**Практическая работа №17 Нормативные методические документы в области защиты информации.**

**Цель:** ознакомиться с нормативными методическими документами в области защиты информации, систематизировать сведения о нормативно-методических документах, приобрести опыт самостоятельного поиска и анализа.

**Ход работы**

1. Используя любой интернет-браузер, нашли нормативно-методические документы из представленного перечня.
2. Вставили недостающие реквизиты в перечень нормативных методических документов

֍ 1. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

֍ 2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам». Гостехкомиссия России. - М., 2002.

☼ 3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические **требования**. Госстандарт России. - М., 1995.

☼ 4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения . Госстандарт России. - М., 2006.

☼ 5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения - М., 2006.

☼ 6. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Bведение и общая модель.

☼ 7. ГОСТ Р ИСО/МЭК 15408-2-2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт России. - М., 2013.

☼ 8. ГОСТ Р ИСО/МЭК 15408-3-2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

☼ 9. ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

☼ 10. ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

☼ 11. ГОСТ Р ИСО/МЭК 27002-2012. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», введен в действие с 01.01.2014

☼ 12. ГОСТ Р ИСО/МЭК 27003-2012. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».

☼ 13. ГОСТ Р ИСО/МЭК 27004-2011. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».

☼ 14. ГОСТ Р ИСО/МЭК 27005-2010. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

☼ 15. ГОСТ Р ИСО/МЭК 27006-2008. «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

☼ 16. ГОСТ Р ИСО/МЭК 27011-2012. «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».

☼ 17. ГОСТ Р ИСО/МЭК 27031-2012. «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».

☼ 18. ГОСТ Р ИСО/МЭК 27033-1-2011. «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».

☼ 19. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

☼ 20. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

☼ 21. ГОСТ Р 34.10-2012. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

☼ 22. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования.

☼ 23. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования.

☺ 24. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

♫25. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

♫26. Приказ ФСБ России от 30 августа 2012 г. № 440 «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

♫27. Приказ ФСБ России от 08 августа 2009 г. № 149/7/2/6-1173 «Об утверждении типового регламента проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

♫28. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

♫29. «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». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.

♫30. Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

♫31. Приказ ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

♫32. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

҉ 33. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты».

҉ 34. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений».

ᴥ 35. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

ᴥ 36. Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи в случае прекращения деятельности аккредитованного удостоверяющего центра».

ᴥ 37. Приказ Минкомсвязи России от 23 ноября 2011 г. № 321 «Об утверждении Административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по организации ведения единого государственного реестра сертификатов ключей подписей удостоверяющих центров, обеспечению доступа к нему и к реестру сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, физических лиц и организаций».

ᴥ 38. Приказ Минкомсвязи России от 27 октября 2011 г. № 282 «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».

ᴥ 39. Приказ Минкомсвязи России от 05 октября 2011 г. № 436 «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

ᴥ 40. Приказ Минкомсвязи России от 23 ноября 2011 г. № 320 «Об аккредитации удостоверяющих центров».

ᴥ 41. Приказ Минкомсвязи России от 13 апреля 2012 г. № 108 «Об обеспечении осуществления Министерством связи и массовых коммуникаций РФ функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров».

֍ 42. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». - М., 1999.

֍ 43. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». - М, 1992.

֍ 44. Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». - М., 1992.

֍ 45. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М, 1992.

֍ 46. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». -М., 1992.

֍ 47. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». - M., 1992.

֍ 48. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1997.

҉ 49. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.

҉ 50. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.

҉ 51. Приказ ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

҉ 52. Приказ ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

҉ 53. Приказ ФСТЭК России от 14 марта 2014г. №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».

҉ 54. Приказ ФСТЭК России от 12 июля 2012 г. № 83 «Об утверждении административного регламента федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».

۩55. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2011 г. № 312 «Об утверждении административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных».

**Контрольные вопросы**

1. В составленном перечне отметьте правовые документы, регламентирующие технические условия?
   1. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
   2. ГОСТ Р 50739-95.
   3. Приказ ФСБ России от 30 августа 2012 г. № 440.
   4. Приказ ФСТЭК России от 12 июля 2012 г. № 83.
2. В составленном перечне отметьте правовые документы, регламентирующие организационные условия?
3. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152
4. Приказ ФСБ России от 10 июля 2014 г. № 378
5. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники».
6. Приказ ФСТЭК России от 18 февраля 2013г. № 21
7. Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством?

ГОСТ Р ИСО/МЭК 15408-1-2002.

ГОСТ Р ИСО/МЭК 15408-2-2013.

ГОСТ Р ИСО/МЭК 15408-3-2013.

ГОСТ Р ИСО/МЭК 27000-2012.

ГОСТ Р ИСО/МЭК 27001-2006.

ГОСТ Р ИСО/МЭК 27002-2012.

ГОСТ Р ИСО/МЭК 27003-2012.

ГОСТ Р ИСО/МЭК 27004-2011.

ГОСТ Р ИСО/МЭК 27005-2010.

ГОСТ Р ИСО/МЭК 27006-2008.

ГОСТ Р ИСО/МЭК 27011-2012.

1. Составьте классификацию исследованных документов по органу, принявшему тот или иной документ. Признак принадлежности к классу отметьте в перечне специальным значком.

҉ - ФСТЭК

☼ - Госстандарт

♫ - ФСБ

֍ - Гостехкомиссия

☺ - ФАПСИ

ᴥ - Минкомсвязь

۩ - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

1. Какова доля документов, регламентирующих организацию работ по защите персональных данных?

~11%

1. Какова доля документов, регламентирующих организацию работ по обороту средств технической защиты?

~7%