МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»
Кафедра «Информационная безопасность автоматизированных систем»

«УТВЕРЖДАЮ»
проректор по учебной работе
проф. Лобачева Г.В.

_____

ПРОГРАММА
междисциплинарного вступительного экзамена
для поступающих в магистратуру по направлению
10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
Профиль «Безопасность автоматизированных систем»

Программа утверждена на заседании кафедры ИБС
19 сентября 2017 г. протокол № 4
Зав. кафедрой ИБС, руководитель магистерской программы
по профилю _____В.Б. Байбурин

Саратов 2017

Криптографические методы защиты информации

1. Классификация шифров. Простейшие шифры. Композиции шифров.
2. Системы шифрования с секретным и открытым ключами.
3. Хэш – функция. Особенности построения. Виды хэш – функций.
4. Коды аутентичности сообщения.
5. Блочные и поточные шифры.
6. Электронная цифровая подпись. Принципы построения.
7. Алгоритм Диффи – Хелмана.
8. Алгоритм RSA.
9. Криптографические протоколы согласования ключей.
10. Серверы ключей. Система управления ключами Kerberos.

Программно-аппаратные средства защиты информации

11. Основные понятия программно-аппаратной защиты информации.
12. Модели разграничения доступа
13. Механизм замкнутой программной среды
14. Понятие доверительной загрузки операционной системы
15. Программно-аппаратные средства идентификации и аутентификации. Общие понятия. Классификация.
16. Программно-аппаратные средства организации виртуальных частных сетей
17. Общий порядок сертификации средств защиты информации
18. Средства защиты программного обеспечения от несанкционированного использования.
19. Общая характеристика средств нейтрализации компьютерных вирусов.
20. Межсетевые экраны, классификация, требования.

Правовое обеспечение информационной безопасности

21. Информация как объект правового регулирования.
22. Задачи государственной системы информационной безопасности.
23. Понятие и виды защищаемой информации по законодательству РФ.
24. Федеральные законы, регулирующие деятельности в сфере защиты информации.
25. Правовые режимы конфиденциальной информации: содержание и особенности.
26. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
27. Система государственных и отраслевых стандартов России в сфере ИБ.
28. Понятия лицензирования по российскому законодательству. Правовая регламентация лицензионной деятельности в области защиты информации.
29. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации.
30. Аттестация объектов информатизации.
31. Политика информационной безопасности.
32. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
33. Ответственность за правонарушения в области информационной безопасности.

Техническая защита информации

34. Виды, источники и носители защищаемой информации.
35. Концепция и методы инженерно-технической защиты информации.
36. Классификация технической разведки. Возможности видов технической разведки. Основные этапы и процедуры добывания информации технической разведкой

37. Характеристика государственной системы противодействия технической разведке Нормативные документы по противодействию технической разведке.
38. Структура, классификация и основные характеристики технических каналов утечки информации.
39. Визуально-оптический технический канал утечки информации
40. Материально-вещественный технический канал утечки информации
41. Виброакустический технический канал утечки информации
42. Электромагнитный технический канал утечки информации
43. ПЭМиН канал утечки информации
44. Маскировка и шифрование речевой информации в каналах связи.
45. Скрытое получение информации при помощи специальных технических средств.
46. Юридические и технические аспекты классификации и экспертизы СТС
47. Демаскирующие признаки объектов наблюдения и источников опасных сигналов. Скрытие объектов наблюдения
48. Разновидности закладных устройств. Обнаружение и локализация закладных устройств, подавление их сигналов
49. Радиомониторинг. Технические средства для ведения радиомониторинга. Организация радиомониторинга на объекте информатизации
50. Виды контроля эффективности защиты информации. Методы расчета и инструментального контроля показателей защиты информации на объекте информатизации
51. Процедурные вопросы лицензирования объекта информатизации.
52. Организация работы службы (отдела) защиты конфиденциальной информации
53. Применение современных методов защиты конфиденциальной информации. Secure communications by chaotic signals

