Государственное бюджетное образовательное учреждение высшего профессионального образования
Московской области

«ФИНАНСОВО - ТЕХНОЛОГИЧЕСКАЯ АКАДЕМИЯ»

«УТВЕРЖДАЮ»
Проректор по учебной и
учебно-методической работе
_____ И.В. Христофорова
«___»_____2013 г.

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Программа

Итогового экзамена

Направление подготовки: 090900 68 Информационная безопасность

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Королев 2013

Воронов А.Н. Программа итогового экзамена.– Королев МО: ФТА, 2013 – 20 с.

Рецензент: Соляной Владимир Николаевич

Программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего профессионального образования (ФГОС) по направлению подготовки магистров 090900 Информационная безопасность, утвержденного Ученым советом ФТА, протокол №1 от 03 сентября 2012 года.

РЕКОМЕНДОВАНО
Учебно-методическим советом
Протокол № 1
от « 24» сентября 2013 г.

Программа рассмотрена и одобрена
на заседании кафедры
Информационной безопасности

Протокол № 8
от «15» апреля 2013 г.
Заведующий кафедрой
Соляной В.Н.

Программа утверждена на заседании Совета факультета

Протокол № 9
от «11» июня 2013 г.

Декан факультета
Привалов В.И.

1. Общие положения

Итоговый экзамен является компонентом итоговой аттестации выпускника - магистра, наряду с выпускной квалификационной работой (ВКР) – магистерской диссертацией.

Целью итогового экзамена является выявление и объективная оценка уровня специальной подготовки выпускника относительно общих требований, определяемых ФГОС уровнем сформированности общекультурных и профессиональных компетенций по направлению подготовки магистра информационной безопасности региона.

К итоговому экзамену допускаются магистранты, завершившие полный курс обучения по основной профессиональной образовательной программе и успешно прошедшие все предшествующие аттестационные испытания, предусмотренные учебным планом.

Итоговый экзамен проводит экзаменационная комиссия, создаваемая приказом ректора на основании положения об итоговой аттестации выпускников высших учебных заведений. Председатель комиссии утверждается в установленном порядке.

Прием итогового экзамена осуществляется комиссией (ИЭК), наделенной необходимыми полномочиями, по экзаменационному билету. Экспертной оценке в процессе государственного экзамена подвергаются устные ответы экзаменующегося на вопросы экзаменационного билета и на вопросы членов ИЭК и письменное решение экзаменационной задачи, представленное экзаменующимся в ИЭК, и его устные ответы на вопросы членов ИЭК.

Оценка результатов сдачи государственного экзамена осуществляется по шкале оценок: "отлично", "хорошо", "удовлетворительно", "неудовлетворительно".

Решение об оценке ИЭК принимает коллегиально и утверждает путем голосования ее членов, простым большинством голосов. Решение экзаменационной комиссии оформляется соответствующим протоколом.

Программа итогового экзамена доводится до сведения выпускников не позднее, чем за 6 месяцев до проведения экзамена.

Перечень общепрофессиональных и специальных дисциплин, включенных в программу, определяется с учетом профессиональной квалификации «магистр», присваиваемой выпускникам направления подготовки информационная безопасность

2. Требования к результатам освоения ООП ВПО

Программа итогового экзамена носит комплексный, системный, междисциплинарный характер и ориентирована на выявление у выпускника общепрофессиональных и специальных знаний и умений.

Выпускник должен:

ЗНАТЬ:

- предполагаемые источники угроз информационной безопасности региона и порядок их выявления;
- возможные каналы утечки информации и предполагаемые информационные атаки на охраняемых объектах региона;
- методы и средства защиты информационных объектов, основные мероприятия по управлению информационной безопасностью в регионе;
- основные принципы организации технического, программного и информационного обеспечения защищенных информационных технологий региона;
- методы концептуального проектирования технологий обеспечения информационной безопасности региона;
- средства проектирования и модели жизненного цикла систем информационной безопасности региона;
- методы оценки эффективности проектируемых систем информационной безопасности региона;
- основы моделирования систем информационной безопасности региона, особенности проектирования адаптивных систем безопасности;
- основные направления совершенствования безопасности объектов региона с помощью средств защиты;
- основные тенденции развития теории и методологии проектирования систем информационной безопасности региона.

