АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ УНИВЕРСИТЕТ
КООПЕРАЦИИ, ЭКОНОМИКИ И ПРАВА»

ПРОГРАММА

вступительных испытаний при приеме на обучение
по программам подготовки научно-педагогических кадров
в аспирантуре
по профилю «Методы и системы защиты информации,
информационная безопасность»
направления подготовки научно-педагогических кадров
10.06.01 «Информационная безопасность»

Издательство
Белгородского университета
кооперации, экономики и права
2014

ПРЕДИСЛОВИЕ

Программа для вступительного экзамена по направлению 10.06.01 «Информационная безопасность» по профилю «Методы и системы защиты информации, информационная безопасность».

Сдача вступительного экзамена осуществляется в форме собеседования по перечню вопросов, которые представлены в конце программы. Вопросы охватывают такие темы как:

- теория и методология обеспечения информационной безопасности и защиты информации;
- объекты защиты информации;
- методы и средства защиты информации;
- криптографические методы защиты информации;
- проектирование и теория защиты данных в АСОД;
- системы опознания и разграничения доступа к информации;
- защита информации в ПЭВМ;
- защита информации в вычислительных сетях;
- оценка качества и эффективности систем защиты информации.

Уровень знаний оценивается по четырех балльной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

ПРОГРАММА И РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ДЛЯ ПОСТУПАЮЩИХ В АСПИРАНТУРУ ПО СПЕЦИАЛЬНОСТИ 05.13.19 «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ТЕМА 1. Теория и методология обеспечения информационной безопасности и защиты информации

Предмет информации. Понятие важности и ценности информации. Классификация информации по уровню важности. Виды и формы представления информации. Единицы измерения количества информации. Единицы измерения количества информации. Понятие аналогового и цифрового сигналов. Основные процессы, которым подвергается информация в вычислительных системах: ввод, обработка, хранение, вывод. Пути обеспечения информационного единства в АСУ.

Понятие сущности безопасности информации. Основное отличие информации, как объекта права собственности от права собственности материального объекта. Правомочия собственника с точки зрения права собственности. Понятия права распоряжения, права владения и права пользования. Инфраструктура, предотвращения нарушения прав собственности па информацию. Федеральный закон «Об информации, информационных технологиях и защите информации». Понятие государственной, коммерческой, личной и служебной тайн. Цель обеспечения безопасности информации. Основные направления информационной безопасности. Понятие информационной, экономической, оборонной, социальной и экономической безопасности. Основные причины, создающие возможности применения информационного оружия против России. Понятие информационной безопасности и защиты информации.

Основной перечень мероприятий, используемых в качестве защиты автоматизированных систем обработки данных и их характеристика. Меры по реализации и сопровождению

политики безопасности. Архитектура административной группы управления защитой. Мониторинг функционирования АСОД.

Понятие безопасности автоматизированных систем обработки данных. Пути достижения безопасности АСОД. Виды достижения безопасности АСОД и их характеристики. Понятия случайных и преднамеренных воздействий. Ошибки человека. Аварийные ситуации. Классификация угроз по цели, принципу воздействия и характеру воздействия на АСОД, по причине появления ошибки защиты, способу активного воздействия на объект. Наиболее распространенные угрозы безопасности АСОД и их характеристики. Информационная интегральная безопасность и ее структура. Основные этапы выполнения анализа риска. Классификация угроз системе передачи данных.

Нормативные документы оценки безопасности России, США и Европейских стран. Руководящие документы в области компьютерной безопасности России, США («оранжевая книга»). Понятие классов безопасности США. Руководящие документы РФ в области защиты информации. Основные функции разграничения доступа. Типы классов защищенности от несанкционированного доступа к информации (НСД). Особенности европейских критериев, предъявляемых к системе защиты информации.

ТЕМА 2. Объекты защиты информации

Классификация АСОД по способу построения. Понятия сосредоточенных и распределенных систем обработки данных. Многомашинные и многопроцессорные вычислительные комплексы. Структурная схема ЭВМ с точки зрения обработки информации. Вычислительные системы и системы телеобработки данных. Вычислительные сети: глобальные, региональные и локальные; информационные, вычислительные и информационно-вычислительные. Автоматизированные системы управления: глобальные, региональные и локальные.

Понятия проектирования автоматизированных систем обработки данных. Цель, задачи и содержание технического

задания на проектирование АСОД. Стадии проектирования и испытания АСОД. Понятия условий и режимов эксплуатации АСОД.

ТЕМА 3. Методы и средства защиты информации

Основные методы защиты информации: ограничение доступа, контроль доступа к аппаратуре, разграничение доступа, разделение привилегий на доступ, криптографическое преобразование информации, законодательные меры. Комплексные средства автоматизации и организация его обслуживания. Современные методы защиты информации в вычислительных сетях.

