Аннотация дисциплины

Технологии идентификации и аутентификации пользователей и субъектов информационных процессов

специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Общая трудоемкость изучения дисциплины составляет 3 ЗЕД (108 часов).

Форма обучения: очная и заочная.

Рабочая программа дисциплины «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов» составлена на основании федеральных государственных требований к структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура), утвержденных приказом Минобрнауки РФ от 16.03.2011 г. № 1365; паспорта специальности научных работников 05.13.19 «Методы и системы защиты информации, информационная безопасность», учебного плана ЮЗГУ, программы-минимума кандидатского экзамена, утвержденного приказом Минобрнауки РФ от 08.10.2007 г. № 274.

Цель изучения дисциплины - приобретение необходимых теоретических знаний по обеспечению информационной безопасности компьютерных систем и сетей; различные способы защиты компьютерных систем от несанкционированного доступа; различные модели управления доступом к информационным ресурсам, которые используются в современных защищенных системах; принципы построения симметричных и асимметричных криптографических систем; основные современные алгоритмы симметричного и асимметричного шифрования и особенности их программной реализации.
Задачи дисциплины: получить знания о защите информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); знать основные элементы организационного обеспечения информационной безопасности; знать и уметь использовать способы защиты информации от несанкционированного доступа; математические и методические средства защиты.
В результате изучения дисциплины аспирант должен:
знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности
уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации.
владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации
Виды учебной работы: лекции, практические занятия, самостоятельная работа аспирантов.

Изучение дисциплины заканчивается кандидатским экзаменом.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Проректор по научной работе
(наименование должности полностью)

О.Г. Добросердов
(подпись, инициалы, фамилия)

«28» 06 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии идентификации и аутентификации пользователей и субъектов информационных процессов

(наименование дисциплины)

направление подготовки 10.06.01

шифр согласно ФГОС ВО

Информационная безопасность

наименование направления подготовки

Методы и системы защиты информации, информационная безопасность

наименование профиля (специализация подготовки)

квалификация (степень) выпускника: Исследователь. Преподаватель-исследователь

форма обучения очная

(очная, заочная)

Курск – 2016

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (уровень подготовки кадров высшего образования) направления подготовки 10.06.01 «Информационная безопасность», на основании учебного плана профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 11 «27» 06 2016 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения аспирантов по направлению подготовки 10.06.01 «Информационная безопасность», профиля (специализации) «Методы и системы защиты информации, информационная безопасность» на заседании кафедры информационной безопасности, протокол № 1 от «30» 08 2016 г.

Зав. кафедрой _____ М.О. Таныгин

Разработчик программы _____ Ю.А. Халин

Согласовано:

Директор научной библиотеки _____ В.Г. Макаровская

Начальник отдела аспирантуры и докторантуры _____ О.Ю. Прусова

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №1 «28» 08 2017 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №__ «__»_____20__г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №__ «__»_____20__г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____

1 Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения ОП

1.1 Цель преподавания дисциплины

Целями преподавания дисциплины являются:

— приобретение студентами необходимых теоретических знаний по обеспечению информационной безопасности компьютерных систем и сетей;

— различные способы защиты компьютерных систем от несанкционированного доступа;

— различные модели управления доступом к информационным ресурсам, которые используются в современных защищенных системах;

— принципы построения симметричных и асимметричных криптографических систем;

— основные современные алгоритмы симметричного и асимметричного шифрования и особенности их программной реализации.

1.2 Задачи изучения дисциплины

Задачами освоения дисциплины являются:

— получить знания о защите информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение);

— знать основные элементы организационного обеспечения информационной безопасности;

— знать и уметь использовать способы защиты информации от несанкционированного доступа; математические и методические средства защиты.

1.3 Компетенции, формируемые в результате освоения дисциплины

У обучающихся формируются следующие компетенции:

ОПК-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;

ПК-5 – способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа;

УК-1 - способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Системы документооборота и средства защиты циркулирующей в них информации» (Б1.В.ДВ.2) находится в вариативной части базового блока УП, изучается на 3 курсе, в 5 семестре.