Уметь:

- осуществлять классификацию охраняемых объектов, средств защиты и требований к системе информационной безопасности региона;
- проводить анализ защищённости объектов региона и определять классы защиты информации;
- использовать гипотетические модели защиты информации при выборе соответствующих способов и средств информационной безопасности региона;
- осуществлять выбор функциональной структуры системы обеспечения информационной безопасности региона;
- обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности региона;
- правильно формулировать требования к проектированию систем информационной безопасности региона;
- определять основные задачи и функции проектирования систем информационной безопасности региона;

- определять структуру системы проектирования и основные периоды жизненного цикла систем информационной безопасности региона;
- выполнять основные этапы проектирования систем информационной безопасности региона;
- организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности региона;

Владеть навыками:

- выявления и анализа потенциально существующих угроз безопасности информации и охраняемым объектам региона;
- применения основных методов анализа и оценки рисков, методов определения размеров возможного ущерба защищаемым объектам региона;
- грамотного применения на практике основных методов и средств защищённых информационных технологий в регионе;
- применения методик организации и управления системой информационной безопасности в регионе.
- постановки задач по проектированию систем информационной безопасности региона;
- построения технологического процесса применения систем информационной безопасности при проектировании;
- применения основных методов анализа и оценки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности региона;

В результате освоения ООП ВПО выпускник овладел следующим компетенциями:

ОК:

- (ОК-1) способен совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности;
- (ОК-2) способен к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;
- (ОК-6) способен самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой его деятельности;

ПК:

- (ПК-1) способен понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем

информационной безопасности, оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией развития организации;

- (ПК-2) способен проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты;
- (ПК-4) способен самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты;
- (ПК-6) способен анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;
- (ПК-8) способен осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методик и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;
- (ПК-9) способен проводить экспериментальные исследования защищённости объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента;
- (ПК-10) способен оформлять научно-технические отчеты, обзоры, готовить публикации по результатам выполненных исследований, научные доклады;
- (ПК-11) способен выполнять педагогическую работу в средних специальных и высших учебных заведениях в должностях преподавателя и ассистента под руководством ведущего преподавателя и профессора (доцента) по дисциплинам направления;
- (ПК-14) владеет способностью организовать работу по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России и др.
- (ПК-15) владеет способностью разрабатывать проекты методических и нормативных документов, технической документации, а также предложения и мероприятия по реализации разработанных проектов и программ.

3. Перечень дисциплин

Программа Итогового экзамена состоит из блоков, включающих в себя следующие дисциплины:

1. Методы, организация и проведение научных исследований;
2. Теоретические основы управления;

3. Экономико-управленческие аспекты обеспечения информационной безопасности;
4. Инструментальные методы выявления технических каналов утечки информации;
5. Основы теории информационной безопасности;
6. Управление информационной безопасностью;
7. Организационно-правовые механизмы обеспечения информационной безопасности;
8. Теоретические основы компьютерной безопасности;
9. Концептуальное проектирование технологий обеспечения информационной безопасности;
10. Информационная безопасность финансово-кредитных структур;

4. Перечень оценочных заданий

Программа Итогового экзамена включает:

Теоретические вопросы:

1. Сущность и особенности научных исследований по информационной безопасности.
2. Общенаучные методы исследования (анализ и синтез) в области информационной безопасности.
3. Методы творческого мышления (эвристические и алгоритмические) в области информационной безопасности.
4. Моделирование при исследовании задач (проблем) в области информационной безопасности.
5. Научное прогнозирование возможных ситуаций по информационной безопасности.
6. Научно-технический потенциал в области информационной безопасности.
7. Этапы исследовательской деятельности в области информационной безопасности.
8. Характеристика теоретических исследований по информационной безопасности.
9. Характеристика экспериментальных исследований по информационной безопасности.
10. Внедрение научных исследований и их эффективность.
11. Цели и функции управления: понятие цель управления и понятие функция управления. Понятия управленческое решение и управленческое воздействие.
12. Внутренняя и внешняя среда в технологии управления, основные свойства

организационного управления, критерии эффективности управления системами и объектами.

