МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра вычислительной техники и защиты информации

УТВЕРЖДАЮ

Проректор по учебной работе

_____ Зарипов Н.Г.

«02» 09 2015 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОГО МОДУЛЯ

«Методы и системы защиты информации, информационная безопасность»

Направление подготовки кадров высшей квалификации

10.06.01 Информационная безопасность

Программа

Методы и системы защиты информации, информационная безопасность

Квалификация выпускника

Исследователь. Преподаватель-исследователь

Форма обучения – очная

Уфа 2015

Содержание

1. Место дисциплины в структуре образовательной программы

Модуль «Методы и системы защиты информации, информационная безопасность» является дисциплиной вариативной части общеобразовательной программы.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки научно-педагогических кадров высшей квалификации (аспирантура) 10.06.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 30.07.2014 г. N 874 и приказа Министерства образования и науки Российской Федерации от 30.04.2015 N 464 "О внесении изменений в федеральные государственные образовательные стандарты высшего образования (уровень подготовки кадров высшей квалификации)". Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Целью освоения дисциплины «Методы и системы защиты информации, информационная безопасность» в соответствии с общими целями основной профессиональной образовательной программы является: ознакомление с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов, а также формирование знаний, умений и владений в соответствии с компетентностной моделью, представленной в основной профессиональной образовательной программе по направлению подготовки научно-педагогических кадров высшей квалификации (аспирантура).

Основными задачами изучения дисциплины являются:

а) овладение теоретическими, практическими и методическими вопросами классификации угроз информационным ресурсам;

б) ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;

в) изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;

г) приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;

д) формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

Дисциплина «Методы и системы защиты информации, информационная безопасность» является обязательной дисциплиной вариативной части блока 1 ОПОП. Предшествующими дисциплинами учебного плана аспирантуры являются дисциплины базовой части блока 1 – Иностранный язык и История и философия науки, а также вариативной части блока 1 – Психология и педагогика, Методика работы над литературными источниками. Дисциплина «Методы и системы защиты информации, информационная безопасность» служит основой для последующего изучения разделов ОПОП блока 1 – Дисциплины по выбору, блока 2 – Практики, Блока 3 – Научные исследования, блока 4 – ГИА, а также формирования профессиональной компетентности в профессиональной области, связанной с обеспечением информационной

безопасности в том числе критически важных объектов, а также использованием существующих и разработкой новых методов и систем защиты информации.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), сформировавшего данную компетенцию
1	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	Базовый	Методика работы над литературными источниками
2	Способность проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки	УК-2	Повышенный	История и философия науки
3	Готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	УК-4	Повышенный	Иностранный язык

*- ***пороговый уровень*** *дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;*

-базовый уровень *позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;*

-повышенный уровень *предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.*

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность;	ОПК-1	Базовый	Дисциплина по выбору
2	Способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;	ОПК-2	Базовый	Дисциплина по выбору
3	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;	ОПК-3	Пороговый	Научно-исследовательская практика
4	Способность принимать эффективные проектные решения в условиях неопределенности и риска для задач обеспечения информационной безопасности	ПК-1	Базовый	Научные исследования
5	Способность разрабатывать новые и исследовать существующие защитные механизмы и средства обеспечения информационной безопасности	ПК-2	Базовый	Научные исследования

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине «Методы и системы защиты информации, информационная безопасность»:

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность;	ОПК-1	цели исследования, основные методологические подходы исследования процессов обеспечения информационной безопасности; общие принципы и закономерности в построении, функционировании и развитии, управлении и моделировании процессов обеспечения информационной безопасности	использовать методологии и методы научного исследования на уровнях теоретического познания и эмпирического исследования, использования общелогических методов и приемов исследования;	системными правилами выявления причин нарушения системных принципов функционирования объектов в области обеспечения информационной безопасности
2	Способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;	ОПК-2	научных основ развития теории, создания, внедрения и эксплуатации перспективных объектов профессиональной деятельности	аккумулировать имеющийся опыт исследований, синтезировать усовершенствованные решения в самостоятельной научно-исследовательской деятельности с использованием современных информационно-коммуникационных технологий	навыком оценки состояния развития перспективного научного направления по имеющейся информации; формализации знаний; выявления проблем существующих методов исследования в области профессиональной деятельности
3	Способность обоснованно оценивать степень	ОПК-3	действующие стандарты в области информационно	анализировать логику различного рода суждений; формировать	критического восприятия информации; обоснования

	соответствия защищаемых объектов информатизации и информацион-ных систем действующим стандартам в области инфор-мационной безопасности;		й безопасности; Критерии, устанавливаю-щие степень соответствия защищаемых объектов стандартам информационно й безопасности	требования защиты объектов информатизации и информационных систем;	оценки степени защищенности объектов информатизации и информационных систем;
4	Способность принимать эффективные проектные решения в условиях неопределенност и и риска для задач обеспечения информацион-ной безопасности	ПК-1	основные организационны е и правовые методы обеспечения безопасности информационны х систем; современные методы защиты локальной и удаленной вычислительных сетей; методы анализа безопасности информационны х систем с использованием отечественных и зарубежных стандартов в области информацион-ной безопасности; методы организации работы коллектива по проведению научных исследований в области информацион-ной безопасности.	разрабатывать и исследовать методы защиты локальной и удаленной вычислительных сетей; проводить анализ безопасности информационных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности; разрабатывать математические модели отдельных средств защиты информации, а также модели безопасности защищаемых информационных систем в целом; проводить обоснование и выбор рационального решения по уровню защищенности информационной системы с учетом заданных требований; разрабатывать предложения по совершенствованию управления безопасностью	навыками применения организационных и правовых мер для обеспечения безопасности информационных систем; навыками применения современных методов защиты локальной и удаленной вычислительных сетей; навыками разработки формальных моделей политик безопасности, политик управления доступом и информационным и потоками в информационных системах; методами анализа безопасности информационных систем с использованием отечественных и зарубежных стандартов в области информационной безопасности; навыками организации работы коллектива по проведению

				информационных систем и сетей; организовать работу коллектива по проведению научных исследований в области информационной безопасности; адаптировать и обобщать результаты современных исследований.	научных исследований в области информационной безопасности; методами адаптации и обобщения результатов современных исследований.
5	Способность разрабатывать новые и исследовать существующие защитные механизмы и средства обеспечения информацион-ной безопасности	ПК-2	современные методы и средства защиты информации при ее передаче и хранении; существующие защищенные протоколы обмена информацией; современные методы исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкциониров анного доступа в информационны е системы, обнаружения вредоносных программ; формальные модели политик безопасности, политик управления доступом и ин-формационными потоками в информацион-ных системах.	обосновывать выбор методов защиты информации при ее передаче и хранении, защищенные протоколы обмена информацией; выявлять возможности совершенствования научных методов и алгоритмов исследования свойств сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированн ого доступа в информационные системы, обнаружения вредоносных программ.	навыками применения существующих защищенных протоколов обмена информацией; современными методами исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкционирован ного доступа в информационные системы, обнаружения вредоносных программ; современными методами и средствами защиты информации при ее передаче и хранении.

