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" _____ 2015 г.

ПРОГРАММА НАУЧНЫХ ИССЛЕДОВАНИЙ

Направление подготовки научно-педагогических 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

Программа Научных исследований / Составитель: Селиванова М.В. Уфа: УГАТУ, 2015. - 17 с.

Программа Научных исследований является приложением к Основной профессиональной образовательной программе высшего образования по направлению 10.06.01 Информационная безопасность и направленности Методы и системы защиты информации, информационная безопасность.

Программа Научных исследований обсуждена и одобрена научно-техническим советом УГАТУ

«29» августа 2014 г., протокол № 7

Председатель _____ проректор по НиИД Мухов А.Г.

Составитель _____ *М.В. Селиванова*

Программа одобрена на заседании кафедры вычислительной техники и защиты информации

"17" декабря 2014г., протокол № 23

Заведующий кафедрой

_____ /В.И. Васильев/ 20 декабря 15

личная подпись *расшифровка подписи* *дата*

Программа Научных исследований утверждена на заседании Научно-методического совета по УГСН 10.06.01 Информационная безопасность

"19" 12 2014г., протокол № 10

Председатель НМС _____ В.И. Васильев

Начальник ООПМА _____ И.А. Лакман

Директор библиотеки _____ С.Ф. Мустафина

104

Содержание

1. Цели и задачи Научных исследований

Целью Научных исследований является формирование у аспиранта навыков самостоятельной научно-исследовательской деятельности в области разработки и исследования методов и систем защиты информации и обеспечения информационной безопасности, навыков проведения научных исследований в составе научного коллектива, а также подготовку диссертации на соискание ученой степени кандидата наук по выбранной направленности. В научные исследования входят научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук

Задачами Научных исследований являются:

- формирование комплексного представления о специфике деятельности научного работника направления 10.06.01 Информационная безопасность (направленность: Методы и системы защиты информации, информационная безопасность) очной формы обучения;
- обеспечение становления профессионального научно-исследовательского мышления аспирантов, формирование четкого представления об основных профессиональных задачах, способах их решения;
- формирование умений использовать современные технологии сбора информации, обработки и интерпретации полученных эмпирических данных, владение современными методами исследований;
- формирование готовности и базовых умений самостоятельного формулирования и решения задач, возникающих в ходе научно-исследовательской деятельности и требующих углубленных профессиональных знаний;
- овладение методами исследования, в наибольшей степени соответствующими специальности программы;
- формирование способности к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач;
- формирование способности проектировать и осуществлять комплексные исследования на основе целостного системного научного мировоззрения;
- формирование готовности участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач;
- развитие и совершенствование качеств личности, необходимых в научно-исследовательской деятельности: способность планировать и решать задачи собственного профессионального и личностного развития, способность следовать этическим нормам в профессиональной деятельности;
- сбор материала для выпускной квалификационной работы (ВКР) и кандидатской диссертации;
- формирование способности подготавливать и оформлять научные публикации, отчеты, патенты и доклады, участвовать в семинарах и конференциях;
- внесение аспирантом личного вклада в научно-исследовательскую программу, осуществляемую кафедрой.

2.Требования к результатам НИР

В результате выполнения Научного исследования в целях подготовки диссертации на соискание ученой степени кандидата наук аспирант должен обладать следующими компетенциями:

1. Способность следовать этическим нормам в профессиональной деятельности (УК-5).

В результате освоения данной компетенции аспирант должен:

Знать: основные понятия, категории этики и культуры делового и профессионального общения, методики сознательного использования их в анализе и разрешении конкретных ситуаций делового общения.

Уметь: грамотно применять психологические методы и технологии эффективной коммуникации; анализировать и разрешать в теории и на практике традиционные и нестандартные конкретные задачи и ситуации делового и профессионального общения; применять знания закономерностей общения в профессиональной деятельности, проявлять чуткость, тактичность, заинтересованность и сопереживание в общении с деловыми партнерами.

Владеть: системой психологических качеств, определяющих эффективность общения в современной социокультурной ситуации.

2. Способность планировать и решать задачи собственного профессионального и личностного развития (УК-6).

В результате освоения данной компетенции аспирант должен:

Знать: роль мотивации в творческой профессиональной деятельности как самодостаточной и саморегулируемой системы.

Уметь: осуществлять систематическую работу по самообразованию, совершенствованию профессионально значимых умений и навыков; анализировать и оценивать социальную информацию.

Владеть: навыками использования полученных знаний и методов для анализа проблем в профессиональной деятельности.

3. Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3).

В результате освоения данной компетенции аспирант должен:

Знать: действующие стандарты в области информационной безопасности; Критерии , устанавливающие степень соответствия защищаемых объектов стандартам информационной безопасности.

Уметь: анализировать логику различного рода суждений; формировать требования защиты объектов информатизации и информационных систем.

Владеть: навыками критического восприятия информации; обоснования оценки степени защищенности объектов информатизации и информационных систем.

4. Способность организовать работу коллектива по проведению научных исследований в области информационной безопасности (ОПК-4).

В результате освоения данной компетенции аспирант должен:

Знать: социально-культурное содержание деятельности исследователя, исследователя-преподавателя; технологии управления организационными структурами; особенности ведения совместного научного исследования.

Уметь: соблюдать правила служебного этикета, нормы профессиональной этики для установления нормального социально-психологического контакта; анализировать и оценивать социальную информацию; разрабатывать план выполнения научного исследования для распараллеливания работ по нему.

Владеть: навыками проведения коллективного исследования; организации и оптимизации рабочего времени для сохранения здоровья при больших профессиональных нагрузках.

5. Способность принимать эффективные проектные решения в условиях неопределенности и риска для задач обеспечения информационной безопасности (ПК-1).

В результате освоения данной компетенции аспирант должен:

Знать: основные организационные и правовые методы обеспечения безопасности информационных систем; современные методы защиты локальной и удаленной вычислительных сетей; методы анализа безопасности информационных систем с использованием отечественных и зарубежных стандартов в области информационной

безопасности; методы организации работы коллектива по проведению научных исследований в области информационной безопасности.

Уметь: 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 информационных систем и сетей; организовать работу коллектива по проведению научных исследований в области информационной безопасности; адаптировать и обобщать результаты современных исследований.

Владеть: 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 информационными 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 научных исследований в области информационной безопасности; методами адаптации и обобщения результатов современных исследований.

6. Способностью разрабатывать новые и исследовать существующие защитные механизмы и средства обеспечения информационной безопасности (ПК-2).

В результате освоения данной компетенции аспирант должен:

Знать: 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 несанкционированного доступа в информационные системы, обнаружения вредоносных программ; формальные модели политик безопасности, политик управления доступом и информационными потоками в информационных системах.

Уметь: 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 несанкционированного доступа в информационные системы, обнаружения вредоносных программ.

Владеть: навыками применения существующих защищенных протоколов обмена информацией; современными методами исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ; современными методами и средствами защиты информации при ее передаче и хранении.