3 Содержание и объем дисциплины

3.1 Содержание дисциплины и лекционных занятий

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 часов

Таблица 3.1 –Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	
в том числе:	36,1
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
экзамен	не предусмотрено
зачет	0,1
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
Самостоятельная работа обучающихся (всего)	72
Контроль/экз (подготовка к экзамену)	не предусмотрено

Таблица 3.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел, темы дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*	Компетенции
		лек., час	лаб., час	пр., час			
1	2	3	4	5	6	7	8
1	Основные понятия информационной безопасности	1, 2 часа	0	1, 2 часа	У-1, У-2, У-4	С 1-2 недели	ОПК-1, ПК-5, УК-1
2	Криптографические методы и средства обеспечения информационной безопасности	2, 2 часа	0	2, 2 часа	У-1, У-2, У-3, У-6	С 3-5 недели	ОПК-1, ПК-5, УК-1
3	Организационно-правовое обеспечение информационной безопасности	3, 2 часа	0	3, 2 часа	У-1, У-2, У-3, У-6, МУ-1, МУ-2	КО 6-7 недели	ОПК-1, ПК-5, УК-1
4	Инженерно-техническое обеспечение информационной безопасности.	4, 2 часа	0	4, 2 часа	У-2, У-3, У-5, У-7, МУ-1, МУ-2	КО 8-9 недели	ОПК-1, ПК-5, УК-1
5	Программно-аппаратное обеспечение информационной безопасности.	5, 2 часа	0	5, 2 часа	У-2, У-3, У-5, У-7, МУ-4	КО 10-11 недели	ОПК-1, ПК-5, УК-1
6	Методы и средства защиты от несанкционированного доступа.	6, 2 часа	0	6, 2 часа	У-1, У-2, У-3, У-6, МУ-3, МУ-4	Кл 12-13 недели	ОПК-1, ПК-5, УК-1
7	Методы разграничения доступа	7, 4 часа	0	7, 4 часа	У-1, У-2, У-3, У-6, МУ-3, МУ-4	Кл 14-15 недели	ОПК-1, ПК-5, УК-1
8	Средства защиты от компьютерных вирусов	8, 2 часа	0	8, 2 часа	У-1, У-2, У-3, У-6, МУ-3, МУ-4	Кл 16-18 недели	ОПК-1, ПК-5, УК-1
	ИТОГО	18		18		З	

Э– экзамен, КР – курсовая работа; КП – курсовой проект, К – контрольная работа, З – зачет, С – собеседование, СР – семестровая работа, Кл – коллоквиум, КО – контрольный опрос, МК – автоматизированный программированный контроль (машинный контроль).

Таблица 3.3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Основные понятия информационной безопасности	Понятия и определения в информационной безопасности. Основные закономерности возникновения и классификация угроз информационной безопасности.
2	Криптографические методы и средства обеспечения информационной безопасности	Криптографические методы и средства обеспечения информационной безопасности: симметричные и асимметричные алгоритмы шифрования, хеш-функции, электронная цифровая подпись
3	Организационно-правовое обеспечение информационной безопасности	Организационные мероприятия по защите информации. Законодательные меры по защите информации. Обеспечение информационной безопасности в Internet.
4	Инженерно-техническое обеспечение информационной безопасности.	Инженерно-техническое обеспечение безопасности информации Составляющие инженерно-технической защиты Меры по защите зданий и помещений
5	Программно-аппаратное обеспечение информационной безопасности.	Специализированные программные средства защиты от несанкционированного доступа, шифрования, компьютерной стеганографии и защиты от вирусов различных производителей.
6	Методы и средства защиты от несанкционированного доступа.	Идентификация и установление подлинности объекта (субъекта). Организационные мероприятия по защите информации. Законодательные меры по защите информации. Системы защиты информации от несанкционированного доступа
7	Методы разграничения доступа	Разграничение и контроль доступа к информации. Методы и средства защиты информации от случайного воздействия. Методы защиты информации от аварийных ситуаций.
8	Средства защиты от компьютерных вирусов	Классификация "компьютерных вирусов". Файловые вирусы. Загрузочные вирусы. Макровирусы. Сетевые вирусы. Источники "компьютерных вирусов". Основные правила защиты от "компьютерных вирусов". Антивирусные программы. Восстановление пораженных объектов.

