3. Федеральное законодательство

- Федеральный закон от 29 июня 2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статью 14 Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"»
- Федеральный закон от 05 апреля 2013 г. № 44-ФЗ (ред. от 31.12.2014) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;
- Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
- **Федеральный закон от 27 июля 2006 г. № 149-ФЗ** «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
- Трудовой кодекс РФ. Глава 14. «Защита персональных данных работника».

4. Указы и распоряжения Президента Российской Федерации

- Указ Президента Российской Федерации № 260 от 22 мая 2015 года «О некоторых вопросах информационной безопасности Российской Федерации».
- Указ Президента Российской Федерации № 537 от 12 мая 2009 года «О стратегии национальной безопасности Российской Федерации до 2020 года»;
- Указ Президента Российской Федерации № 351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Указ Президента Российской Федерации № 1576 от 01 ноября 2008 года «О совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации»;
- Указ Президента Российской Федерации № 1085 от 16 августа 2004 года «Вопросы Федеральной Службы по техническому и экспортному контролю» (в ред. Указов Президента РФ от 22.03.2005 № 330, от 20.07.2005 № 846, от 30.11.2006 № 1321, от 23.10.2008 № 1517, от 17.11.2008 № 1625);
- Указ Президента Российской Федерации № 960 от 11 августа 2003 года «Вопросы Федеральной Службы Безопасности Российской Федерации» (в ред. Указов Президента РФ от 11.07.2004 № 870, от 31.08.2005 № 1007, от 01.12.2005 № 1383, от 12.06.2006 № 602, от 27.07.2006 № 799, от 28.12.2006 № 1476, от 28.11.2007 № 1594, от 28.12.2007 № 1765, от 01.09.2008 № 1278, от 23.10.2008 № 1517, от 17.11.2008 № 1625, от 22.04.2010 № 499, от 14.05.2010 № 589);
- Распоряжение Президента Российской Федерации № 366-рп от 10 июля 2001 года «О подписании конвенции о защите физических лиц при автоматизированной обработке персональных данных»;

- **Доктрина информационной безопасности** Российской Федерации от 9 сентября 2000 г. № Пр-1895;
- Указ Президента Российской Федерации № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера» (в ред. Указов Президента РФ от 23.09.2005 № 1111, от 13.07.2015 № 357);
- Указ Президента Российской Федерации № 170 от 20 января 1994 года «Об основах государственной политики в сфере информатизации» (в ред. Указов Президента РФ от 26.07.95 № 764, от 17.01.97 № 13, от 09.07.97 № 710);
- Указ Президента Российской Федерации № 2334 от 31 декабря 1993 года «О дополнительных гарантиях прав граждан на информацию» (в ред. Указов Президента РФ от 17.01.1997 № 13, от 01.09.2000 № 1606);

5. Постановления Правительства Российской Федерации

- Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «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»;
- Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;
    - Перечень документов, необходимых для получения лицензии на деятельность по технической защите конфиденциальной информации
    - Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации
- Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;
    - Перечень документов, необходимых для получения лицензии на разработку и производство средств защиты конфиденциальной информации
    - Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения видов работ, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности»;
- Постановление Правительства Российской Федерации от 06 октября 2011 г. № 826 «Об утверждении типовой формы лицензии»;
- Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных»;

- Постановление Правительства Российской Федерации от 02 марта 2005 г. № 110 «Об утверждении порядка осуществления государственного надзора за деятельностью в области связи»;
- Постановление Правительства Российской Федерации от 30 июня 2004 г. № 320 «Об утверждении Положения о Федеральном агентстве связи»;
- Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;
- Постановление Правительства Российской Федерации от 03 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