3 Место Научных исследований в структуре ОПОП научно-педагогических кадров высшей квалификации

Содержание Научных исследований является логическим продолжением разделов ОПОП блока 1 (базовой и вариативной частей в целом), педагогической практики и служит основой для последующего изучения разделов ОПОП блока 4 – ГИА, прохождения научно-исследовательской практики, 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.

Научное исследование является составной частью программы подготовки аспирантов и относится к блоку 3 "Научные исследования", который в полном объеме относится к вариативной части программы. Блок 3 базируется на базовой части Блока 1 "Дисциплины (модули)", в том числе направленные на подготовку к сдаче кандидатских экзаменов, на наборе дисциплин (модулей) вариативной части Блока 1 "Дисциплины (модули)", которые определяются в соответствии с направленностью программы аспирантуры, а также на Блоке 2 «Практики» вариативной части программы. Научное исследование является составной частью подготовки к государственной итоговой аттестации и защите диссертации на соискание ученой степени кандидата наук (Блок 4).

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	Повышен-ный	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	Повышен-ный	История и философия науки, Природа сознания
3.	Готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач;	УК-3	Повышен-ный	Иностранный язык
4.	Готовность	УК-4	Повышен-	Иностранный

	использовать современные методы и технологии научной коммуникации на государственном и иностранном языках		ный	язык
5.	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	Повышен-ный	Методы и системы защиты информации, информационная безопасность; и дисциплина по выбору
6.	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	Повышен-ный	Методы и системы защиты информации, информационная безопасность; и дисциплина по выбору
7.	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;	ОПК-3	Базовый	Научно-исследовательская практика
8.	Готовность к преподавательской деятельности по основным образовательным программам высшего	ОПК-5	Повышен-ный	Педагогическая практика

	образования			
9.	Способность принимать эффективные проектные решения в условиях неопределенности и риска для задач обеспечения информационной безопасности	ПК-1	Базовый	Методы и системы защиты информации, информационная безопасность
10.	Способность разрабатывать новые и исследовать существующие защитные механизмы и средства обеспечения информационной безопасности	ПК-2	Базовый	Методы и системы защиты информации, информационная безопасность

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), для которой данная компетенция является входной
1.	Способность следовать этическим нормам в профессиональной деятельности	УК-5	Повышенный	ГИА
2.	Способность планировать и решать задачи собственного профессионального и личностного развития	УК-6	Повышенный	ГИА
3.	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информа-ционной безопасности;	ОПК-3	Повышенный	ГИА
4.	Способность организовать работу коллектива по проведению научных	ОПК-4	Повышенный	ГИА

	исследований в области информационной безопасности;			
5.	Способность принимать эффективные проектные решения в условиях неопределенности и риска для задач обеспечения информационной безопасности	ПК-1	Повышенный	ГИА
6.	Способность разрабатывать новые и исследовать существующие защитные механизмы и средства обеспечения информационной безопасности	ПК-2	Повышенный	ГИА

4. Структура и содержание Научных исследований

4.1 Структура Научных исследований

Общая трудоемкость Научных исследований составляет 177 зачетных единиц, 6372 часа.

№ раздела	Наименование раздела Научных исследований	Трудоемкость, часы
1	Организационный этап	927
2	Подготовительный этап	783
3	Исследовательский этап: анализ литературных источников	675
4	Исследовательский этап: математическое моделирование	828
5	Исследовательский этап: экспериментальное исследование	639
6	Исследовательский этап: анализ результатов эксперимента	639
7	Исследовательский этап: подготовка к публикации результатов научных исследований	1080
8	Заключительный этап	747
Итого		**6318**

4.2 Содержание Научных исследований

Научные исследования должны позволить собрать необходимый материал для выполнения диссертационной работы на соискание ученой степени кандидата наук. Ниже приведен примерный план Научных исследований аспирантам по семестрам.

№ п/п	Разделы (этапы)	Виды научно-исследовательской работы, включая самостоятельную работу	Трудоемкость (в часах)	Формы текущего контроля
1 семестр	Организа-ционный этап	Организационное собрание для разъяснения целей, задач, содержания и порядка проведения Научного исследования	927	Собеседование
		Планирование Научного исследования, включающее ознакомление с тематикой исследовательских работ в данной области		Индивидуальный план аспиранта 1 семестра
		Выбор темы исследования, и обоснование ее актуальности		Тема диссертации, доклад
		Подготовка отчета о проделанных Научных исследованиях		Отчет о Научных исследованиях
2 семестр	Подготовитель-ный этап	Планирование Научного исследования 2го семестра	783	Индивидуальный план аспиранта 2 семестра
		Постановка целей, задач исследования		Цели, задачи диссертации
		Характеристика современного состояния изучаемой проблемы		Аналитический отчет
		Разработка программы и инструментария собственного исследования		Программа и инструментарий исследования, методология
		Подготовка отчета о проделанной научно-		Отчет о

		исследовательской работе		Научных исследованиях
3 семестр	Исследовательский этап: анализ литературных источников	Планирование Научного исследования 3го семестра	675	Индивидуальный план аспиранта 3 семестра
		Составление библиографического списка по теме диссертации		Библиографический список
		Работа с источниками научной информации по теме диссертации		Реферативный / аналитический обзор / рецензия
		Изучение федеральных и региональных законов и нормативно-правовых актов по теме исследования		Обзор законодательной базы
		Анализ основных результатов и положений, полученных ведущими специалистами в области проводимого исследования, оценка их применимости в рамках диссертационного исследования		База данных
		Подготовка отчета о проделанной научно-исследовательской работе		Отчет о Научных исследованиях
4 семестр	Исследовательский этап: математическое моделирование	Планирование Научного исследования 4го семестра	828	Индивидуальный план аспиранта 4 семестра
		Оценка предполагаемого личного вклада автора в разработку темы		Элементы научной новизны/статья
		Разработка основных направлений теоретической концепции научного исследования по теме диссертации		Реферат / научный доклад / статья
		Выбор моделей и методик расчетов показателей		Методики и модели

		эффективности результатов исследования		
		Выбор методов оценки достоверности и достаточности данных исследования		Собеседование
		Подготовка отчета о проделанной научно-исследовательской работе		Отчет о Научных исследованиях
5 семестр	Исследовательский этап: экспериментальное исследование	Планирование Научного исследования 5го семестра	639	Индивидуальный план аспиранта 5 семестра
		Проведение практической работы и получение первых результатов научного исследования		Реферат / научный доклад / статья
		Расчет показателей эффективности результатов проведенного исследования с помощью выбранных моделей и методик		Результаты расчетов
		Оценка достоверности полученных результатов исследования		Реферат / научный доклад / статья. Собеседование.
		Подготовка отчета о научном исследовании		Отчет о Научном исследовании
6 семестр	Исследовательский этап: анализ результатов эксперимента	Планирование Научного исследования 6го семестра	639	Индивидуальный план аспиранта 6 семестра
		Проведение практической работы и получение новых результатов научного исследования		Реферат / научный доклад / статья
		Расчет показателей эффективности результатов проведенного исследования с		Результаты расчетов

