

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Тамбовский государственный университет имени Г.Р.Державина»

Институт математики, физики и информатики

УТВЕРЖДАЮ

Директор института математики,
физики и информатики

Е.С. Жуковский

«15» января 2014 г.

ПРОГРАММА АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

для лиц, поступающих в порядке перевода из других образовательных организаций
высшего образования,

по специальности

«Информационная безопасность»

Квалификация «Бакалавр»

Тамбов 2014

Программа аттестационных испытаний для лиц, поступающих в порядке перевода из других образовательных организаций высшего образования, по специальности «Безопасность информационных технологий в правоохранительной сфере» составлена профессорско-преподавательским составом кафедры «Информатики и информационных технологий» и утверждена на заседании Ученого совета института математики, физики и информатики Тамбовского государственного университета имени Г.Р. Державина.

Протокол № 5 от «15» января 2014 г.

ПЕРЕВОД НА 1 КУРС

Аттестационное испытание по дисциплине «Математика»

СОДЕРЖАНИЕ ПРОГРАММЫ (АННОТАЦИИ ТЕМ)

Введение в математический анализ

Действительные числа. Изображение действительных чисел на прямой. Расширения множества действительных чисел.

Абсолютная величина числа. Целая часть числа. Промежутки. Окрестности.

Произведение отображений, суперпозиция функций. Обратное отображение, обратная функция. Переменная величина.

Функции действительного переменного. График. Способы задания. Некоторые типы функций (ограниченные и неограниченные, монотонные, четные и нечетные, периодические).

Сходящиеся последовательности. Бесконечные пределы. Частичные пределы.

Единственность предела. Ограниченность сходящейся последовательности.

Предел функции в точке.

Предел функции на бесконечности. Бесконечные пределы. Предел суперпозиции.

Теоремы о пределах.

Односторонние пределы. Два замечательных предела:

$$\lim_{x \rightarrow 0} \frac{\sin x}{x}$$

$$\lim_{x \rightarrow 0} (1 + x)^{\frac{1}{x}}$$

Сравнение функций, стремящихся к нулю и бесконечности. Асимптоты.

Непрерывность функции в точке. Непрерывность на множестве. Односторонняя непрерывность. Точки разрыва. Арифметические действия над непрерывными функциями. Непрерывность суперпозиции.

Дифференциальное исчисление

Производная. Геометрический смысл производной. Уравнение касательной.

Механический смысл производной.

Теорема о линейном приближении. Связь дифференцируемости с непрерывностью.

Производные некоторых элементарных функций.

Правила вычисления производных. Производная суперпозиции. Производная обратной функции. Производные высших порядков.

Кривые на плоскости, заданные параметрически. Функции, заданные параметрически.

Их дифференцирование.

Условие постоянства функции. Условие монотонности функции. Максимумы и минимумы. Необходимое условие экстремума. Достаточное условие экстремума.

Нахождение наибольшего и наименьшего значений функции.

Выпуклость. Точки перегиба. Схема исследования функции. Построение графиков.

Дифференциал. Правила вычисления дифференциалов. Дифференциалы высших порядков.

Интегральное исчисление

Первообразная функция. Неопределенный интеграл. Свойства неопределенного интеграла. Таблица интегралов. Замена переменной в неопределенном интеграле.

Интегрирование по частям.

Задача интегрирования в конечном виде. Простые дроби и их интегрирование.

Интегрирование рациональных функций.

Интегрирование некоторых иррациональных функций. Интегрирование некоторых трансцендентных функций.

Интегрируемость непрерывной функции. Интегрируемость функций с конечным числом точек разрыва. Линейность определенного интеграла. Аддитивность (по промежутку) определённого интеграла. Неравенства для определённого интеграла. Теорема о среднем значении.

Векторная алгебра.