Понятие установления идентификации подлинности субъекта (объекта). Варианты установления подлинности. Методы идентификации. Блок-схема алгоритма идентификации и установления подлинности пользователя. Особенности автоматизированной передачи документов по каналам связи. Основные задачи и принципы построения защиты информации в трактах передачи данных в АСУ.

Понятие программных средств защиты данных и их особенности. Задачи, решаемые при организации систем защиты данных с использованием только программных средств. Классификация программных защитных средств. Применение экспертных и самообучающихся систем для организации защиты данных.

Понятие электромагнитных излучений и наводок, их опасность, с точки зрения утечки секретной информации, и НСД к ней. Меры безопасности для защиты информации от побочного электромагнитного излучения и наводок. Пути повышения надежности АСОД. Понятие дублирования и утроения, функционального контроля и диагностики систем. Методы функционального контроля: программные методы, программно-логические методы контроля, алгоритмические методы контроля, тестовые методы контроля, комбинированные методы, аппаратные методы, контроль при дублировании

оборудования, контроль по модулю. Классификация методом кот роля достоверности информации в АСОД. Понятие структурной, временной и информационной избыточности.

ТЕМА 4. Криптографические методы защиты информации

Назначение, область применения и состав криптологии. Понятия открытого ключа, секретного ключа, шифра, обратимости, преобразования шифра, обратимого преобразования шифра, шифратора и дешифратора, криптографического алгоритма, криптографических протоколов, и их назначение. Виды криптографических протоколов. Стойкость криптосистемы. Классификация криптосистем. Методы асимметричной криптографии.

Понятие и виды' шифропреобразований. Понятие преобразования перестановки и преобразования замены. Компоненты преобразования перестановки. Понятия ключа и операции перестановки по ключу. Шифр замены Ю. Цезаря. Шифр замены Гронсфельда. Таблица Вижинера. Двойной квадрат Чарльза Уитстона. Криптографический шифр К. Гаусса с рандомизацией и Джилберта Вернамом с побитным шифрованием. Правило Керхофа.

Понятие криптографической системы с секретным ключом. Модели симметричной и блочной симметричной криптографических систем. Модель детерминированной системы шифрования. SP-узлы, SP-сети К. Шеннона. Стандарт США для шифрования данных DES. Отечественный ГОСТ 28147-89 (алгоритм криптографического преобразования). Криптографическая система Вернама. Теоретическая и практическая стойкость криптографических систем по Шеннону. Синхронные и самосинхронизирующиеся поточные криптографические системы. Управление ключами в системах криптографической информации. Односторонние функции и их применение в криптографии. Открытое распределение ключей (схема Диффи-Хеллмана). Односторонняя функция с секретом. Криптографическая система с открытым ключом. Цифровая

подпись. Схема цифровой подписи Эль Гамаля. Существующие стандарты цифровой подписи.

ТЕМА 5. Проектирование и теория защиты данных в АСОД

Этапы развития концепции защиты информации. Вычисли тельная система как объект защиты информации. Потенциальны угрозы информации в вычислительных системах. Возможные каналы НСД в вычислительных системах. Алгоритм проектировании разработки систем защиты информации в вычислительных сетях Понятие автоматизированной системы с безопасной обработкой данных. Основные требования, предъявляемые к защите информации в вычислительных сетях. Защита информации в комплекса) средств автоматизации ее обработки.

Понятие модели ожидаемого поведения нарушителя. Характеристики наиболее опасного нарушителя. Модель элементарной защиты. Варианты определения прочности созданной преграды. Понятие автоматизированной преграды и ее назначение. Определение прочности преграды при организационных мерах защиты Определение прочности преграды зашиты при учете отказа системы. Модель многозвенной защиты. Суммарная прочность дублированных преград в многозвенной (многоуровневой) защите.

ТЕМА 6. Системы опознания и разграничения доступа к информации

Назначение системы опознания и разграничения доступа к информации (СОРДИ). Основные функции СОРДИ. Пароли, их назначения, хранение и использование. Алгоритм контроля и управления разграничением доступа к информации. Факторы, влияющие на эффективность работы СОРДИ.

Пароль, его назначение и характеристики. Выбор длины пароля по формуле Андерсона. Комбинированная система паролей. Одноразовые пароли, их достоинства и недостатки.

Обстоятельства раскрытия паролей. Меры предосторожности для защиты паролей. Методы закрытия паролей.

Карты как носители кодов паролей. Основные типы носителей кодов паролей и требования, предъявляемые к ним. Структура карты. Схема взаимного удостоверения. Проверка подлинности карт. Типы карт, используемых в АСОД. Этапы и: меры защиты ПО и информации от НСД при вводе, выводе и транспортировке. Аппаратно-программные технологии защиты данных. Электронные ключи и их особенности и возможности. Понятия смарт-карт-технологий. Метод модульного диалога как средство дополнительной проверки на санкционированность обращения.