		помощью выбранных моделей и методик		
		Оценка достоверности полученных результатов исследования		Реферат / научный доклад / статья. Собеседование.
		Подготовка отчета о Научном исследовании		Отчет о Научном исследовании
7 семестр	Исследователь-ский этап: подготовка к публикации результатов научных исследований	Планирование Научного исследования 7го семестра	1080	Индивидуальный план аспиранта 7 семестра
		Представление и конкретизация основных результатов исследования, представляющих научную новизну		Основные результаты диссертации (научная новизна)
		Анализ, оценка и интерпретация результатов исследования		Реферат / научный доклад / статья
		Оценка практической значимости будущей диссертации		Реферат / научный доклад / статья
		Подготовка отчета о Научном исследовании		Отчет о Научном исследовании
8 семестр	Заключитель-ный этап	Планирование Научного исследования 8го семестра	747	Индивидуальный план аспиранта 8 семестра
		Окончательное оформление выпускной квалификационной работы (ВКР)		Диссертация на соискание ученой степени кандидата наук
Итого трудоемкость (в часах)			6318	

Научное исследование ведется в форме индивидуальной самостоятельной работы под руководством научного руководителя.

Трудоемкость индивидуального задания составляет 6318 часов. Индивидуальное задание отражается в индивидуальном плане (графике) работы аспиранта.

Целью выполняемого задания является развитие способности аспиранта самостоятельно осуществлять научно-исследовательскую работу, связанную с решением сложных

профессиональных задач в инновационных условиях, основным результатом которой станет написание и успеш1ная защита кандидатской диссертации.

Выполнение индивидуального задания имеет своей целью формирование комплексного представления о специфике деятельности научного работника направления 10.06.01 Информационная безопасность (направленность: Методы и системы защиты информации, информационная безопасность). Научные исследования имеют своей целью формирование умений, навыков в соответствии с компетентностной моделью выпускника аспирантуры по данному направлению.

Ниже перечислены компетенции, на формирование которых направлено выполнение индивидуального аспирантом:

1) способность следовать этическим нормам в профессиональной деятельности (УК-5);
2) способность планировать и решать задачи собственного профессионального и личностного развития (УК-6);
3) способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3);
4) способность организовать работу коллектива по проведению научных исследований в области информационной безопасности (ОПК-4);
5) способность принимать эффективные проектные решения в условиях неопределенности и риска для задач обеспечения информационной безопасности (ПК-1);
6) способность разрабатывать новые и исследовать существующие защитные механизмы и средства обеспечения информационной безопасности (ПК-2).

Научно-исследовательская работа ведется в форме индивидуальной самостоятельной работы под руководством научного руководителя.

Формами проведения научно-исследовательской работы могут являться:

- выполнение заданий научного руководителя в соответствии с утвержденным планом научного исследования;
- участие в межкафедральных семинарах, теоретических семинарах (по тематике исследования), а также в научной работе кафедры;
- выступление на конференциях молодых ученых, проводимых в УГАТУ, в других вузах, а также участие в других научных конференциях и круглых столах;
- подготовка и публикация тезисов докладов, научных статей;
- участие в реальном научно-исследовательском проекте, выполняемом на кафедре рамках бюджетных и внебюджетных научно-исследовательских программ (или в рамках полученного гранта).

Итогом работы является подготовка и защита диссертации на соискание ученой степени кандидата наук.

Перечень форм научно-исследовательской работы в семестре для аспирантов первого, второго, третьего и четвертого годов обучения может быть конкретизирован и дополнен научным руководителем в зависимости от специфики темы кандидатской диссертации.

5. Место, сроки и формы проведения Научных исследований

Местом для проведения Научных исследований являются кафедра вычислительной техники и защиты информации и другие кафедры УГАТУ, научно-исследовательские лаборатории Университета, научно-исследовательские и проектные институты, другие учреждения/организации и их подразделения, располагающие современной научной и производственной аппаратурой.

Образовательная программа предусматривает научное исследование аспиранта на протяжении всего срока обучения по программе.

Учебным планом подготовки предусмотрены следующие научные исследования: распределенные:

1) научные исследования (I курс, 1 семестр) – девятнадцать недель;
2) научные исследования (I курс, 2 семестр) – двадцать недель;
3) научные исследования (II курс, 3 семестр) – восемнадцать недель;
4) научные исследования (II курс, 4 семестр) – двадцать недель;

выделенные:

5) научные исследования (III курс, 5 семестр) – одиннадцать недель;
6) научные исследования (III курс, 6 семестр) – тринадцать недель;
7) научные исследования (IV курс, 7 семестр) – девятнадцать недель;
8) научные исследования (IV курс, 8 семестр) – пятнадцать недель.

6. Формы аттестации

Контроль Научных исследований производится в соответствии с Положением о проведении промежуточной аттестации и текущего контроля успеваемости аспирантов.

Текущий контроль аспирантов направления 10.06.01 Информационная безопасность (направленность: Методы и системы защиты информации, информационная безопасность) может проводиться в дискретные временные интервалы научным руководителем аспиранта в следующих формах:

выполнение индивидуальных заданий;

выполнение коллективных заданий;

выступление на кафедре на научном семинаре, действующем на постоянной основе;

формирование элементов отчета по Научным исследованиям.

Отдельно оцениваются личностные качества аспиранта (аккуратность, организованность, исполнительность, инициативность и др.).

Формой промежуточной аттестации является составление и защита отчета по Научному исследованию. Результаты этой работы рассматриваются на заседаниях кафедры два раза в год: в период полугодовой и итоговой (за год) аттестации аспирантов. Результаты годовых аттестаций утверждаются на заседаниях Ученого совета университета.

Научный руководитель ставит дифференцированную оценку (зачет) по итогам научного исследования аспиранта. Оценка по Научному исследованию в каждом семестре приравнивается к оценкам по теоретическому обучению и учитывается при подведении итогов общей успеваемости аспиранта.

Аспиранты, не выполнившие программу по Научному исследованию, либо получившие неудовлетворительную оценку, могут быть не аттестованы.

Фонды оценочных средств, включают типовые индивидуальные задания, формы внешнего, внутреннего оценивания и самооценки (для включения в отчет по Научным исследованиям), позволяющие оценить результаты обучения по научным исследованиям.

№ п/п	Контролируемые разделы	Код контролируемой компетенции (или ее части)	Уровень освоения, определяемый этапом формирования компетенции	Наименование оценочного средства

1	Исследовательский этап: анализ литературных источников (3 семестр)	УК-5	Базовый	Вопросы по теме, материалы для тестирования
2	Исследовательский этап: математическое моделирование (4 семестр)	ПК-2	Повышенный	Вопросы по теме, материалы для тестирования
3	Исследовательский этап: экспериментальное исследование (5 семестр)	ОПК-4	Повышенный	Задания по теме, материалы для тестирования
		ПК-1	Повышенный	
4	Исследовательский этап: анализ результатов эксперимента (6 семестр)	УК-6	Повышенный	Задания по теме, материалы для тестирования
5	Исследовательский этап: подготовка к публикации результатов научных исследований (7 семестр)	ОПК-3	Повышенный	Вопросы по теме, материалы для тестирования
		УК-5	Повышенный	

Комплект оценочных материалов.
Раздел 1.
Вопросы по теме.

