Оглавление

[Лекция 1. Основные правовые понятия. Источники права. Основы государственного устройства РФ в области ИБ. 2](#_Toc207963330)

[Доктрина информационной безопасности РФ 2](#_Toc207963331)

[Основные правовые понятия 2](#_Toc207963332)

[Лекция 2. Информационная безопасность государства 7](#_Toc207963333)

[Информационная безопасность государства 7](#_Toc207963334)

[Этапы развития ИБ 8](#_Toc207963335)

[Государственная политика в сфере информационной безопасности основывается на принципах: 9](#_Toc207963336)

[Внутренние угрозы информационной безопасности государства: 9](#_Toc207963337)

[Внешние угрозы информационной безопасности государства: 10](#_Toc207963338)

[Основные меры защиты ИБ РФ: 10](#_Toc207963339)

[Объектом правового регулирования могут быть конкретные формы существования информации 11](#_Toc207963340)

[Лекция 3. НПА в области ОИБ 12](#_Toc207963341)

[Нормативные правовые акты российской федерации 12](#_Toc207963342)

[Основные федеральные законы в области ИБ 12](#_Toc207963343)

[Основными указами и распоряжениями Президента в области информации, информационных технологий и защиты информации 13](#_Toc207963344)

[Основными постановлениями и распоряжениями Правительства РФ в области информации, информационных технологий и защиты информации 14](#_Toc207963345)

[Основными нормативными актами федеральных органов исполнительной власти, уполномоченными в области информации, информационных технологий и защиты информации 15](#_Toc207963346)

# Лекция 1. Основные правовые понятия. Источники права. Основы государственного устройства РФ в области ИБ.

## Доктрина информационной безопасности РФ

Утверждена Указом  
 Президента Российской Федерации  
 от 5 декабря 2016 г. №646

- не является нормативным актом прямого действия;

- определяет основные понятия ИБ в РФ;

- защищает национальные интересы в информационной сфере;

- определяет основные информационные угрозы и состояние информационной безопасности

- определяет стратегические цели и основные направления обеспечения информационной безопасности;

- дает организационные основы обеспечения информационной безопасности РФ;

- в соответствии с ней должны разрабатываться законы и подзаконные акты в области ИБ;

- уделяет существенное внимание вопросам технологий.

## Основные правовые понятия

**Информация** -

1. информация является одним из важнейших ресурсов жизнедеятельности современного общества;
2. информация является в современном обществе объектом публичных, гражданских и иных правовых отношений;
3. информация в современных условиях является мощным средством оказания вредоносного воздействия на самые различные сферы современного общества

ЭТО результаты отображения и обработки в человеческом сознании внутреннего и окружающего мира — предметов, явлений, процессов, событий, действий других людей и т. п., накапливаемых и используемых как отдельным человеком, так и обществом в целом, а также получаемых, накапливаемых и используемых в созданных человеком информационных системах.

**Защита информации** - предупреждение, выявление, обнаружение, нейтрализация

угроз, ликвидация их последствий (Различают правовую, техническую, криптографическую, физическую ЗИ)  
  
**Безопасность информации** - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность, целостность.   
  
**Информационная безопасность** - это состояние защищенности информационной среды

**Информационная безопасность РФ** - это состояние защищенности личности, общества и государства от внутренних и внешних   
информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ , оборона и безопасность государства, т.е.   
защита конституционного строя, суверенитета, территориальной целостности РФ с использованием информационных средств.

**Информационная сфера** - совокупность информации, объектов информатизации, информационных систем, сайтов интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений».

**Информационная сфера** - совокупность информации, объектов информатизации, информационных систем, сайтов интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений».

**Защищаемая информация** - информация, подлежащая защите в соответствии с требованиями федерального законодательства Российской Федерации, руководящих и методических документов ФСБ России, ФСТЭК России и (или) требованиями, установленными обладателем этой информации.

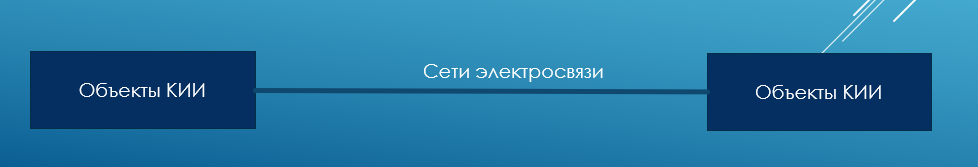
**Носитель информации** - это материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ( люди, документы)

**Обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

**Угроза** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации   
**Свойства угроз**: избирательность, предсказуемость и вредоносность

* Избирательность характеризует нацеленность угрозы на нанесение вреда тем или иным конкретным свойствам объекта безопасности.
* Предсказуемость характеризует наличие признаков возникновения угрозы, позволяющих заранее прогнозировать возможность появления угрозы и определять конкретные объекты защиты, на которые она будет направлена (в том числе на нарушение какого свойства информации, конфиденциальности, целостности или доступности, она будет направлена).
* Вредоносность характеризует возможность нанесения вреда различной тяжести объекту безопасности.