Понятие вектора. Коллинеарность, компланарность векторов. Операция умножения вектора на число. Операция сложения векторов. Линейная зависимость и независимость векторов. Скалярное произведение и его свойства. Вычисление скалярного произведения через координаты сомножителей. Работа силы. Векторное произведение и его свойства.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

1. Действительные числа. Абсолютная величина числа.
2. Понятие отображения и функции. График отображения.
3. Функции действительного переменного. Способы задания. График функции.
4. Некоторые типы функций (четные и нечетные, ограниченные,
5. монотонные, периодические).
6. Сходящиеся последовательности. Единственность предела.
7. Бесконечный предел последовательности.
8. Ограниченность сходящейся последовательности.
9. Арифметические действия над сходящимися последовательностями.
10. Сходимость монотонной последовательности.
11. Число «е».
12. Лемма о вложенных отрезках.
13. Предел функции в точке.
14. Предел функции на бесконечности.
15. Первый замечательный предел.
16. Непрерывность функции в точке. Непрерывность функции на множестве.
17. Непрерывность обратной функции.
18. Теорема об ограниченности функции.
19. Правила вычисления производных.
20. Производная суперпозиции функций.
21. Производная обратной функции.
22. Условие постоянства функции.
23. Условие монотонности функции.
24. Максимумы и минимумы функции.
25. Необходимое условие экстремума. Достаточные условия экстремума (без доказательства).
26. Выпуклость. Точки перегиба.
27. Определение дифференциала. Геометрический смысл. Дифференциал суперпозиции. Дифференциалы высших порядков.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

а) основная литература

1. Фихтенгольц Г.М. Основы математического анализа. Т.1,2 М.:Просвещение, 1972.
2. Фихтенгольц Г.М., Курс дифференциального и интегрального исчисления, т 1,2,3, издание любое.

3. Бохан К.А. и др. Курс математического анализа, т.1 М: Просвещение, 1972.
4. Зорич. В.А. Математический анализ ч.1,2 М.: Наука, 1981.
5. Ильин В.А., Позняк Э.Г., Основы математического анализа, ч. II, М.: Наука, 1973
6. Камынин Л.И., Курс математического анализа, т1,.2, МГУ, 1995.
7. Кудрявцев Л.Д., Курс математического анализа, т.1.2, М.,1988.
8. Смирнов В.И., Курс высшей математики, т.2
9. Шилов Г.Е.. Математический анализ. Функции одного переменного. ч.1-2. М.: Наука, 1970.
10. Спивак М., Математический анализ на многообразиях, М.: Мир,1968. 11. Виленкин и др. Сборник задач по математическому анализу. ч.1. М.: Просвещение,1971.
11. Берман Г.Н., Сборник задач по курсу математического анализа, М.: Наука, 1969. Давыдов Н.А. и др. Сборник задач по математическому анализу. М.: Наука, 1971. Демидович Б.П. Сборник задач по курсу математического анализа, М.: 1972.
12. Кудрявцев Л.Д. и др. Сборник задач по математическому анализу. Функции нескольких переменных, СПб.: Кристалл, 1994

ПЕРЕВОД НА 2 КУРС

Аттестационное испытание по дисциплине «Технологии и методы программирования»

СОДЕРЖАНИЕ ПРОГРАММЫ (АННОТАЦИИ ТЕМ)

1. *Краткие сведения о языке программирования Pascal.* Создание простейших программ. Типы данных. Алгоритмические конструкции.
2. *Объекты и классы.* Классы. Поля и методы. Определение доступа к полям и методам. Понятие инкапсуляции.
3. *Работа с классами.* Создание конструкторов и деструкторов. Перегрузка методов.
4. *Наследование.* Понятие наследования. Механизм наследования.
5. *Полиморфизм.* Переопределение свойств и методов.
6. *Работа с Windows API.* Вызов WinAPI функций для работы с параметрами среды. Функции для работы с файлами. Функции для работы с процессами и потоками. Создание оконных приложений.
7. *Визуальное программирование.* Создание оконных приложений. Добавление элементов управления и обработчиков событий.
8. *Работа с базами данных.* Создание и удаление баз данных. Выполнение и обработка запросов к базам данных.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

1. Типы данных.
2. Конструкции ветвления
3. Циклы
4. Создание подпрограмм.
5. Создание классов.
6. Конструкторы и деструкторы.
7. Наследование
8. Полиморфизм
9. Работа с базами данных.
10. Создание оконных приложений средствами WinAPI
11. Работа с процессами, потоками и памятью с помощью Win API
12. Создание оконных приложений с помощью WinAPI
13. Создание оконных приложений с помощью форм.
14. Создание элементов управления и меню в оконных приложениях.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