1. Что такое информация?
2. Чем отличаются данные от информации?
3. Какая информация является входной и выходной для организации?
4. Что такое информация из внешней и внутренней среде организации?
5. Каковы свойства информации?
6. Что такое документ, документооборот?
7. Какова классификация документов?
8. Какие преимущества обеспечивает унификация форм документов?
9. Что понимают под информационными ресурсами?
10. В чем заключается управление информационными ресурсами?
11. Перечислите технические каналы утечки информации.
12. Перечислите средства защиты акустического канала

13. Перечислите средства защиты визуального канала
14. Перечислите средства защиты вибрационного канала
15. Перечислите средства защиты электромагнитного канала
16. Перечислите средства защиты индукционного канала
17. Что такое программно-аппаратные средства защиты информации?
18. Что такое программные средства защиты информации?
19. Какие механизмы реализуют программно-аппаратные средства защиты информации?
20. Какие компьютерные угрозы безопасности существуют?
21. Что такое сниффинг? Какие методы защиты против него существуют?
22. Что такое IP-Spoofing? Какие методы защиты против него существуют?
23. Что такое сетевая разведка? Какие методы защиты против нее существуют?
24. Что такое переполнение буффера? Какие методы защиты против него существуют?
25. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
26. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
27. Что такое фишинг? Какие методы защиты против него существуют?
28. Что такое компьютерный вирус? Какие виды вирусов существуют?
29. Опишите механизм работы вируса. Как вирус может проникнуть на компьютер?
30. Какие существуют механизмы работы антивируса? Опишите их.
31. Что такое Firewall?
32. Что такое шифр?
33. Какие виды шифров существуют?
34. Что такое симметричный шифр? Какие симметричные шифры используются сейчас?
35. Что такое ассиметричный шифр? Какие ассиметричные шифры используются сейчас?
36. Что такое хеш-функция? Какие виды хеш-функций вы знаете?
37. Какие хеш-функции используются сейчас?
38. Что такое цифровая подпись?
39. Что такое инфраструктура открытых ключей?
40. Что такое аутентификация? Что такое идентификация?
41. Какие протоколы аутентификации вы знаете?
42. Какие криптографические протоколы используются в компьютерных сетях? Опишите их.

Материалы для тестирования.

Выберите из предложенных один вариант

1. Основными характеристиками защищаемой информации являются:
a) конфиденциальность, целостность и статичность;
b) конфиденциальность, целостность и доступность;
c) аутентификация, целостность и доступность;
d) аутентификация, статичность и время создания;

2. Известность содержания информации только имеющим соответствующие полномочия субъектам – это:

a) Целостность;
b) Статичность;
c) Конфиденциальность;
d) Аутентификация;

3. Неизменность информации в условиях её случайного и (или) преднамеренного искажения и разрушения – это:
a) целостность;
b) конфиденциальность;
c) доступность;
d) идентификация;

4. Возможность получения информации или информационной услуги за приемлемое время – это:
a) конфиденциальность;
b) целостность;
c) доступность;
d) статичность;

5. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:
a) уязвимость; b) атака;
c) угроза;
d) нет верного ответа;

6. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого её состояния, при котором создаются условия для реализации угроз безопасности информации - это:
a) атака;
b) угроза;
c) уязвимость;
d) статичность;

7. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:
a) статичность;
b) атака;
c) угроза; d) изъян;

8. Классификацию угроз ИБ можно выполнить по нескольким критериям:
a) по аспекту информационной безопасности;
b) по компонентам информационной системы;
c) по способу осуществления;
d) все ответы верны;

9. Конфиденциальная информация может быть разделена на:
a) предметную и служебную;
b) служебную и закрытую;
c) предметную и открытую;
d) открытую и закрытую;

10. Целостность информации может быть разделена на:
a) статическую и динамическую;
b) статическую и служебную;
c) служебную и динамическую;
d) все верно;

11. Примером нарушения статической целостности не является:
a) ввод неверных данных;
b) несанкционированное изменение данных;
c) изменение программного модуля вирусом;
d) внесение дополнительных пакетов в сетевой трафик;

12. Примером нарушения динамической целостности не является:
a) нарушение атомарности транзакций;
b) внесение дополнительных пакетов в сетевой трафик;
c) несанкционированное изменение данных;
d) дублирование данных;

13. Угроза отказа служб может быть разбита на следующие типы:
a) отказ пользователей;
b) внутренний отказ информационной системы;
c) отказ поддерживающей инфраструктуры;
d) все ответы верны;
14. Что не относится к внутреннему отказу ИС:
a) ошибки при переконфигурировании системы;
b) отказы программного и аппаратного обеспечения;
c) разрушение данных;
d) нарушение работы систем связи;

15. Что не относится к отказу служб:
a) нарушение работы систем связи;
b) разрушение и повреждение помещений;
c) нарушение работы электропитания;
d) разрушение данных;

16. Нарушители" классифицируются по одному из следующих критериев:
a) уровень профессиональной подготовки противника;
b) тип доступа противника к системе;
c) способы атаки;
d) все ответы верны;

17. Высококвалифицированный специалист, стремящейся обойти защиту компьютерной системы:
a) Крякер;
b) Хаб;
c) Хакер;
d) Юзер;

18. Наибольшую угрозу ИС составляют:
a) Юзер;
b) Агент;
c) Хакер;
d) Крякер;

19. На сколько больших классов делятся каналы утечки информации:
a) Два;
b) Три;
c) Четыре;
d) Пять;

20. Что не относится к косвенным каналам утечки информации:
a) дистанционное видеонаблюдение;
b) использование полущивающих устройств; перехват побочных электромагнитных излучений и наводок;
c) хищение носителей информации;

21. Какая угроза отказа служб устраняется административно-правовыми методами:
a) отказ пользователей;
b) отказ программного обеспечения;
c) нарушение работ систем связи;
d) разрушение и повреждение помещений

22. К каналам, предполагающим изменение элементов информационной структуры относится:
a) намеренное копирование файлов и носителей информации;
b) маскировка под других пользователей, путём похищение идентифицирующей их информации;
c) хищение носителей информации;
d) незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.

23. Что относится к каналам, не требующим изменение элементов ИС
a) намеренное копирование файлов и носителей информации;

b) незаконное подключение специальной регистрирующей аппаратуры;
c) злоумышленное изменение программ;
d) злоумышленный вывод из строя средств защиты информации;

24. Какая направленность атак неверно сформулирована?
a) атаки на уровне операционной системы;
b) атаки на уровне системного администратора;
c) атаки на уровне сетевого программного обеспечения;
d) атаки на уровне систем управления базами данных.

25. К какому типу атак относится прослушивание передаваемых сообщений:
a) Пассивная атака;
b) Модификация потока данных;
c) Повторное использование;
d) Отказ в обслуживании;

Раздел 2.
Вопросы по теме.

