

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОГО ЗАДАНИЯ №1**

**В РАМКАХ ДИСЦИПЛИНЫ «ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

**Цель:** ознакомиться с классификацией и регламентами автоматизированных систем (АС) различного назначения, получить знания применимости регламентов для конкретных АС.

**Методы и приемы:** изучение теоретических источников, формулирование определений, частично-поисковая работа, анализ.

**Ключевые слова:** автоматизированные системы (АС), регламенты АС, объекты информатизации, информационная безопасность, персональные данные, информационная система, государственные информационные системы информация, информационно-коммуникационные технологии, защита информации, ФСТЭК РФ, ФСБ.

Автоматизированная система, обрабатывающая служебную тайну - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами)

|  |  |
| --- | --- |
| 1. 149-ФЗ от 27 июля 2006 г. | + |
| 2. Указ Президента РФ от 17 марта 2008 г. № 351 | + |
| 3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г. | - |
| 4. Пост. Правительства РФ № 512 от 6 июля 2008 г. | - |
| 5. Пост. Правительства РФ № 687 от 15 сентября 2008 г. | - |
| 6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г. | + |
| 7. СТР-К | + |
| 8. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты» | + |
| 9. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений» | + |
| 10. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года  «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | - |
| 11. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» | - |
| 12. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 | - |
| 13. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Термины и определения», 1992 | + |
| 14. РД Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», 1992 | + |
| 15. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992 | + |
| 16. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992 | + |
| 17. РД Гостехкомиссии «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992 | - |
| 18. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997 | + |
| 19. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006 | - |
| 20. Методика оценки угроз безопасности информации. ФСТЭК России,  2021 | - |
| 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» | - |
| 22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» | + |

Автоматизированная система обрабатывающая коммерческую тайну - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких

сведений введен режим коммерческой тайны)

|  |  |
| --- | --- |
| 1. 149-ФЗ от 27 июля 2006 г. | + |
| 2. Указ Президента РФ от 17 марта 2008 г. № 351 | - |
| 3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г. | - |
| 4. Пост. Правительства РФ № 512 от 6 июля 2008 г. | - |
| 5. Пост. Правительства РФ № 687 от 15 сентября 2008 г. | - |
| 6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г. | - |
| 7. СТР-К | + |
| 8. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты» | - |
| 9. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений» | - |
| 10. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года  «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | - |
| 11. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» | - |
| 12. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 | - |
| 13. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Термины и определения», 1992 | - |
| 14. РД Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», 1992 | + |
| 15. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация  автоматизированных систем и требования по защите информации», 1992 | + |
| 16. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992 | - |
| 17. РД Гостехкомиссии «Временное положение по организации  разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в  автоматизированных системах и средствах вычислительной техники», 1992 | - |
| 18. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997 | - |

Автоматизированная система управления технологическими процессами (АСУТП) - автоматизированные системы управления, обеспечивающие контроль и управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (в том числе системы диспетчерского управления, системы сбора (передачи) данных, системы, построенные на основе программируемых логических контроллеров, распределенные системы управления, системы управления станками с числовым программным управлением).

|  |  |
| --- | --- |
| 1. 152-ФЗ от 27 июля 2006 г. | - |
| 2. 98-ФЗ от 29 июля 2004 г. | - |
| 3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г. | - |
| 4. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты» | + |
| 5. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений» | + |
| 6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года  «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | - |
| 7. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 | - |
| 8. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992 | + |
| 9. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997 | + |
| 10. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006 | + |
| 11. 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» | - |
| 12. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» | - |
| 13. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессамина критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» | + |

Ключевая информационная система - информационно-управляющая или информационно-коммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

|  |  |
| --- | --- |
| 1. 152-ФЗ от 27 июля 2006 г. | - |
| 2. Пост. Правительства РФ № 1119 от 1 ноября 2012 г. | - |
| 3. Пост. Правительства РФ № 1233 от 3 ноября 1994 г. | + |
| 4. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты» | - |
| 5. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений» | + |
| 6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года  «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | - |
| 7. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 | - |
| 8. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992 | - |
| 9. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992 | - |
| 10.Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры | - |
| 11. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры | + |
| 12. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры | + |
| 13.Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. | + |
| 14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008. | - |
| 15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006 | - |
| 16. Методика оценки угроз безопасности информации. ФСТЭК России, 2021 | - |
| 17. 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» | - |
| 18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» | - |
| 19. 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» | + |

