

## Раздел 2 Нормативно-правовая база по информационной безопасности

### 2.1 Нормативные правовые акты

Нормативно-правовую базу по защите информации в РФ образуют виды документов, показанные на рисунке 2.1.



Рисунок 2.1 - Нормативно-правовая база по защите информации в РФ

Таблица 2.1 – Нормативные правовые акты

Нормативные правовые акты	
<b>"Гражданский кодекс Российской Федерации (часть первая)"</b> от 30.11.1994 N 51-ФЗ (ред. от 05.05.2014) (с изм. и доп., вступ. в силу с 01.09.2014)	Определяет правовое положение участников гражданского оборота, основания возникновения и порядок осуществления вещественных и интеллектуальных прав
<b>"Гражданский кодекс Российской Федерации (часть четвертая)"</b> от 18.12.2006 N 230-ФЗ (ред. от 12.03.2014)	Определяет правовое положение участников гражданского оборота, основания возникновения и порядок осуществления вещественных и интеллектуальных прав
Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 21.07.2014) <b>"О связи"</b> (с изм. и доп., вступ. в силу с 01.08.2014)	Определяет правовое положение участников процесса обмена информацией

Продолжение таблицы 2.1

<b>Нормативные правовые акты</b>	
<b>"Уголовный кодекс Российской Федерации"</b> от 13.06.1996 N 63-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 04.08.2014)	Устанавливает преступность и наказуемость деяний на территории России. Статьи 272-274 устанавливают уголовную ответственность за неправомерный доступ к компьютерной информации
Федеральный закон от 28 декабря 2010 г. №390-ФЗ <b>«О безопасности»</b>	Определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления в области безопасности, а также статус Совета Безопасности РФ
Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 21.07.2014) <b>"Об информации, информационных технологиях и о защите информации"</b>	Регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации
Федеральный закон от 27 июля 2006 г. № 152-ФЗ <b>«О персональных данных»</b>	Регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации
Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 28.06.2014) <b>"Об электронной подписи"</b>	Регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий

Продолжение таблицы 2.1

Нормативные правовые акты	
Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 21.07.2014) <b>"О лицензировании отдельных видов деятельности"</b>	Регулирует отношения, возникающие при разработке, принятии, применении и исполнении требований к продукции или к связанным с ними процессам проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; оценке соответствия
Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 23.06.2014) <b>"О техническом регулировании"</b>	Регулирует отношения между юридическими и физическими лицами, государственными органами, возникающие, изменяющиеся или прекращающиеся по поводу установления обязательных технических норм и правил, подтверждения соответствия продукции, процессов ее производства обязательным требованиям, стандартизации, аккредитации органов по сертификации и испытательных лабораторий, привлечения к ответственности в случаях несоответствия требованиям технических регламентов и финансирования работ в области технического регулирования. Имеет важнейшее значение для определения порядка оценки соответствия средств защиты установленным требованиям
Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) <b>"О коммерческой тайне"</b>	Регулируются отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции. Действие Закона распространяется на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована. Законом определяются права обладателя коммерческой тайны, регулируются отношения, связанные с коммерческой тайной, полученной при выполнении государственного контракта для государственных нужд. Также устанавливаются требования к охране конфиденциальности информации, составляющей коммерческую тайну, в том числе при трудовых отношениях и в гражданско-правовых отношениях.

Продолжение таблицы 2.1

Нормативные правовые акты	
Проект Федерального закона « <b>О служебной тайне</b> » № 124871-4, июль 2014 г	Регулируются отношения, возникающие в связи с отнесением сведений к служебной тайне, их защитой и снятием ограничений на доступ к указанным сведениям
Указ Президента РФ от 06.03.1997 N 188 (ред. от 23.09.2005) " <b>Об утверждении Перечня сведений конфиденциального характера</b> "	Перечень утвержден в целях совершенствования порядка опубликования и вступления в силу актов Президента РФ, Правительства РФ и нормативных правовых актов федеральных органов исполнительной власти
Указ Президента РФ от 16.08.2004 N 1085 (ред. от 01.09.2014) " <b>Вопросы Федеральной службы по техническому и экспортному контролю</b> "	Определено, что Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности; уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля; органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну
Указ Президента РФ от 06.05.2011 N 590 (ред. от 25.07.2014) " <b>Вопросы Совета Безопасности Российской Федерации</b> "	Регламентирован порядок проведения заседаний Совета Безопасности РФ, работы его аппарата и постоянных комиссий. Совет формирует госполитику в области обеспечения национальной безопасности, контролирует ее реализацию, а также прогнозирует, выявляет, оценивает угрозы, военную опасность, разрабатывает меры по их нейтрализации