Безопасность операционных систем

54. Аутентификация: типы и сетевые протоколы. Методы аутентификации в ОС Microsoft Windows 7/8.1/10. Их типичные уязвимости.
55. Структура процессов и потоков, режимы выполнения программного кода.
56. Архитектура операционной системы Microsoft Windows 7.
57. Форматы хешей ОС Microsoft Windows 7/8.1/10.
58. Принцип работы подсистемы безопасности LSA в ОС Microsoft Windows 7/8.1/10 и монитора ссылок безопасности SRM.
59. Механизм авторизации в ОС Microsoft Windows 7/8.1/10. Оценка прав доступа к объектам с наследованием разрешений.
60. Уровни целостности в ОС Microsoft Windows 7/8.1/10. Механизм UAC
61. Обзор протокола Kerberos. Структура билета Kerberos.
62. Аудит безопасности (журналы аудита, настройка аудита в ОС Microsoft Windows 7/8.1/10).
63. Принцип работы и настройки политик ограниченного использования программ. Технология Applocker в ОС Microsoft Windows 7/8.1/10.

Безопасность сетей ЭВМ

64. Основные этапы проведения удаленной атаки на вычислительную сеть. Типы сетевых атак.
65. Клиент-серверная система DNS. Атаки на DNS-серверы. Рекомендации по защите DNS-серверов.
66. Определение топологии сети. Особенности работы утилит tracert и traceroute.
67. Сканирование компьютеров в вычислительной сети. Типы пакетов ICMP. Способы защиты от сканирования сети.
68. Сканирование портов. Типы сканирования. Защита от сканирования портов.

69. Способы определения производителя и версии сетевых служб на удаленном хосте.
70. Протокол SMB в ОС Windows. Уязвимости в протоколе SMB. Возможные меры защиты.
71. Протоколы удаленного управления автоматизированными системами. Возможные меры защиты.
72. Уязвимости сетевой службы службы SNMP. Возможные меры защиты.
73. Способы удаленного подбора паролей к сетевым службам. Возможные меры защиты.
74. Сертифицированные средства автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем, сравнение их возможностей.
75. DDOS-атаки и их современные разновидности. Возможные меры защиты.

Л И Т Е Р А Т У Р А

1. Соломон Д., Руссинович М. Внутреннее устройство Microsoft Windows. Мастер-класс: Пер. с англ. СПб.: Питер; М.: Издательско-торговый дом "Русская редакция", 2014.
2. Девянин П.Н. Модели безопасности компьютерных систем: учеб. пособие для вузов / П.Н. Девянин. - М.: ИЦ "Академия", 2005. - 144 с.
3. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
4. Скембрей Дж., Мак-Клар С. Секреты хакеров. Безопасность Microsoft Windows Server 2003 – готовые решения. – М.: Вильямс, 2004. – 512 с.
5. Дейтел Х.М., Дейтел П.Дж., Чофнес Д.Р. Операционные системы. Основы и принципы: Третье издание. М.: ООО «Бином-Пресс», 2006 г., 1024 с.
6. Побегайло А.П. Системное программирование в Windows. СПб.: БХВ-Петербург, 2006.
7. Мельников В.П. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 5-е изд., стер. - Электрон. текстовые дан. - М.: ИЦ "Академия", 2011. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/Ld_154.pdf
8. Пластун И.Л. Технология построения защищенных автоматизированных систем и сетей [Электронный ресурс]: учеб. пособие / И.Л. Пластун; Саратовский гос. техн. ун-т. - Электрон. текстовые дан. - Саратов : СГТУ, 2010. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 260_10.pdf
9. Губенков А.А. Информационная безопасность вычислительных сетей [Электронный ресурс]: учеб. пособие / А.А. Губенков; Сарат. гос. техн. ун-т (Саратов). - Электрон. текстовые дан. - Саратов: СГТУ, 2009. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 479_09.pdf
10. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие / П. Б. Хорев. - М. : ИЦ "Академия", 2005, 2006, 2007, 2008. - 256 с.
11. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие / П. Б. Хорев. - 4-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с.
12. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 5-е изд., стер. - Электрон. текстовые дан. - М.: ИЦ "Академия", 2011. - 1 эл. опт. диск (CD-ROM). - Режим доступа: http://lib.sstu.ru/books/Ld_154.pdf.
13. Куприянов, А. И. Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с.
14. Пластун, И. Л. Технология построения защищенных автоматизированных систем и сетей : учеб. пособие для студ. спец. 075500, 220400 / И. Л. Пластун ; М-во образования и науки Рос. Федерации, Саратовский гос. техн. ун-т. - Саратов : СГТУ, 2010. - 96 с.