6. Документы уполномоченных федеральных органов

6.1. ФСБ России

- Приказ ФСБ России, ФСТЭК России, Минкомсвязь России № 151/786/461 от 31 декабря 2013 г. «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"».
- Приказ ФСБ России № 416, ФСТЭК № 489 от 31 августа 2010 г. «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;
- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических средств защиты информации (Положение ПКЗ-2005))» (в ред. Приказа ФСБ РФ от 12.04.2010 №173);

6.2. ФСТЭК России

- Информационное сообщение ФСТЭК России от 6 апреля 2015 г. № 240/13/357 «О новой редакции перечней технической (технологической) документации национальных стандартов и методических документов…»;
- Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- Информационное сообщение ФСТЭК России от 15 июля 2013 г. № 240/22/2637 «По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах…» (в связи с изданием приказов ФСТЭК России от 11 февраля 2013 г. № 17 и от 18 февраля 2013 г. № 21);
- 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»;
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Информационное сообщение ФСТЭК России от 30 июля 2012 г. № 240/24/3095 «Об утверждении требований к средствам антивирусной защиты».
- Информационное сообщение ФСТЭК России от 30 мая 2012 г. № 22/2222 «По вопросу необходимости получения лицензий ФСТЭК России на деятельность по технической защите конфиденциальной информации»;

6.3. Роскомнадзор России

- Приказ Россвязькомнадзора № 996 от 05 сентября 2013 г. «Об утверждении требований и методов по обезличиванию персональных данных»;
- Приказ Управления Роскомнадзора по Москве и Московской области от 02.02.2010 № 013-од «Типовой регламент №26 проведения проверки по контролю (надзору) за деятельностью, связанной с обработкой персональных данных с использованием средств автоматизации или без использования таких средств».
- Приказ Россвязькомнадзора № 18 от 30 января 2010 г. «Об утверждении административного регламента федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных»;
- Приказ Россвязькомнадзора № 104 от 25 августа 2009 г. «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»;
- Письмо Россвязькомнадзора от 13 мая 2009 г. № ДС-П11-2502 «Об осуществлении трансграничной передачи персональных данных».
- Приказ Россвязькомнадзора № 08 от 17 июля 2008 г. «Об утверждении образца формы уведомления об обработке персональных данных»;

7. Национальные стандарты в области информационной безопасности

- Перечень Государственных стандартов Российской Федерации в области защиты конфиденциальной информации и персональных данных.

8. Нормативно-методические и руководящие документы

- ФСТЭК России. Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.);
- Методические рекомендации по применению приказа Роскомнадзора от 05 сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию персональных данных».
- ФСТЭК России. «Решение в связи с изданием приказа ФСТЭК России от 5 февраля 2010 г.№58…» от 5 марта 2010 г.;
- ФС Б России. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21 февраля 2008 г. №149/54-144);
- ФСБ России. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21 февраля 2008 г. №149/6/6-622);

- ФСТЭК России. «Базовая Модель угроз безопасности персональных данных при обработке в информационных системах персональных данных» (выписка) (утв. Заместителем директора ФСТЭК России 15 февраля 2008 г.);
- ФСТЭК России. «Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных» (утв. Заместителем директора ФСТЭК России 14 февраля 2008 г.)
- ФСТЭК России. «Положение по аттестации объектов информатизации по требованиям безопасности информации»(утв. Председателем ГТК при Президенте РФ 25 ноября 1994 г.);
- ФСТЭК России. «Сборник руководящих документов по защите информации от несанкционированного доступа» 1992 г.;
- ФСТЭК России. Форма заявления о предоставлении лицензии юридическому лицу;

Руководящие документы ФСТЭК.

1) Средства ВТ. Защита от НСД. Термины и определения.
2) Средства вычислительной техники. Защита от несанкционированного доступа. Показатели защищенности.
3) Автоматизированные системы. Защита от несанкционированного доступа. Показатели защищенности.
4) Межсетевые экраны. Средства вычислительной техники. Показатели защищенности.
5) Средства вычислительной техники и автоматизированные системы. Программное обеспечение средств защиты информации.
6) Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.