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 9 зачетных единиц (324 часа).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.		
	2 семестр	3 семестр	4 семестр
Лекции (Л)	4	6	
Практические занятия (ПЗ)	6	8	
Лабораторные работы (ЛР)	–	–	–
КСР	–	–	–
Курсовая проект работа (КР)	–	–	–
Расчетно - графическая работа (РГР)	–	–	–
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	89	85	62
Подготовка и сдача экзамена	–	–	20
Подготовка и сдача зачета	14	20	
Вид итогового контроля (зачет, экзамен)	зачет	зачет с оценкой	экзамен

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов				Литература, рекомендуемая аспирантам	Виды интерактивных образовательных технологий**
		Аудиторная работа		СРС	Всего		
		Л	ПР				
1	**Введение в дисциплину.** Характеристика учебной дисциплины, ее место и роль в системе знаний, связь с другими дисциплинами. Краткая историческая справка. **Раздел 1. Концепция информационной безопасности.** Тема №1. Актуальность информационной безопасности. Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Тема №2. Лицензирование и сертификация в области защиты информации. Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования. Тема №3. Основные нормативные руководящие документы. Международные стандарты информационного обмена. Критерии безопасности компьютерных	2	2	40	44	6.1, №8	Лекция классическая, проблемное обучение

	систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.						
	Раздел 2. Угрозы информации. Тема №4. Информационная безопасность сетей. Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ. Тема №5. Способы совершения компьютерных преступлений. Тема №6. Уязвимость сети Интернет. Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.	2	4	49	55	6.1, №4 6.1, №5 6.1, №9	Лекция классическая, проблемное обучение
	Раздел 3. Виды возможных нарушений безопасности информационной системы. Тема №7. Компьютерные преступления. Классификация компьютерных преступлений. Виды противников или «нарушителей». Тема №8. Вредоносные программы. Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам. Тема №9. Вирусы. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.	2	4	40	46	6.1, №3 6.1, №1	Проблемная лекция, лекция-визуализация, проблемное обучение

	Раздел 4. Информационная безопасность информационных систем. Тема №10. Теория информационной безопасности информационных систем. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Тема №11. Криптографические способы защиты информации. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись. Тема №12. Организация информационной безопасности компании. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.	4	4	45	53	6.1, №1 6.1, №6 6.1, №7	Проблемная лекция, лекция-пресс-конференция, проблемное обучение

	Раздел 5. Методы и средства защиты компьютерной информации. Тема №13. Обеспечения информационной безопасности. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Тема №14. Контроль доступа к информации. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Тема №15. Методы и средства защиты информации. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Тема №16. Антивирусное ПО. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.	4	6	62	72	6.1, №2 6.1, №10	Проблемная лекция, лекция-пресс-конференция, проблемное обучение

Занятия, проводимые в интерактивной форме, составляют 30 % от общего количества аудиторных часов по дисциплине «Методы и системы защиты информации, информационная безопасность».

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Лицензирование и сертификация в области защиты информации. Основные нормативные руководящие документы.	2
2	2	Информационная безопасность сетей. Способы совершения компьютерных преступлений. Уязвимость сети Интернет.	4
3	3	Компьютерные преступления. Вредоносные программы. Вирусы.	4
4	4	Теория информационной безопасности информационных систем. Криптографические способы защиты информации.	4
5	5	Обеспечения информационной безопасности Контроль доступа к информации. Методы и средства защиты информации. Антивирусное ПО.	4
6	5	Установка и настройка программного антивирусного комплекса	2

4. Учебно-методическое обеспечение самостоятельной работы аспирантов

Раздел 1. Концепция информационной безопасности.

Вопросы для самостоятельного изучения (подготовке к обсуждению):

1. Компьютерные преступления, законодательные и нормативные документы.
2. Правила функционирования системы лицензирования.
3. Правовое обеспечение защиты информации в России и за рубежом.
4. Руководящие документы Гостехкомиссии.
5. Международные стандарты информационного обмена.
6. Критерии безопасности компьютерных систем. «Оранжевая книга».
7. Правовое регулирование защиты персональных данных в РФ.

Раздел 2. Угрозы информации.

Вопросы для самостоятельного изучения:

1. Угрозы безопасности информации и их классификация.
2. Государственная система защиты информации, обрабатываемой техническими средствами.
3. Требования к защите информации, оценка возможностей противоборствующей стороны.
4. Методология разработки и анализа средств защиты.
5. Классические модели защиты информации.
6. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

Расчетные задания:

1. Определение класса сети.
2. Вычисление адреса сети, широковещательного адреса по имеющемуся IP.
3. Определение количества сетевых узлов, хостов, подсетей.

Раздел 3. Виды возможных нарушений безопасности информационной системы.
Вопросы для самостоятельного изучения:

1. Обобщенная структура IP-сети. Сетевые ресурсы.
2. 2. Классы каналов связи. Основы IP-адресации и маршрутизации.
3. 3. Технические и программные средства сетевой передачи данных и сегментации сети.
4. Характеристика объекта информатизации (выделенного помещения), как объекта защиты от технических разведок.
5. 2. Цели и задачи защиты информации от утечки по техническим каналам (технической защиты информации).
6. 3. Характеристики и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
7. Исследование параметров радиоканала системы перехвата речевой информации.
8. 2. Основные технические характеристики средств акустической разведки. Методика применения средств акустической разведки.
9. Разновидности вредоносных программ

Практические задания:

1. Основные технические характеристики систем пространственного и линейного электромагнитного зашумления. Разработка рекомендаций по установке систем пространственного и линейного электромагнитного зашумления для защиты объектов информатизации.
2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных.
3. Разработка документов, регламентирующих порядок обработки персональных данных.
4. Лицензирование деятельности по защите ПДн.
5. Сертификация средств защиты информации.
6. Аттестация ИСПДн.
7. Биометрическая аутентификация.

Раздел 4. Информационная безопасность информационных систем.

Вопросы для самостоятельного изучения:

1. Способы восстановления работоспособности операционных систем.
2. Резервное копирование и восстановление данных.
3. Аварийное восстановление системы.
4. Аппаратные и механические средства защиты ПЭВМ
5. 2. Электронные ключи
6. 3. Аппаратный модуль доверенной загрузки «Соболь»
7. Обзор средств криптографической защиты конфиденциальной информации.
8. Средства криптографической защиты конфиденциальной информации DioNIS FW 16000 КВ2.
9. Функции защиты DioNIS FW.
10. Изучение стандартов шифрования AES и Rjndael
11. Настройка криптографических функций. Работа с ключевой информацией.
12. Фильтры. Стратегии формирования фильтров
13. Трансляция адресов (NAT). Настройка NAT-обработчика

Практические задания:

1. Настройка защитных механизмов ОС Windows 7 (XP)
2. Настройка защитных механизмов ОС Unix
3. Настройка защитных механизмов ОС Linux
4. Разработка политики аудита в СЗИ Secret Net.