13. Экономические, организационно-распорядительные и социально-психологические методы управления.
14. Основы управление информационными потоками и техническими объектами.
15. Методология анализа и синтеза организационных и технических систем управления.
16. Методология и организация процесса разработки управленческих решений. Этапы выработки управленческих решений.
17. Система управления проектами и проектное финансирование.
18. Критерии и методы оценки эффективности проектов.
19. Государственное регулирование информационной сферой. Общие положения: система органов государственной власти, регулирующих информационную сферу; правовые режимы информационных ресурсов; правовое регулирование информационных технологий, информационных систем и информационных ресурсов; информационный рынок.
20. Функции, задачи, структура и организация работы региональных центров информационной безопасности.
21. Общая характеристика новых базовых положений по организационно-экономическому обеспечению информационной безопасности.
22. Система комплексного управления рисками предприятия как ключевой корпоративный механизм и форма обеспечения экономико-информационной безопасности на микроуровне.
23. Концепция качества страхового механизма как основа решения проблемы по корпоративным информационных рискам.
24. Концепция контроллинга как ключевой корпоративный механизма в системе обеспечения информационно-экономической безопасностью.
25. Сущность существующих подходов по выбору модели организационного управления в условиях жесткого информационного противостояния.
26. Технологии обеспечения информационной безопасности систем организационного управления экономическими объектами на основе информационных систем поддержки принятия управленческих решений.
27. Сущность обеспечения информационной безопасности принятии организационно-управленческих решений в современных конкурентных условиях.
28. Механизм принятия решений по управлению информационными рисками основанный на формировании и использовании региональных ситуационных центров информационной безопасности.

29. Проектирование защищенной корпоративной информационной системы на основе развертывания региональных ситуационных центров информационной безопасности.
30. Схема взаимодействия компонентов региональной системы управления информационной безопасностью на основе ситуационного центра.
31. Каналы утечки информации, обрабатываемой техническими средствами.
32. Метод выявления технических каналов утечки информации с использованием индикаторов электромагнитных излучений.
33. Метод выявления технических каналов утечки информации с использованием радиочастотомера.
34. Метод выявления технических каналов утечки информации с использованием сканирующего радиоприемника.
35. Метод выявления технических каналов утечки информации с использованием анализатора спектра.
36. Метод выявления технических каналов утечки информации с использованием нелинейного локатора.
37. Метод выявления технических каналов утечки информации с использованием металлодетектора.
38. Методика проведения измерений акустического сигнала за пределами ограждающих конструкций.
39. Методика проведения измерений вибрационного сигнала на системах отопления и оконных стеклах.
40. Требования к измерительной аппаратуре при проведении измерений вибрационного сигнала.
41. Проблема информационной войны в современных условиях.
42. Базовое содержание основ теории информационной безопасности.
43. Основные теоретико-прикладные показатели уязвимости защищаемого информационного ресурса.
44. Теоретико-прикладные модели оценки ущерба от реализации информационных угроз.
45. Современные методологические основы проектирования комплексных систем обеспечения информационной безопасности.
46. Методологические основы выработки и оптимизации управленческих решений по информационной безопасности (характеристика основных этапов принятия и реализации решений).
47. Функции, задачи, структура и организация работы региональных центров информационной безопасности.
48. Теоретико-прикладные основы экономического анализа целесообразности

мероприятий по информационной безопасности.

49. Теоретико-прикладные основы обеспечения информационной безопасности «облачных» информационных технологий.
50. Анализ состояния и прогноз развития теории информационной безопасности.
51. Серия международных стандартов по методам обеспечения (управления) информационной безопасности.
52. Серия международных стандартов на отдельные процессы управления информационной безопасностью.
53. Отраслевые стандарты в области управления информационной безопасностью – стандарты банковской системы РФ.
54. Политика информационной безопасности (понятие, содержание, разработка и внедрение).
55. Управление управления информационной безопасностью (понятие, содержание и особенности).
56. Особенности управления информационной безопасностью информационно- телекоммуникационными технологиями организаций.
57. Система управления информационной безопасностью организаций (область действия, документационное обеспечение, политика, поддержка).
58. Характеристика основных процессов по управлению информационной безопасностью организаций (планирование, реализация, проверка и совершенствование).
59. Организация управленческих процессов по информационной безопасности: постановка задачи, выявление, документирование, мониторинг и измерение контрольных параметров.
60. Построение и внедрение систем управления информационной безопасностью организаций (в целом всей системы управления и отдельных управленческих процессов).
61. Основные цели и задачи правовой защиты информации.
62. Методы правовой защиты информации.
63. Доктрина информационной безопасности РФ (назначение и содержание).
64. Основные положения Федерального закона «О персональных данных».
65. Основные понятия, связанные с банковской тайной и правовая основа ее защиты.
66. Понятие объектов интеллектуальной собственности и правовая основа ее защиты
67. Федеральный закон «Об информации, информационных технологиях и защите информации».