Нормативные правовые акты	
Указ Президента РФ от 17.03.2008 N 351 (ред. от 25.07.2014) <b>"О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"</b>	Регламентированы меры по обеспечению ИБ РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена. Не допускается подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники (ВТ), применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу РФ, в том числе к международной компьютерной сети «Интернет». При необходимости такое подключение производится только с использованием специально предназначенных для этого средств защиты информации
Постановление Правительства РФ от 1 ноября 2012 г. № 1119 <b>«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»</b>	В целях реализации конституционного права граждан на неприкосновенность частной жизни, личную и семейную тайну установлены требования к обеспечению безопасности персональных данных при их обработке с использованием средств автоматизации
Постановление Правительства РФ от 26 января 2006 г. № 45 <b>«Об организации лицензирования отдельных видов деятельности»</b>	Перечисляются федеральные органы исполнительной власти, осуществляющие лицензирование, и лицензируемые указанными органами виды деятельности
Постановление Правительства РФ от 31 августа 2006 г. № 532 <b>«О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»</b>	Определяется порядок лицензирования деятельности по разработке и (или) производству средств защиты конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями, которым предусматриваются лицензионные требования и условия к соискателям, а также перечень документов, представляемых для получения лицензии

Продолжение таблицы 2.1

<b>Нормативные правовые акты</b>	
Постановление Правительства РФ от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»	Уточнен перечень предъявляемых к соискателям лицензий требований и документов, представляемых для получения лицензии. Определен перечень грубых нарушений лицензионных требований
Постановление Правительства РФ от 29 августа 2001 г. № 633 «О порядке размещения и использования на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации иностранных технических средств наблюдения и контроля»	Определяется порядок размещения и использования технических средств иностранного производства, либо российского, доработанных с участием представителей иностранной стороны, предназначенных для проведения измерений и регистрации параметров в физических средах, проведения химических и биологических исследований, определения местоположения или идентификации объектов, а также средств обработки и передачи результатов измерений и регистрации
Постановление Правительства РФ № 211 от 21.03.2012 г "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»	Приведены основные меры по защите персональных данных, обрабатываемых в информационных системах государственных и муниципальных органов

## 2.2 Нормативно-методические и методические документы

Таблица 2.2 – Нормативно-методические и методические документы

<b>Нормативно-методические и методические документы</b>	
<b>Доктрина информационной безопасности Российской Федерации</b> , утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895	Доктрина служит основой для: формирования государственной политики в области обеспечения ИБ РФ; подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения ИБ РФ; разработки целевых программ обеспечения ИБ РФ

Продолжение таблицы 2.2

<b>Нормативно-методические и методические документы</b>	
<p><b>Приказ ФСТЭК РФ от 28.08.2007 № 181 (ред. от 15.10.2010) «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации»</b> (Зарегистрировано в Минюсте РФ 03.10.2007 № 1023) - утратил силу в связи с изданием Приказа ФСТЭК № 83 от 12.07.2012г.</p>	<p>Приведен перечень лицензионных требований и условий, определен список документов, прилагаемых к заявлению о предоставлении (переоформлении) лицензии, регламентирована процедура их рассмотрения. Регламентирован порядок проведения проверок соблюдения лицензиатом лицензионных требований и условий. Установлен порядок ведения реестра лицензий на осуществление деятельности по технической защите конфиденциальной информации и предоставления информации из него</p>
<p><b>Приказ ФСТЭК РФ от 28.08.2007 № 182 (ред. От 15.10.2010) «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации»</b> (Зарегистрировано в Минюсте РФ 27.09.2007 № 10193)</p>	<p>Определены основные требования и условия осуществления деятельности по разработке и (или) производству средств защиты конфиденциальной информации. Определены перечни сведений, указываемых в заявлении о предоставлении лицензии по установленной форме, и документов, прилагаемых к такому заявлению</p>
<p><b>Положение о сертификации средств защиты информации по требованиям безопасности информации,</b> утвержденное приказом Гостехкомиссии России от 27 октября 1995 г. № 199</p>	<p>Определяет оргструктуру Системы сертификации, функции субъектов и процедуру последней. Урегулирован порядок госконтроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами. Закреплены общие требования к нормативным и методическим документам по сертификации. Приведены перечень средств, подлежащих сертификации в указанной системе, а также формы ряда документов</p>