5. Настройка и управление аудитом в СЗИ Secret Net.
6. Просмотр и управление журналами аудита.
7. Использование сканеров безопасности;
8. Подключение криптомаршрутизатора DioNIS FW 16000 КВ2 к TCP/IP-сетям. Конфигурирование ODI-интерфейса.
9. Настройка функций маршрутизации DioNIS FW 16000 КВ2
10. Фильтры. Стратегии формирования фильтров
11. Трансляция адресов (NAT). Настройка NAT-обработчика
12. Установка и настройка совместной работы КриптоПро CSP, ПКСЗИ ШИПКА, Rutoken, eToken

Раздел 5. Методы и средства защиты компьютерной информации.

Вопросы для самостоятельного изучения:

1. Механизм защиты входа в систему.
2. Полномочное и избирательное разграничение доступа.
3. Организационные вопросы защиты программ и данных компьютерных систем и сетей.
4. 2. Цели, функции и задачи защиты информации в сетях ЭВМ.
5. 3. Современные средства обеспечения информационной безопасности вычислительных сетей.
6. Сканеры безопасности;
7. Защита от внешних атак.;
8. Внутренняя безопасность.
9. Понятие электронной подписи.
10. Взаимосвязь между протоколами аутентификации и электронной подписи.
11. Хэш - функция и ее использование в системах электронной подписи. Схемы ЭП.

Практические задания:

1. Хеш-функция MD2.
2. Однонаправленные (односторонние) функции с секретом и их применение.
3. Составление протокола проверок объекта защиты в соответствии с требованиями информационной безопасности.
4. Проведение аттестации объекта защиты по вариантам
5. Конфигурирование комплексной системы защиты информации
6. Стандарт цифровой подписи DSS.
7. Обобщенная модель электронной цифровой подписи.
8. Схема Диффи-Хеллмана, схема Эль-Гамаля.
9. Цифровая подпись на основе алгоритма RSA.
10. Стандарт цифровой подписи DSS.
11. Генерация цифровой подписи.
12. Проверка цифровой подписи.

5. Фонд оценочных средств

Оценка уровня освоения дисциплины осуществляется в виде текущего и промежуточного контроля успеваемости аспирантов университета, и на основе критериев оценки уровня освоения дисциплины.

Контроль представляет собой набор заданий и проводится в форме контрольных мероприятий по оцениванию фактических результатов обучения аспирантов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

– учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине и пр.);

– степень усвоения теоретических знаний;

– уровень овладения практическими умениями и навыками по всем видам учебной работы;

– результаты самостоятельной работы.

Активность обучающегося на занятиях оценивается на основе выполненных работ и заданий, предусмотренных ФОС дисциплины.

Оценивание проводится преподавателем независимо от наличия или отсутствия обучающегося (по уважительной или неуважительной причине) на занятии. Оценка носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период.

№ п/п	**Контролируемые разделы (темы) дисциплины**	Код контролируемой компетенции (или ее части)	Уровень освоения, определяемый этапом формирования компетенции	Наименование оценочного средства*
1	Раздел 1. Концепция информационной безопасности.	ПК-1	Базовый	ЗПР, Т
2	Раздел 2. Угрозы информации.	ОПК-3	Пороговый	ЗПР, Т, ДС
3	Раздел 3. Виды возможных нарушений безопасности информационной системы.	ПК-2	Базовый	ЗПР, ДЗ, КА
4	Раздел 4. Информационная безопасность информационных систем.	ОПК-2	Базовый	ЗПР, ДЗ, КА
5	Раздел 5. Методы и средства защиты компьютерной информации.	ОПК-1	Базовый	ЗПР, ДЗ, КА

** Планируемые формы контроля: защита практической работы (ЗПР), домашнего задания (ДЗ) написание доклада/сообщения (ДС), тестирование, собеседование (Т), кейс-анализ (КА), контрольная работа (КР) и т.д.*

Вопросы к зачету

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.

2. Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.

3. Шифры замены и перестановки. Моно- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.

4. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.

5. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.

6 Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.

7. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.

8. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.

9. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.

10. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования.

11. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

12. Теория сложности вычислений. Классификация алгоритмов.

13. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.

14. Криптосистема Эль-Гамаля.

15. Электронная подпись. Варианты электронной подписи на основе алгоритмов RSA и Эль-Гамаля.

16. Хэш-функции и их применение. Хеш-функция MD2.

17. Однонаправленные (односторонние) функции с секретом и их применение.

18. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамаля.

19. Цифровая подпись на основе алгоритма RSA.

20. Стандарт цифровой подписи DSS. Генерация цифровой подписи. Проверка цифровой подписи.

21. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Протоколы аутентификации с использованием nonce и временны́х меток.

22.Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования. Протокол обмена сеансовыми ключами. Вскрытие "человек-в-середине". Протокол "держась за руки".

23. Сертификация ключей с помощью цифровых подписей. Разделение секрета. Метки времени. Пример протокола защиты базы данных.

24. Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Вижинера, использующей простой XOR.

25. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.

Критерии оценки:

– оценка «Зачет» выставляется аспиранту, показавшему систематическое знание учебно-программного материала, умение правильно выполнять задания, предусмотренные программой, усвоившему учебный материал литературы по дисциплине, рекомендованной в учебной программе по дисциплине, способному к самостоятельному пополнению и обновлению своих знаний в ходе дальнейшей учебы и профессиональной деятельности.

– оценка «Незачет» выставляется аспиранту, обнаружившему пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки при ответе на зачете, не владеющему материалом в объеме, необходимом для дальнейшей учебы и профессиональной деятельности по специальности. Как правило, оценка «неудовлетворительно» ставится аспирантам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по данной дисциплине.

Вопросы к экзамену

1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.
2. Безопасность информационных ресурсов и документирование информации
3. персональные данные о гражданах

4. Вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации
5. Российское законодательство по защите информационных технологий
6. Правовая защита программного обеспечения авторским правом.
7. Проблемы защиты информации в информационных системах.
8. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах
9. защита локальных сетей и операционных систем;
10. Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.
11. Содержание системы средств защиты компьютерной информации в информационных системах.
12. Защищенная информационная система и система защиты информации;
13. законодательная, нормативно-методическая и научная база системы защиты информации.
14. Требования к содержанию нормативно-методических документов по защите информации;
15. Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры;
16. Политика безопасности:
17. Программно-технические методы и средства защиты информации;
18. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера;
19. Типы несанкционированного доступа и условия работы средств защиты
20. Симметричные криптосистемы: основные понятия и определения;
21. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.
22. Изучение американского стандарта шифрования данных DES;
23. Отечественный стандарт шифрования данных; режим простой замены;
24. Режим гаммирования; режим гаммирования с обратной связью;
25. Режим выработки имитовставки; блочные и поточные шифры.
26. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.
27. Концепция криптосистемы с открытым ключом;
28. Криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе);
29. Схема шифрования Полига—Хеллмана;
30. Схема шифрования Эль-Гамаля.
31. Методы идентификации и проверки подлинности пользователей компьютерных систем. проблема аутентификации данных и электронная цифровая подпись;
32. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов;
33. Отечественный стандарт хэш-функции;
34. Алгоритм цифровой подписи RSA;
35. Алгоритм цифровой подписи Эль-Гамаля (EGSA);
36. Алгоритм цифровой подписи DSA;
37. Отечественный стандарт цифровой подписи.
38. Защита компьютерных систем от удаленных атак через сеть Internet.
39. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.
40. Программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО;
41. Защита от НСД со стороны сети; абонентское шифрование и ЭЦП;

42. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).
43. Классификация способов защиты; защита от отладок и дизассемблирования;
44. способы встраивания защитных механизмов в программное обеспечение;
45. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.
46. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах;
47. Список практических вопросов и задач на экзамене по дисциплине
48. Алгоритмы шифрования последовательности блоков методами DES, ГОСТ 28147-89 во всех режимах;
49. Алгоритмы многораундового шифрования блока методами DES, ГОСТ 28147-89 во всех режимах;
50. Операции, применяемые для шифрования блока в раунде методами DES, ГОСТ 28147-89;
51. Алгоритмы шифрования блока в раунде методами DES, ГОСТ 28147-89;
52. Алгоритмы выработки ключа для шифрования блока в раунде методами DES, ГОСТ 28147-89;
53. Операции в конечном поле GF(28) (умножение, сложение и т.д.);
54. Алгоритм многораундового шифрования методом Rijndael;
55. Алгоритм раундового преобразования при шифровании Rijndael;
56. Операции раундового преобразования и их реализация;
57. Алгоритм выработки раундовых ключей при шифровании Rijndael;
58. Выработка открытого ключа для шифрования алгоритмом RSA. Алгоритм шифрования и подписывания методом RSA;
59. Определение секретного ключа по открытому ключу в алгоритме RSA. Алгоритмы определения взаимной простоты чисел (e и n) и поиска обратного элемента e-1 mod n;
60. Алгоритм поиска примитивных элементов в поле GF(P). Алгоритм Диффи-Хэллмана выработки общего секретного ключа.

Задачи на экзамене:

1. Выработать открытый ключ для шифрования алгоритмом RSA;
2. Зашифровать и подписать открытый текст (ОТ) методом RSA;
3. Определить секретный ключ по открытому ключу в алгоритме RSA;
4. Определить взаимную простоту чисел (e и n) и найти обратный элемент e-1 mod n;
5. Найти (доказать примитивность) примитивный элемент в поле GF(P);
6. Выработать общий секретный ключ по алгоритму Диффи-Хэллмана;
7. Методы поиска и сбора информации.
8. Методика устранения компьютерной информации.
9. Уязвимости Windows.
10. Уязвимости UNIX
11. Защита от копирования переносных носителей.
12. Аппаратные ключи защиты.
13. Современные криптосистемы
14. Виды шифров. Методика кодирования
15. Антивирусное программное обеспечение.
16. Особенности защиты информации при работе в сети.
17. Безопасная работа в Internet.
18. Целесообразность усиления обороны.
19. Защита от побочного электромагнитного излучения и наводок
20. Алгоритмы распределения ключей.

Критерии оценки:

Баллы (рейтинговой оценки)	**Оценка экзамена (стандартная)**	**Требования к знаниям**
92 – 100	*«отлично»*	Оценка «отлично» выставляется аспиранту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, владеет разносторонними навыками и приемами выполнения практических задач по формированию общепрофессиональных компетенций.
75 - 91	*«хорошо»*	Оценка «хорошо» выставляется аспиранту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, а также имеет достаточно полное представление о значимости знаний по дисциплине.
61 – 74	*«удовлетво-рительно»*	Оценка «удовлетворительно» выставляется аспирантуу, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает сложности при выполнении практических работ и затрудняется связать теорию вопроса с практикой.
менее 61	*«неудовлет-ворительно»*	Оценка «неудовлетворительно» выставляется аспиранту, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как

		правило, оценка «неудовлетворительно» ставится аспирантам, которые не могут продолжить обучение без дополнительных занятий по данной дисциплине.

Типовые оценочные материалы

1) Вопросы для собеседования.

Раздел 1. Концепция информационной безопасности.

Вопрос 1. Критерии безопасности компьютерных систем.

- Понятие оценочного стандарта.
- Основные положения "Оранжевой книги".
- Руководящие документы Гостехкомиссии России

Вопрос 2. Международные стандарты информационной безопасности.

- Стандарт ISO/IEC 15408 "Общие критерии".
- Описание требований безопасности и характеристик угроз
- Классы функциональных требований.

Вопрос 3. Общие принципы построения защищенных информационных систем

- Понятие информационных систем.
- Цели защищенных информационных систем
- Концепция "Защищенные информационные системы. Информационный документ корпорации Microsoft."

Вопрос 4. Средства разработки ИС и правила их реализации.

- Основные средства, методика их реализации.
- Проблемы, возникающие при построении защищенных информационных систем.
- Технические и социальные аспекты.

Вопрос 5. Защищенные информационные технологии.

- Защита архитектуры «Клиент - сервер»
- Защита каналов связи в интернет
- Интегральные устройства защиты информации.

2) Тестирование

Раздел 2. Угрозы информации.

Примеры вопросов тестов.

Задание 1.

В *каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?*

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

Задание 2.

Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;

5. все вышеперечисленные средства.

Задание 3.

В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взлома» и/или несанкционированного внесения изменений.

Задание 4.

Естественные угрозы безопасности информации вызваны:

1.деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

Задание 5.

Хакер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 6.

Активный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 7.

Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;
2. фишинг;

3. нигерийские письма;
4. источник слухов;
5. пустые письма.

Задание 8.

По среде обитания классические вирусы разделяются:

1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

Задание 9.

Шифрование методом подстановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

Задание 10.

Метод защиты информации ограничение доступа заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления; 2. в создании физической замкнутой преграды с организацией доступа лиц, связанных
с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

Задание 11.

Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

Задание 12.

Спам, периодически проводящий рассылки не рекламных сообщений:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

Задание 13.

Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от …

1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

Задание 13.

Попытка одного субъекта выдать себя за другого - это:

1. пассивная атака;
2. модификация потока данных»
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

Задание 14.

В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:

1. должностное лицо;
2. терминал;
3. распечатка;
4. форма и размеры лица;
5. оператор.

Задание 15.

Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

Критерии оценки результатов тестирования:

Оценка (стандартная)	Оценка (тестовые нормы: % правильных ответов)
«отлично»	92-100 %
«хорошо»	75-91%
«удовлетворительно»	61-74%
«неудовлетворительно»	менее 6 1%

3) Кейс-задача

Разделы:

4 «Информационная безопасность информационных систем» и

5 «Методы и средства защиты компьютерной информации».

Кейс – это пакет заданий, индивидуальных или групповых, которые очерчивают реальную проблему, не имеющую единственного и очевидного решения. Для поисков оригинального выхода аспирант должен проанализировать проблемную ситуацию, используя знания по изучаемой дисциплине, предложить решения и обосновать выбор именно этих вариантов. Применение кейс-метода позволяет развивать навыки работы с разнообразными источниками информации, а также компетентностные качества личности (аналитические, практические, творческие, коммуникативные, социальные умения).

Методика выполнения кейс-задания включает в себя следующие этапы: индивидуальная самостоятельная работа аспирантов с материалами кейса (идентификация проблемы, формулировка ключевых альтернатив, предложение решения или рекомендуемого действия); работа в малых группах по согласованию видения ключевой проблемы и ее решений; презентация и проверка результатов малых групп на общей дискуссии.