68. Законы РФ «О государственной тайне» и «О коммерческой тайне».
69. Федеральный закон «О лицензировании отдельных видов деятельности».
70. Принципы и документы проведения сертификационных испытаний систем и средств защиты информации и аттестации объектов информатизации по вопросам информационной безопасности.
71. Современная постановка целей и задач по обеспечению компьютерной безопасности (переход к тотальной защите и интенсивным мерам).
72. Основные виды атак на компьютерные системы (КС), их классификация. Проблемы обеспечения информационной безопасности в проводных КС.
73. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.
74. Организация системы безопасности по уровням в компьютерных системах. Уровни и способы защиты, в соответствии с механизмами реагирования на угрозы.
75. Методы и средства обеспечения защиты информации в компьютерных системах (КС).
76. Цифровая подпись. Проблема аутентификации данных или цифровой подписи. Модель аутентификации сообщений.
77. Методы и этапы построения защищённых информационных (автоматизированных) систем. Метод проектирования «снизу вверх». Иерархический метод построения защищенной АС («сверху вниз»).
78. Классификация стандартов в области ИБ компьютерных систем. Оценочные стандарты в области ИБ.
79. Перечень основных документов ФСТЭК РФ по вопросам защиты информации в КС.
80. Основные положения «Общих критериев оценки безопасности информационных технологий».
81. Типология и жизненный цикл проектирования систем и технологий информационной безопасности.
82. Основные требования к проектированию систем и технологий информационной безопасности, цель их проектирования.
83. Универсальные и специальные задачи и функции проектирования систем и технологий информационной безопасности.
84. Структура проектирования систем и технологий информационной безопасности и их функциональных и обеспечивающих частей.
85. Организационно-правовое обеспечение проектирования систем и технологий информационной безопасности, характеристика проектно-технической документации.

86. Состав и основные элементы принципиальной схемы функционирования проектируемой системы и технологий информационной безопасности.
87. Краткая характеристика методологии проектирования систем и технологий информационной безопасности и требования к ней, выбор методов и средств проектирования.
88. Последовательность анализа и оценки эффективности проектирования систем и технологий информационной безопасности.
89. Применение современных интеллектуальных средств проектирования систем и технологий информационной безопасности.
90. Понятие адаптивных систем и технологий информационной безопасности, методы их построения.
91. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.
92. Роль и место службы информационной безопасности в банке.
93. Информационная безопасность подсистем ведения индивидуальных счетов клиентов и работы с банковскими картами.
94. Информационная безопасность подсистем кредитования и валютно – обменных операций.
95. Информационная безопасность подсистема операций с ценными бумагами.
96. Информационная безопасность подсистем инкассации и межбанковского взаимодействия.
97. Информационная безопасность подсистем управления ресурсами (дилинга) и удаленного банковского обслуживания.
98. Информационная безопасность подсистем обеспечения внутренней деятельности и электронного документооборота банка.
99. Информационная безопасность и архитектура системы «Клиент – банк».
100. Информационная безопасность расчетов банковскими картами в Интернете

Практические задания:

1. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 1 (глава 1):

- по правовому обеспечению;
- по организационному обеспечению;

- по техническому обеспечению.

2. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 1 (глава 2):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

3. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 1 (глава 3):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

4. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 2 (глава 1):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

5. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР- 2 (глава 2):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

6. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 2 (глава 3):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

7. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 3 (глава 1):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

8. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 3 (глава 2):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

9. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 3 (глава 3):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

10. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 1 (в целом за всю работу):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

11. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 2 (в целом за всю работу):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

12. Практическое задание:

Сформулировать, обосновать и доложить конкретные практические меры /целесообразный вариант/ по следующим направлениям обеспечения информационной безопасности разработанных предложений (или реализованных процессов) в НИР - 3 (в целом за всю работу):

- по правовому обеспечению;
- по организационному обеспечению;
- по техническому обеспечению.