1. Правовое регулирование в области безопасности информации: законодательная база информатизации общества; структура государственных органов, обеспечивающих безопасность информационных технологий.

2. Информационная безопасность. Основные определения
3. Угрозы информационной безопасности.
4. Модель системы зашиты
5. Организационные меры и меры обеспечения физической безопасности.
6. Идентификация и аутентификация. Методы аутентификации
7. Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей.

8. Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности информации.
9. Методы зашиты внешнего периметра.
10. Системы обнаружения вторжений (Intrusion Detection System, EDS)
11. Протоколирование и аудит
12. Построение систем защиты от угроз нарушения целостности: типовая структура такой системы.
13. Криптографические методы обеспечения целостности информации:
реализация механизма цифровой подписи, криптографические хэш-функции и ее преимущества, коды проверки подлинности.
14. Структура системы защиты от угроз нарушения доступности: поясните
основные составляющие.
15 Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Белла-ЛаПалулы.
16 Формальные модели целостности: модель Кларка-Вилсона, модель Биба.
17 Основные положения ISO/IEC 15408. Критерии оценки безопасности информацион-ных технологий. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002. Структура профиля защиты в соответствии с ГОСТ Р ИСО/МЭК 15408-2002.
18 Основные положения ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"

19 Основные положения ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". Этапы построения и использования СМИБ.
20 Обобщенная схема построения комплексной защиты компьютерной сети предприятия на примере модели Lifecycle Security .
21 Технология функционирования VPN. Типы виртуальных частных сетей, преимущества и недостатки
22 Методика анализа рисков в сфере информационной безопасности CRAMM.
23 Методика анализа рисков в сфере информационной безопасности FRAP.
24 Методика анализа рисков в сфере информационной безопасности OCTAVE.
25 Методика анализа рисков в сфере информационной безопасности RiskWatch.
26 Проведение оценки рисков в соответствии с методикой Microsoft.
27 Опишите суть протокола системы централизованной аутентификации и распределения ключей симметричного шифрования Kerberos Протоколы и механизмы обеспечения информационной безопасности Kerberos, S/MIME, IPSec, AH, ESP, IPSec, NAT. Опишите их назначение и область применения.

Материалы для тестирования.

Выбрать из предложенных вариантов ответов верный:

1. АИС – это:
a) автоматизирванная информационная среда;
b) автоматизирванная информационная схема;
c) автоматизирванная информационная система;
d) автоматизирванная информационная структура;

2. Принципы обеспечения информационной безопасности:
a) системность, комплексность, непрерывность;
b) статичность, комплексность, доступность;
c) комплексность, целостность, доступность;
d) целостность, системность, открытость;

3. Выбор методов и средств, направленных на противодействие комплексу угроз – это:

a) Целостность;
b) Системность;
c) Комплексность;
d) Непрерывность;

4. Возможность изменения применяемых средств ИС – это:
a) Комплексность;
b) Гибкость;
c) Непрерывность;
d) Целостность;

5. Самая распространенная формальная модель доступа к данным:
6. a) Мандатная;
b) Дискреционная;
c) модель Биба;
d) модель Кларка;

7. В дискреционной модели отношения субъекты – объекты представлены в виде:
a) Таблиц;
b) Матриц; c) Схем;
d) все верно;

8. В какой модели доступа каждому объекту системы присвоена метка секретности:
a) модель Кларка;
b) дискреционная;
c) мандатная;
d) модель Биба;

9. Центральный элемент системы защиты, который идентифицирует субъекты, объекты и параметры запрашиваемого доступа субъектов к объектам:
a) сканер безопасности;
b) монитор безопасности;
c) модем безопасности;
d) шина безопасности;

10. К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые:
a) руководством организации
b) Персоналом организации
c) Пользователями
d) Нет верного ответа
11. Из скольких уровней детализации состоит политика безопасности ИС:
a) Трех
b) Четырех
c) Двух
d) Пяти

11. Политика безопасности верхнего уровня, затрагивающая все организацию в целом, включает в себя:
a) решение сформировать или изменить комплексную программу обеспечения информационной безопасности;
b) формулирование целей организации в области информационной безопасности, определение общих направлений в достижении данных целей;

c) обеспечение нормативной базы для соблюдения законов и правил; d) все ответы верны;

12. Самая распространенная сетевая **ос**:
a) Novell Netware;
b) MS Windows;
c) UNIX;
d) Os/2;

13. Наиболее распространёнными методами несанкционированного доступа в операционной системе Unix является:
a) Позволяющие несанкционированно запустить исполняемый код;
b) Позволяющие обойти установленные разграничения прав доступа;
c) Троянские программы;
d) Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов;

14. Наиболее распространёнными методами несанкционированного доступа в операционной системе Windows является:
a) Позволяющие несанкционированно запустить исполняемый код;
b) Позволяющие обойти установленные разграничения прав доступа;
c) Троянские программы;
d) Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.

15. Что не относится к недостаткам ОС Windows?
a) невозможно встроенными средствами гарантированно удалять остаточную информацию;
b) не обеспечивается регистрация выдачи документов на "твёрдую копию", а также некоторые другие требования к регистрации событий;
c) невозможно в общем случае обеспечить замкнутость (или целостность) программной среды;
d) невозможно встроенными средствами обеспечить полноту системы

16. Из скольких уровней состоит правовое обеспечение информационной безопасности:
a) двух уровней;
b) трех уровней;
c) четырех уровней;
d) пяти уровней;

17. Что из перечисленного не входит в первый уровень правового обеспечения информационной безопасности:
a) Конституция РФ (ст. 23, право на тайну переписки);
b) Гражданский кодекс РФ (ст. 139, возмещение убытков от утечек);
c) Федеральный закон "О государственной тайне";
d) постановления Правительства РФ;

18. Что из перечисленного не входит во второй уровень правового обеспечения информационной безопасности:
a) указы Президента РФ;
b) постановления Правительства РФ;
c) Уголовный кодекс РФ (ст. 272-274, неправомерный доступ, распространение вирусов, нарушение правил эксплуатации);
d) постановления пленумов Верховного Суда РФ;

19. Структурные элементы национальной безопасности:
a) Политическая;
b) Экономическая;
c) Военная;
d) все ответы верны;

20. Как на английском пишется термин уязвимость:
a) Vulnerability;
b) Secure;
c) Source;
d) Vain;

21. Систему национальной безопасности образует:
a) органы законодательной, исполнительной и судебной властей;

b) государственные, общественные и иные организации и объединения;
c) граждане, принимающие участие в обеспечении безопасности в соответствии с законом;
d) все ответы верны;

22. В каком году утверждена Доктрина информационной безопасности Российской Федерации:
a) 1998; b) 2000; c) 2002; d) 2004;

23. Что не относится к основным принципам обеспечения национальной безопасности:
a) законность;
b) соблюдение баланса жизненно важных интересов личности, общества и государства;
c) взаимная ответственность личности, общества и государства по обеспечению безопасности;
d) системность;

24. К правовым методам обеспечения информационной безопасности относят:
a) разработка современных методов и средств защиты информации;
b) определение ответственности физических и юридических лиц;
c) усиление контроля за развитием информационного рынка России;
d) повышение степени защищенности законных интересов граждан;

25. Когда был принят Федеральный закон "Об информации, информатизации и защите информации:
a) 2004; b) 2006; c) 2008; d) 2010;

Раздел 3.
Задания по теме.