ТЕМА 7. Защита информации в ПЭВМ

Отличительные особенности ПЭВМ как объекта защиты. Потенциальные угрозы информации, обрабатываемой в ПЭВМ. Возможные каналы НСД. Системы защиты информации от НСД в ПЭВМ. Основные функции управления и контроля в ПЭВМ при автономном режиме ее эксплуатации. Возможные каналы НСД к информации в ПЭВМ и потенциальные угрозы Средства защиты по возможным каналам НСД ПЭВМ. Программно-аппаратные средства разграничения доступа к информации ПЭВМ. Оценка уровня безопасности информации от НСД в ПЭВМ.

ТЕМА 8. Защита информации в вычислительных сетях

Информация, являющаяся предметом зашиты в сети. Структура системы защиты информации в автоматизированных системах управления (АСУ). Базовая эталонная модель взаимодействия открытых систем. Понятие физических средств соединения (каналы связи) и их классификация. Функции канального уровня. Сетевой уровень и его функции. Транспортный уровень и его функции. Сеансовый уровень и его

назначение. Представительный уровень и его основные функции. Прикладной уровень и его функции.

ЛВС как объект зашиты информации. Программное обеспечение сервера и основные модификации соединений ПК в ЛВС.

Потенциальные угрозы безопасности информация: в ЛВС. Система защиты информации от НСД в ЛВС. Распределение средств защиты по возможным к англам НСД ЛВС. Защита информации ЛВС от случайного НСД.

Варианты защиты информации в телекоммуникационных каналах связи (шифрование данных, цифровая подпись, управление доступом к ресурсам сети). Обеспечение целостности данных.

Архитектура клиент-сервер как основа структурирования информационных систем при рассмотрении программно-технических мер безопасности. Экранирующий шлюз и его назначение. Виды регуляторов, используемых при проведении в жизнь, выбранной политики безопасности. Защита в глобальной сети.

ТЕМА 9. Оценка качества и эффективности систем защиты информации

Исходная форма инструментария комплексной оценки качества (КОК) для выбора моделей. Связь комплекса моделей с подсистемами инструментария КОК для оценки различных показателей функционирования информационных систем (ИС). Назначение инструментария КОК. Функциональные возможности КОК. Технологии обеспечения защищенности ИС.

Оценка надежности выполнения функций программно-техническими средствами. Надежность схемы подготовки, передачи, обработки, хранения и отображения информации программно-техническими средствами. Основные данные для проектирования систем защиты информации. Анализ полученных результатов и выводы. Оценка своевременности представления информации. Представление структуры оценки

своевременности предоставления информации. Подготовка данных для проведения расчетов. Представление характеристик временных потоков. Анализ результатов. Выводы. Оценка полноты используемой информации. Оценка актуальности используемой информации. Оценка ошибочности используемой информации после контроля. Оценка корректности обработки информации. Оценка ошибочности действий пользователя и обслуживающего персонала. Оценка защищенности от опасных воздействий. Оценка защищенности информационных и программных ресурсов от несанкционированного доступа.

ТЕМЫ РЕФЕРАТОВ

1. История развития средств защиты информации.
2. Подходы к вопросам защиты информации за рубежом.
3. История развития защиты информации в России.
4. Криптографические методы защиты информации. История развития и назначение.
5. Системы наблюдения за объектом и их назначение.
6. Организационные меры защиты информации и их удельный вес в общем объеме мер по защите информации.
7. Классификация угроз безопасности функционирования автоматизированных систем обработки данных (АСОД).
8. Объекты защиты информации и их классификация.
9. Модели защиты информации.
10. Системы опоздания и разграничения доступа к информации.
11. Программные средства защиты информации.
12. Технические средства защиты информации.
13. Защита информации в компьютерных сетях.
14. Оценка качества и эффективности систем защиты информации.

ВОПРОСЫ ДЛЯ ПОСТУПАЮЩИХ В АСПИРАНТУРУ

1. Что понимается под термином «информационная безопасность»?
2. Какие имеются основные направления в плане информационной безопасностью?
3. Каковы основные функции ФСТЭК России?
4. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации.
5. Каковы функции информационно-телекоммуникационной системы специального назначения (ИТКС) и из каких основных комплексов она состоит?
6. Какие основные мероприятия проведены в государственных структурах, направленные на обеспечение информационной безопасности их функционирования?
7. Роль и основные функции государственных организаций и учреждений, научно-исследовательских организаций и учебных заведений в области обеспечения информационной безопасности страны.
8. Какая система называется безопасной, и какая надежной?
9. Что такое политика безопасности?
10. Что такое достоверная вычислительная база, и из каких компонент она состоит?
11. Каковы основные функции мониторинга системы защиты, и какими средствами она реализуется?
12. Какие противоречивые задачи решаются при создании автоматизированной системы обработки данных?
13. Каковы наиболее распространенные политики безопасности и какими существенными признаками они отличаются друг от друга?
14. Как производится управление информационными потоками?
15. Объясните сущность концепции иерархической де композиции системы и особенности ее применения.