3.2 Лабораторные работы и (или) практические занятия
3.2.2 Практические занятия

Таблица 3.5 –Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Шифры донаучного периода. Криптологии.	2
2	Симметричные криптографические алгоритмы. Алгоритм ГОСТ.	2
3	Асимметричные криптографические алгоритмы. Алгоритм RSA/	2
4	Электронная цифровая подпись.	2
5	Защита компьютерных систем от вредоносных программ.	4
6	Комплексная система защиты информации.	2
7	Методы разграничения доступа.	4
Итого		18

3.3 Самостоятельная работа аспирантов (СРС)

Таблица 3.6 – Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Зашифровать свое ФИО алгоритмом ГОСТ 2 раунда.	2 - 3 неделя	5
2	Зашифровать свои инициалы алгоритмом RSA	4 - 5 неделя	5
3	Создать хеш-функцию.	6 - 7 неделя	5
4	Создание электронную цифровую подпись	8 - 16 неделя	35
5	Виды атак на компьютерную систему		17
6	Методы разграничения доступа	17 - 18 неделя	15
Итого			72

Общие рекомендации аспирантам изложены в Методических указаниях к выполнению самостоятельной работы.

4 Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

Аспиранты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки:

– методических рекомендаций, пособий по организации самостоятельной

– работы студентов;

– тем рефератов;

– вопросов к зачету;

– методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

– удовлетворение потребности в тиражировании научной, учебной и методической литературы.

5 Образовательные технологии

В соответствии с требованиями Федеральным государственным образовательным стандартом высшего образования направления подготовки *10.06.01 – «Информационная безопасность»,* утвержденного Министерством образования и науки Российской Федерации приказом № 301 от 05.04.2017г., реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков аспирантов.В рамках дисциплины предусмотрены встречи с экспертами и специалистами по информационной системам.

Таблица 5.1 – Образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	Семинар на тему «Криптографические методы и средства обеспечения информационной безопасности»	Компьютерная презентация	2
2	Семинар на тему «Инженерно-техническое обеспечение информационной безопасности.»	Компьютерная презентация	2
3	Семинар на тему «Программно-аппаратное обеспечение информационной безопасности»	Компьютерная презентация	2
4	Практическое занятие «Защита компьютерных систем от вредоносных программ»	Разбор конкретных ситуаций	2
5	Практическое занятие «Методы разграничения доступа»	Разбор конкретных ситуаций	2
Итого			10

6 Фонд оценочных средств для проведения промежуточной аттестации

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 6.1 Этапы формирования компетенции

Код компетенции, содержание компетенции	Дисциплины (модули) при изучении которых формируется данная компетенция
1	2
ОПК-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	Б1.В.ОД.4Методология научных исследований при подготовке диссертации Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)

ПК-5 - способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
УК-1 - анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Б1.Б.1 История и философия науки Б1.В.ОД.1 Методология науки и образовательной деятельности Б1.В.ОД.4 Методология научных исследований Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.2 Технология идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.1 Педагогическая практика Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)

Средствами промежуточного контроля успеваемости студентов являются защита практических заданий, опросы на практических занятиях по темам лекций. В конце семестра – зачет. Перечень вопросов к зачеты представлен в приложении Б.

