МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Сибирский государственный аэрокосмический университет
имени академика М.Ф. Решетнева»
(СибГАУ)**

УТВЕРЖДАЮ
Проректор по НИД
_____ Ю.Ю. Логинов
_____ 2017 г.

ПРОГРАММА

ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОСТИ

Направление подготовки:	10.06.01	Информационная безопасность
	шифр	*наименование*
Профиль подготовки:	Методы и системы защиты информации, информационная безопасность	
	наименование	
Форма обучения:	Очная, заочная	
Квалификация выпускника	Исследователь. Преподаватель-исследователь.	
Кафедра-разработчик рабочей программы	Безопасность информационных технологий	

Красноярск 2017

Введение

Целью учебного курса «Методы и системы защиты информации, информационная безопасность» является формирование у аспирантов основополагающего представления о проблемах разработки, совершенствования и применения методов и различного рода средств защиты информации в процессе сбора, хранения, обработки, передачи и распространения информации, а также обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации.

Учебный курс «Методы и системы защиты информации, информационная безопас-ность» позволяет получить знания, охватывающие совокупность проблем, связанных с ис-следованием, разработкой, совершенствованием и применением моделей, методов, техно-логий, средств и систем зашиты информации, а также обеспечением информационной безопасности объектов и процессов обработки, передачи информации во всех сферах дея-тельности от внешних и внутренних угроз.

Задачи учебной дисциплины «Методы и системы защиты информации, информаци-онная безопасность» предусматривают изучение современного состояния науки и научной деятельности в России и за рубежом в области защиты информации, информационной безопасности..

1. Избранные разделы математики.

Линейная алгебра. Понятия группы, кольца, поля, их основные свойства. Основы теории конечных полей. Кольца вычетов. Кольцо многочленов над конечным полем.

Основные понятия теории вероятностей и математической статистики. Вероятностное пространство. Условная вероятность и независимость. Последовательность независимых испытаний. Цепи Маркова. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции. Сходимость последовательностей случайных величин и сходимость распределений. Закон больших чисел. Центральная предельная теорема. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.

Конечные автоматы. Граф перехода автомата. Эксперименты с автоматами. Графы и орграфы. Перечисление графов и отображений. Алгоритмические задачи на графах.

2. Вычислительная техника и программирование.

Архитектура современной ЭВМ. Основные принципы работы ее отдельных компонент. Устройство персонального компьютера: центральный процессор, структура памяти, структура ввода-вывода.

Программный интерфейс вычислительной системы. Языки программирования низкого и высокого уровня. Компиляторы и интерпретаторы. Технология объектно-ориентированного программирования.

Операционные системы. Функции ядра операционной системы. Функции защиты информации. Однопользовательская операционная система MS DOS. Однопользовательская многозадачная операционная система Windows. Многопользовательские многозадачные операционные системы Unix, Windows NT.

Локальные и глобальные вычислительные сети. Типовые конфигурации сети. Протоколы обмена данными. Маршрутизация сообщений в сети.

Системы управления базами данных. Реляционная, иерархическая и сетевая модели. Распределенные базы данных в сетях ЭВМ.

3. Защита информации.

Основные принципы современной концепции обеспечения защиты информации. Исходные предположения о возможностях злоумышленника. Требования к защите с позиции пользователя. Основные методы защиты информации. Методология организации и проведении работ по разработке и анализу средств защиты информации.

Роль законодательного и организационного обеспечения защиты информации. Законы Российской Федерации, составляющие основу правовой базы защиты информации в стране. Особенности российского законодательства в части защиты государственной тайны, коммерческой

тайны и авторских прав. Порядок лицензирования и сертификации деятельности в области зашиты информации

Математические модели формальной теории защиты информации. Угрозы информации и политика безопасности. Классификация систем защиты. Стандарты в области защиты информации в вычислительной системе, "Оранжевая книга" США, российские стандарты.

Криптографические методы зашиты информации. Основные понятия криптографии. Исторические шифры. Теоретическая, практическая и временная стойкость системы криптографической защиты. Криптографические параметры узлов и блоков шифрующих автоматов. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования. Системы асимметричного шифрования, открытый ключ, электронная подпись. Вопросы генерации и распределения ключей. Методология обоснования надежность криптографической защиты.