16. Каковы механизмы защиты, входящие в состав достоверной вычислительной базы и их свойства?

17. Каковы основные функции, выполняемые ядром безопасности совместно с другими службами операционной системы?

18. Перечислите основные принципы реализации политики безопасности.

19. Что такое внутренняя и внешняя безопасность АСОД?

20. Каковы причины случайного воздействия на АСОД?

21. Перечислите и объясните сущности угроз безопасности АСОД?

22. Что такое информационная интегральная безопасность АСОД?

23. Что такое стратегия защиты и в чем состоит суть анализа риска?

24. Каковы угрозы системе передачи данных?

25. Что подразумевается под оценкой безопасности системы?

26. Каковы Руководящие документы Государственной технической комиссии (ГТК) при Президенте РФ в области компьютерной безопасности?

27. Система документации США в области компьютерной безопасности.

28. Каковы основные функции системы разграничения доступа субъектов и их процессов к данным (по документам ГТК РФ)?

29. Каковы классы защищенности средств вычислитель ной техники от НСД к информации (по документам ГТК РФ)?

30. Каковы классы защищенности автоматизированных систем от НСД к информации (по документам ГТК РФ)?

31. Каковы критерии безопасности информационных технологий европейских стран?

32. Состав и функции сотрудников административной группы управления защитой.

33. Что собой представляет системный журнал, и какие возможности открываются при его использовании?

34. Объясните сущность жизненного цикла информации.

35. Информация как объект права собственности.

36. Каковы объекты защиты информации?

37. Каковы методы защиты информации от преднамеренного доступа при использовании простых средств хранения и обработки информации?

38. Что значит разграничение и контроль доступа к информации?

39. Объяснить сущность метода разделения привилегий доступа.

40. Из чего состоит комплекс средств автоматизации и как организуется его обслуживание?

41. Каковы более современные основные методы защиты информации в вычислительных системах?

42. Что понимается под идентификацией и установлением подлинности субъекта (объекта)?

43. В чем заключается суть идентификации и установления подлинности технических средств?

44. В чем заключается суть идентификации и установления подлинности документов?

45. В чем заключается суть идентификации и установления подлинности информации на средствах отображения и печати?

46. Объясните суть комплексного подхода к организации систем защиты данных с применением только программных средств.

47. Какие защитные меры применяются при защите информации от побочного электромагнитного излучения и наводок?

48. Какие методы функционального контроля вычислительных систем Вы знаете?

49. Каковы методы защиты информации от преднамеренного доступа при использовании простых средств

хранения и обработки информации?

50. Что значит разграничение и контроль доступа к информации?

51. Объясните сущность метода разделения привилегий доступа.

52. Из чего состоит комплекс средств автоматизации и как организуется его обслуживание?

53. Каковы современные основные методы защиты информации в вычислительных системах?

54. Что понимается под идентификацией и установлением подлинности субъекта (объекта)?

55. В чем заключается суть идентификации и установления подлинности технических средств?

56. В чем заключается суть идентификации и установления подлинности документов?

57. В чем заключается суть идентификации и установления подлинности информации на средствах отображения и печати?

58. Объясните суть комплексного подхода к организации систем защиты данных с применением только программных средств.

59. Какие защитные меры применяются при защите информации от побочного электромагнитного излучения и наводок?

60. Какие методы функционального контроля вычислительных систем Вы знаете?

61. Что такое «криптология»?

62. Что такое «ключ»?

63. Определите понятие «криптологический алгоритм».

64. Какие функции выполняет криптологический протокол?

65. Что собой представляет криптосистема?

66. Дайте определение стойкости криптосистемы. Какие основные типы криптосистем знаете?

67. Дайте общее определение электронной цифровой подписи.

68. Объясните суть преобразований - перестановка и замена.

69. Приведите пример табличной перестановки с использованием ключевого слова.

70. Что собой представляет система шифрования с использованием таблицы Вижинера?

71. Что собой представляет система шифрования Вернама и укажите ее особенности?

72. Что гласит правило Керкхофа?

73. В чем была слабость шифра Энигмы?

74. Что собой представляет симметричная криптографическая система?

75. Что собой представляет блочная симметричная криптографическая система?

76. Объясните, что такое композиционный блочный шифр и итерационный блочный шифр.

77. Объясните суть алгоритма DES и укажите на его особенности.

78. В каких режимах может работать алгоритм DES?

79. Отечественный алгоритм криптографического преобразования данных (ГОСТ 28147-90) и его отличительные особенности.

80. Какие режимы имеет отечественный алгоритм крипто графического преобразования данных (ГОСТ 28К7-90)?

81. В чем состоит суть алгоритма выработки имитовставки (ГОСТ28147-89)?