- а) основная литература
1. Бобровский С.И. Delphi 7. Учебный курс – СПб.:Питер, 2005.
2. Фаронов В.В. Delphi. Программирование на языке высокого уровня. Учебник для вузов–СПб.:Питер, 2009.
3. Фаронов В.В. Турбо Паскаль 7.0. Учебный курс: учебное пособие/В.В.Фаронов.- М.:КНО РУС,2009.
4. Любавин С.А. Програмуємо в TurboDelphi – TurboDelphi для новичков и не только.-М.:ИТ Пресс, 2008.
5. Лаптев В.В. С++. Объектно-ориентированное программирование: Учебное пособие - СПб.:Питер, 2008.

6. Архангельский А.Я. Программирование в Delphi 7. -М.: Бином-Пресс, 2005.

б) дополнительная литература

1. Ван Тассел Д. Стиль, разработка, эффективность, отладка и испытание программы. М., 1981.

2. Кутьин Н. Программирование на ObjectPascal в Delphi 5.0. -СПб.: ВHV-СПб, 2000.

3. Архангельский А. ObjectPascal в Delphi 5. -М.: Бином, 1999.

4. Страуструп Б. Дизайн и эволюция языка С++. -М.: ДМК Пресс, 2000.

5. М.В. Сухарев. Основы Delphi. Профессиональный подход — СПб.: Наука и Техника, 2004.

6. Фридман А. Основы объектно-ориентированной разработки программных систем. -М.: Фин.и стат., 2000.

7. Йордан Э. Структурные модели в объектно-ориентированном анализе и проектировании. -М.: ЛОРИ, 1999.

8. Коуд П. Объектные модели: Стратегии, шаблоны и приложения. -М.: ЛОРИ, 1999.

9. Гофман В., Хоменко А. Delphi 5. -СПб.: ВHV-СПб, 2000.

10. Фридман А. Основы объектно-ориентированного программирования на языке Си++. -М.: РиС, 1999.

в) программное обеспечение и Интернет ресурсы

1. Microsoft PowerPoint, Microsoft Excel

2. Borland Developer Studio.

ПЕРЕВОД НА 3 КУРС

Аттестационное испытание по дисциплине «Защита от вредоносных программ»

СОДЕРЖАНИЕ ПРОГРАММЫ (АННОТАЦИИ ТЕМ)

Классификация компьютерных вирусов. Определение вируса. Проблемы антивирусной защиты информации. Вирусы и их классификация.

Среда обитания и алгоритмы вирусов. Среда обитания вирусов (файловые; загрузочные; макро; сетевые). Особенности алгоритмов работы вирусов (резидентность; использование стелс-алгоритмов; самошифрование и полиморфичность; использование нестандартных приемов). Деструктивные возможности вирусов (безвредные; неопасные; опасные вирусы; очень опасные). Загрузочные вирусы. Алгоритм работы загрузочного вируса. Файловые вирусы. Способы заражения. Алгоритм работы файлового вируса. Макро-вирусы. Word/Excel/Office-вирусы. Алгоритм работы Word макро-вирусов. Алгоритм работы Excel и Access макро-вирусов. Полиморфик-вирусы. Полиморфные расшифровщики. Уровни полиморфизма. Изменение выполняемого кода. Стелс-вирусы.

Троянские программы. Программы шпионы, программные закладки. “Вредные программы”. Хакерские утилиты удаленных компьютеров ("backdoor"). Возможности утилит скрытого администрирования. Троянские кони (логические бомбы) и их деструктивные действия. Программы- шпионы. "Intended" –вирусы. Конструкторы вирусов и полиморфик-генераторы. "Злые шутки" (hoax). Программы- шпионы. Клавиатурные шпионы. Модели программ-шпионов. Программные закладки. Программный шпионаж.

Методы обнаружения и удаления компьютерных вирусов. Способы противодействия компьютерным вирусам. Обезвреживание и удаление известного вируса. Способы обнаружения и удаления неизвестного вируса. Обнаружение резидентного вируса. Windows-вирусы. Обнаружение файлового вируса. Обнаружение макро-вируса.

