Постановление Правительства РФ от 06.07.2015 № 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 ред. Постановлений Правительства РФ от 14.11.2015 № 1235, от 11.05.2017 № 555)

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

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

Утверждены
постановлением Правительства
Российской Федерации
от 6 июля 2015 г. № 676

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 и дальнейшему хранению содержащейся в их базах данных информации, осуществляемых федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации (далее соответственно - система, органы исполнительной власти) в целях повышения эффективности реализации полномочий органов исполнительной власти в результате использования информационно-коммуникационных технологий.

1(1). При реализации органами исполнительной власти 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 защиты информации, в пределах их полномочий;
б) требования к организации и мерам защиты информации, содержащейся в системе.

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.

3. Создание системы осуществляется в соответствии с техническим заданием с учетом модели угроз безопасности информации, предусмотренной подпунктом «г» пункта 1(2) настоящего документа.

Модель угроз безопасности информации и (или) техническое задание на создание системы 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.

Техническое задание на создание системы должно включать сформированные в соответствии с подпунктом «а» пункта 1(1) настоящего документа требования к защите информации, содержащейся в системе.

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 к эксплуатации системы;
г) мероприятия по подготовке должностных лиц органа исполнительной власти к эксплуатации системы, включая лиц, ответственных за обеспечение защиты информации.

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. № 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. № 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».

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.

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 осуществляет эксплуатацию системы в соответствии с рабочей документацией, указанной в пункте 7 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.

служебная тайна, персональные данные, техническая защита информации, сертификация, аттестация

From:
http://sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://sps-ib.ru/npa:pp676_06.07.2015

Last update: **2017/05/25 11:44**