В концепции содержится:

1) модель нарушителя.

Нарушитель — человек, имеющий доступ к системе, способный:

А) запускать программные средства из определенного набора (согласно его правам доступа);

Б) пользователь, который может запускать процессы в обход средств защиты;

В) способный модифицировать компоненты автоматизированной системы, управлять ее функционированием;

Г) занимающийся проектированием автоматизированных систем.

2) Основные способы несанкционированного доступа:

a. запуск программ пользователя;

b. запуск программ в обход защиты;
c. модификация средств защиты автоматизированной системы;
d. внедрение программных или технических механизмов, нарушающих структуру автоматизированной системы и систем вычислительной техники.

3) Основные принципы защиты от несанкционированного доступа:

1) работа в соответствии с принципами, законами, требованиями, стандартов и иных нормативных документов;

2) использование программно-технических средств;

3) использование программно-технических средств с использованием организационных мер;

4) планирование методов защиты информации на всех этапах работы с автоматизированной системой;

5) защита информации не должна влиять на надежность, быстродействие, возможности конфигурирования автоматизированной системы;

6) оценки контроля эффективности средств защиты.

4) Согласно концепции защита обеспечивается средствами разграничения доступа (СРД).

Защита автоматизированной системы — Защита устройств + защита информационных потоков.

Система вычислительной техники делятся на семь классов, автоматизированная система — на девять классов.

Модели разграничения доступа:

1) Мандатная (полномочная) — все объекты распределяются по уровням секретности. Каждый субъект может записывать или читать информацию с того уровня, над которым преобладает.

Полномочная модель характеризуется следующими правилами:

Каждый объект обладает грифом секретности.

У каждого субъекта доступа имеется свой уровень допуска.

2) Дискреционная (избирательная) — создается матрица доступа.

Любой объект имеет владельца.

Владелец имеет право произвольно ограничивать доступ субъектов к данному объекту.

Наличие хотя бы одного привилегированного пользователя (например админа), который имеет возможность обращаться к любому объекту с помощью любого метода доступа.

Матрица доступа: строки – субъекты, столбцы объекты. В каждой ячейки матрицы хранятся права доступа данного субъекта к данному объекту.

3) Ролевая (в стандартах не упоминается) — вводится понятие роли — абстрактная сущность, которой соответствуют определенные права доступа. Обычно роли прикрепляют к должностям. Один пользователь может играть несколько ролей.

4) Верифицированная — проверенный, доступ подтверждается сторонними организациями, работающих в сфере безопасности.

Классификация автоматизированных систем (из документа "Автоматизированные системы. Защита от несанкционированного доступа. Показатели защищенности.").

Различают девять классов, которые делят на три группы.

Первая группа включает два класса — 3А и 3Б. **Вторая группа** — 2А и 2Б. **Третья группа** — 1А, 1Б, 1В, 1Г, 1Д. Классы 3А и 3Б содержат автоматизированные системы, которые являются однопользовательскими.

Вторая группа — многопользовательские с равным доступом.

Третья группа — многопользовательские с разграничением доступа

Буква А в 3А и 2А означает, что автоматизированная система содержит конфиденциальную информацию. Д — данные для служебного пользования. Г — персональные данные. В — может содержать секретные сведения. Б — с грифом совершенно секретно. А — особой важности.

Перечень мероприятий, используемых при защите:

1) регистрация и учет пользователей

2) идентификация, проверка подлинности, контроль доступа

3) управление потоками информации

4) учет носителей информации

5) очистка памяти

6) сигнализация попыток нарушения защиты

7) шифрование конфиденциальной информации

8) шифрование данных пользователей

9) использование сертифицированных средств криптографической защиты

10) обеспечение целостности системы

11) физическая защита

12) наличие администратора службы защиты информации

13) наличие средств восстановления

14) периодические проверки

15) использование сертифицированных средств защиты информации.