Примеры заданий

Задание 1.

Необходимо построить защищенное соединение между двумя компьютерами. Приведите отчет с результатами выполнения и описанием произведенных действий.
Архитектура защищенного канала может быть:

- сервер-клиент
- клиент-клиент

Задание 2.

Необходимо настроить защищенный обмен между двумя пользователями при помощи криптографических и стеганографических контейнеров. Приведите отчет с результатами выполнения и описанием произведенных действий.

Задание 3.

Необходимо построить централизованную инфраструктуру открытых ключей. Удостоверяющим центром являетесь вы. Необходимо создать не менее двух пользователей, а также сформировать список отозванных сертификатов. Приведите отчет с результатами выполнения и описанием произведенных действий.

Задание 4.

Даны некоторые ценные документы. Необходимо их подписать с помощью цифровой подписи и подготовить их для передачи предварительно зашифровав. Приведите отчет с результатами выполнения и описанием произведенных действий.

Критерии оценки:

- оценка «отлично» выставляется аспиранту, если он аргументировал выполнение задания, подтверждая знание материала, и сделал выводы по проделанной работе;
- оценка «хорошо» выставляется аспиранту, если он аргументировал только некоторые этапы выполнения задания;
- оценка «удовлетворительно», если задачи выполнены без обоснования применения необходимых действий;
- оценка «неудовлетворительно», если задание не выполнено.

Критерии оценки:

Оценка	В рамках формируемых компетенций аспирант демонстрирует
Неудовлетворительно	продемонстрировано знание и понимание теоретического содержания курса со значительными пробелами, несоответствующими компетенциям, формируемым при изучении данной дисциплины
Удовлетворительно	знание и понимание теоретического содержания курса с незначительными пробелами; несформированность некоторых практических умений при применении знаний в конкретных ситуациях, низкое качество выполнения учебных заданий (не выполнены, либо оценены числом баллов, близким к минимальному); низкий уровень мотивации учения;
Хорошо	полное знание и понимание теоретического содержания курса, без пробелов; недостаточную сформированность некоторых практических умений при применении знаний в конкретных ситуациях; достаточное качество выполнения всех предусмотренных программой обучения учебных заданий (ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками); средний уровень мотивации учения;
Отлично	полное знание и понимание теоретического содержания курса, без пробелов; сформированность необходимых практических умений при применении знаний в конкретных ситуациях, высокое качество выполнения всех предусмотренных программой обучения учебных заданий (оценены числом баллов, близким к максимальному); высокий уровень мотивации учения.

4) Типовые задания.
Раздел 3. Виды возможных нарушений информационной системы.
Раздел 5. Методы и средства защиты компьютерной информации

Вариант № 1 Организация криптографической защиты почтовых сообщений, а также сообщений передаваемых с помощью online-служб (ICQ, Miranda и др.)
Вопросы:
1. В чем преимущество использования передачи зашифрованного сообщения
2. По какому алгоритму происходит шифрование данных?
3. Что такое электронно-цифровая подпись (ЭЦП)?
4. Какой алгоритм используется в данной программе?
5. Назовите назначение использование ЭЦП?
6. В чем отличие ЭЦП от алгоритма шифрования?

Вариант № 2 Криптографической системы PGP
Вопросы:
1. В чем преимущество использования передачи зашифрованного сообщения.
2. По какому алгоритму происходит шифрование данных?
3. Что такое электронно-цифровая подпись (ЭЦП)?
4. Какой алгоритм используется в данной программе?
5. Назовите назначение использование ЭЦП? 6.
В чем отличие ЭЦП от алгоритма шифрования?

Вариант № 3 Криптографическая защита информации от несанкционированного использования на персональных компьютерах, ноутбуках и сменных носителях
Вопросы:
1. В чем преимущество хранения данных в зашифрованном виде?
2. По какому алгоритму происходит шифрование данных?
3. Какие алгоритмы используется в данной программе?

Вариант № 4 Обеспечение информационной безопасности посредствам разграничения доступа к ресурсам в операционной системы Windows NT
Вопросы:
1. Охарактеризуйте существующие модели разграничения доступа?
2. Перечислите плюсы и минусы существующих моделей разграничения доступа?
3. Создайте папку «исследование» и для ограниченного пользователя назначьте атрибут «только просмотр», локально.
4. Повторите тоже самое задание для сетевого варианта.

Вариант № 5 Обеспечение сетевой безопасности посредствам встроенного файрвола в систему Windows NT
Вопросы:
1. Заблакируйте все сетевые сеансы
2. Настройти запретительные правила для протокола POP3.

Вариант № 6 Ограничение доступа к различным компьютерным ресурсам с использованием программного продукта Win Lock Professional 4.5.
Вопросы:
1. Ограничьте работу пользователя ПК по времени.
2. Запретите использование флеш-носителей.

Вариант № 7 Формирование групповой политики информационной безопасности: Active Directory
Вопросы:
1. Сфорируйте домен рабочей группы.
2. Сформируйте шаблон безопасности.

Вариант № 8 Программная виртуализация гостевой операционной системы на примере программного продукта Virtualbox
Вопросы:
1. Как монтировать раздел диска или CD-ROM?
2. Возможно ли внутри виртуальной машины запустить еще одну виртуальную машину?

Вариант № 9 Организация VPN соединения стандартными средствами Windows Server 2003
Вопросы:
1. Каковы назначения VPN соединения
2. Установите взломостойкий пароль для подключения к VPN соединению.

Критерии оценки:

Оценка	**В рамках формируемых компетенций аспирант демонстрирует**
Неудовлетворительно	продемонстрировано знание и понимание теоретического содержания курса со значительными пробелами, несоответствующими компетенциям, формируемым при изучении данной дисциплины
Удовлетворительно	знание и понимание теоретического содержания курса с незначительными пробелами; несформированность некоторых практических умений при применении знаний в конкретных ситуациях, низкое качество выполнения учебных заданий (не выполнены, либо оценены числом баллов, близким к минимальному); низкий уровень мотивации учения;
Хорошо	полное знание и понимание теоретического содержания курса, без пробелов; недостаточную сформированность некоторых практических умений при применении знаний в конкретных ситуациях; достаточное качество выполнения всех предусмотренных программой обучения учебных заданий (ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками); средний уровень мотивации учения;

Отлично	полное знание и понимание теоретического содержания курса, без пробелов; сформированность необходимых практических умений при применении знаний в конкретных ситуациях, высокое качество выполнения всех предусмотренных программой обучения учебных заданий (оценены числом баллов, близким к максимальному); высокий уровень мотивации учения.

5) Темы докладов/сообщений.

Раздел 2. Угрозы информации.