82. Чем отличаются поточные симметричные криптографические системы?

83. Какими характеристиками оценивается стойкость криптографических систем?

84. Что подразумевается под понятием «вычислительная сложность «алгоритма»?

85. Из этих этапов состоит процесс управления ключами?

86. Для каких целей применяются случайные последовательные простые числа в криптографии?

87. Чем характеризуются односторонние функции, и для каких целей они применяются?

88. В чем состоит суть схемы открытого распределения ключей Диффи-Хеллмана?

89. Чем характеризуются односторонние функции с секретом?

90. Чем отличается криптографическая система с открытым ключом

91. Каков алгоритм криптографического преобразования с открытым ключом RSA, и каковы его характеристики?

92. В чем заключается суть электронной цифровой подписи?

93. Как проверяется целостность сообщения?

94. Каковы компоненты реализации электронной цифровой подписи?

95. Какова схема реализации цифровой подписи Эль Гамаля?

96. На чем основывается проверка подписи, сформирован ной по схеме Эль Гамаля?

97. Что такое хэш-функция?

98. Чем отличаются хэш-функции с ключом и без ключа?

99. Где применяются хэш-функции?

100. Как производится распределение ключей в симметричных криптографических системах?

101. В чем суть трехэтапного протокола Шамира для передачи ключа?

102. Охарактеризуйте отечественный стандарт элек тронной цифровой подписи ГОСТ Р 34. 10-94.

103. Какие основные отличительные особенности исторических этапов создания механизмов зашиты информации, а также разработки средств, способов и методов защиты, применяемых в системах зашиты?

104. Концепции защиты информации.

105. Какова концептуальная основа построения защиты

информации вычислительных системах?

106. Вычислительная система как объект защиты.

107. Каковы потенциальные угрозы в вычислительной системе?

108. Каковы концептуальные основы построения системы защиты в вычислительной системе?

109. Охарактеризуйте возможные каналы несанкционированного доступа в вычислительной системе.

110. Общий алгоритм проектирования и разработки системы защиты информации в ВС.

111. Каковы основные мероприятия по предупреждению и контролю НСД в ВС?

112. Каковы концептуальные основы проектирования защиты информации от НСД в вычислительной сети и АСУ?

113. Каковы основные требования в области защиты ин формации в вычислительных сетях?

114. Укажите состав средств и структуру системы защиты информации от НСД в комплексах средств автоматизации.

115. Каковы основные характеристики потенциального нарушителя?

116. Из чего состоит модель элементарного нарушителя и как определяется прочность преграды (но вариантам)?

117. Как определяется прочность защиты при наличии у преграды нескольких обходных путей?

118. Как функционирует автоматизированная преграда (объясните повременной диаграмме контроля НСД)?

119. Как определяется прочность преграды при использовании организационных мер защиты?

120. Каким образом определяется прочность преграды защиты при учете отказа системы?

121. Как определяется суммарная прочность дублированных преград в многозвенной защите?

122. Что представляет собой эталонная модель взаимодействия открытых систем?

123. Укажите основные принципы построения системы

защиты информации в сетях.

124. ЛВС как объект защиты информации.

125. Какие средства управления зашитой информации ЛВС Вы знаете?

126. Что знаете об антивирусных средствах?

127. 129.Укажите основные сервисные службы защиты ин формации, рекомендованные OSI.

128. Что Вы знаете об архитектуре клиент-сервер и о ее безопасности?

129. Какие функции выполняются межсетевыми экранами?

130. Какие имеются разновидности межсетевых экранов?

131. Чем отличаются прокси-серверы?

132. Какие имеются основные программные средства, обеспечивающие безопасность в сетях?

ЛИТЕРАТУРА

1. Конституция Российской Федерации.

2. Гражданский кодекс Российской Федерации от 22.12.95 // Собрание законодательства Российской Федерации. 1996. №5. Ст. 410.

3. Уголовный кодекс Российской Федерации от 24.05.96 // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 155.

4. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09.09.2000 // Российская газета. 2000. 28 сент. С. 4-6.

5. Об оперативно-розыскной деятельности: Закон РФ от 05.07.95 // Собрание законодательства Российской Федерации. 1995. №33. Ст. 3349.

6. О Федеральной фельдъегерской связи: Закон РФ от 16.11.94 // Собрание законодательства Российской Федерации. 1994. №34. Ст. 3547.

7. О Федеральных органах правительственной связи и информации: Закон РФ от 19.02.93 // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. № 12. Ст. 423.

8. Об органах Федеральной службы безопасности в Российской Федерации: Закон РФ от 22.02.95 // Собрание законодательства Российской Федерации. 1995. № 15. Ст. 1269.

9. О безопасности: Закон РФ от 05.03.92 // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – № 15. – Ст. 769.

