**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.

**Контрольные вопросы**

1 Регламентирующие технические условия:

1. «\_\_\_ 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 \_\_ каналам». Гостехкомиссия России. - М., 2002.
3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические \_\_\_ . Госстандарт России. - М., 1995.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие \_\_\_ . Госстандарт России. - М., 2006.
5. ГОСТ Р ИСО/МЭК 15408-1-\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Bведение и общая модель.
6. ГОСТ Р ИСО/МЭК 15408-2-\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт России. - М., 2013.
7. ГОСТ Р ИСО/МЭК 15408-3-\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
8. ГОСТ Р ИСО/МЭК 27033-1-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
9. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки \_\_\_ . Защита криптографическая. Алгоритм криптографического преобразования.
10. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. \_\_\_ защита информации. Процессы формирования и проверки электронной цифровой подписи.
11. ГОСТ Р 34.10-\_\_\_ . Государственный стандарт Российской Федерации. Информационная технология. \_\_\_ защита информации. Процессы формирования и проверки электронной цифровой подписи.
12. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция \_\_\_ .
13. ГОСТ Р 34.11-\_\_\_ . Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция \_\_\_ .
14. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих \_\_\_ 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.
15. Приказ ФСБ России от 27 декабря 2011 г. № \_\_\_ «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».
16. Приказ ФСБ России от 27 декабря 2011 г. № \_\_\_ «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».
17. Приказ ФСБ России от \_\_\_ июля \_\_\_ г. № \_\_\_ «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».
18. Приказ \_\_\_ России от 20 марта 2012 г. № \_\_\_ «Об утверждении требований к средствам антивирусной защиты».
19. Приказ \_\_\_ России от 6 декабря 2011 г. № \_\_\_ «Об утверждении требований к системам обнаружения вторжений».
20. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по \_\_\_ персональных данных».
21. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «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».
22. Приказ Минкомсвязи России от 05 октября 2011 г. № \_\_\_ «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».
23. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «Об аккредитации удостоверяющих центров».
24. Приказ Минкомсвязи России от 13 апреля 2012 г. № \_\_\_ «Об обеспечении осуществления Министерством связи и массовых коммуникаций РФ функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров».
25. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть \_\_\_ . Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия \_\_\_ возможностей». - М., 1999.
26. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. \_\_\_ и определения». - М, 1992.
27. Руководящий документ Гостехкомиссии России «\_\_\_ защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». - М., 1992.
28. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от \_\_\_ доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М, 1992.
29. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от \_\_\_ доступа к информации. Показатели защищенности от несанкционированного доступа к информации». -М., 1992.
30. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. \_\_\_ экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1997.
31. «Базовая модель угроз безопасности персональных данных при их обработке в \_\_\_ системах персональных данных». ФСТЭК России. - М., \_\_\_ .
32. «Методика определения \_\_\_ угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.
33. Приказ ФСТЭК России от 18 февраля \_\_\_ г. № \_\_\_ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
34. Приказ ФСТЭК России от 11 февраля \_\_\_ г. № \_\_\_ «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
35. Приказ ФСТЭК России от 14 марта \_\_\_ г. № \_\_\_ «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».

2 Регламентирующие организационные условия:

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и \_\_\_ - М., 2006.
2. ГОСТ Р ИСО/МЭК \_\_\_ -2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
3. ГОСТ Р ИСО/МЭК 27001-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
4. ГОСТ Р ИСО/МЭК 27002-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», введен в действие с 01.01.2014
5. ГОСТ Р ИСО/МЭК 27003-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».
6. ГОСТ Р ИСО/МЭК 27004-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
7. ГОСТ Р ИСО/МЭК 27005-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
8. ГОСТ Р ИСО/МЭК 27006-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
9. ГОСТ Р ИСО/МЭК 27011-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».
10. ГОСТ Р ИСО/МЭК 27031-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».
11. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № \_\_\_ «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».
12. Приказ ФСБ России от 9 февраля 2005 г. № \_\_\_ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
13. Приказ ФСБ России от 30 августа 2012 г. № \_\_\_ «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).
14. Приказ \_\_\_ 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».
15. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в \_\_\_ системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.
16. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих \_\_\_ 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.
17. Приказ ФСБ России от \_\_\_ июля \_\_\_ г. № \_\_\_ «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».
18. Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки \_\_\_ подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования \_\_\_ подписи в случае прекращения деятельности аккредитованного удостоверяющего центра».
19. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «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».
20. Приказ Минкомсвязи России от 27 октября 2011 г. № \_\_\_ «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».
21. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «Об аккредитации удостоверяющих центров».
22. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в \_\_\_ системах и средствах вычислительной техники». - M., 1992.
23. Приказ ФСТЭК России от 18 февраля \_\_\_ г. № \_\_\_ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
24. Приказ \_\_\_ 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».
25. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2011 г. № \_ «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».

3 Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством?