**КИИ**- критическая информационная инфраструктура - объекты критической информационной инфраструктуры государства, а также сети электросвязи, используемые для организации взаимодействия таких объектов.









# Лекция 2. Информационная безопасность государства

****

Информационная безопасность государства - защита конституционного строя, суверенитета, территориальной целостности с использованием -информационных средств.

**Жизненно важные интересы государства**:

- Создание целей для реализации интересов личности и общества в информационной сфере.

- Формирование институтов общественного контроля органов государственной власти.

- Безусловное обеспечение законности и правопорядка.

- Создание условий для развития собственной информационной инфраструктуры.

- Формирование системы подготовки и реализации решений органов государственной власти, обеспечивающих национальные интересы страны.

-Защита государственной информационной системы и информационных ресурсов (защита государственной тайны).

- Защита единого информационного пространства страны.

- Разделение равноправного и взаимного международного сотрудничества.

****

## Этапы развития ИБ

* I этап — до 1816 года
  + характеризуется использованием естественно возникавших средств информационных коммуникаций.
* II этап — начиная с 1816 года
  + начало использования искусственно создаваемых технических средств электро-и радиосвязи
* III этап — начиная с 1935 года
  + связан с появлением радиолокационных и гидроакустических средств.
* IV этап — начиная с 1946 года
  + Изобретение и внедрение в практическую деятельность электронно-вычислительных машин (компьютеров).
* V этап — начиная с 1965 года
  + создание и развитие локальных информационно-коммуникационных сетей.
* VI этап — начиная с 1973 года
  + использование сверхмобильных коммуникационных устройств с широким спектром задач.
* VII этап — начиная с 1985 года
  + создание и развитие глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения.

Можно предположить, что очередной этап развития информационной безопасности, связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов. Все это изложено в доктрине ИБ

## Государственная политика в сфере информационной безопасности основывается на принципах:

* законности: соблюдение конституции и законодательства РФ;
* баланса интересов граждан вне зависимости от их социального и политического статуса.
* конструктивное взаимодействие всех гос.органов по защите ИБ
* достаточность сил и средств для осуществления ОИБ, в том числе и благодаря мониторингу угроз
* соблюдение норм международного права

Наиболее важными направлениями деятельности обеспечения информационной безопасности являются:

* внесение изменений в законодательство страны, регулирование отношений в области обеспечения информационной безопасности;
* законодательное разграничение полномочий в области информационной безопасности;
* уточнение статуса иностранных информационных агентств, СМИ и журналистов;
* законодательное закрепление приоритета развития национальных сетей связи.

## Внутренние угрозы информационной безопасности государства:

- размывание единого правового пространства страны из-за принятия субъектами РФ не соответствовавших Конституции РФ правовых актов;

- разрушение единого информационного пространства России;

- вытеснение российских информационных агентств и средств массовой информации с внутреннего информационного рынка;

- монополизация информационного рынка;

- блокирование деятельности государственных средств массовой информации по информированию российской, зарубежной аудитории;

- ослабление роли русского языка как государственного языка РФ;

- несанкционированное целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем;

- низкая эффективность информационного обеспечения государственной политики (дефицит кадров, отставание информационных систем от международных стандартов).

## Внешние угрозы информационной безопасности государства:

а) использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

6) использование информационно-коммуникационных технологий в террористических целях ;

в) использование информационно-коммуникационных технологий в экстремистских целях;

г) использование информационно-коммуникационных технологий в преступных целях для совершения различных видов мошенничества;

д) использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

е) использование отдельными государствами технологического доминирования в информационном , ограничения доступа других государств к передовым информационно-коммуникационным технологиям.