Профилактика вирусного заражения и уменьшение предполагаемого ущерба. Профилактика вирусного заражения и уменьшение предполагаемого ущерба. Использование специализированных программ.

Антивирусные программные средства. Антивирусные программы. Типы антивирусов. Комплексные средства. Методика использования антивирусных программ. Профилактика заражения компьютера.

Основные правила защиты. Основные правила защиты. Проблема защиты от вирусов. Восстановление пораженных объектов. Защита от программных закладок.

Прогнозы развития вредоносных программ и антивирусного ПО. Прогнозы развития вирусов, троянских программ, программ-шпионов. Рейтинг антивирусных программных средств. Прогнозы развития средств противодействия.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

1. Определение компьютерного вируса.
2. Классификация компьютерных вирусов.
3. Отличительные черты файловых вирусов.
4. Сравнительные характеристики различных файловых вирусов.
5. Способы заражения файловыми вирусами.

6. Принцип размножения файловых червей.
7. Link- вирусы. OBJ и LVB вирусы.
8. Алгоритм работы файловых вирусов.
9. Отличительные черты загрузочных вирусов.
10. Алгоритм работы загрузочных вирусов.
11. Актуальность загрузочных вирусов.
12. Опасность загрузочного вируса.
13. Макро-вирус как особая разновидность вируса.
14. Алгоритм работы макро-вирусов.
15. Отличительные черты полиморфных вирусов.
16. Уровни полиморфизма.
17. Полиморфизм макро-вирусов.
18. Отличительные особенности стелс-вирусов.
19. Способы маскировки стелс-вирусов.
20. Стелс-алгоритм в макро-вирусов.
21. Отличительные черты сетевых вирусов- “червей”.
22. Способы проникновения сетевого вируса в компьютерную систему
23. Алгоритм работы сетевых вирусов.
24. Отличительные черты различных типов троянских коней.
25. Классифицируйте троянские кони.
26. Почтовые троянские программы.
27. Утилиты удаленного управления компьютером (backdoor).
28. Алгоритм работы захватчиков.
29. Основные причины распространенности троянских программ.
30. Программные закладки.
31. Модели воздействия программных закладок на компьютер.
32. Деструктивные действия программных закладок.
33. Способы противодействия компьютерным вирусам.
34. Обезвреживание и удаление известного вируса.
35. Способы обнаружения и удаления неизвестного вируса.
36. Обнаружение резидентного вируса.
37. Обнаружение Windows-вирусов.
38. Обнаружение файлового вируса.
39. Обнаружение макро-вируса.
40. Профилактика вирусного заражения и уменьшение предполагаемого ущерба.
41. Методы защиты от клавиатурных шпионов.
42. Меры противодействия программам шпионам.
43. Антивирусные программы. Типы антивирусов.
44. Методика использования антивирусных программ.
45. Профилактика заражения компьютера. Основные правила защиты.
46. Проблема защиты от макро-вирусов.
47. Восстановление пораженных объектов.
48. Защита от программных закладок.
49. Рейтинг антивирусных программных средств. Прогнозы.
50. Требования к антивирусным программам.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

а) основная литература

1. Прокди Р.Г., Вулф М.М., Разумовский Н.Т. Защита компьютера от вирусов, - М:Наука и техника, 2009, 192 с.

2. Бойцев О. М. Защити свой компьютер на 100 % от вирусов и хакеров, - СПб:Питер, 2008, 288 с.
3. Донцов Д.А. Как защитить компьютер от ошибок, вирусов, хакеров. -СПб:Питер; 2008, 160 с.
4. Скляров И.С. Хакерские фишки, -М:Лори, 2008, 384 с.
5. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации, - М:Academia, 2008, 256 с.
6. Касперский Е. В., Компьютерное зловредство, Изд - Питер, 2007г, 207с.
7. Касперски К., Компьютерные вирусы изнутри и снаружи, Изд - Питер, 2007г, 526с.