1. Определение базовых понятий. Понятие криптографии, шифра, ключа, взлома шифра.
2. Задачи и методы криптографии. Секретность, аутентификация, целостность, неоспоримость.
3. Виды шифров. Симметричны, ассиметричные, блочные и потоковые шифры. Принцип Керкхоффса.
4. Криптографические примитивы. Хэш-функция и её применения. Генераторы псевдослучайных чисел.
5. Понятие протокола. Определение протокола, условия протоколов. Виды протоколов.
6. Основные криптографические протоколы. Схема обмена ключами, аутентификация, распределение ответственности, цифровая подпись. Вспомогательные криптографические протоколы.

7. Электронная цифровая подпись. Задачи, решаемые цифровой подписью. Схема создания и проверки электронной цифровой подписи.

8. Модели основных криптоаналитических атак. Атака методом сведения к середине. Словарная атака. Четыре основных подхода к анализу криптографических протоколов.

Материалы для тестирования.

Выбрать из предложенных вариантов ответов верный:

1. От какого арабского слова происходит Термин шифр:
a) Символ;

b) Пароль;
c) Цифра;
d) Код;

2. Как переводится слово криптография:
a) Тайнопись;
b) Рукопись;
c) Алгоритм; d) Пароль;

3. Чем занимается криптография:
a) составлением алгоритмов шифрования информации;
b) составлением алгоритмов передачи информации;
c) составлением прикладных программ;
d) составлением инструментальных программ;

4. Исследование криптографических алгоритмов с целью оценки их стойкости и поиска слабых мест называется:
a) Криптографией;
b) Криптоанализом;
c) Шифрованием;
d) Кодированием;

5. Процесс преобразования открытого текста в шифртекст называется:
a) Enciphering;
b) Deciphering;
c) Cryptanalysis;
d) Algorithm;

6. Процесс преобразования шифрованного текста в исходный называется: a) Enciphering ;
b) Algorithm;
c) Deciphering;
d) Cryptanalysis;

7. Элемент позволяющий выбрать одно конкретное преобразование из множества преобразований – это:
a) Ключ;
b) Пароль;
c) Код;
d) Шифр;

8. Раскрытие ключа шифрования без привлечения методов криптоанализа называется:
a) Компрометацией;
b) Криптоанализом;

c) Шифрованием;
d) Криптографией;

9. Какая из перечисленных задач не относится к задачам криптографии:
a) Секретность;
b) Целостность;
c) Аутентификация;
d) Системность;

10. Выберите два основных типа криптографических алгоритмов:
a) Симметричные и асимметричные;
b) Симметричные и циклические;
c) Структурные и циклические;
d) Блочные и асимметричные;

11. В каких алгоритмах ключ расшифрования совпадает с ключом шифрования:
a) Блочных;
b) Циклических;
c) Симметричных;
d) Асимметричных;

12. В современных шифрах применяется принцип:
a) Керкхоффса;
b) Хофмана;
c) Шенона;
d) Эль гаммеля;

13. Криптографические устройства псевдослучайных чисел – это:
a) Стартер;
b) Генератор; c) Шина;
d) Магистраль;

14. Последовательность шагов, которые предпринимают две или большое количество сторон для совместного решения задачи – это:
a) Аудит;
b) Протокол;
c) Аутентификация;
d) Идентификация;

15. К основным криптографическим протоколам не относят:
a) обмен ключами;
b) аутентификацию;
c) цифровую подпись;
d) датирование;

16. Что не относится к Сервисам безопасности:
a) идентификация и аутентификация;
b) Шифрование;
c) инверсия паролей;
d) контроль целостности;

17. Что не относится к разделам криптографии:
a) Симметричные криптосистемы;

b) Системы электронной подписи;
c) Управление передачей данных;
d) Управление ключами;

18. Какого шифра не существует:
a) Шифр Цезаря;
b) Шифр Кардано;
c) Шифр Трисемуса;
d) Шифр Хартли;

19. Набор простых логических правил, легко применимых на практике и позволяющих выявить отдельные изъяны криптографических протоколов:
a) Бан – логика;
b) Пан – логика;
c) Ран – логика;
d) Фан – логика;

20. Процесс подтверждения подлинности пользователя – это:
a) Идентификация;
b) Аутентификация;
c) Методология;
d) Интеграция;

21. Каким шифром является DES
a) Симметричным;
b) Асимметричным;
c) Блочным;
d) Каскадным;

22. Сколько ключей надо перебрать Для взлома алгоритма шифрования DES ,который имеет рабочую длину 56 бит:
a) 2^{56}
b) 2^{5}
c) 56^{2}
d) 2^{6}

23. Как по-другому называют ключ шифрования:
a) Сменный шифр;

b) Сменный элемент;
c) Сменная буква;
d) Сменный символ;

24. Какого типа электронной подписи не существует:
a) DSA;
b) RSA; c) DTS; d) CPO;

25. Каким шифром является RSA:
a) Симметрицным;
b) Асимметричным;
c) Блочным;
d) Компазиционным;

Раздел 4.

Задания по теме.

1. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”).
2. Руководящие документы Гостехкомиссии России.
3. Международные стандарты информационной безопасности
4. Общие принципы построения защищенных систем.
5. Средства разработки и правила их реализации.
6. Фундаментальные проблемы, возникающие при построении защищенных информационных систем.

Материалы для тестирования.

Выбрать из предложенных вариантов верный:

1. Совокупность взаимодействующих компонентов ИС и связей между ними - это:

a) Схема;
b) Система;
c) Структура;
d) Цикл;

2. Что не входит в нормативно- методическое обеспечение создания АС:

a) международные стандарты ISO;
b) стандарты Российской Федерации ГОСТ Р.;
c) стандарты организации-заказчика;
d) стандарты администрирования;

3. Как называется период времени, который начинается с момента принятия ре-шения о необходимости создания АС и заканчивается в момент ее полного изъятия из эксплуатации:

a) ЖЦ АС;
b) ЖС АС;
c) ЖР АИ;
d) ЖМ ИС;

4. Совокупность функциональных и физических характеристик, установленных в технической документации и реализованных в программно-аппаратном комплексе – это

a) Конфигурация АС;
b) Структура АС;
c) Архитектура АС;
d) Нет верного ответа;

5. Совокупность свойств, которые характеризуют способность АС удовлетворять заданным требованиям:

a) Количество АС;
b) Качество АС;
c) Организация АС;
d) Все ответы верны;

6. Структура системы, определяющая последовательность выполнения и взаимосвязей целей и задач на протяжении ЖЦ:

a) План;
b) Модель;
c) Макет;

d) Схема;
7. Набор основных правил, определяющих организацию системы:
a) Конфигурация АС;
b) Структура АС;
c) Архитектура АС;
d) Нет верного ответа;