1. Стоимостные характеристики информации и их соотношения.
2. Internet как среда для компьютерных преступлений.
3. Основные задачи информационной безопасности.
4. Основные методы обеспечения защиты информационной системы.
5. Определение и классификация угроз.
6. Потенциальные противники: классификация и характеристика.
7. Каналы утечки информации.
8. Классификация атак и их характеристики.
9. Сетевые атаки: основные виды.
10. Формулирование основных положений информационных положений.
11. Принципы обеспечения информационной безопасности.
12. Формальные модели доступа к данным.
13. Монитор безопасности и его функции.
14. Политика безопасности информационных систем
15. Таксономия нарушений информационной безопасности вычислительной системы.
16. Уровни правового обеспечения информационной безопасности.
17. Доктрина информационной безопасности России.
18. Задачи и методы криптографии.
19. Виды шифров. Принцип Керкхоффса.
20. Основные криптографические протоколы.
21. Модели основных криптоаналитических атак.
22. Основные аппаратные средства защиты. Основные программные средства защиты.
23. Основные методы идентификации и аутентификации.
24. Сервисы управления доступом.
25. Протоколирование и аудит. Задачи аудита.
26. Основы защиты Internet-подключений.
27. Вирусы. Виды вирусов.
28. Антивирусное программное обеспечение.
29. Стандарты обеспечения информационной безопасности.
30. Общие принципы построения защищенных систем.

Критерии оценки:

- оценка «отлично» выставляется аспиранту, если тема сообщения раскрыта полностью и даны верные ответы на дополнительные вопросы;
- оценка «хорошо» выставляется аспиранту, если тема сообщения раскрыта не полностью, но с помощью наводящих вопросов аспирант смог дать верные ответы на дополнительные вопросы;
- оценка «удовлетворительно» выставляется аспиранту, если тема сообщения раскрыта не полностью или даны неверные ответы на дополнительные вопросы;
- оценка «неудовлетворительно», если аспирант не выполнил задание или его работа не соответствует заданию.

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная литература

1. Обеспечение информационной безопасности. Под редакцией А.П. Курило. М. Альпина, 2011. – 364 с.

2. Безопасность Oracle глазами аудитора: нападение и защита. А.М. Поляков. М. ДМК, 2012. – 432 с.

3. Аверченков В. И. Организационная защита информации: учебное пособие для вузов 3-е изд., стер. - М.: Флинта, 2011. 224 с. - http://www.biblioclub.ru

4. Гафнер В.В. Информационная безопасность. Учебное пособие. – М.: Феникс, 2013. – 324 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность. (Изд.:3). – М.: ФОРУМ, 2011. – 432 с.

6. Гашков С.Б. Криптографические методы защиты информации. – М: Академия, 2014 – 304 с.

7. Петров А.А. Компьютерная безопасность. Криптографические методы защиты информации - М.: Академия, 2010 – 448 с.

8. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. — М.Форум:Инфра - М, 2012. — 591 с.

9. Радько, Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев.– М,: Издательство: РадиоСофт, 2010. -232с.

10. Андрончик, А.Н. Защита информации в компьютерных системах: практический курс. Учеб. пособие /А.Н. Андрончик, В.В., Н.А. Домуховский и др.; под ред. Н.И. Синадского. - Екатеринбург, УГТУ-УПИ, 2012. - 224с.

6.2 Дополнительная литература

1. Максим М. , Поллино Д. Безопасность беспроводных сетей - М.: ДМК Пресс, 2012. - 283 с. - http://www.biblioclub.ru

2. Торстейнсон П.Криптография и безопасность в технологии .NET./П. Торстейнсон, Г.А. Ганеш, пер. с англ.- М: БИНОМ. Лаборатория знаний, 2013. – 479с.: ил.

3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. -СПб.:БХВ – Петербург, 2009 – 576 с.

4. Зозуля, Ю. Windows 7 на 100%. - СПб: Питер, 2014. – 432 с.

5. Росенко, А.П. Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование. - М.: Красанд , 2014. - 240 с.

6. Чипига, А.Ф. Информационная безопасность автоматизированных систем. - М.: Гелиос АРВ, 2010. - 336 с.

7. Новиков, А. Обеспечение защиты персональных данных Обеспечение защиты персональных данных. / А. Новиков, А. Рогачев, И. Баймакова. – М.: 1С-Паблишинг, 2010. - 216 с.

8. Ватаманюк, А.И. Создание и обслуживание сетей в Windows 7. - СПб: Питер, 2010. – 224 с.

9. Станек, У. Windows 7 для продвинутых. Настройка, работа и администрирование. - СПб.: Питер, 2010. - 576 с.

10. Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия. - М.:Интернет-университет информ.технологий, 2011. – 531 с.

Периодические издания:

1. БДИ: Безопасность, Достоверность, Информация
2. Безопасность информации
3. Бизнес и безопасность в России
4. Вопросы защиты информации (Всероссийский научно-исследовательский институт межот-

раслевой информации)
5. Делопроизводство (ЗАО «Бизнес-Школа «Интел-Синтез»)
6. Документоведение, документационное обеспечение управления (библиографический указатель и экспресс-информация ОЦНТИДАД ВНИИДАД ГАС РФ)
7. Защита информации. Конфидент
8. Мир безопасности
9. Системы безопасности (Компания «Гротек»)
10. Секретарское дело (ЗАО «Бизнес-Школа «Интел-Синтез»)
11. Секьюрити
12. Телохранитель
13. Частный сыск, охрана, безопасность (Интерпол Москва, Издательский дом «Мир безопасности»)
14. Records Management Quarterly
15. Security Management
16. Security Industry and Product News

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

1. «Asterisk». Раздел «Безопасность телекоммуникационных систем» http://www.asterisk.by/node/819
2. «Публикации по информационной безопасности сетей». http://daily.sec.ru/publication.cfm?rid=45&pid=7681
3. . «Информзащита»; http://www.infosec.ru/
4. «Информационная безопасность» http://www.itsec.ru/articles2/focus/doverie-i-bezopasn-osnovn-tendenc-v-razvitii-sotrudnich-v-rss
5. IKSMEDIA.RU Он-лайн. Электронный журнал». http://www.iks-media.ru/articles/2357972.html
6. «Обеспечение информационной безопасности телекоммуникационных систем и сетей электросвязи» http://www.tsogu.ru/media/files/2011/01_28/210709.pdf
7. «Защищенные системы связи» http://spo.hiik.ru/zcc/
8. «Радио и связь» http://www.radiosv.ru/books_k.htm
9. ФСТЭК России www.fstec.ru
10. www.securitylab.ru
11. www.cyberpol.ru
12. www.azi.ru
13. www.infotecs.ru
14. www.infosec.ru
15. www.infoforum.ru
16. www.cnews.ru
17. ww.brighttalk.com
18. www.coresecurity.com
19. r-a-permyakov.blogspot.com
20. www.ancud.ru
21. www.lancrypto.ru
22. www.pgp.com
23. www.rsa.com.
24. www.infosec.ru
25. www.confident.ru

26. www.cobra.ru
27. www.accord.ru
28. www.cobra.ru
29. www.aladdin.ru
30. www.guardant.ru
31. www.microsoft.com
32. msdn.microsoft.com
33. www.citforum.ru
34. www.unixware.ru
35. www.osp.ru
36. www.infotecs.ru
37. www.checkpoint.com
38. www.elvis.ru

Лицензионное программное обеспечение:

- межсетевой экран Infotecs Personal Firewall;
- сканер уязвимостей Microsoft BaseLine Analyzer;
- сканер сетевой безопасности GFI LanGuard (демо-версия);
- сканер уязвимостей ISS Internet Scanner (демо-версия);
- средство анализа защищенности «Сканер-ВС»(версия для учебных заведений»;
- система комплексного анализа информационной безопасности MaxPatrol;
- сканер безопасности XSpider 7.8;
- система защита информации на компьютерах, съемных носителях и внешних устройствах Infowatch Endpoint Security;
- распределенный межсетевой экран для управления доступом внутри защищаемой сети Trust Access;
- комплексное решение для защиты информации от интернет угроз и вредоносных программ на сетевых рабочих местах Security Studio Endpoint Protection;
- средство защиты информации от несанкционированного доступа и контроля выполнения ИБ-политик для виртуальных инфраструктур на базе VMware vSphere и Microsoft Hyper-V VGate;
- проактивное средство обнаружения хакерских вторжений и несанкционированного доступа к информации Security Studio Honeypot Manager;
- программное обеспечение шифрования и генерации ключей для MSDOS Crtools 3.01;
- программное обеспечения Криптон API функций прикладного программирования Криптон;
- программное обеспечение Crypton Emulator эмулятора криптоплаты ;
- программное обеспечение шифрования и генерации ключей для Windows «Криптон-шифрование»;
- программное обеспечение Криптон- подпись;
-программное обеспечение шифрования в офисных программах Crypton Word;
- программное обеспечение создания защищенных прозрачных дисков «Индис» (демо-версия);
- программное обеспечение создания защищенных прозрачных дисков «Криптосейф» (демо-версия);
- программное обеспечение прозрачного шифрования «Strong Disk» (демо-версия);
- программное обеспечение прозрачного шифрования «ViPNeT SafeDisk» (демо-версия);
- программное обеспечение шифрования файлов «ViPNeT DISCGuise» (демо-версия);
- программное обеспечение ассиметричного шифрования для MSDOS CrSoft;
- программное обеспечение формирования электронной подписи «Криптон-Подпись»;
- программное обеспечение асимметричного шифрования фирмы Lan Crypto «Криптоофис»(демо-версия);
- программный пакет ассиметричного шифрования PGP (демо-версия);
- стеганографическая программа Stools;
- стеганографическая программа JSteg;
- стеганографический пакет Steganos Privacy Suite (пробная версия);

- система защиты информации Secret Net (пробная версия);
- система защиты информации Dallas Lock (демо-версия);
- система защиты информации «Аккорд Win 32»;
- система защиты информации «Страж»;
- DLP система «Device Lock» (демо-версия);
- контур информационной безопасности SearchInform (демо-версия»);
- программный пакет SystemInternals;

6.4 Методические указания к практическим занятиям

Практические занятия являются обязательным компонентом учебного процесса, который является дополнением к лекционной форме обучения и предназначается для более углубленной проработки тем, затронутых на лекции.

Как правило, темы практических занятий включают в себя вопросы курса, для обсуждения которых требуется специальная подготовка аспирантов и соискателей с использованием рекомендуемой учебной литературы, источников и лекций. Методической особенностью практических занятий по данному курсу является применение двух основных форм работы с аспирантами и соискателями:

1) аудиторной – в виде выступления или устного обсуждения изучаемых тем;

2) самостоятельной – включающей изучение лекционного материала, учебной, монографической литературы и первоисточников, подготовку и написание реферата и докладов.

Подготовку к практическому занятию следует вести в следующем порядке:

1. Внимательно ознакомиться с планом практического занятия, списком рекомендуемой литературы;
2. Прочитать конспект лекций по теме практического занятия;
3. Обратиться к рекомендуемой учебной литературе по данной теме;
4. Внимательно изучить и постараться усвоить основные понятия изучаемой темы, так как эффективное освоение курса невозможно без владения специальной терминологией;
5. В ходе изучения темы практического занятия необходимо подготовить тезисы или конспект в тетради для практических занятий. Особенно это касается вопросов, предназначенных для самостоятельного изучения. Эти записи могут быть использованы на практических занятиях как подсказка при публичном выступлении.

Работу с литературой следует начинать с анализа списка рекомендуемой литературы по дисциплине, перечисленного в рабочей программе. Каждая тема из разделов тематического плана дисциплины и каждый вид занятий снабжен ссылками на источники литературы, что значительно упрощает поиск необходимой информации. Выбрав нужный источник, следует найти интересующий раздел по оглавлению или алфавитному указателю, а также одноименный раздел конспекта лекций или учебного пособия. В случае возникших затруднений в понимании учебного материала следует обратиться к другим источникам, где изложение может оказаться более доступным. Необходимо отметить, что работа с литературой не только полезна как средство более глубокого изучения любой дисциплины, но и является неотъемлемой частью профессиональной деятельности будущего исследователя.

6.5 Методические разработки к практическим занятиям

1. Криптоанализ симметричных алгоритмов на основе частотного анализа. Сост. В.Е.Кладов. – Уфа, 2015. –21 с.
2. Криптоанализ алгоритма шифрования на основе линейного генератора случайной последовательности. Сост. В.Е.Кладов. – Уфа, 2015. –27 с.
3. Исследование криптоалгоритма AES. Сост. В.Е.Кладов. – Уфа, 2015. –20 с.
4. Аппаратные и программные средства симметричного шифрования фирмы «Криптон». Сост. В.Е.Кладов. – Уфа, 20152015. –37 с.
5. Российские программные средства ассиметричной криптографии: лабораторный практикум. Сост. В.Е.Кладов. – Уфа, 2015. –32 с.

6. Система защиты информации от несанкционированного доступа «Secret Net 5.0-С Сост. В.Е.Кладов. – Уфа, 2015. –30 с.
7. Система защиты информации от несанкционированного доступа «Страж NT». Сост. В.Е.Кладов. – Уфа, 2015. –28 с.
8.Защита информационных процессов в операционных системах Windows 2000/XP. Субъект доступа. Сост. В.Е.Кладов. – Уфа, 2015. – 43 с.
9. Защита информационных процессов в операционной системе Windows 2000/XP. Защита файлов и каталогов с помощью файловой системы NTFS Сост. В.Е.Кладов. – Уфа, 2015. – 35 с.
10. Защита компьютеров с помощью межсетевых экранов при работе в Интернет. Сост. В.Е.Кладов. – Уфа, 2015. – 39 с.

7. Указания по освоению дисциплины

Приступая к изучению дисциплины, необходимо в первую очередь ознакомиться с содержанием рабочей программы дисциплины.

Лекции имеют целью дать систематизированные основы научных знаний о методах и средствах защиты информации. При изучении и проработке теоретического материала необходимо:

- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в рабочей программе литературные источники4
- ответить на контрольные вопросы по теме;
- при подготовке к текущему контролю и к промежуточной аттестации использовать материалы ФОС;

Практические занятия проводятся с целью углубления и закрепления знаний, полученных на лекциях и в процессе самостоятельной работы над нормативными документами, учебной и научной литературой. При подготовке к практическому занятию необходимо:

- изучить, повторить теоретический материал по заданной теме;
- повторить типовые задания, выполняемые в аудитории.

Рекомендации по работе с научной и учебной литературой

Работа с учебной и научной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на практических занятиях, к контрольным работам, тестированию, зачету и экзамену. Она включает проработку лекционного материала и изучение рекомендованных источников и литературы по тематике лекций.