Продолжение таблицы 2.2

<b>Нормативно-методические и методические документы</b>	
<p><b>Положение по аттестации объектов информатизации по требованиям безопасности информации,</b> утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.</p>	<p>Устанавливает основные принципы и оргструктуру системы аттестации, порядок проведения, контроля и надзора за ней и эксплуатацией аттестованных объектов. Определены требования к нормативным и методическим документам по аттестации объектов. Приведены формы заявки на проведение аттестации и аттестата соответствия</p>
<p><b>Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации,</b> утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.</p>	<p>Устанавливает основные принципы аккредитации предприятий, организаций и учреждений в качестве названных лабораторий и органов по сертификации средств защиты информации в системе сертификации последних по требованиям безопасности информации. Определен порядок аккредитации и ее аннулирования</p>
<p><b>Типовое положение об испытательной лаборатории,</b> утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.</p>	<p>Определены основные задачи, функции, права и обязанности испытательных лабораторий, относящихся к системе сертификации, созданной Гостехкомиссией России</p>
<p><b>Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации</b> (утв. Приказом Государственной технической комиссии при Президенте РФ от 5 января 1996 г. № 3)</p>	<p>Определен порядок работы органа по аттестации объектов информатики по требованиям безопасности информации. Определены права, обязанности и ответственность органа по аттестации</p>
<p><b>Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации</b> (утв. Приказом Государственной технической комиссии при Президенте РФ от 5 января 1996 г. № 3)</p>	<p>Устанавливает требования к органу по сертификации средств обработки, передачи и контроля защищенности информации. Определены функции, права, обязанности и ответственность органа по сертификации</p>



<b>Нормативно-методические и методические документы</b>	
Руководящий документ. <b>Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.)	Определяет систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа, являющейся частью общей проблемы безопасности информации. Концепция предназначена для заказчиков, разработчиков и пользователей средств и систем, которые применяются для обработки, хранения и передачи информации, требующей защиты
Руководящий документ. <b>Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.)	Устанавливает единый на территории России порядок исследований и разработок в области защиты информации, обрабатываемой АС различного уровня и назначения, от НСД; создания средств ВТ общего и спецназначения, защищенных от утечки, искажения или уничтожения информации за счет НСД; создания программных и техсредств защиты информации от НСД в составе систем защиты секретной информации в создаваемых АС
Руководящий документ. <b>Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.)	Устанавливает классификацию средств ВТ по уровню защищенности от НСД
Руководящий документ. <b>Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.)	Определены требования по защите информации в АС различных классов. Установлено 9 классов защищенности. Каждый класс характеризуется минимальной совокупностью требований по защите. Классы делятся на 3 группы, отличающиеся особенностями обработки информации

<b>Нормативно-методические и методические документы</b>	
Руководящий документ. <b>Защита от несанкционированного доступа к информации. Термины и определения</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.)	Устанавливает термины и определения понятий в области защиты средств ВТ и АС
Руководящий документ. <b>Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 25 июля 1997 г.)	Устанавливает классификацию экранов по уровню защищенности от НСД. Классификация основана на перечне показателей защищенности и совокупности описывающих их требований
Руководящий документ. <b>Защита информации. Специальные защитные знаки. Классификация и общие требования</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 25 июля 1997 г.)	Устанавливает классификацию и требования к знакам, предназначенным для контроля доступа к объектам защиты, а также для защиты документов от подделки
Руководящий документ. <b>Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей</b> (утв. Решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. № 114)	Устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного производства) средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей

Продолжение таблицы 2.2

<b>Нормативно-методические и методические документы</b>	
<p>Руководящий документ. <b>Безопасность информационных технологий. Критерии оценки безопасности информационных технологий</b> (введен в действие приказом Государственной технической комиссии при Президенте РФ от 19 июня 2002 г. № 187)</p>	<p>Приведены требования к безопасности информационных технологий. В документе определены виды требований безопасности: функциональные и требования доверия. Приведены меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем ИТ для удовлетворения предъявленных к ним функциональных требований. Установлены основные конструкции представления требований безопасности (профиль защиты, задание по безопасности). Документ содержит основные методические положения по оценке безопасности ИТ</p>
<p><u>Приказ ФСТЭК России от 31 августа 2010 г. N 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»</u></p>	<p>Изложены требования к обеспечению безопасности информации, содержащейся в информационных системах общего пользования</p>
<p>Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»</p>	<p>Приведен состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»</p>
<p><b>Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных</b> (выписка) (утв. ФСТЭК России 15 февраля 2008 г.)</p>	<p>Приводится систематизированный перечень таких угроз безопасности персональных данных. Дано обобщенное описание информационных систем как объектов защиты, возможных источников угрозы, основных классов уязвимостей, возможных видов деструктивных воздействий, а также основных способов их реализации</p>
<p><b>Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации</b> (утв. ФСБ РФ 21 февраля 2008 г. № 149/54-144)</p>	<p>Методические рекомендации предназначены для операторов и разработчиков информационных систем персональных данных и охватывают вопросы защиты персональных данных с помощью криптосредств</p>

Продолжение таблицы 2.2

<b>Нормативно-методические и методические документы</b>	
<b>Нормативно-методический документ.</b> <b>«Специальные требования и рекомендации по технической защите конфиденциальной информации» СТР-К</b> (утв. Приказом Гостехкомиссии России от 30 августа 2002 г. № 282)	Определяет порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей государственной тайны
Решение Гостехкомиссии РФ от 21.10.1997 № 61 <b>«О защите информации при вхождении России в международную информационную систему «Интернет»</b>	Приведены рекомендации Гостехкомиссии РФ по совершенствованию защиты информационных ресурсов РФ при вхождении в международную информационную систему «Интернет»
<b>Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам</b>	Документ ограниченного распространения
Приказ ФСТЭК РОССИИ от 14 марта 2014 г. N 31 <b>«Об утверждении требований к обеспечению защиты информации в АСУ производственными и технологическими процессами»</b>	Изложены требования к обеспечению безопасности информации в АСУ
Приказ ФСТЭК России от 11 февраля 2013 г. N 17 <b>«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»</b>	Изложены требования к обеспечению безопасности информации не составляющей государственную тайну, содержащейся в государственных информационных системах»

<b>Нормативно-методические и методические документы</b>	
<b>Информационное сообщение ФСТЭК России от 15.07.2013 N 240/22/2637 "По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и приказа ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"</b>	Информационное сообщение по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России №17 и №21
<b>«Методический документ. Меры защиты информации в государственных информационных системах».</b> Утвержден ФСТЭК России 11.02.2014 г.	Приведено содержание мер защиты информации в государственных информационных системах и методические рекомендации по их применению
<b>«Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г № 996 «Об утверждении требований и методов по обезличиванию персональных данных».</b> Утвержден Роскомнадзором 13.12.2013 г	Изложены требования и методы по обезличиванию персональных данных и методические рекомендации по их применению
<b>Приказ Роскомнадзора от 5 сентября 2013 г № 996 «Об утверждении требований и методов по обезличиванию персональных данных»</b>	Изложены требования и методы по обезличиванию персональных данных

## 2.3 Международные стандарты в области информационной безопасности

Таблица 2.3.1 – Международные стандарты в области информационной безопасности

№ п/п	Стандарт/ Нормативный акт	Разработчик	Статус
1	<b>ISO/IEC TR 13335</b> Information technology – Guidelines for the management of information technology security. Семейство международных стандартов «Информационная технология. Методы и средства обеспечения безопасности» [21]	Международная организация по стандартизации (ИСО)	Международные стандарты
2	<b>ISO/IEC 15408</b> Security technigues. Evalution criteria for IT security. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий	ИСО	Международные стандарты
3	<b>ISO/IEC 19791</b> Information technology. Security techniques. Security assessment of operational systems. Информационные технологии. Методы безопасности. Оценка безопасности автоматизированных систем		
4	<b>ISO/IEC 2700x</b> Information technology – Security techniques. Семейство международных стандартов по управлению информационной безопасностью (разрабатывается подкомитетом ISO/IEC JTC 1/SC 27)	ИСО	Международные стандарты
5	<b>BSI IT</b> Baseline Protection Manual. Standart security safeguards. Руководство по базовому уровню защиты информационных технологий	Германское информационное агентство безопасности	Национальные стандарты
6	<b>BS-7799</b> серия стандартов по созданию и сертификации систем управления ИБ	Британский институт стандартизации (BSI)	
7	<b>NIST SP800-53</b> Recommended Security Controls for Federal Information Systems. Рекомендуемые меры контроля безопасности для Федеральных информационных систем	Национальный институт по стандартизации и технологиям (NIST)	

