НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

«УТВЕРЖДАЮ»

Проректор по научной работе

_____ Драгунов В.К.

«16» июня 2015 г.

Программа аспирантуры

Направление 09.06.01 Информатика и вычислительная техника

Направленность (специальность) 05.13.17 Теоретические основы информатики

РАБОЧАЯ ПРОГРАММА

дисциплины по выбору

«Методы и средства защиты информации в компьютерных системах и сетях»

Индекс дисциплины по учебному плану: Б1.В.ДВ.3.2

Всего: 72 часа

Семестр 5, в том числе 6 часов – контактная работа,
48 часов – самостоятельная работа,
18 часов – контроль

Программа составлена на основе федерального государственного образовательного стандарта высшего образования (уровень подготовки кадров высшей квалификации) по направлению подготовки 09.06.01 Информатика и вычислительная техника, утвержденного приказом Минобрнауки России от 30 июля 2014 г. № 875, и паспорта специальности, указанной в номенклатуре специальностей научных работников 05.13.17 Теоретические основы информатики, утвержденной приказом Минобрнауки России от 25 февраля 2009 г. № 59.

ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является приобретение необходимых теоретических знаний и практических навыков разработки и использования методов и средств обеспечения информационной безопасности компьютерных систем и сетей.

Задачами дисциплины являются:

– ознакомление с общей постановкой задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацией методов ее решения;

– изучение современных методов и средств идентификации и аутентификации субъектов компьютерных систем и сетей, разграничения их доступа к данным, построения и использования симметричных и асимметричных криптографических систем;

– приобретение навыков выбора, разработки и использования изученных методов и средств защиты данных при создании безопасных информационных систем.

В процессе освоения дисциплины **формируются следующие компетенции**:

– способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1);

– готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4);

– владение культурой научного исследования, в том числе с использованием современных информационно-коммуникационных технологий (ОПК-2);

– владение методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности (ОПК-7);

– способность разрабатывать научно-техническую документацию, оформлять научно-технические отчеты, обзоры, публикации по результатам выполненных исследований на государственном и иностранном языках (ПК-2);

– владение методами обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации (ПК-10).

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБРАЗОВАНИЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен демонстрировать **следующие результаты образования**:

знать:

– общую постановку задачи защиты информации в компьютерных системах и сетях и классификацию методов ее решения (ОПК-2);

– способы несанкционированного доступа к данным и способы авторизации пользователей компьютерных систем и сетей (ПК-10);

– математические основы построения симметричных и асимметричных криптографических систем (УК-1);

уметь:

– применять методы и средства разграничения полномочий пользователей и управления доступом к данным в компьютерных системах и сетях (ПК-10);

– использовать методы и средства криптографической защиты информации (ПК-10);

– анализировать, выбирать и применять методы и средства защиты от вредоносных программ (ОПК-2);

владеть:

– терминологией и навыками ведения профессиональной дискуссии по соответствующей тематике (ПК-2);

– навыками поиска информации о новых методах и средствах защиты информации в компьютерных системах и сетях (УК-4);

– навыками выбора эффективных средств защиты информации и безопасных информационных технологий (ОПК-7).

КРАТКОЕ СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

Комплексное обеспечение защиты информации в компьютерных системах и сетях (6 часов самостоятельной работы)

Проблема защиты информации и подходы к ее решению. Категории информации с ограниченным доступом. Угрозы информационной безопасности и каналы утечки информации. Комплексный подход к защите информации.

Классификация методов защиты информации. Использование интеллектуальных методов для защиты информации. Правовое обеспечение защиты информации.

Методы и средства разграничения доступа к объектам компьютерных систем и сетей (12 часов самостоятельной работы)

Способы несанкционированного доступа к объектам компьютерных систем и сетей. Дискреционное, мандатное и ролевое управление доступом к объектам.

Архитектура подсистемы безопасности и ее основные компоненты в современных операционных системах для серверов, настольных компьютеров и мобильных устройств.