## Основные меры защиты ИБ РФ:

* Защита КИИ
* Снижение зависимости страны от ИТ
* Противодействие распространению фейков и злонамеренной информации в сети интернет
* Продвижение позиции РФ на международном уровне

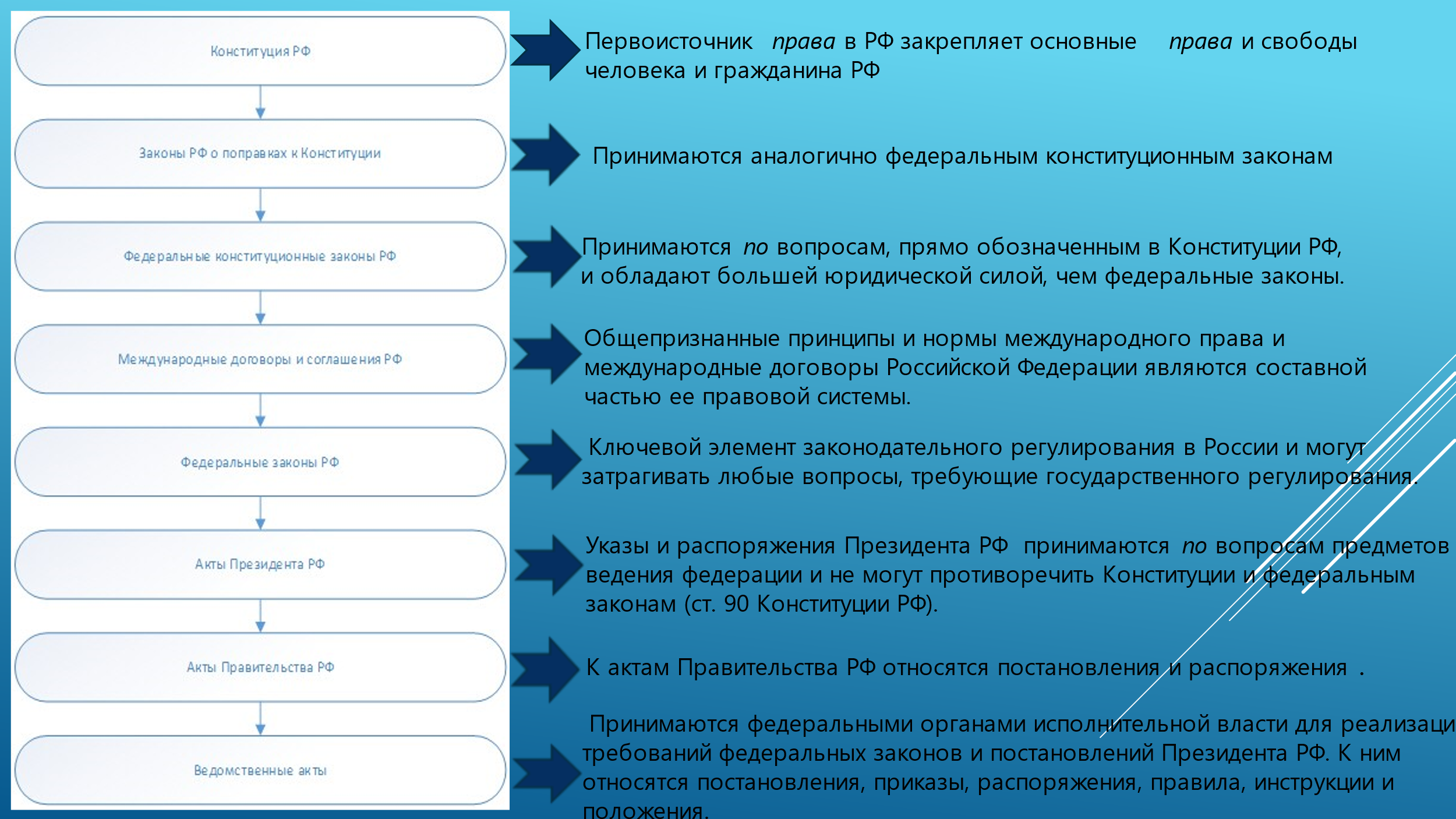
Объектом правового регулирования могут быть конкретные формы существования информации:

* документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
* информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
* информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
* правовая защита информации – законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.



# Лекция 3. НПА в области ОИБ

Нормативные правовые акты российской федерации в области   
информации, информационных технологий и защиты информации основываются на Конституции российской федерации и включают в себя:  
   
• федеральные конституционные законы;   
• федеральные законы и законы российской федерации;   
• указы и распоряжения президента российской федерации;   
утвержденные президентом российской федерации концептуальные и доктринальные документы;   
• постановления и распоряжения правительства российской   
федерации;   
• документы, утвержденные правительством российской федерации;   
• нормативные правовые акты федеральных органов исполнительной власти, уполномоченных в названной области.