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 6.2 Показатели и критерии определения уровня сформированности компетенций (частей компетенций)

№ п/п	Код компетенции (или её части)	Уровни сформированности компетенции		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
1	ОПК–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.	Знать: методологию исследовательской деятельности, основные проблемы в области информационной безопасности; Уметь: определять программу проведения исследований, Владеть: способностью к критическому анализу результатов научного творчества	Знать: основы культуры научного исследования в информационной безопасности, Уметь: использовать и применять их в современных информационно-коммуникационных технологиях Владеть: планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач	Знать: основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач Уметь: использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельностях Владеть: организационными формами и методами проведения научных исследований;
2	ПК-5 – способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств

			теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации
3	УК-1 - способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 6.3 Паспорт комплекта оценочных средств

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия информационной безопасности Криптографические методы и средства обеспечения информационной безопасности	ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Лекция с элементами проблемного изложения	См. МУ	Оценивая ответ, члены комиссии учитывают следующие *основные критерии*: – уровень теоретических знаний (подразумевается не только формальное воспроизведение информации, но и понимание предмета, которое подтверждается правильными ответами на дополнительные, уточняющие вопросы, заданные членами комиссии); – умение использовать теоретические знания при анализе конкретных проблем, ситуаций; – качество изложения материала, то есть обоснованность, четкость, логичность ответа, а также его полнота (то есть содержательность, не исключающая сжатости); - способность устанавливать внутри- и межпредметные связи, оригинальность и красота мышления, знакомство с дополнительной литературой и множество
		ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Собеседование	См. МУ	
2	Организационно-правовое обеспечение информационной безопасности Инженерно-техническое обеспечение информационной безопасности.	ОПК-1 ПК-5 УК-1	Лекция	Лекция с элементами проблемного изложения	См. МУ	
		ОПК-1 ПК-5 УК-1	Практическое занятие	Практическая работа	См. МУ	
3	Программно-аппаратное обеспечение информационной безопасности. Методы и средства защиты от несанкционированного доступа.	ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Практическая работа		
4	Методы	ОПК-1	Лекция	Сообще	См.	

	разграничения доступа	ПК-5 УК-1	Практическое занятие	ние студента Практическая работа	МУ	других факторов. *Критерии оценок:* Оценка *зачтено* – исчерпывающее владение программным материалом, понимание сущности рассматриваемых процессов и явлений, твѐрдое знание основных положений дисциплины, умение применять концептуальный аппарат при анализе актуальных проблем. Логически последовательные, содержательные, конкретные ответы на все вопросы экзаменационного билета и на дополнительные вопросы членов комиссии, свободное владение источниками. Предложенные в качестве самостоятельной работы формы работы (примерный план исследовательской деятельности; пробная рабочая программа) приняты без замечаний. Оценка *не зачтено* – отсутствие ответа хотя бы на один из основных вопросов, либо грубые ошибки в ответах, полное непонимание смысла проблем, не достаточно полное владение терминологией. Отсутствие выполненных самостоятельных дополнительных работ.
		ОПК-1 ПК-5 УК-1	Лекция Практическое занятие			
5	Основные понятия информационной безопасности	ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Сообщение студента	См. МУ	
6	Криптографические методы и средства обеспечения информационной безопасности Организационно-правовое обеспечение информационной безопасности	ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Практическая работа		
7	Инженерно-техническое обеспечение информационной безопасности. Программно-аппаратное обеспечение информационной безопасности.	ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Практическая работа		
8	Методы и средства защиты от несанкционированного доступа.	ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ОПК-1 ПК-5 УК-1	Лекция Практическое занятие	Практическая работа		

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Список методических указаний, используемых в образовательном процессе, представлен в п. 7.2;
- Оценочные средства представлены в учебно-методическом комплексе дисциплины.