10. О внесении изменений и дополнений в Закон Российской Федерации «О государственной тайне»: Закон РФ от 06.10.97 // -1997.-№41.-Ст. 4673.

11. О государственной тайне: Закон РФ от 21.07.93 // Журнал официальной информации. Кадастр. 1993. – № 35. С. 3-41.

12. Об информации, информационных технологиях и защите информации: Закон РФ от 25.01.95 // Собр. закон. РФ. – 1995. – № 8. – Ст. 609.

13. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности: Постановление Правительства РФ от 04.09.95 № 870 // Собрание законодательства Российской Федерации. 1995. № 37. Ст. 3619.

14. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности: Постановление Правительства РФ от 04.09.95 № 870 // Собрание законодательства Российской Федерации. 1995. № 37. Ст. 3619.

15. О перечне сведений, которые не могут составлять коммерческую тайну: Постановление Правительства Российской Федерации от 05.12.91 // Собрание постановлений правительства РСФСР. 1992. №12. Ст. 7.

16. Перечень должностных лиц органов государственной власти, наделенных полномочиями по отнесению к государственной тайне: Распоряжение Президента РФ от 11.02.95 № 73 // Собрание актов Президента и Правительства Российской Федерации. 1994. №7. Ст. 506

17. Положение о Государственной технической комиссии при Президенте Российской Федерации: Указ Президента Российской Федерации от 19.02.99 № 212 // Собрание законодательства Российской Федерации. 1999. № 8. Ст. 1010.

18. Утверждение Положения о Федеральной службе безопасности Российской Федерации: Указ Президента РФ от 23.06.95 № 633 // Собрание законодательства Российской Федерации. 1995. № 26. Ст. 2453.

19. О создании Государственной технической комиссии при Президенте РФ: Указ Президента РФ от 05.01.92 № 97/ Ведомости съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1992. №3. Ст. 109.

20. Об утверждении перечня сведений конфиденциального характера: Указ Президента Российской Федерации от 06.03.97 № 188 // Собрание законодательства Российской Федерации. 1997. №10. Ст. 4775.

21. Об утверждении перечня сведений, отнесенных к государственной тайне: Указ Президента РФ от 24.01.98 № 61 // Собрание законодательства Российской Федерации. 1998. № 5. Ст. 561.

22. ГОСТ Р 50922 – 2005 Защита информации. Основные термины и определения. – М.: Изд. стандартов, 2005.

23. ГОСТ Р 6.30 – 97 Унифицированные системы документации. Система организационно – распорядительной документации. Требования к оформлению документов. – М.: Изд. стандартов, 1997.

24. *Алексенцев А.И.* Защита информации: Словарь базовых терминов и определений. – М: РГГУ, 2000.

25. *Алексенцев А.И.* Конфиденциальное делопроизводство. – М.: Интел-Синтез, 2003.

26. *Алферов А.П.* и др. Основы криптографии. Учеб. пособие. – М: Гелиос, 2004

27. *Баскаков СИ.* Радиотехнические цепи и сигналы.: Учеб. для вузов. Изд.3-е, перераб. и доп./ СИ. Баскаков. – М.: Высш. шк., 2000. – 462с.

28. *Безкоровайный М.М., Костогрызов А.И., Львов В.М.* Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КСК»: Руководство системного аналитика. – М.: Вооружение. Политика. Конверсия. 2002. – 305 с, 2-е изд

29. Безопасность информационных технологий. Учебник для вузов. М.: Диасофт, 2004, 1000с.

30. Бизнес – Безопасность - Телекоммуникации. Терминологический словарь. – М.: Радио и связь, 2001.

31. *Бобровников, Л.З.* Радиотехника и электроника: Учеб. для вузов. – 4-е изд. перераб. и доп. / Л.З. Бобровников. – М.: Недра, 1999. – 374с.

32. *Богданов М. А.* Криптография и компьютеры // ИНТЕРКОМПЬЮТЕР № 5/90.

33. *Варфоломеев А.А.* Методы криптографии и их применение в банковских технологиях. – М.: МИФИ, 1995. – 116 с.

34. *Варфоломеев А.А., Домнина О.С, Пеленицын М.Б.* Управление ключами в системах криптографической защиты банковской информации. Учебное пособие. – М.: 1996. – 128 с.

35. *Варфоломеев А.А., Жуков А.Е., Мельников А.Б., Устюжанин Д.Д.* Блочные криптосистемы. Основные свойства и методы анализа стойкости. – М.: МИФИ, 1998.

36. Введение в защиту информации в автоматизированных системах: учеб. пособие для вузов / Малюк А.А., Пазизин С.В., Погожий Н.С. – М. : Горячая линия-Телеком, 2005.

37. *Вегнер, А. Ю. Крутиков* и др. – М.: Радио и связь, 1992.

38. *Вентцель Е.С., Овчарова Л.А.* Теория вероятностей. Задачи и упражнения. – М.: 1973.