## Основные федеральные законы в области ИБ

* Самый основной закон в РФ это Конституция РФ
* Конститу́ция Росси́йской Федера́ции — высший нормативный правовой акт Российской Федерации. Принята на Всенародном голосовании 12 декабря 1993 года, вступила в силу 25 декабря 1993 года. Конституция обладает высшей юридической силой и закрепляет основы конституционного строя России, государственное устройство, права и свободы человека и гражданина, образование представительных, исполнительных, судебных органов власти и систему местного самоуправления, а также конституционные поправки и пересмотр Конституции.
* Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: Этот закон регулирует отношения в области информации, включая ее создание, хранение, передачу и использование, а также устанавливает меры по защите информации, включая требования к информационным системам.
* Федеральный закон от 21.07.1993 г. № 5485-1 «О государственной тайне»: Закон определяет порядок защиты государственной тайны, устанавливает категории секретной информации и определяет ответственность за ее раскрытие, обеспечивая безопасность государственных интересов.
* Федеральный закон от 08.08.2024 г. № 98-ФЗ «О коммерческой тайне»: Закон регулирует защиту коммерческой тайны, определяет условия, при которых информация может считаться коммерческой тайной, а также устанавливает правила ее хранения и использования.
* Федеральный закон от 1.09.2025 г. № 152-ФЗ «О персональных данных»: Этот закон регулирует обработку персональных данных, устанавливает права субъектов данных и обязанности операторов по защите персональной информации, включая условия ее сбора и хранения.
* Федеральный закон от 28.04.2024г. № 63-ФЗ «Об электронной подписи»: Закон устанавливает правовые основы использования электронных подписей, регулирует их виды, порядок создания и применения, а также требования к их ключам.
* Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»: Этот закон определяет правила лицензирования определенных видов деятельности, включая порядок получения и аннулирования лицензий, а также требования к лицензируемым субъектам.
* От 26.06.2017 г 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Этот закон касается компаний, которые работают в сферах, критически важных для жизни государства — таких, что сбой в их работе отразится на здоровье, безопасности и комфорте граждан России.

Основными указами и распоряжениями Президента в области информации, информационных технологий и защиты информации являются:   
  
• Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации«  
• Доктрина информационной безопасности РФ, утвержденная указом президента российской федерации от 05.12.2016 г. №646;   
• Указ президента РФ от 06.03.1997 г. № 188 «об утверждении перечня сведений конфиденциального характера»;   
• Указ президента РФ от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности российской федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;   
• Указ президента РФ от 03.04.1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;   
• Стратегия развития информационного общества в российской федерации на 2017-2030 гг., Утвержденная указом президента РФ от 09.05.2017 г. № 203.

Основными постановлениями и распоряжениями Правительства РФ в области информации, информационных технологий и защиты информации являются:   
• Постановление Правительства РФ от 26.06.1995 г. № 608 « О сертификации средств защиты информации»;   
• Постановление Правительства РФ от 03.03.2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;   
• Постановление Правительства РФ от 03.02.2012 г. № 79 « О лицензировании деятельности по технической защите конфиденциальной информации»;   
• Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите   
персональных данных при их обработке в информационных системах персональных данных»;   
• Постановление Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятых в соответствии с ним нормативными правовыми актами,   
операторами, являющимися государственными или муниципальными органами»;   
• Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке   
обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;   
• Постановление Правительства РФ от 16.04.2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств….»;   
• Постановление Правительства РФ от 15.04.1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;   
• Постановление Правительства РФ от 21.11.2011 г. № 957 «Об организации лицензирования отдельных видов деятельности».

Основными нормативными актами федеральных органов исполнительной власти, уполномоченными в области информации, информационных технологий и защиты информации, являются:   
 • Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (Гостехкомиссия России, 1992);   
• Положение о сертификации средств защиты информации   
по требованиям безопасности информации. Утверждено Приказом Гостехкомиссии России от 27.10.1995 г. № 199;   
• Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден Приказом председателя Гостехкомиссии России от 19.06.2002 г. № 187;   
• Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008 г.;   
• Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14.02.2008 г.;   
• Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1992);   
• Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992;   
• Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1997;   
• Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден Приказом председателя Гостехкомиссии России от 04.06.1999 г. № 114;   
• Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;   
• Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;   
• Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены Приказом ФСБ России и ФСТЭК России от 31.08.2010 г. № 426/489.

Кроме перечисленных нормативных правовых актов в области   
информации, информационных технологий и защиты информации важными являются следующие государственные стандарты:

• ГОСТ Р 50922—2006 «Защита информации. Основные термины и определения»;   
• ГОСТ Р 51275—2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;   
• ГОСТ Р 51583—2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;   
• ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;   
• ГОСТ 34.601 —90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;   
• ГОСТ 34.602—89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;   
• ГОСТ 34.201—89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных   
систем»;   
• РД 50-34.698—90 «Методические указания. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».  
 