также уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных и требований настоящего документа.

Техническое задание на создание системы и (или) модель угроз безопасности информации согласуются с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации.

В случае если в соответствии с технико-экономическим обоснованием, указанным в подпункте "е" пункта 2(1) настоящего документа, объем требуемого федеральным органам исполнительной власти финансирования на реализацию необходимых для создания системы мероприятий составляет более 100 миллионов рублей, техническое задание согласуется указанными федеральными органами исполнительной власти с уполномоченным федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, на соответствие государственной политике в сфере информационных технологий, а также единой технической политике, утверждаемой президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности.

Техническое задание на создание системы должно включать в себя сформированные в соответствии с подпунктами "а" и "в" пункта 1(1) настоящего документа требования о защите информации, содержащейся в системе.

Сроки согласования каждого из указанных в настоящем пункте документов не могут превышать 20 рабочих дней.

4. Техническое задание на создание системы и модель угроз безопасности информации утверждаются должностным лицом органа исполнительной власти, на которое возложены соответствующие полномочия.

5. Порядок создания системы включает следующие последовательно реализуемые этапы:

- а) разработка документации на систему и ее части;
- б) разработка рабочей документации на систему и ее части;
- в) разработка или адаптация программного обеспечения;
- г) пусконаладочные работы;
- д) проведение предварительных испытаний системы;

- е) проведение опытной эксплуатации системы;
- ж) проведение приемочных испытаний системы.

6. Этап разработки документации на систему и ее части включает разработку, согласование и утверждение документации в объеме, необходимом для описания полной совокупности проектных решений (в том числе по защите информации) и достаточном для дальнейшего выполнения работ по созданию системы.

7. Этап разработки рабочей документации на систему и ее части включает разработку, согласование и утверждение документации, содержащей сведения, необходимые для выполнения работ по вводу системы в эксплуатацию и ее эксплуатации, и порядка эксплуатации системы, содержащего сведения, необходимые для выполнения работ по поддержанию уровня эксплуатационных характеристик (качества) системы (в том числе по защите информации), установленных в проектных решениях, указанных в пункте 6 настоящего документа, в том числе:

а) перечень действий сотрудников при выполнении задач по эксплуатации системы, включая перечень, виды, объемы и периодичность выполнения работ по обеспечению функционирования системы;

б) контроль работоспособности системы и компонентов, обеспечивающих защиту информации;

в) перечень неисправностей, которые могут возникнуть в процессе эксплуатации системы, и рекомендации в отношении действий при их возникновении;

г) перечень режимов работы системы и их характеристики, а также порядок и правила перевода системы с одного режима работы на другой с указанием необходимого для этого времени.

8. Этап разработки или адаптации программного обеспечения включает разработку программного обеспечения системы, выбор и адаптацию приобретаемого программного обеспечения, а также в установленных случаях и порядке сертификацию разработанного программного обеспечения системы и средств защиты информации по

требованиям безопасности информации.

9. Этап пусконаладочных работ включает автономную наладку технических средств и программного обеспечения частей системы, загрузку информации в ее базу данных, комплексную наладку технических средств и программного обеспечения системы, включая средства защиты информации.

10. Этап проведения предварительных испытаний включает:

а) разработку программы и методики предварительных испытаний, в соответствии с которыми осуществляется проверка системы на работоспособность и соответствие техническому заданию на ее создание;

б) проверку системы на работоспособность и соответствие техническому заданию на ее создание;

в) устранение выявленных при проведении таких испытаний неисправностей и внесение изменений в документацию и рабочую документацию на систему;

г) оформление протокола испытаний и акта о приемке системы в опытную эксплуатацию.

11. Этап проведения опытной эксплуатации включает:

а) разработку программы и методики опытной эксплуатации;

б) опытную эксплуатацию системы в соответствии с программой и методикой опытной эксплуатации;

в) доработку программного обеспечения системы и дополнительную наладку технических средств в случае обнаружения недостатков, выявленных при опытной эксплуатации системы;

г) оформление акта о завершении опытной эксплуатации, включающего перечень недостатков, которые необходимо устранить до начала эксплуатации системы.

12. Этап проведения приемочных испытаний включает:

а) испытания системы на соответствие техническому заданию на ее

создание в соответствии с программой и методикой приемочных испытаний;

б) анализ результатов устранения недостатков, указанных в акте о завершении опытной эксплуатации;

в) оформление акта о приемке системы в эксплуатацию.

III. Требования к порядку ввода системы в эксплуатацию

13. Основанием для ввода системы в эксплуатацию является правовой акт органа исполнительной власти о вводе системы в эксплуатацию, определяющий перечень мероприятий по обеспечению ввода системы в эксплуатацию и устанавливающий срок начала эксплуатации.