8. Под угрозой удаленного администрирования в компьютерной сети понимается угроза:
a) несанкционированного управления удаленным компьютером;
b) внедрения агрессивного программного кода в рамках активных объектов Web-страниц;
c) перехвата или подмены данных на путях транспортировки;
d) вмешательства в личную жизнь;

9. Наиболее эффективное средство для защиты от сетевых атак:
a) использование сетевых экранов или «firewall»
b) использование антивирусных программ
c) посещение только «надёжных» Интернет-узлов
d) использование только сертифицированных программ-броузеров при доступе к сети Интернет

10. Первым оценочным стандартом, получившим широкое распространение, стал стандарт Министерство обороны США:
a) Красная книга;
b) Оранжевая книга;
c) Синяя книга;
d) Желтая книга;

11. В каком году появился стандарт Министерство обороны США «Критерии оценки доверенных компьютерных систем»:
a) 1982;
b) 1983;
c) 1984;
d) 1985;

12. В стандарте Критерии оценки доверенных компьютерных систем» Степень доверия оценивается:
a) По двум критериям;
b) По трем критериям;
c) По четырем критериям;
d) Нет верного ответа;

13. Какого вида защиты нет в оранжевой книге:
a) Дискреционная защита;
b) Верифицированная защита;
c) Мандатная защита;
d) Максимальная защита;

14. Какой категории требований безопасности нет в «Оранжевой книге»:
a) политика безопасности;
b) подотчетность;
c) Корректность;
d) Статичность;

15. Как расшифровывается Стандарт ISO:
a) International Organization for System;
b) Information Organization for Standardization;
c) International Organization for Standardization;
d) International Organization for sertification;

16. Когда вышел стандарт ISO в области информационной безопасности:
a) 1998;
b) 1999; c) 1997; d) 2000;

17. Какой из этих уровней не рассматривают при формальном подходе к разработке ИС:
a) Цели;
b) Средства;
c) Реализация;
d) Финансы;

18. Как называется информационный документ, описывающий методику разработки защищенных систем:
a) Защищенные информационные системы;
b) Открытые информационные системы;
c) Скрытые информационные системы;
d) Доступные информационные системы;

19. Как переводится выражение Fair Information Practices:
a) Принцип честного использования информации;
b) Принцип скрытого использования информации;
c) Принцип закрытого использования информации;
d) Принципами открытого использования информации;

20. Какой из этих стандартов является одним из наиболее известных стандартов в области защиты информации:
a) information technology — Information security management;
b) information technology — Information system management;
c) information grafic — Information security management;
d) information technology — Information security office;

21. Стандарт для беспроводных локальных сетей – это:
a) Стандарт IEEE 801.11;
b) Стандарт IEEE 802.11;
c) Стандарт IEEE 802.12;
d) Стандарт IEEE 802.111;

22. Какой алгоритм придуман стандартом IEEE 802.11 для защиты WLAN:
a) Wep;
b) Web;
c) Wna;
d) Win;

23. Как переводится термин Wi-Fi
a) Wyb Fidelity;
b) Web Fidelity;
c) Wna Fidelity;
d) Wireless Fidelity;

24. Перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет – это:

a) Set;
b) Sid;
c) Ser;
d) Sis;

25. В каком году Гостехкомиссия (ГТК) при Президенте РФ опубликовала пять руководящих документов, посвященных вопросам защиты от несанкционированного доступа к информации:

a) 1990;
b) 1991;
c) 1992;
d) 1994;

Раздел 5.

Вопросы по теме.

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.
31. Методы поиска и сбора информации.
32. Методика устранения компьютерной информации.
33. Уязвимости Windows.
34. Уязвимости UNIX
35. Защита от копирования переносных носителей.

36. Аппаратные ключи защиты.
37. Современные криптосистемы
38. Виды шифров. Методика кодирования
39. Навесная защита
40. Антивирусное программное обеспечение.
41. Особенности защиты информации при работе в сети.
42. Безопасная работа в Internet.
43. Целесообразность усиления обороны.
44. Защита от побочного электромагнитного излучения и наводок
45. Алгоритмы распределения ключей.

Материалы для тестирования.
Выбрать из предложенных вариантов верный:

1. Что не относится к основным аппаратным средствам защиты информации:
a) пластиковые карты;
b) электронные замки;
c) магнитные карты;
d) видео карты;

2. Какой из перечисленных уровней предусматривает логическую защиту информации:
a) внешний уровень, охватывающий всю территорию расположения ВС;
b) уровень отдельных сооружений или помещений;
c) уровень технологических процессов хранения, обработки и передачи информации;
d) Уровень компонентов ВС;

3. Какой из перечисленных классов не относится к классам защиты информации:
a) Физический;
b) Программно-аппаратный;
c) Технологический;
d) Организационный;

4. Какие из перечисленных средств применяются для физической защиты информации:
a) лазерные и оптические системы;
b) механические и электронные замки;
c) телевизионные системы наблюдения;
d) все верно;

5. Для регистрации событий подключения к ВС ведется:
a) Видеонаблюдение;
b) База данных;
c) Аудит;
d) Протокол;

6. Защита от НСД со стороны пользователей в современных системах в основном реализуется:
a) парольная защита;
b) аутентификация;
c) идентификация;
d) все верно;

7. Какой из перечисленных способов не используется для аутентификации пользователя:
a) запрос секретного пароля;

b) применение микропроцессорных карточек;
c) биометрические средства;

e) Датирование;

8. Сложный вариант электронного ключа – это:
a) Пластиковая карта;
b) Жетон;
c) Шифр;
d) Подпись;

9. Из множества существующих средств аутентификации, наиболее надежными являются:
a) средства распознавания;
b) биометрические средства;
c) электронный ключ;
d) микропроцессорные карточки;

10. Что не относится к биометрическим средствам:
a) Отпечаток пальца;
b) Сетчатка глаза;
c) Голос;
d) Имя;

11. Сбор и накопление информации о событиях ИС – это:
a) Протоколирование;
b) Аудит;
c) Журнал данных;
d) Синтез;

12. Анализ накопленной информации, проводимый оперативно или периодически:
a) Синтез;
b) Протоколирование;
c) Аудит;
d) Нет правильного варианта;

13. При протоколировании рекомендуют записывать следующую информацию:
a) Дата и время события;
b) Результат события;
c) Источник запроса;
d) Все верно;

14. исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения:
a) паразит; b) вирус;
c) призрак;
d) нет верного ответа;

15. По особенностям реализуемого алгоритма вирусы делятся на:
a) спутники, стелсы, паразиты, призраки;
b) стелсы, спутники, призраки, черви;
c) паразиты, призраки, черви, стелсы;
d) нет верного ответа;

16. Рекламная рассылка – это:
a) спак;
b) спам; c) спар; d) сапс;

17. Что необходимо иметь для проверки на вирус жесткого диска:
a) защищенную программу;
b) загрузочную программу;
c) файл с антивирусной программой;
d) антивирусную программу, установленную на компьютер;

18. Основными путями проникновения вирусов в компьютер являются:
a) Гибкие диски;
b) Компьютерные сети;
c) Неадекватный пользователь;
d) Все верно;