Материалы для проведения промежуточных и итоговых аттестаций

1. Информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира, называется
1. ценной
2. своевременной
3. достоверной
4. конфиденциальной

2. Такое состояние всех компонент компьютерной системы (КС), при котором обеспечивается защита информации от возможных угроз на требуемом уровне, называется
1. конфиденциальность КС
2. доступность КС
3. защищенность КС
4. безопасность КС
5. такого понятия не существует

3. Процедура распознавания пользователя по его идентификатору
1. санкционированный доступ
2. несанкционированный доступ
3. идентификация
4. аутентификация
5. нет правильных ответов

4. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена
1. конфиденциальность
2. целостность
3. аутентичность
4. надежность
5. точность

5. Наука о способах двунаправленного преобразования информации с целью конфиденциальной передачи ее по незащищенному каналу

1. криптология
2. криптография
3. стеганография
4. криптоанализ

6. Одно из требований, предъявляемым к криптоалгоритмам

1. длина зашифрованного сообщения должна быть равна длине открытого текста
2. длина зашифрованного сообщения должна быть меньше длины открытого текста
3. длина открытого текста должна быть меньше длины зашифрованного сообщения
4. не должно быть никакой зависимости между длиной зашифрованного сообщения и длиной открытого текста

7. Объектом защиты является

1. комплекс средств, обрабатывающих информацию
2. информация, хранящаяся, обрабатываемая в компьютерных системах
3. информация, передаваемая по незащищенному каналу
4. персонал, обслуживающий компьютерную систему

8. Единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности называется

1. идентификацией
2. аутентификацией
3. политикой информационной безопасности
4. системой защиты информации
5. программной информационной безопасности

9. Предметом защиты является:

1. компьютерная система
2. информация, хранящаяся, обрабатываемая в компьютерных системах
3. информация, передаваемая по незащищенному каналу
4. персонал, обслуживающий компьютерную систему

10. Шифрование – это:

1. процесс преобразования открытой информации в закрытую с уменьшением ее объема
2. процесс преобразования закрытой информации в открытую с сохранением прежнего объема
3. процесс преобразования открытой информации в закрытую с сохранением прежнего объема

4. процесс преобразования закрытой информации в открытую с увеличением прежнего объема

11. Симметричная криптография подразумевает:

1. использование одного и того же ключа как для зашифрования, так и для расшифрования
2. использование одного (открытого) ключа для зашифрования, второго (секретного) – для расшифрования
3. использование одного (секретного) ключа для зашифрования, второго (открытого) – для расшифрования
4. использование механических и химических способов сокрытия информации
5. сокрытие самого факта передачи информации

12. Стеганография подразумевает:

1. использование одного и того же ключа как для зашифрования, так и для расшифрования
2. использование одного (открытого) ключа для зашифрования, второго (секретного) – для расшифрования
3. использование одного (секретного) ключа для зашифрования, второго (открытого) – для расшифрования
4. использование механических и химических способов сокрытия информации
5. сокрытие самого факта передачи информации

13. При шифровании методом подстановки:

1. знак исходного текста заменяется одним или несколькими знаками, порядок следования символов изменяется
2. знак исходного текста заменяется одним или несколькими знаками, порядок следования символов не изменяется
3. знак исходного текста не заменяется другими знаками, и порядок следования символов в сообщении не изменяется
4. знак исходного текста не заменяется другими знаками, но порядок следования символов изменяется

14. Шифры, переставляющие элементы открытых данных в некотором новом порядке, называются шифрами:

1. подстановки
2. замены
3. перестановки
4. упорядочивания

15. Асимметричная криптография подразумевает:

1. использование одного и того же ключа как для зашифрования, так и для расшифрования

2. использование одного (открытого) ключа для зашифрования, второго (секретного) – для расшифрования
3. использование одного (секретного) ключа для зашифрования, второго (открытого) – для расшифрования
4. использование механических и химических способов сокрытия информации
5. сокрытие самого факта передачи информации

16. Размер ключа в ГОСТ 28147-89:
1. 16 бит
2. 16 байт
3. 32 бит
4. 32 байт
5. 64 бит
6. 128 бит
7. нет правильных вариантов

17. Секретными элементами российского шифра ГОСТ 28147-89 являются:
1. размер ключа и алгоритм шифрования
2. алгоритм шифрования и ключ шифрования
3. ключ шифрования и таблица замен
4. таблица замен и состав блоков
5. таблица замен и алгоритм шифрования