Методы и средства защита информации в глобальных компьютерных сетях (межсетевые экраны, сканеры уязвимостей, системы обнаружения и предотвращения атак, системы контроля содержания). Интегрированные системы безопасности.

Методы и средства аудита событий безопасности. Стандарты оценки безопасности компьютерных систем и информационных технологий.

Криптографические методы и средства защиты информации

(12 часов самостоятельной работы)

Основы алгебры вычетов. Способы создания симметрических криптосистем. Абсолютно стойкий шифр.

Криптографические системы DES, AES и ГОСТ 28147-89. Применение и обзор современных симметричных криптосистем.

Принципы построения асимметричных криптосистем. Протокол Диффи-Хеллмана. Криптографические системы RSA, Эль-Гамаля и на основе эллиптических кривых.

Электронная подпись и ее применение. Функции хеширования и способы их построения. Использование асимметричных криптосистем.

Использование технологии VPN для безопасной передачи данных в сети.

Криптография и стеганография. Методы компьютерной стеганографии и их применение.

Методы и средства аутентификации пользователей и сообщений

(12 часов самостоятельной работы)

Способы аутентификации пользователей в компьютерных системах и сетях. Аутентификация на основе паролей. Организация базы учетных записей и хранения паролей в современных операционных системах и системах управления базами данных.

Аутентификация с использованием устройств. Двухфакторная аутентификация. Аутентификация пользователей на основе их биометрических характеристик. Аутентификация на основе знаний о пользователе.

Аутентификация пользователей при удаленном доступе. Протоколы прямой (S/Key, CHAP) и непрямой (RADIUS, Kerberos) аутентификации.

Протоколы автономной аутентификации при удаленном доступе (SSL, TLS). Инфраструктура открытых ключей и средства ее создания.

Методы и средства защиты от вредоносных программ и несанкционированного копирования информации

(6 часов самостоятельной работы)

Вредоносные программы, их признаки и классификация. Компьютерные вирусы и программные закладки. Методы и средства обнаружения и удаления вредоносных программ.

Проблема защиты прав на объекты интеллектуальной собственности. Принципы построения систем защиты от несанкционированного копирования. Защита программ от изучения. Методы обфускации программ.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБРАЗОВАНИЯ ПО ДИСЦИПЛИНЕ

Промежуточная аттестация по итогам освоения дисциплины:

5 семестр – дифференцированный зачет.

Вопросы для самоконтроля

1. В каких формах может быть представлена информация?
2. Что относится к информации ограниченного доступа?
3. Что понимается под защитой информации?
4. Что относится к основным характеристикам защищаемой информации?
5. Что такое угроза безопасности информации? Каковы основные виды угроз?
6. Какие существуют каналы утечки конфиденциальной информации?
7. В чем сущность системно-концептуального подхода к защите информации в компьютерных системах?
8. Почему проблема защиты информации не может быть решена с помощью только формальных методов и средств?
9. В чем сущность организационной защиты информации?
10. Каковы уровни правового обеспечения информационной безопасности?
11. Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?
12. Какие требования предъявляются к комплексным системам защиты информации?
13. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?
14. Какие существуют способы несанкционированного доступа к информации в компьютерных системах?

15. Какие способы аутентификации пользователей могут применяться в компьютерных системах?

16. В чем основные недостатки парольной аутентификации и как она может быть усилена?

17. Какие биометрические характеристики пользователей могут применяться для их аутентификации? В чем преимущества подобного способа подтверждения подлинности?

18. Какие элементы аппаратного обеспечения могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем?

19. Что называют двухфакторной аутентификацией?

20. Что лежит в основе работы протокола S/Key? Что такое парольная инициализация?

21. На чем основан протокол CHAP? Какие требования выдвигаются к используемому в нем случайному числу?

22. Для чего предназначен протокол Kerberos?

23. Какие применяются разновидности межсетевых экранов?

24. Что такое VPN и для чего они предназначены?

25. В чем состоят функции средств анализа защищенности компьютерных систем и их основные недостатки?

26. В чем сущность систем обнаружения атак на компьютерные системы?

27. Для чего предназначен редактор объектов групповой политики Windows? Где сохраняются результаты его работы?