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

1. Минкомсвязь
   1. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по \_\_\_ персональных данных».
   2. Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки \_\_\_ подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования \_\_\_ подписи в случае прекращения деятельности аккредитованного удостоверяющего центра».
   3. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «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».
   4. Приказ Минкомсвязи России от 27 октября 2011 г. № \_\_\_ «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».
   5. Приказ Минкомсвязи России от 05 октября 2011 г. № \_\_\_ «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».
   6. Приказ Минкомсвязи России от 23 ноября 2011 г. № \_\_\_ «Об аккредитации удостоверяющих центров».
   7. Приказ Минкомсвязи России от 13 апреля 2012 г. № \_\_\_ «Об обеспечении осуществления Министерством связи и массовых коммуникаций РФ функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров».
2. Правительство РФ
   1. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические \_\_\_ . Госстандарт России. - М., 1995.
   2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие \_\_\_ . Госстандарт России. - М., 2006.
   3. ГОСТ Р 50922-2006. Защита информации. Основные термины и \_\_\_ - М., 2006.
   4. ГОСТ Р ИСО/МЭК 15408-1-\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Bведение и общая модель.
   5. ГОСТ Р ИСО/МЭК 15408-2-\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт России. - М., 2013.
   6. ГОСТ Р ИСО/МЭК 15408-3-\_\_\_ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
   7. ГОСТ Р ИСО/МЭК \_\_\_ -2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
   8. ГОСТ Р ИСО/МЭК 27001-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
   9. ГОСТ Р ИСО/МЭК 27002-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», введен в действие с 01.01.2014
   10. ГОСТ Р ИСО/МЭК 27003-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».
   11. ГОСТ Р ИСО/МЭК 27004-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
   12. ГОСТ Р ИСО/МЭК 27005-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
   13. ГОСТ Р ИСО/МЭК 27006-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
   14. ГОСТ Р ИСО/МЭК 27011-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».
   15. ГОСТ Р ИСО/МЭК 27031-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».
   16. ГОСТ Р ИСО/МЭК 27033-1-\_\_\_ «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
   17. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки \_\_\_ . Защита криптографическая. Алгоритм криптографического преобразования.
   18. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. \_\_\_ защита информации. Процессы формирования и проверки электронной цифровой подписи.
   19. ГОСТ Р 34.10-\_\_\_ . Государственный стандарт Российской Федерации. Информационная технология. \_\_\_ защита информации. Процессы формирования и проверки электронной цифровой подписи.
   20. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция \_\_\_ .
   21. ГОСТ Р 34.11-\_\_\_ . Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция \_\_\_ .
   22. Приказ \_\_\_ 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».
   23. Приказ \_\_\_ России от 20 марта 2012 г. № \_\_\_ «Об утверждении требований к средствам антивирусной защиты».
   24. Приказ \_\_\_ России от 6 декабря 2011 г. № \_\_\_ «Об утверждении требований к системам обнаружения вторжений».
   25. Приказ \_\_\_ 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».
   26. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2011 г. № \_ «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».
3. ФСБ
   1. Приказ ФСБ России от 9 февраля 2005 г. № \_\_\_ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
   2. Приказ ФСБ России от 30 августа 2012 г. № \_\_\_ «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).
   3. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в \_\_\_ системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.
   4. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих \_\_\_ 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.
   5. Приказ ФСБ России от 27 декабря 2011 г. № \_\_\_ «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».
   6. Приказ ФСБ России от 27 декабря 2011 г. № \_\_\_ «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».
   7. Приказ ФСБ России от \_\_\_ июля \_\_\_ г. № \_\_\_ «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».
4. Гостехкомиссия
   1. «\_\_\_ 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 \_\_ каналам». Гостехкомиссия России. - М., 2002.
   3. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть \_\_\_ . Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия \_\_\_ возможностей». - М., 1999.
   4. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. \_\_\_ и определения». - М, 1992.
   5. Руководящий документ Гостехкомиссии России «\_\_\_ защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». - М., 1992.
   6. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от \_\_\_ доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М, 1992.
   7. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от \_\_\_ доступа к информации. Показатели защищенности от несанкционированного доступа к информации». -М., 1992.
   8. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в \_\_\_ системах и средствах вычислительной техники». - M., 1992.
   9. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. \_\_\_ экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1997.
5. ФАПСИ
   1. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № \_\_\_ «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».
6. ФСТЭК
   1. «Базовая модель угроз безопасности персональных данных при их обработке в \_\_\_ системах персональных данных». ФСТЭК России. - М., \_\_\_ .
   2. «Методика определения \_\_\_ угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.
   3. Приказ ФСТЭК России от 18 февраля \_\_\_ г. № \_\_\_ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
   4. Приказ ФСТЭК России от 11 февраля \_\_\_ г. № \_\_\_ «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
   5. Приказ ФСТЭК России от 14 марта \_\_\_ г. № \_\_\_ «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».

Признак принадлежности к классу смотрите в первом и втором вопросах.

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

1. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в \_\_\_ системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.
2. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих \_\_\_ 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.
3. Приказ ФСБ России от \_\_\_ июля \_\_\_ г. № \_\_\_ «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».
4. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № \_\_\_ «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».
5. Приказ ФСТЭК России от 18 февраля \_\_\_ г. № \_\_\_ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
6. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2011 г. № \_ «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».
7. Какова доля документов, регламентирующих организацию работ по обороту средств технической защиты?

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

1. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № \_\_\_ «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».
2. Приказ ФСБ России от 9 февраля 2005 г. № \_\_\_ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
3. Приказ ФСБ России от 30 августа 2012 г. № \_\_\_ «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).

**Вывод:** Мы ознакомились с нормативными методическими документами в области защиты информации, систематизировали сведения о нормативно-методических документах, приобрели опыт самостоятельного поиска и анализа.