18. Хэширование (Hashing) в криптографии - это:
1. преобразование блока произвольного размера в блок фиксированного размера
2. преобразование блока фиксированного размера в блок другого, заранее заданного размера
3. процедура генерации ключей для ЭЦП
4. расширение последнего блока сообщения до требуемой длины
5. уменьшение последнего блока сообщения до требуемой длины

19. Необратимость хэш-функции означает:
1. хеш-функция имеет бесконечную область определения
2. хеш-функция имеет конечную область значений
3. легко создать хэш-код по данному сообщению, но невозможно восстановить сообщение по данному хэш-коду
4. изменение входного потока информации на один бит меняет около половины всех бит выходного потока
5. изменение входного потока информации на один бит меняет все биты выходного потока

20. Что такое RSA?
1. шифр Rich Standard Advanced

2. шифр Rich Standard Algorithm
3. шифр RightSecurityAlgorithm
4. шифр, названный по именам его создателей: Rivest, Shamir, Adleman
5. шифр RichSizeAlgorithm
6. RealSignatureAlgorithm

Отчет по индивидуальным заданиям.

1. Выполните первый цикл алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

2. Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

3. Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

Вопросы к коллоквиуму:

1. Основные понятия информационной безопасности.
2. Классификация атак.
3. Механизмы и сервисы безопасности.
4. Способы и средства нарушения конфиденциальности.
5. Методы разграничения доступа.
6. Классификация вирусов.
7. Классификация антивирусных программ.
8. Организационно-правовое обеспечение информационной безопасности
9. Инженерно-техническое обеспечение информационной безопасности.
10. Программно-аппаратное обеспечение информационной безопасности.
11. Комплексная система защиты информации.
12. Методы и средства защиты от несанкционированного доступа.
13. Методы разграничения доступа.

Вопросы к зачету:

1. Основные задачи службы защиты информации предприятия.
2. Что такое информационная безопасность? Понятия и определения в информационной безопасности
3. Пользователи и злоумышленники в Internet.
4. Причины уязвимости сети Internet.
5. Основные закономерности возникновения и классификация угроз информационной безопасности.
6. Пути и каналы утечки информации.
7. Удаленные атаки на интрасети.
8. Классификация "компьютерных вирусов".

9. Файловые вирусы.
10. Загрузочные вирусы.
11. Макровирусы.
12. Сетевые вирусы.
13. Источники "компьютерных вирусов".
14. Основные правила защиты от "компьютерных вирусов".
15. Антивирусные программы.
16. Восстановление пораженных объектов.
17. Стандарт США "Оранжевая книга".
18. Перечислите руководящие документы Гостехкомиссии Российской Федерации?
19. Разграничение и контроль доступа к информации.
20. Идентификация и установление подлинности объекта (субъекта).
21. Методы и средства защиты информации от случайного воздействия.
22. Методы защиты информации от аварийных ситуаций.
23. Организационные мероприятия по защите информации.
24. Законодательные меры по защите информации.
25. Обеспечение информационной безопасности в Internet.

Рейтинговый контроль не предусмотрен.

Описание оценочных средств и шкал оценивания ответов см. в Таблице 6.3.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная и дополнительная литература

а) Основная литература:

1. Таныгин, М. О. Программно-аппаратные системы защиты информации [Текст] : учебное пособие / Юго-Западный гос. ун-т ; Министерство образования и науки Российской Федерации, Юго-Западный государственный университет. – Курск : ЮЗГУ, 2012. - 147 с.
2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : учебное пособие / Л. В. Кнауб, Е. Новиков, Ю. Шитов. - Красноярск : Сибирский федеральный университет, 2011. – 160 с. – Режим доступа : Biblioclub.ru
3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=276557
4. Методологические основы построения защищенных автоматизированных систем [Электронный ресурс] : учебное пособие / А. В. Душкин [и др.]. – Воронеж : ВГУИТ, 2013. - 258 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=25585

б) Дополнительная литература:

1. Гатченко, Н. А. Криптографическая защита информации [Электронный ресурс] : учебное пособие / Н. А. Гатченко, А. С. Исаев.- СПб. : НИУ ИТМО, 2012. - 142 с. - Режим доступа : http://window.edu.ru
2. Ветров Ю. В. Криптографические методы защиты информации в телекоммуникационных системах [Электронный ресурс] / Ю. В. Ветров, С. Б. Макаров . - СПб. : Изд-во Политехн. ун-та, 2011. – 174 с. – Режим доступа : http://window.edu.ru
3. Техника защиты информации. Защита информации [Текст] : требования к средствам высоконадежной биометрической аутентификации / Федеральное агентство по техническому регулированию и метрологии, Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому экспортному контролю (ГНИИИ ПТЗИ ФСТЭК России), Технический комитет по стандартизации ТК 362 "Защита информации". - Изд. офиц.введен впервые, введен 27.12.2006. - М. : Стандартинформ, 2007. - 19 с.
4. Жуков, И. Ю. Стохастические методы и средства защиты информации в компьютерных системах и сетях [Текст] / под ред. И. Ю. Жукова. - М. : КУДИЦ-ПРЕСС, 2009. - 512 с.
5. Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с.

6. Семкин, С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации [Текст] : учебное пособие / С. Н. Семкин [и др.]. - М. : Гелиос АРВ, 2005. - 192 с.

7. Тихонов, В. А. Информационная безопасность : концептуальные, правовые, организационные и технические аспекты [Текст] : учебное пособие / В. А. Тихонов, В. В. Райх. - М. : Гелиос АРВ, 2006. – 528 с.

7.2 Перечень методических указаний

1. Защита информации от несанкционированного доступа [Текст] : учебно-методическое пособие / А. А. Веретенников; НОУ ВПО "Региональный открытый социальный институт", Кафедра программного обеспечения. - Курск: РОСИ, 2006. - 40 с.

2. Первичное развертывание сети ViPNet [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. – Курск : ЮЗГУ, 2014. - 26 с.

3. Действия при изменениях в структуре сети ViPNet [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. – Курск : ЮЗГУ, 2014. - 26 с.

4. Настройка межсетевого взаимодействия [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. – Курск : ЮЗГУ, 2014. - 20 с.

5. ViPNet Деловая почта [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. – Курск : ЮЗГУ, 2012. - 20 с.

7.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Корпорация Microsoft [официальный сайт]. Режим доступа: http://www.microsoft.com/

2. Рускоязычный сайт сообщества Ubuntu [сайт]. Режим доступа: http://ubuntu.ru/

7.4 Перечень информационных технологий

1. MicrosoftOfficePowerPoint;
2. MicrosoftOfficeExcel;
3. ДиспетчеррисунковMicrosoftOffice:
4. MATLAB.

7.5 Другие учебно-методические материалы

Программно-аппаратный комплекс защиты информации «SECRETNET 5.0»/ Методические указаний по выполнению лабораторной работы. Состав. В.Н. Лопин, М.О. Таныгин, КГТУ, Курск, 2008.

Базы данных, информационно-справочные и поисковые системы:

1. www.edu.ru - федеральный портал «Российское образование»
2. www.elibrary.ru/defaultx.asp - научная электронная библиотека.

8 Материально-техническое обеспечение дисциплины

Для обеспечения учебного процесса используются: лекционная аудитория, оснащенная мультимедийными средствами, аудитория для практических занятий, компьютерная аудитория, обеспечивающая выход в ИНТЕРНЕТ.

8 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

№ изменения	Номера страниц				Всего	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1		3			1	01.09.17	Приказ ФГБОУ «Юго-Западный государственный университет» № 576 от 31.08.2017 г. « О внесении изменений в приказ №263 от 29.03.2017 г. « Об утверждении норм времени для расчета учебной и других видов работы»
2		8			1	01.09.17	Приказ № 301 от 05.04.2017 г.
3		21-22			2	13.12.17	Протокол заседания кафедры ИСиТ №10 от 13.12.17