39. Военная наука. Теоретический труд. Под ред. Радионова И.Н. – М: ВАГШ, 1992.

40. *Гайкович В., Першин А.* Безопасность электронных банковских систем. – М.: Компания «ЕДИНАЯ ЕВРОПА», 1994.

41. *Галатенко В.А.* Основы информационной безопасности: Курс лекций. – М.: Интернет – Университет, 2004.

42. *Галатенко В.А.* Стандарты информационной безопасности: Курс лекций. М.: Интернет – Университет, 2004.

43. *Грабовски Б.* Краткий справочник по электронике. Пер. с фран. / Б. Грабовски. – М.: ДМК Пресс, 2001.

44. *Гринберг А.С, Горбачев Н.Н.* Защита информационных ресурсов государственного предприятия: Учебник для вузов. – М.: Юнити, 2003.

45. *Гриншпак Л.А., Левин Е.М.* Электронные ключи для защиты информации // Мир ПК. – 1991. – № 4.

46. *Девянин П.Н. Михальский О. О., Правиков Д.И.* Теоретические основы компьютерной безопасности. – М: Горячая линия - Телеком, 2002.

47. *Демаков Ю.П.* Радиоматериалы и радиокомпоненты.

Часть П. Компоненты электронных схем. Характеристики, применение, расчет: Учеб. пособие для вузов. / Ю.П. Демаков – Ижевск: ИжГТУ, 1999.

48. *Дептел Г.* Введение в операционные системы. В 2-х т. Т 2. / Пер.с англ. – М: Мир, 1987.

49. *Доля А.Д.* Некоторые варианты построения матричных сетей сбора сигналов о несанкционированном доступе в вычислительной системе // Спб.: «Вопросы спец. радиоэлектроники». – Сер. СОИУ. – 1987. – Вып. 3.

50. *Доля А.Д.* Некоторые варианты построения сетей сбора сигналов несанкционированного доступа в вычислительной системе // Сб. «Вопросы спец. радиоэлектроники». – Сер. СОИУ. – 1986. – Вып. 3.

51. *Домарёв В.В.* Безопасность информационных технологий. Методология создания систем защиты. – М.: ДиаСофт, 2002.

52. *Домашев А.В,* и др. Программирование алгоритмов защиты информации. Учеб. Пособие. Изд. 2-е, исправленное и дополненное. – М.: Издатель Молгачева СВ., Издательство «Нолидж», 2002.

53. *Зегжда Д.П., Ивашка А.М.* Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.

54. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2002.

55. *Игнатьев В.А.* Защита информации в корпоративных информационно-вычислительных сетях: Монография. – Старый Оскол: ООО «ТНТ», 2005.

56. *Игнатьев В.А.* Информационная безопасность современного коммерческого предприятия: Монография. – Старый Оскол: ООО «ТНТ», 2005.

57. Информационная безопасность открытых систем: учеб. для вузов: В 2 т. / СВ. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: Горячая линия-Телеком, 2006.

58. Информационная безопасность. Экономические аспекты управления защищенными информационными

ресурсами: монография / Прокушева А.П., Пономаренко СВ., Прокушев Я.Е. – Белгород : Кооперативное образование, 2006.

59. История государства и права России в документах и материалах /Автор-сост. И.Н.Кузнецов. – 2-е изд. – Мн.: Амалфея, 2003.

60. *Конеев И.И., Беляев И.И.* Информационная безопасность предприятия: Учебник для вузов. - СПб.: БХВ - Петербург, 2003.

61. *Кремер Н.Ш.* Теория вероятностей и математическая статистика: учеб. для вузов / Кремер Н.Ш. – 2-е изд., перераб. и доп. – М. : ЮНИТИ, 2007.

62. *Куприянов А.И.* Основы защиты информации: учеб. пособие / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов, стер. – М.: Академия, 2008.

63. Лачин В.И. Электроника. /В.И. Лачин, Н.С. Савелов. – М.: Феникс, 2001.

64. *Малюк А.А* Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие для вузов / Малюк А.А. – М.: Горячая линия-Телеком, 2004.

65. *Мельников В.* Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997.

66. *Мельников В.* Криптография от папируса до компьютера. - М: ABF, 1996. – 335с.

67. *Опадчий Ю. Ф.* и др. Аналоговая и цифровая электроника. (Полный курс): Учебник для вузов. / Ю. Ф. Опадчий, О.П. Глуд-кин, А. И. Гуров.; Под ред. О. П. Глудкина – М.:Телеком, 2000.

68. Операционная система UNIX. Курс лекций. Учебное пособие / Г.В. Курячий – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2004.

69. Основы информационной безопасности: Учеб.пособие / Белов Е.Б., Мещеряков Р.В., Шелупанов А.А.; ред. Лось В.П. – М.: Горячая линия, 2006.