14. Правовой акт органа исполнительной власти о вводе системы в эксплуатацию включает:

а) мероприятия по разработке и утверждению организационно-распорядительных документов, определяющих мероприятия по защите информации в ходе эксплуатации системы, разработка которых предусмотрена нормативными правовыми актами и методическими документами федерального органа исполнительной власти в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, а также национальными стандартами в области защиты информации;

б) мероприятия по аттестации системы по требованиям защиты информации, в результате которых в установленных законодательством Российской Федерации случаях подтверждается соответствие защиты информации, содержащейся в системе, требованиям, предусмотренным законодательством Российской Федерации об информации, информационных технологиях и о защите информации;

в) мероприятия по подготовке органа исполнительной власти, а также частного партнера в случае заключения соглашения о государственно-частном партнерстве либо концессионера в случае заключения концессионного соглашения к эксплуатации системы;

г) мероприятия по подготовке должностных лиц органа исполнительной власти, а также работников частного партнера в случае заключения соглашения о государственно-частном партнерстве либо работников концессионера в случае заключения концессионного соглашения к эксплуатации системы, включая лиц, ответственных за обеспечение защиты информации;

д) мероприятия по оформлению прав на использование компонентов системы, являющихся объектами интеллектуальной собственности.

15. Ввод системы в эксплуатацию не допускается в следующих случаях:

а) невыполнение установленных законодательством Российской Федерации требований о защите информации, включая отсутствие действующего аттестата соответствия требованиям безопасности информации;

б) отсутствие в реестре территориального размещения объектов контроля, предусмотренном Правилами осуществления контроля за размещением технических средств информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями, на территории Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. N 675 "О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона "Об информации, информационных технологиях и о защите информации", сведений о размещении технических средств информационной системы на территории Российской Федерации;

в) невыполнение требований настоящего раздела, выявленных в ходе осуществления контроля в соответствии с Правилами осуществления контроля за соблюдением требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. N 675 "О порядке осуществления контроля за соблюдением

требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона "Об информации, информационных технологиях и о защите информации";

г) отсутствие надлежащего оформления прав на использование компонентов системы, являющихся объектами интеллектуальной собственности.

16. Срок начала эксплуатации системы не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом органа исполнительной власти о вводе системы в эксплуатацию.

IV. Требования к порядку развития системы

17. Мероприятия по развитию системы осуществляются в соответствии с требованиями, установленными для создания системы, за исключением требования к разработке концепции.

V. Требования к порядку эксплуатации системы

18. Основанием для начала эксплуатации системы является наступление срока, установленного правовым актом органа исполнительной власти о вводе системы в эксплуатацию, указанным в пункте 13 настоящего документа.

19. Орган исполнительной власти, частный партнер или концессионер осуществляют эксплуатацию системы в соответствии с рабочей документацией, указанной в пункте 7 настоящего документа.

19(1). Эксплуатация системы не допускается в случаях, указанных в части 7 статьи 14 Федерального закона "Об информации, информационных технологиях и о защите информации", а также в пункте 15 настоящего документа.

VI. Требования к порядку вывода системы из эксплуатации и дальнейшего хранения содержащейся в ее базах данных информации

20. Основанием для вывода системы из эксплуатации является:

а) завершение срока эксплуатации системы, в случае если такой срок был установлен правовым актом органа исполнительной власти о

вводе системы в эксплуатацию;

б) нецелесообразность эксплуатации системы, в том числе низкая эффективность используемых технических средств и программного обеспечения, изменение правового регулирования, принятие управленческих решений, а также наличие иных изменений, препятствующих эксплуатации системы;

в) финансово-экономическая неэффективность эксплуатации системы.

21. При наличии одного или нескольких оснований для вывода системы из эксплуатации, указанных в пункте 20 настоящего документа, орган исполнительной власти утверждает правовой акт о выводе системы из эксплуатации.

22. Правовой акт о выводе системы из эксплуатации включает:

а) основание для вывода системы из эксплуатации;

б) перечень и сроки реализации мероприятий по выводу системы из эксплуатации;

в) порядок, сроки, режим хранения и дальнейшего использования информационных ресурсов, включая порядок обеспечения доступа к информационным ресурсам выводимой из эксплуатации системы и обеспечения защиты информации, содержащейся в выводимой из эксплуатации системе;

г) порядок, сроки и способы информирования пользователей о выводе системы из эксплуатации.

23. Перечень мероприятий по выводу системы из эксплуатации включает:

а) подготовку правовых актов, связанных с выводом системы из эксплуатации;

б) работы по выводу системы из эксплуатации, в том числе работы по деинсталляции программного обеспечения системы, по реализации прав на программное обеспечение системы, демонтажу и списанию технических средств системы, обеспечению хранения и дальнейшего использования информационных ресурсов системы;

в) обеспечение защиты информации в соответствии с документацией на систему и организационно-распорядительными документами по защите информации, в том числе архивирование информации, содержащейся в системе, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

24. Если нормативными правовыми актами Российской Федерации не установлено иное, то сроки хранения информации, содержащейся в базах данных системы, определяются органом исполнительной власти и не могут быть меньше сроков хранения информации, которые установлены для хранения документов в бумажном виде, содержащих такую информацию.

25. Срок вывода системы из эксплуатации не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о выводе системы из эксплуатации.