19. Компьютерные вирусы:
a) возникают в связи со сбоями в аппаратных средствах компьютера;
b) пишутся людьми специально для нанесения ущерба;
c) зарождаются при работе неверно написанных программных продуктов;
d) являются следствием ошибок в операционной системе;

20. Загрузочные вирусы характеризуются тем, что:
a) поражают загрузочные сектора дисков;
b) поражают программы в начале их работы;
c) запускаются при загрузке компьютера;
d) изменяют весь код заражаемого файла;

21. Может ли присутствовать компьютерный вирус на чистой дискете (на дискете отсутствуют файлы)?
a) Нет;
b) да, в области данных;
c) да, в области каталога;
d) да, в загрузочном секторе дискеты;

22. Вирус, у которого каждая следующая копия в заражённых объектах отличается от предыдущих – это:
a) Стелс;
b) Спутник;
c) Призрак;
d) Паразит;

23. Самые популярные антивирусные программы – это:
a) kaspersky, avg, panda;
b) avast, kaspersky, dr web;
c) McAfee, avg, panda;
d) kaspersky, avg, Symantec;

24. Какие программы относятся к антивирусникам:
a) kaspersky, avg, paint;
b) avp, dr web, avast;
c) avg, paint, McAfee;
d) avast, kaspersky, corel;

25. Когда появились первые антивирусные утилиты:
a) 1980;
b) 1982;
c) 1984;
d) 1986;

7. Учебно-методическое и информационное обеспечение практики

В целях обеспечения самостоятельной работы аспирантов по научному исследованию, научный руководитель:

- выдает индивидуальный план работы в каждом семестре и консультирует по разработке программы и инструментария исследования;
- дает рекомендации по изучению специальной литературы и методов исследования;
- осуществляет контроль над соблюдением сроков выполнения программы исследования;
- оценивает результаты НИР и качество отчета, предлагает мероприятия по их совершенствованию.

Аспирант при прохождении практики:

- проводит исследование по выбранной теме в соответствии с программой;
- получает от научного руководителя указания, рекомендации и разъяснения по всем вопросам, связанным с организацией и подготовкой НИР;
- сдает отчет о выполненной работе в соответствии с установленной формой отчетности.

По завершению научного исследования в семестре аспирант оформляет представляет на кафедру вычислительной техники и защиты информации письменный отчет и бланк аттестации аспиранта. К отчету могут прилагаться копии статей, тезисов докладов, опубликованных за текущий семестр, а также докладов и выступлений аспирантов на научно-исследовательских семинарах, конференциях (круглых столах).

В научном исследовании применяются активные и интерактивные виды научно-исследовательской активности, например, совместное обсуждение материала, круглые столы по вопросам участия в научных конференциях по теме предмета; обсуждение материалов конференций и статей в последних научных журналах, широко освещающих тематику информационной безопасности, например, «Information Security», выполнение аспирантами под руководством преподавателя обзоров отечественной и зарубежной литературы по заданной теме.

Учебно-методическое и информационное обеспечение НИР.

1) Основная литература:

1. Герасимов, Б.И. Основы научных исследований / Б.И. Герасимов, В.В. Дробышева, Н.В. Злобина и др. – М.: Форум: НИЦ Инфра-М, 2013. – 272 с. – Режим доступа: http://znanium.com/bookread.php?book=390595;

2. Овчаров, А.О. Методология научного исследования: Учебник / А.О. Овчаров, Т.Н. Овчарова. – М.: НИЦ ИНФРА-М, 2014. – 304 с. – Режим доступа: http://znanium.com/bookread.php?book=427047;

3. Резник, С.Д. Аспирант вуза: технологии научного творчества и педагогической деятельности: Учебное пособие / С.Д. Резник. - 3-е изд., перераб. - М.: НИЦ Инфра-М, 2012. – 520 с. – Режим доступа: http://znanium.com/bookread.php?book=341977;

2) Дополнительная литература:

1. Авдонина, Л.Н. Письменные работы научного стиля: Учебное пособие / Л.Н.

Авдонина, Т.В. Гусева. – М.: Форум: НИЦ Инфра-М, 2012. – 72 с. – Режим доступа: http://znanium.com/bookread.php?book=327992;

2. Аникин, В.М. Диссертация в зеркале автореферата: Методическое пособие для аспир. и соискат. учен. степени.../В.М.Аникин, Д.А.Усанов – 3-е изд., перераб. и доп. – М.: НИЦ ИНФРА-М, 2013. – 128 с. – Режим доступа: http://znanium.com/bookread.php?book=405567;

3. Кожухар, В. М. Основы научных исследований [Электронный ресурс] : Учебное пособие / В. М. Кожухар. – М.: Дашков и К, 2013. – 216 с. – Режим доступа: http://znanium.com/bookread.php?book=415587;

Кузнецов, И.Н. Диссертационные работы. Методика подготовки и оформления / И.Н. Кузнецов. – 4-е изд. – М. : Дашков и Ко, 2012. – 488 с. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=229293;

4. Резник, С.Д. Научное руководство аспирантами: Практическое пособие / С.Д. Резник. – 2-е изд., перераб. и доп. – М.: НИЦ Инфра-М, 2012. – 477 с. – Режим доступа: http://znanium.com/bookread.php?book=304108;

5. Резник, С.Д. Эффективное научное руководство аспирантами: Монография / С.Д. Резник, С.Н. Макарова; Под общ. ред. С.Д. Резника. – 2-е изд., перераб. – М.: НИЦ ИНФРА-М, 2014. – 152 с. – Режим доступа: http://znanium.com/bookread.php?book=443292.

3) Источники Интернет:

1. Официальный сайт Министерства образования и науки Российской Федерации [Электронный ресурс]. – Режим доступа: http://mon.gov.ru;
2. Справочная правовая система «Консультант Плюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru.

8. Материально-техническое обеспечение Научных исследований

Минимально необходимый для реализации научно-исследовательской работы перечень материально-технического обеспечения включает в себя:

- лекционные аудитории (оборудованные мультимедийным оборудованием и имеющие выход в Интернет);
- аудитории для проведения семинарских и практических занятий (оборудованные учебной мебелью);
- компьютерные аудитории с выходом в Интернет;
- информационно-библиотечный центр;
- специально оборудованные аудитории для самостоятельной работы аспирантов, оснащенные компьютерами с доступом к базам данных и Интернет.

Используемые информационные технологии: используется пакет офисных программ, выход в Интернет, доступ к полнотекстовым справочным правовым системам, например, КонсультантПлюс, Гарант, доступ к электронным библиотечным системам и т.д.

9 Реализация Научных исследований лицами с ОВЗ

Выбор мест и способов прохождения Научных исследований для обучающихся инвалидов и лиц с ОВЗ осуществляется с учетом требований их доступности, а также рекомендованных условий и видов труда. В таком случае требования к структуре и содержанию научных исследований адаптируются под конкретные ограничения возможностей здоровья обучающегося, и отражаются в индивидуальном задании на Научные исследования