б) дополнительная литература

1. Зайцев О.В. ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита, -СПб:BHV, 2006, 304 с.
2. Собейкис В.Г. Азбука хакера 3. Компьютерная вирусология , -М:Майор, 2006, 512 с.
3. Моисеев Н. А. Развитие вирусов и антивирусов. – М.: Просвещение, 2002. – 402с.
4. Прокопенко К. Л. Вирусы и антивирусы. – С-Пб.: Синтег, 2003. – 275 с.
5. Федоров Е. Л. Вирусы в 21 веке. С-Пб.:Знание, 2003. – 371с.

в) программное обеспечение и Интернет ресурсы

1. УМК “Защита компьютерных систем от деструктивных программ”.
2. Электронный обучающий ресурс «Методы выявления уязвимых мест и принципы построения систем защиты программного обеспечения».
3. Электронный обучающий ресурс «Сканеры безопасности».
4. Электронный обучающий ресурс «Антивирусы. Учебно-методический комплекс».
5. Электронный обучающий ресурс «Комплексные средства защиты компьютерных систем: лабораторный практикум».
6. Электронный обучающий ресурс «Защита компьютерной системы посредством программного межсетевоего экрана прикладного уровня».
7. Поиск по сайтам Лаборатории Касперского [электронный ресурс]. – Режим доступа <http://www.kaspersky.ru/>

ПЕРЕВОД НА 4 КУРС

Аттестационное испытание по дисциплине

«Программно-аппаратные средства защиты информации»

СОДЕРЖАНИЕ ПРОГРАММЫ (АННОТАЦИИ ТЕМ)

Предмет и задачи программно-аппаратной защиты информации. Предмет и задачи программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации.

Системы идентификации. Программно-аппаратная идентификация субъекта. Понятие протокола идентификации. Идентифицирующая информация.

Защита данных от несанкционированного доступа. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа и разграничение доступа. Иерархический доступ к информационным ресурсам. Защита сетевого ресурса. Протоколирование доступа к файлам.

Доступ к данным со стороны процесса. Процессы и данные. Способы фиксации факта доступа. Надежность систем ограничения доступа. Защита файлов от модификации. Электронная цифровая подпись.

Программно-аппаратные средства шифрования. Построение аппаратных компонент криптозащиты данных. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратного средства криптозащиты.

Методы и средства ограничения доступа к компонентам ЭВМ. Ограничение доступа к компонентам ЭВМ. Защита программ от несанкционированного копирования. Пароли и ключи. Организация хранения ключей.

Защита программ от изучения. Общие принципы защиты от изучения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям.

Защита от разрушающих программных воздействий. Деструктивные программы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия предупреждения разрушающего воздействия. Понятие изолированной программной среды.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

1. Предмет и задачи программно-аппаратной защиты информации.
2. Предмет и задачи программно-аппаратной защиты информации.
3. Классификация методов и средств программно-аппаратной защиты информации.
4. Идентификация.
5. Идентификация субъекта.
6. Понятие протокола идентификации.
7. Идентифицирующая информация.
8. Защита данных от несанкционированного доступа.
9. Основные подходы к защите данных от несанкционированного доступа.

10. Шифрование.
11. Контроль доступа и разграничение доступа.
12. Иерархический доступ к файлу.
13. Защита сетевого файлового ресурса.
14. Фиксация доступа к файлам.
15. Доступ к данным со стороны процесса.
16. Процессы и данные.
17. Способы фиксации факта доступа.
18. Надежность систем ограничения доступа.
19. Защита файлов от изменения.
20. Электронная цифровая подпись.
21. Программно-аппаратные средства шифрования.
22. Построение аппаратных компонент криптозащиты данных.
23. Защита алгоритма шифрования.
24. Принцип чувствительной области и принцип главного ключа.
25. Необходимые и достаточные функции аппаратного средства криптозащиты.
26. Методы и средства ограничения доступа к компонентам ЭВМ Ограничение доступа к компонентам ЭВМ.
27. Защита программ от несанкционированного копирования.
28. Пароли и ключи.
29. Организация хранения ключей.
30. Защита программ от изучения.
31. Общие принципы защиты от изучения.
32. Защита от отладки.
33. Защита от дизассемблирования.
34. Защита от трассировки по прерываниям.
35. Защита от разрушающих программных воздействий.
36. Компьютерные вирусы как особый класс разрушающих программных воздействий.
37. Необходимые и достаточные условия недопущения разрушающего воздействия.
38. Понятие изолированной программной среды.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