28. В чем сущность, достоинства и недостатки дискреционного управления доступом к объектам?

29. Какие правила применяются при предоставлении доступа субъекта к объекту в соответствии с мандатным управлением доступом? В чем их смысл?

30. Какие основные компоненты входят в состав подсистемы безопасности операционной системы Windows?

31. Где хранится регистрационная база данных пользователей Windows?

32. Как организовано хранение паролей в Windows?

33. Какие дополнительные средства защиты паролей пользователей может быть применены в Windows?

34. Что такое маркер доступа субъекта Windows и какая информация в нем содержится?

35. Как осуществляется разграничение доступа к объектам в Windows?

36. Из чего состоит дескриптор безопасности объекта в Windows? При каком обязательном условии файлы и папки могут иметь дескрипторы безопасности?

37. Как происходит изменение прав доступа к объектам Windows и кто это может делать?

38. Что относится к параметрам политики аудита в Windows?

39. Где хранится информация об учетных записях пользователей и групп в операционных системах семейства Unix?

40. Как сохраняются пароли пользователей в операционных системах семейства Unix? Что такое затенение паролей?

41. Как разграничивается доступ субъектов к объектам в операционных системах семейства Unix?

42. Как назначаются права доступа к вновь создаваемым объектам в Windows и Unix?

43. Какая модель управления доступом к объектам применяется в Windows и в Unix?

44. Как устанавливаются параметры аудита в операционных системах семейства Unix?

45. Почему операции над вычетами находят широкое применение в современной криптографии?

46. В чем разница между симметричными и асимметричными криптографическими системами?

47. Какие основные способы применяются при создании алгоритмов симметричной криптографии?

48. В чем разница между потоковыми и блочными шифрами?

49. Какой шифр может считаться идеальным (по К.Шеннону)?

50. Какие симметричные криптосистемы используются в настоящее время?

51. В каких режимах могут использоваться блочные шифры?

52. Какие из режимов блочных шифров могут использоваться для проверки аутентичности и целостности шифротекста?

53. Что лежит в основе асимметричной криптографии?

54. В чем особенности и основные сферы применения асимметричных криптосистем?

55. На чем основана криптостойкость систем RSA, Эль-Гамаля и эллиптических кривых?

56. Что такое электронная подпись (ЭП), как она получается и проверяется?

57. Какова роль в системах ЭП функций хеширования?

58. Какую роль исполняют удостоверяющие центры? Что такое сертификат открытого ключа?

59. В чем заключаются принципы и методы компьютерной стеганографии?

60. Для решения каких задач применяются методы компьютерной стеганографии?

61. В чем разница между криптографией и стеганографией?

62. Что называется провайдером криптографического обслуживания в Windows?

63. На каких принципах строится взаимодействие прикладной программы и криптопровайдера в Windows?

64. Как обеспечиваются в операционной системе аутентичность и целостность криптопровайдера?

65. Что хранится в контейнере ключей пользователя при работе с криптопровайдером в Windows?

66. В чем заключается защита от несанкционированного доступа к документам Microsoft Office?

67. Как обеспечить надежную защиту от несанкционированного доступа к документам Microsoft Office?

68. Как получить электронную подпись для документа Microsoft Office? Как может быть получен сертификат открытого ключа автора документа?

69. Как функционирует шифрующая файловая система операционной системы Windows?

70. Для чего предназначен агент восстановления данных шифрующей файловой системы в Windows? Как обеспечивается возможность восстановления зашифрованных файлов?

71. Какие программы относят к разряду вредоносных?

72. Что такое компьютерный вирус?

73. Какие существуют виды компьютерных вирусов?

74. Какие типы файлов могут заражаться файловыми вирусами?

75. Как происходит заражение программных файлов?

76. Почему файлы документов могут содержать вирусы?

77. Как включить встроенную защиту от вредоносных макросов в программах Microsoft Office? В чем недостатки этой защиты?

78. Какие существуют основные каналы заражения вредоносными программами объектов компьютерной системы?