Конспект лекций должен содержать реферативную запись основных вопросов лекции, предложенных преподавателем схем (при их демонстрации), основных источников литературы по темам, выводы по каждому вопросу. Конспект должен быть выполнен в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки. Конспекты научной литературы при самостоятельной подготовке к занятиям должны быть выполнены также аккуратно, содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим аспирантом.

В процессе работы с учебной и научной литературой аспирант может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы, которые).

Самостоятельная работа аспирантов

Методические указания по организации внеаудиторной самостоятельной работы на занятии способствуют организации последовательного изучения материала, вынесенного на самостоятельное освоение в соответствии с учебным планом, программой учебной дисциплины/профессионального модуля и имеет такую структуру как:

- тема;
- вопросы и содержание материала для самостоятельного изучения;
- форма выполнения задания;
- алгоритм выполнения и оформления самостоятельной работы;
- критерии оценки самостоятельной работы;
- рекомендуемые источники информации (литература основная, дополнительная, нормативная, ресурсы Интернет и др.).

Самостоятельная работа как вид деятельности аспиранта многогранна. В качестве форм самостоятельной работы при изучении дисциплины «Методы и системы защиты информации. Информационная безопасность» предлагаются:

- работа с научной и учебной литературой;
- подготовка доклада к практическому занятию;
- более глубокое изучение с вопросами, изучаемыми на практических занятиях;
- подготовка к тестированию, зачету или экзамену;
- выработка умения самостоятельно и критически подходить к изучаемому материалу.

Технология самостоятельной работы должна обеспечивать овладение знаниями, закрепление и систематизацию знаний, формирование умений и навыков. Апробированная технология характеризуется алгоритмом, который включает следующие логически связанные действия аспиранта:

- чтение текста (учебника, пособия, конспекта лекций);
- конспектирование текста; - решение задач и упражнений;
- подготовка к практическим занятиям;
- ответы на контрольные вопросы;
- составление планов и тезисов доклада.

Подготовка доклада/сообщения к занятию

Основные этапы подготовки доклада:

- выбор темы;
- консультация преподавателя;
- подготовка плана доклада;
- работа с источниками и литературой, сбор материала;
- написание текста доклада;
- оформление рукописи и предоставление ее преподавателю до начала доклада, что определяет готовность аспиранта к выступлению;
- выступление с докладом, ответы на вопросы.

Тематика доклада согласовывается с преподавателем.

8 . Материально-техническое обеспечение дисциплины

Для проведения различных видов аудиторных занятий используются:

- лекционные аудитории с современными средствами демонстрации 5-301, 5-314, 5-313, 5-317;
- оборудование для оснащения междисциплинарных, межкафедральных, межфакультетских лабораторий, в том числе современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

5-306 – лаборатория микропроцессорных средств и систем;

5-401 – лаборатория интегрированных информационно-управляющих систем;

5-407 – лаборатория оптоэлектронных устройств ввода информации;

5-413 – лаборатория электроники и систем связи;

5-415 – лаборатория схемотехники ЭВМ;

5-417 – лаборатория защиты информации;

5-418 – лаборатория технических средств защиты информации.

- вычислительное и телекоммуникационное оборудование и программные средства, необходимых для реализации ОПОП и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности: компьютерная техника: Intel Core i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb; серверы: CPU Intel Xenon E3-1240 V3 3.4GHz/4core/1+8Mb/80W/5GT ASUS P9D-C /4L LGA1150 / PCI-E SVGA 4xGbLAN SATA ATX 4DDR-III HDD 3 Tb SATA 6Gb/s Seagate Constellation CS 3,5" 7200rpm 64 Mb Crucia <CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11;

- компьютерные : 5-304 (el c2DE 7400 BOX/2x2Gb/320 Mb SATA-II 300 Seagate Barrocuda 7200, 121512 ASuStek 00431199 – 6 шт.); 5-313 Asus P5KPL-AM IN Soc-775/Pentium DuelCone E54002.70/Intel Power 32Mb/DVD-R/RW NEC AD-5260 S00432076 – 6шт.; 5-317 Asus H97 H-E, Intel Core i-5-4430, Zelman CNPS80F? Kingston KVR13N958/4, FOX<2801B5>, HDD Western Digital 3,5", WD10 EZEX SATS – III 1Tb, DVD RAMDVD+ R/RWCDRW Samsung SM-224DB SATS, ATX - 5 шт.; 5-220 Intel Core i3 2100 (3,1/5000/3M /Soc-1155 Gigabyte GA-H61M-S2-B3/2048) Mb DDR III 1333МГГц/HDD 500 Gb SATA –III Seagate ST 500 DM002/DVD+/-RW Sony AD 5280S-OB SATA/ATX – 7шт.,

- суперкомпьютер УГАТУ:год установки – 2007 г., сборка IBM совместно с компанией АйТи;

- операционные системы семейств Microsoft Windows и Suse Linux:

операционная система Windows XP / 7 /8;

операционная система Windows Server 2008 R2 /2012;

операционная система Mindriva 2010;

операционная система OpenSuSe;

- помещения (аудитории), специально оборудованные для осуществления образовательного процесса с использованием сведений, составляющих государственную тайну, удовлетворяющие требованиям нормативных правовых документов по режиму секретности и технической защите информации;

- специальные средства вычислительной техники и программного обеспечения, предназначенные для осуществления образовательного процесса с использованием сведений, составляющих государственную тайну, удовлетворяющие требованиям нормативных правовых документов по режиму секретности и технической защите информации.

9. Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ

согласования рабочей программы

Направление подготовки: 10.06.01 Информационная безопасность
код и наименование

Направленность подготовки (программа): Методы и системы защиты информации, информационная безопасность

Дисциплина: Методы и системы защиты информации, информационная безопасность

Учебный год 2015 / 2016

РЕКОМЕНДОВАНА заседанием кафедры Вычислительная техника и защита информации
наименование кафедры

протокол № 13 от "7" апреля 2016 г.
Заведующий кафедрой _____ Васильев В.И. 10 апреля 14
подпись расшифровка подписи

Исполнители:
К. техн. н., доцент _____ Селиванова М.В.
должность подпись расшифровка подписи

СОГЛАСОВАНО:

Заведующий кафедрой[1]
_____ Васильев В.И. 10 апреля 14.
наименование кафедры личная подпись расшифровка подписи дата

Председатель НМС по УГСН 10.06.01 Информационная безопасность
протокол № 10 от "11" 12 2014 г.

_____
личная подпись расшифровка подписи

Библиотека _____ С.Ф. Мусагитова 20.12.14.
личная подпись расшифровка подписи дата

Начальник отдела аспирантуры _____ Р.К. Фаттахов 21.12.14.
личная подпись расшифровка подписи дата

Рабочая программа зарегистрирована в ООПМА и внесена в электронную базу данных
Начальник _____ И.А. Лакман 20 апреля 15
личная подпись расшифровка подписи дата

[1] Согласование осуществляется с выпускающими кафедрами (для рабочих программ, подготовленных на кафедрах, обеспечивающих подготовку для других направлений и специальностей)

1509