5. Принцип формирования экзаменационных билетов

Экзаменационный билет содержит 3 теоретических вопроса, 1 практическое задание.

6. Описание формы проведения экзамена

По направлению подготовки магистров информационной безопасности предусмотрена комплексная форма экзамена.
На подготовку к ответу предусмотрено 40 минут. При подготовке возможно использование следующих печатных материалов:

1. Программа итогового экзамена;
2. Методические рекомендации по проведению итогового экзамена.
3. Перечень вопросов, выносимых на итоговый междисциплинарный экзамен.
4. При подготовке ответов на практическое задание каждый магистрант использует свои отчёты по НИР – 1,2,3.

А также вычислительных средств ПК («Power Point", "MS Office", специализированные программные комплексы), интерактивная доска. Недопустимо использование ресурсов Интернет сети и других ЛВС.

7. Критерии формирования экзаменационной оценки

При проведении итогового экзамена по направлению подготовки Информационная безопасность. Приняты следующие критерии оценок:
отлично – получены ответы на все вопросы билета, дополнительные вопросы членов ИЭК, проявлено академическое мышление, умение использовать вычислительную технику и специальную терминологию, владение современными информационными технологиями, умение аргументировано отвечать и защищать свою позицию, вести дискуссию по обсуждаемым проблемам;
хорошо – отсутствует полный ответ на один из вопросов билета, либо ответ на один дополнительный вопрос;
удовлетворительно – отсутствует ответ на один из вопросов билета, отсутствует полный ответ на два дополнительных вопроса, практическое задание выполнено с ошибками;
неудовлетворительно – отсутствует ответ на два вопроса билета, не выполнено практическое задание.

8. Список рекомендуемой литературы

8.1 Основная литература:

1. Абдикеев Н. М. Информационный менеджмент: Учебник. - М.: ИНФРА – М, 2010.
2. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2012.
3. Белый В.М., Зиновьев В.Н., Маренникова И.В. Теория информационного менеджмента. Монография /под ред. Д.П.Н.,академика РАЕН Т.Е.Старцевой Ярославль-Королёв; Издательство «Канцлер», 2010.
4. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
5. Ворона В. А., Тихонов В. А. Концептуальные основы создания и применения системы защиты объектов. — М.: Горячая линия-Телеком, 2012.
6. Журин С. И. Практика и теория использования детекторов лжи - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2011.
7. Заботина Н.Н. Проектирование информационных систем. Учебное пособие. – М.: «ИНФРА-М», 2011.
8. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., и др. Технические средства и методы защиты информации. Учебное пособие. 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012.
9. Киселёв Г. М., Бочкова Р. В., Сафонов В. И. Информационные технологии в экономике и управлении. Учебное пособие. М.: Издательско-торговая корпорация «Дашков и К°», 2012.
10. Коваленко Ю.Ю. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. - М.: Горячая линия – Телеком, 2012.
11. Кожухар В.М. Основы научных исследований. Учебное пособие. – М.: «Дашков и К»,2012.
12. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.. Основы управления информационной безопасностью. Учебное пособие для вузов. – 2-е издание исправленное. Серия «Вопросы управления информационной безопасностью. Выпуск 1» кн. 1. - М.: Горячая линия – Телеком, 2013.
13. Литвинская О.С. Основы теории передачи информации: Учебное пособие - М.: КНОРУС, 2010.
14. Логунов Ф.Б. Региональная и национальная безопасность. Учебное пособие. – М.:ИНФРА-М, 2011.
15. Малюк А.А. Теория защиты информации. – М.: Горячая линия – Телеком, 2013.
16. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно - психологической войны. – 3-е издание, стереотип. - М.: Горячая линия – Телеком, 2013.

17. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. Вопросы управления информационной безопасностью. – М.: Горячая линия – Телеком, 2012.
18. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов. - М.: Горячая линия – Телеком, 2012.
19. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2012.
20. Румянцев З.П. Общее управление организацией. Теория и практика: Учебник.- М.: ИНФРА, 2011.
21. Титоренко Г.А. Информационные системы и технологии управления: учебник для студентов вузов. – 3-е издание, перер. и доп.- М.: ЮНИТИ – ДАНА, 2010.
22. Чепига А.Ф. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010.
23. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. – М.: «ФОРУМ»: ИНФРА-М, 2008.
24. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. М.: ИД «Форум»: ИНФРА-М., 2010.
25. Шепитько Г.Е. Экономика защиты информации: Учебное пособие. – М.: МФЮУ, 2011.
26. Шкляр М.Ф. Основы научных исследований. Учебное пособие. – М.: «Дашков и К»,2012.

8.2 Дополнительная литература:

1. Астахов А.М. Искусство управления информационными рисками.- М.:ДМК Пресс, 2010.
2. Баранчиков А.И., Баранчиков П.А., Пылькин А.Н.. Алгоритмы и модели ограничения доступа к записям баз данных. М. Горячая линия – Телеком, 2011.
3. Гамза В.А., Ткачук И.Б. Безопасность банковской деятельности: Учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010.
4. Исаев Г.Н. Проектирование информационных систем. Учебное пособие. – М.: Издательство «Омега-Л», 2013.
5. Ивасенко А. Г., Гридасов А. Ю., Павленко В. А. Информационные технологии в экономике и управлении. Учебное пособие. М.: КноРус, 2010.
6. Ковалева Н.Н. Информационные право России . Изд.-торг. корп. «Дашков и К°». М.: 2010.

7. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).
8. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационо - правовое и методическое обеспечение информационной безопасности. Учебное пособие. Санкт-Перепбургский национальный исследовательский университет информационных технологий, механики, оптики. 2013.
9. Коваленко В.В. Проектирование информационных систем. Учебное пособие. – М.: ФОРУМ, 2012.
10. Малюк А.А. Введение в информационную безопасность: Учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2011.
11. Новиков Ф.М. и Новиков Д.А. Методология научного исследования. Учебно-методическое пособие. М.: «ЛИБРОКОМ», 2010.
12. Пастухова И.П. Основы учебно-исследовательской деятельности студентов. Учебно-методическое пособие. – М.: Издательский центр «Академия», 2010.
13. Петраков А. В. Защитные информационные технологии аудиовидео-электросвязи. Учебное пособие. М.: Энергоатомиздат, 2010.
14. Радько Н.М. и др. Риск-модели информационно-телекоммуникацион-ных систем при реализации угроз удаленного и непосредственного доступа. – М.: РадиоСофт 2010.
15. В.А. Проектирование и исследование комплексных систем безопасности. Учебное пособие. – СПб.: НИУ ИТМО, 2013.
16. Силаенков А.Н. Проектирование системы информационной безо-пасности. Учебное пособие. – Омск: Издательство ОмГТУ, 2009.
17. Торокин А.А. Инженерно-техническая защиты информации: Учебное пособие. М.: Гелиос АРВ, 2009.
18. Хасаншин И.А. Системы поддержки принятия решений в управлении региональным электронным правительством. – М.: Горячая линия-Телеком, 2013.
19. Шашенкова Е.А. Исследовательская деятельность. Словарь. – М.: УЦ «Перспектива», 2010.
20. Шепитько Г.Е. Теория информационной безопасности и методология защиты информации. – М.: РГСУ, 2012.
21. Щульц В.П. и др. Информационное управление в условиях активного противоборства: модели и методы. – М.: Наука, 2011.
22. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: Учеб. пособие. – М.: Книжный мир, 2009.

8.3 Электронные образовательные ресурсы

1. Учебный портал с электронно-методическими комплексами (do.kimes).
2. Универсальная библиотека онлайн (www.biblioclub.ru):
   - Информационная безопасность вычислительной техники. Учебное пособие. Спицын В.Г. Издатель: Эль Контент, 2011.
   - Основы информационной безопасности. Учебное практическое пособие. Сычёв Ю.Н. Издатель: Евразийский открытый институт, 2010.
   - Краткий энциклопедический словарь информационной безопасности Издатель: Энергия, 2010.
3. Polpred.com (www.polpred.com).
4. Единое окно доступа (www.window.edu.ru).
5. Издательский дом «Гребенников» (http://grebennikov.ru/).
6. ЭБС «Руконт» (www.rucont.ru).
7. Электронные книги: электронная библиотека пособий на компакт дисках. ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348.