№ п/п	Стандарт/ Нормативный акт	Разработчик	Статус
8	<b>COBIT</b> (Control Objectives for Information and related Technology). Цели контроля для информационных и смежных технологий	Ассоциация аудиторов информационных систем (ISACA)	Профессиональный стандарт
9	<b>FISCAM</b> (Federal Information System Controls Audit Manual). Федеральное руководство по аудиту информационных систем	Главная счетная палата США (GAO)	Отраслевые стандарты
10	<b>PCI DSS</b> (Payment Card Industry Data Security Standard). Стандарт безопасности данных в индустрии платежных карт	Отраслевая ассоциация платежных карт Payment Card Industry (PCI)	
11	<b>HIPAA</b> (Health Insurance Portability and Accountability Act) Security Rule / Health Insurance Reform: Security Standards. Стандарт безопасности медицинских сведений	Министерство здравоохранения и социального обеспечения США (DHHS)	
12	<b>SPP ICS</b> (System Protection Profile for Industrial Control Systems). Стандарт обеспечения безопасности АСУ ТП	NIST	Индустриальный (промышленный) стандарт
13	<b>СТО БР ИББС-1.0-2014</b> Обеспечение информационной безопасности организаций банковской системы Российской Федерации (РФ)	Банк России	Стандарт банка России



Важное значение для организации ОИБ играет семейство стандартов **ISO/IEC 2700х**.

Таблица 2.3.2 – стандарты ISO/IEC 2700х

<b>Название стандарта</b>	<b>Содержание стандарта</b>
<b>ISO27000</b>	Определения и основные принципы. Планируется унификация со стандартами COBIT и ITIL
<b>ISO27001</b>	Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2)
<b>ISO27002</b>	Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью
<b>ISO27003</b>	Руководство по внедрению системы управления информационной безопасностью
<b>ISO27004</b>	Измерение эффективности системы управления информационной безопасностью
<b>ISO27005</b>	Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности (на основе BS 7799-3)
<b>ISO27006</b>	Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью
<b>ISO27007</b>	Руководство для аудитора систем управления информационной безопасностью
<b>ISO27008</b>	Information technology. Security techniques. Guidance for auditors on ISMS controls (DRAFT) – Руководство по аудиту механизмов контроля систем управления информационной безопасностью. Будет служить дополнением к стандарту ISO 27007
<b>ISO27010</b>	Управление информационной безопасностью при коммуникациях между секторами
<b>ISO27011</b>	Руководство по управлению информационной безопасностью для телекоммуникаций
<b>ISO27013</b>	Руководство по интегрированному внедрению ISO 27000 и ISO 27001
<b>ISO27014</b>	Базовая структура управления информационной безопасностью
<b>ISO27015</b>	Руководство по внедрению систем управления информационной

	безопасностью в финансовом и страховом секторе
<b>ISO27031</b>	Руководство по обеспечению готовности информационных и коммуникационных технологий к их использованию для управления непрерывностью бизнеса
<b>ISO 27033</b>	Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Новый стандарт возможно будет включать в себя более 7 частей
<b>ISO27034</b>	Безопасность приложений
<b>ISO27035</b>	Управление инцидентами безопасности

Продолжение таблицы 2.3.2

Название стандарта	Содержание стандарта
<b>ISO27036</b>	Руководство по идентификации, сбору и/или получению и обеспечению сохранности цифровых свидетельств. Проект разрабатывается на базе британского стандарта BS 10008:2008 «Evidential weight and legal admissibility of electronic information. Specification»
<b>ISO 27799</b>	Управление информационной безопасностью в сфере здравоохранения

#### 2.4 Стандарты РФ, соответствующие международным стандартам в области информационной безопасности

Наиболее востребованными стандартами РФ, соответствующими международным стандартам в области информационной безопасности, являются стандарты, показанные на рисунке 2.2. Более полный перечень отечественных стандартов в области информационной безопасности приведен в списке использованной литературы.



Рисунок 2.2 - Наиболее востребованные стандарты РФ соответствующие международным стандартам в области информационной безопасности