Защита информации от технической разведки. Основные физические каналы утечки информации о функционировании информационной системы Узлы и блоки оборудования информационнойсистемы, уязвимые для технической разведки. Технические параметры современных средств перехвата побочных сигналов. Методы и средства зашиты от инженерно-технической разведки. Методика оценки качества инженерно-технической защиты.

Особенности защиты информации в вычислительной системе. Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника. Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит). Защита информации в локальных и глобальных вычислительных сетях и ее особенности. Роль и задачи администратора вычислительной системы и службы безопасности.

Разрушающие программные воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействий. Классификация вирусов. Методы выявления и защиты от вирусов. Изолированные программные среды. Защита программных продуктов от изменения и контроль целостности, зашита от изучения.

Методика анализа алгоритмов защиты программных реализаций информационных систем. Методы восстановления алгоритмов защиты в программных продуктах Оценка уровня криптографической защиты типовых программных продуктов. Анализ особенностей выработки и распределения ключей. Анализ возможности внедрения криптографических закладок. Экспресс-анализ защищенности сетевого компьютера от удаленных атак через сеть.

Вопросы для экзамена:

1) Линейная алгебра. Понятия группы, кольца, поля, их основные свойства.
2) Основы теории конечных полей. Кольца вычетов. Кольцо многочленов над конечным полем.
3) Основные понятия теории вероятностей и математической статистики.
4) Вероятностное пространство.
5) Условная вероятность и независимость. Последовательность независимых испытаний.
6) Цепи Маркова.
7) Случайные величины и их характеристики: функция распределения, моменты, характеристические функции. Сходимость последовательностей случайных величин и сходимость распределений.
8) Закон больших чисел. Центральная предельная теорема.
9) Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
10) Конечные автоматы. Граф перехода автомата. Эксперименты с автоматами.
11) Графы и орграфы. Перечисление графов и отображений.
12) Алгоритмические задачи на графах.
13) Архитектура современной ЭВМ. Основные принципы работы ее отдельных компонент.
14) Устройство персонального компьютера: центральный процессор, структура памяти, структура ввода-вывода.
15) Программный интерфейс вычислительной системы.
16) Языки программирования низкого и высокого уровня. Компиляторы и интерпретаторы.
17) Технология объектно-ориентированного программирования.

18) Операционные системы.
19) Функции ядра операционной системы. Функции защиты информации.
20) Однопользовательская операционная система MS DOS.
21) Однопользовательская многозадачная операционная система Windows.
22) Многопользовательские многозадачные операционные системы Unix, Windows NT.
23) Локальные и глобальные вычислительные сети. Типовые конфигурации сети.
24) Протоколы обмена данными. Маршрутизация сообщений в сети.
25) Системы управления базами данных. Реляционная, иерархическая и сетевая модели.
26) Распределенные базы данных в сетях ЭВМ.
27) Основные принципы современной концепции обеспечения защиты информации. Исходные предположения о возможностях злоумышленника.
28) Требования к защите с позиции пользователя. Основные методы защиты информации.
29) Методология организации и проведении работ по разработке и анализу средств защиты информации.
30) Роль законодательного и организационного обеспечения защиты информации. Законы Российской Федерации, составляющие основу правовой базы защиты информации в стране.
31) Особенности российского законодательства в части защиты государственной тайны, коммерческой тайны и авторских прав.
32) Порядок лицензирования и сертификации деятельности в области зашиты информации
33) Математические модели формальной теории защиты информации.
34) Угрозы информации и политика безопасности.
35) Классификация систем защиты.
36) Стандарты в области защиты информации в вычислительной системе, "Оранжевая книга" США, российские стандарты.
37) Криптографические методы зашиты информации. Основные понятия криптографии.
38) Исторические шифры. Теоретическая, практическая и временная стойкость системы криптографической защиты.
39) Криптографические параметры узлов и блоков шифрующих автоматов.
40) Методы получения псевдослучайных последовательностей.
41) Современные поточные и блочные алгоритмы шифрования.
42) Системы асимметричного шифрования, открытый ключ, электронная подпись. Вопросы генерации и распределения ключей.
43) Методология обоснования надежность криптографической защиты.
44) Защита информации от технической разведки. Основные физические каналы утечки информации о функционировании информационной системы
45) Узлы и блоки оборудования информационной системы, уязвимые для технической разведки.
46) Технические параметры современных средств перехвата побочных сигналов.
47) Методы и средства зашиты от инженерно-технической разведки.
48) Методика оценки качества инженерно-технической защиты.
49) Особенности защиты информации в вычислительной системе. Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника.
50) Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит).
51) Защита информации в локальных и глобальных вычислительных сетях и ее особенности.
52) Роль и задачи администратора вычислительной системы и службы безопасности.
53) Разрушающие программные воздействия.
54) Компьютерные вирусы как особый класс разрушающих программных воздействий. Классификация вирусов.
55) Методы выявления и защиты от вирусов.
56) Изолированные программные среды.
57) Защита программных продуктов от изменения и контроль целостности, зашита от изучения.
58) Методика анализа алгоритмов защиты программных реализаций информационных систем.
59) Методы восстановления алгоритмов защиты в программных продуктах.