79. Какие методы автоматического обнаружения и удаления вирусов существуют? В чем их достоинства и недостатки?

80. Как может происходить проникновение программной закладки в компьютерную систему?

81. Какие существуют методы защиты от программных закладок? Что такое изолированная программная среда?

82. Что называется защитой от несанкционированного копирования?

83. На каких принципах должна основываться разработка системы защиты от копирования?

84. Какие требования предъявляются к системам защиты от копирования?

85. Из каких основных компонентов состоит типовая система защиты от копирования?

86. Какие методы могут использоваться для защиты программных средств от изучения алгоритмов их работы?

87. Для чего предназначены методы обфускации и почему они применяются в системах защиты от копирования?

88. В чем достоинства и недостатки программно-аппаратной защиты от копирования на основе электронных ключей?

89. Почему невозможно создание абсолютно надежной системы защиты от копирования?

Вопросы для проведения зачета

1. Проблема защиты информации и подходы к ее решению.

2. Основные понятия защиты информации.

3. Угрозы безопасности и каналы утечки информации.

4. Классификация методов и средств защиты информации.

5. Правовое обеспечение защиты информации.

6. Способы нарушения защищенности информации и защиты от него в компьютерных системах и сетях.

7. Организация базы учетных записей пользователей в современных операционных системах.

8. Способы аутентификации пользователей.

9. Аутентификация пользователей на основе паролей.

10. Аутентификация пользователей на основе модели «рукопожатия».

11. Программно-аппаратная защита от локального несанкционированного доступа («электронный замок»).

12. Аутентификация пользователей на основе их биометрических характеристик.

13. Протокол S/Key.

14. Протокол CHAP.

15. Протокол RADIUS.

16. Протокол Kerberos.

17. Протокол IPSec.

18. Виртуальные частные сети.

19. Разграничение прав пользователей в современных операционных системах.

20. Дискреционное, мандатное и ролевое разграничение доступа к объектам.

21. Подсистема безопасности ОС Windows.

22. Разграничение доступа к объектам в ОС Windows.

23. Разграничение доступа к объектам в ОС Unix.

24. Аудит событий безопасности в современных операционных системах.

25. Средства защиты информации в глобальных компьютерных сетях.

26. Стандарты оценки безопасности компьютерных систем и информационных технологий.

27. Основы алгебры вычетов.

28. Способы симметричного шифрования.

29. Абсолютно стойкий шифр. Генерация, хранение и распространение криптографических ключей.

30. Криптографическая система DES и ее модификации.

31. Криптографическая система ГОСТ 28147-89.

32. Применение и обзор современных симметричных криптосистем.

33. Принципы построения и свойства асимметричных криптосистем.

34. Криптографическая система RSA.

35. Протокол Диффи-Хеллмана.

36. Криптографические системы Эль-Гамаля и эллиптических кривых.

37. Электронная подпись и ее применение.

38. Функции хеширования и способы их построения.

39. Протокол SSL.

40. Криптографические средства современных операционных систем.
41. Файловая система с шифрованием в ОС Windows.
42. Компьютерная стеганография и ее применение.
43. Принципы построения систем защиты от копирования.
44. Защита программных средств от изучения.
45. Вредоносные программы, их признаки и классификация.
46. Методы обнаружения и удаления вредоносных программ.

Критерии оценки за освоение дисциплины определены в Инструктивном письме И-23 от 14 мая 2012 г.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература:

1. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия-Телеком, 2011.

2. Хорев П.Б. Программно-аппаратная защита информации. М.: Форум, 2013.

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: Форум, 2012.

4. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. М.: Академия, 2009.

5. Хорев П.Б. Защита информационных систем. М.: Издательский дом МЭИ, 2010.

Дополнительная литература:

6. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. М.: КноРус, 2013.

7. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2008.

8. Хорев П.Б. Криптографические интерфейсы и их использование. М.: Горячая линия-Телеком, 2007.

9. Галатенко В.А. Стандарты информационной безопасности. – 2-е изд. – М.: Интернет-Ун-т информ. технологий, 2012. – 264 с.