70. Основы информационной безопасности: Учебное пособие / Галатенко В.А. Под редакцией члена-корреспондента

РАН В.Б. Бетелина / М.:-ИНТУИТ.РУ "Интернет-университет Информационных Технологий", 2004.

71. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций. Учебное пособие I Лапонина О.Р. под ред. В.А. Сухомлина. – М.: Интернет-Ун-т Информ. Технологий. 2005.

72. *Павлов В.Н.* и др. Схемотехника аналоговых электронных устройств.: Учеб. для вузов. 2-е изд. / В.Н. Павлов, В.Н. Ногин. – М.: Телеком, 2001.

73. *Переход Н. Г.* Измерение параметров сигнала в электрических цепях. Учебное пособие. - Белгород: Кооперативное образование, 2006. – 106с.

74. *Переход Н. Г.* Основные виды и способы преобразования сигналов: Учебное пособие. – Белгород: Кооперативное образование, 2004.

75. *Переход Н.Г.* Вероятностные методы в теории информационных систем: Учебно-методическое пособие. – Белгород: Издательство БУКЭП, 2011. – 92 с.

76. *Переход Н.Г.* Оптимальные методы обработки параметров случайных сигналов в электромагнитных каналах утечки информации: Монография. – Белгород: Кооперативное образование, 2009. – 153 с.

77. *Пономаренко В.В., Пономаренко С.А.* Защита и обработка конфиденциальных документов: Учеб. пособие. – Белгород: Издательство Белгородского университета потребительской кооперации, 2009. – 271 с.

78. *Пономаренко С.А.* Организационная защита инормации: Учебное пособие: в 2-х частях. – Белгород: Издательство БУКЭП, 2011. – Ч. 1. – 286 с.

79. *Пономаренко С.А.* Организация и управление службой защиты информации: Учебное пособие. – Белгород: Издательство БУПК, 2010. – 282 с.

80. *Пономаренко С.В.* Инженерно-техническая защита информации: Учеб. пособие. – Белгород: Кооперативное образование, 2006. – Ч. 1.

81. *Пономаренко С.В., Прокушев Я.Е.* Инженерно-

техническая защита информации: Учеб. пособие. – Белгород: Кооперативное образование, 2006. – Ч. 2.

82. *Пономаренко С.В., Прокушев Я.Е.* Программно-аппаратная защита информации: Учеб. пособие для студ. спец. 090103.65 «Организация и технология защиты информации», 080801.65 «Прикладная информатика в экономике». – Белгород: Кооперативное образование, 2009.

83. *Пономаренко СВ.* Информационная безопасность в событиях и фактах. – М.: Синтег, 2004.

84. Правовое обеспечение информационной безопасности: Учебник / Под общей научной редакции В.А. Минаева, А.П. Фисуна, СВ. Скрыля, СВ. Дворянкина и др. – М.: Маросейка, 2008.

85. Проблемы информационно-психологической безопасности: сборник статей и материалов конференций РАН. – М.: Институт психологии, 1996.

86. *Прокис Док.* Цифровая связь. / Дж. Прокис; Пер. с англ, под ред. Д. Д. Кловского. – М.: Радио и связь, 2000.

87. *Прокушев Я.Е.* Криптографическая защита информации: Учеб. пособие. – Белгород: Кооперативное образование, 2005.

88. *Семкин С.Н., Семкин А.Н.* Основы правового обеспечения информационной безопасности. – Орел: «Навигатор-технолоджи», 2003.

89. *Серго А.Г.* Основы права интеллектуальной собственности. Курс лекций: учеб. пособие для вузов / Серго А.Г., Пущин В.С. - М.: Интернет-Ун-т Информ. Технол., 2005.

90. *Скиба Владимир.* Руководство по защите от внутренних угроз информационной безопасности / Скиба Владимир, Курбатов Владимир. – СПб.: Питер, 2008.

91. Стандарты информационной безопасности: Учебное пособие / Галатенко В.А. Под редакцией члена-корреспондента РАН В.Б. Бетелина / М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2004.

92. *Столлингс В.* Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – ML: Издательский

дом «Вильяме», 2004. – 672

93. Толковый словарь терминов по системам, средствам и услугам связи: Справ, издание. / В. А. Докучаев, О. Н. Иванова, З.А. Красавина и др.; Под ред. В. А. Докучаева. – М.: Радио и связь, 2000.

94. *Торокин А. А.* Теоретические основы компьютерной безопасности: Учеб. для вузов. – М.: Радио и связь, 2000.

95. *Федоров П. Д.* Толковый словарь по электронике./ Н. Д. Федоров, Д. Н. Федоров. – М.: 2001.

96. *Шеннон К. Э.* Теория связи в секретных системах. Работы по теории информации и кибернетике. – М.: ВКЮБ, 1963.

97. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М: Триумф, 2006.

СОДЕРЖАНИЕ