60) Оценка уровня криптографической защиты типовых программных продуктов.
61) Анализ особенностей выработки и распределения ключей.
62) Анализ возможности внедрения криптографических закладок.
63) Экспресс-анализ защищенности сетевого компьютера от удаленных атак через сеть.

А) Основная литература:

1) Борисов М.А. Основы организационно-правовой защиты информации : учеб. пособие / М. А. Борисов, О. А. Романов. - 3-е изд., перераб. и доп. - Москва : ЛЕНАНД, 2014. - 248 с.

2) Золотарев, В. В. Управление информационной безопасностью : учеб. пособие : в 3 ч. / сост. Е. А. Данилова. - Красноярск : СибГАУ. – 2010. Ч. 1 : Анализ информационных рисков. - 144 с.

3) Крук, Б. И. Телекоммуникационные системы и сети : учеб. пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; ред. В. П. Шувалов. - 4-е изд., испр. и доп. - Москва : Горячая линия-Телеком. – 2013. Т. 1 : Современные технологии. - 620 с. ил.

4) Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства : учеб. пособие / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2008. - 544 с.

5) Жданов О.Н. Методы и средства криптографической защиты информации : учеб. пособие / О. Н. Жданов, В. В. Золотарев. - Красноярск : СибГАУ, 2008. - 256 с.

Б) Дополнительная литература:

1) Жданов О.Н. Алгоритмы блочного шифрования : учеб. пособие / О. Н. Жданов, Т. А. Чалкин, Д. М. Чурмантаев. - Красноярск : СибГАУ, 2010. - 172 с.

2) Жуков В. Г. Беспроводные локальные сети стандартов IEEE 802.11a/b/g : учеб. пособие / В. Г. Жуков. - Красноярск : СибГАУ, 2010. - 128 с.

3) Ищейнов В. Я. Защита конфиденциальной информации : учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2009. - 256 с. : ил.

4) Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. - Москва : Форум : ИНФРА-М, 2013. - 416 с.

5) Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В. Ф. Шаньгин. - Москва : Форум : ИНФРА - М, 2013. - 592 с.

6) Инновационные направления современных международных отношений : учеб. пособие / ред.: А. В. Крутских, А. В. Бирюков. - Москва : Аспект-Пресс, 2010. - 295 с.

7) Информационные технологии : учебник / ред. В. В. Трофимов. - Москва : Юрайт, 2011. - 624 с. : ил.

8) Мельников В.П. Информационное обеспечение систем управления : учебник / В. П. Мельников. - Москва : Академия, 2010. - 336 с. : ил.

9) Федотова Е. Л. Информационные технологии и системы : учеб. пособие / Е. Л. Федотова. - Москва : Форум, 2011. - 352 с. : ил.

10) Макарова Н.В. Информатика : учебник / Н. В. Макарова, В. Б. Волков. - Санкт-Петербург : "Питер", 2011. - 576 с.