**Информационная система персональных данных** **- совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.**

|  |  |
| --- | --- |
| 1. 152-ФЗ от 27 июля 2006 г. | + |
| 2. 149-ФЗ от 27 июля 2006 г. | + |
| 3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г. | + |
| 4. Пост. Правительства РФ № 512 от 6 июля 2008 г. | - |
| 5. Пост. Правительства РФ № 687от 15 сентября 2008 г. | + |
| 6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г. | - |
| 7. Пост. Правительства РФ № 211 от 21 марта 2012 г. | + |
| 8. Пост. Правительства РФ № 953 от 24 ноября 2009 г. | - |
| 9. СТР-К | + |
| 10. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты» | + |
| 11. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений» | + |
| 12. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года  «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | - |
| 13. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» | + |
| 14. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры | - |
| 15. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры | - |
| 16. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры | - |
| 17. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры | - |
| 18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 | - |
| 19. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006 | - |
| 20. Методика оценки угроз безопасности информации. ФСТЭК России, 2021 | + |
| 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» | + |
| 22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» | - |
| 23. 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» | - |

**Государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно Федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.**

|  |  |
| --- | --- |
| 1. 149-ФЗ от 27 июля 2006 г. | + |
| 2. 98-ФЗ от 29 июля 2004 г. | - |
| 3. Указ Президента РФ от 17 марта 2008 г. № 351 | + |
| 4. Пост. Правительства РФ № 1119 от 1 ноября 2012 г. | - |
| 5. Пост. Правительства РФ № 1233 от 3 ноября 1994 г. | + |
| 6. СТР-К | + |
| 7. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты» | + |
| 8. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений» | + |
| 9. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года  «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | - |
| 10. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры | - |
| 11. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры | - |
| 12. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры | - |
| 13. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры | - |
| 14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 | - |
| 15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006 | - |
| 16. Методика оценки угроз безопасности информации. ФСТЭК России,2021 | + |
| 17. 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» | - |
| 18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». | + |
| 19. 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» | - |

Информационная система общего пользования - федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно- телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации.

|  |  |
| --- | --- |
| 1. 98-ФЗ от 29 июля 2004 г. | - |
| 2. Пост. Правительства РФ № 1119 от 1 ноября 2012 г. | - |
| 3. Пост. Правительства РФ № 1233 от 3 ноября 1994 г. | - |
| 4. Пост. Правительства РФ № 211 от 21 марта 2012 г. | - |
| 5. Пост. Правительства РФ № 953 от 24 ноября 2009 г. | + |
| 6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | + |
| 7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 | - |
| 8. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006 | - |
| 9. Методика оценки угроз безопасности информации. ФСТЭК России, 2021 | - |
| 10. 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» | - |
| 11. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» | - |
| 12. 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» | - |

Контрольные вопросы

1. Пример служебной тайны.
2. Налоговая тайна

СТР-К - Специальные требования и рекомендации по технической защите конфиденциальной информации

1. Пример коммерческой тайны.
2. Маркетинговая стратегия
3. Данные о клиентах
4. Технологические наработки

ФЗ – Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

1. АСУТП - Автоматизированная система управления технологическим процессом

Состоит из:

Датчики мониторинга, объекты управления, объекты сбора данных, датчики контроля качества

1. Объекты КИИ:
2. Информационные системы
3. Информационно-телекоммуникационные сети
4. Автоматизированные системы управления субъектов критической информационной инфраструктуры

ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации” от 26.07.2017 №187-ФЗ

1. ИСПДн - Информационная система персональных данных

Пример:

1. Системы клиентского учета
2. Системы кадрового учета
3. Банковские системы

ФЗ “О персональных данных” от 27.07.2006 №152-ФЗ

Постановление Правительства РФ от 1 ноября 2012 №1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”

Приказ ФСТЭК России от 18.02.2013 №21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

1. ГИС - Государственная информационная система

Пример ГИС:

1. ГосСОПКА
2. ГИС о государственных и муниципальных платежах
3. Федеральный регистр муниципальных нормативных правовых актов

Приказ ФСТЭК России от 11 февраля 2013 “Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах”

1. ИСОП - Информационная система общего пользования

Пример ИСОП:

1. Госуслуги
2. ЕМИАС
3. Мос.ру