а) основная литература

1. Фленов М.Е. Компьютер глазами хакера. 2-е изд., СПб:ВНУ, 2009, 352 с.
2. Бернет С., Пэйн С. Официальное руководство RSA Security, -М: Бином, 2009, 384 с.
3. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации, - М:Academia, 2008, 256 с.
4. Складов И.С. Хакерские фишки, -М:Лори, 2008, 384 с.
5. Сердюк В.А. Новое в защите от взлома корпоративных систем, -М:Техносфера, 2007, 360 с.
6. Кэрриэ Брайан, Криминалистический анализ файловых систем, - СПб:Питер, 2007, 480 с.

б) дополнительная литература

1. Панов А. Реверсинг и защита программ от взлома, -М: ВНУ, 2006, 256 с.
2. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности, -М:Academia, 2006, 240 с.
3. Байбурин В.Б., Бровкина М.Б. и др. Введение в защиту информации – М.: ФОРУМ: ИНФРА-М, 2004 -128 с.

4. Форд Дж. Ли, Персональная защита от хакеров: Руководство для начинающих, Пер. с англ., Изд - КУДИЦ-Образ, 2002г, 272с.
5. Лукацкий А. Обнаружение атак, 2-е издание. Киев: БХВ, 2002, 608 стр.
6. Хогланд, Грег, Мак-Гроу, Гари – Взлом программного обеспечения: анализ и использование программного кода.: Перевод с английского – М.: Издательский дом «Вильямс», 2005 – 400с.: ил.
7. Левин М., Как стать хакером: Интеллектуальное руководство по хакингу и фрикингу, Изд - Новый издательский дом, 2005г, 319с.
8. Митник К.Д. Искусство вторжения, Пер. с англ., Изд - ДМК Пресс, 2005г, 279с.

в) программное обеспечение и Интернет ресурсы

1. УМК “Специальное и прикладное программное обеспечение. Блок 1. Шпионское программное обеспечение, руткиты, программные закладки: обнаружение и нейтрализация”.
2. УМК “Моделирование систем защиты информации. Блок 2. Формальные модели безопасности”.
3. УМК “Криптографическая защита информации. Блок 2. Блочные методы”.
4. УМК “Криптографическая защита информации. Блок 3. Поточковые методы”.
5. УМК “Криптографическая защита информации. Блок 4. Ассиметричные методы”.
6. УМК «Программно-аппаратная защита информации. Блок 1. Теоретические и практические аспекты защиты программного обеспечения на основе уникальных характеристик рабочей среды конечного пользователя».
7. УМК «Программно-аппаратная защита информации. Блок 2. Изолированные программные среды».
8. УМК «Программно-аппаратная защита информации. Блок 3. Защита программ от изучения: защита от активной отладки».
9. УМК «Программно-аппаратная защита информации. Блок 4. Защита программ от изучения: защита от дизассемблирования».
10. УМК «Программно-аппаратная защита информации. Блок 5. Защита программ от изучения: теоретические и технические аспекты выявления работы защищённого приложения в аномальных и искусственных средах».
11. Электронный обучающий ресурс «Методы выявления уязвимых мест и принципы построения систем защиты программного обеспечения».
12. Электронный обучающий ресурс «Принципы создания и работы защищенных приложений».
13. Электронный обучающий ресурс «Слагаемые степени защищенности корпоративных автоматизированных систем».
14. Электронный обучающий ресурс «Анализаторы уязвимостей в программном коде удаленных компьютерных систем».
15. Электронный обучающий ресурс «Защита корпоративных серверов от атаки методом SQL-инъекций».
16. Электронный обучающий ресурс «Защита компьютерной системы посредством программного межсетевого экрана прикладного уровня».
17. Электронный обучающий ресурс «Распределенный анализ стойкости парольных подсистем сервисов POP3, SMTP, FTP» .
18. Электронный обучающий ресурс «Создание ложной цели для удаленного злоумышленника».
19. Электронный обучающий ресурс «Защита информации на основе программно-аппаратных средств».