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

Алгоритмы факторизации натуральных чисел как средство реализации ассиметричного шифрования
(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 № 01 «26» 08 2017 г. на заседании кафедры информационной безопасности.

Зав. кафедрой / протокол №1 от 28.08.2017

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 № 9 «26» 03 2018 г. на заседании кафедры информационной безопасности.

Зав. кафедрой / протокол №12 от 29.06.2018

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 № 9 «24» 06 2019 г. на заседании кафедры информационной безопасности.

Зав. кафедрой / протокол №11 от 27.06.2019

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 №11 «29» 06 2020г. на заседании кафедры информационной безопасности.

Зав. кафедрой / протокол N 1 от 31.08.2020

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 №8 «31» 05 2021г. на заседании кафедры информационной безопасности.

Зав. кафедрой / протокол N 11 от 28.06.2021

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____

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

Целью преподавания дисциплины являетсяформирование у студентов системы знаний в области информационной безопасности и применения на практике ассиметричного шифрования.

1.2 Задачи изучения дисциплины

Задачами освоения дисциплины являются:

- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- ознакомление с симметричными и ассиметричными криптосистемами, изучение скремблеров, алгоритмов RSA, AES, Виженера, электронно-цифровой подписи;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно – программных систем идентификации и аутентификации;
- изучение моделей безопасности операционных систем UNIX, WindowsXP-Professional, Windows 7;
- изучение классификации межсетевых экранов, функций межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение методики проектирования систем защиты информации;
- изучение методики управления процессами функционирования систем защиты.

1.3 Компетенции, формируемые в результате освоения дисциплины

У обучающихся формируются следующие компетенции:

ПК-1 - способностью к решению научных и технических проблем разработки новых и совершенствования имеющихся методов и средств защиты информации и обеспечения информационной безопасности объектов;

ПК-3 – способность анализировать степень защищенности и совершенствовать системы документооборота и средства защиты циркулирующей в них информации;

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;

УК-6 –способность планировать и решать задачи собственного профессионального и личностного развития.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Алгоритмы факторизации натуральных чисел как средство реализации ассиметричного шифрования » (Б1.В.ДВ.2) находится в вариативной части базового блока УП, изучается на 3 курсе, в 6 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	Проблемы информационной безопасности сетей	1, 2 часа	0	1, 2 часа	У-1, У-2,	С 1-2 недели	ПК-1, ПК-3, УК-1, УК-6
2	Политика безопасности	2, 2 часа	0	2, 2 часа	У-1, У-2, У-3, У-6	С 3-4 недели	ПК-1, ПК-3, УК-1, УК-6
3	Криптографическая защита информации	3, 2 часа	0	3, 2 часа	У-1, У-2, МУ-1, МУ-2	КО 5-6 недели	ПК-1, ПК-3, УК-1, УК-6
4	Технологии аутентификации	4, 2 часа	0	4, 2 часа	У-2, У-3, У-5, У-7, МУ-1, МУ-2	КО 7-8 недели	ПК-1, ПК-3, УК-1, УК-6
5	Модели безопасности операционных систем	5, 2 часа	0	5, 2 часа	У-2, У-3, У-5, У-7,	КО 9-10 недели	ПК-1, ПК-3, УК-1, УК-6
6	Методы факторизации натуральных чисел	6, 2 часа	0	6, 2 часа	У-1, У-2, У-3, У-6,	К 11-12 недели	ПК-1, ПК-3, УК-1, УК-6
7	Аппаратно ориентированные алгоритмы факторизации	7, 2 часа	0	7, 2 часа	У-2, У-3, У-5, У-7, МУ-1, МУ-2	КО 13-14 недели	ПК-1, ПК-3, УК-1, УК-6
8	Требования к системам защиты информации	8, 2 часа	0	8, 2 часа	У-2, У-3, У-5, У-7, МУ-1, МУ-2	КО 15-16 недели	ПК-1, ПК-3, УК-1, УК-6
9	Проектирование систем защиты информации	9, 2 часа	0	9, 2 часа	У-2, У-3, У-5, У-7, МУ-1, МУ-2	К 17-18недели	ПК-1, ПК-3, УК-1, УК-6
	ИТОГО	18		18		З	

Таблица 3.3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Проблемы информационной безопасности сетей	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP – сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.
2	Политика безопасности	Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети: физическая безопасность, логическая безопасность, защита ресурсов, определение административных полномочий, аудит и оповещение.
3	Криптографическая защита информации	Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные криптосистемы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Скремблеры. Стандарт шифрования AES. Алгоритм шифрования RSA. Ассиметричные криптосистемы на базе эллиптических кривых. Функция хэширования. Электронная цифровая подпись (ЭЦП). Защита электронного документооборота с использованием ЭЦП.
4	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно – программные системы идентификации и аутентификации.
5	Модели безопасности операционных систем	Угрозы безопасности операционной системы. Понятие защищенной операционной системы. Основные функции подсистемы защиты операционной системы. Идентификация, аутентификация и авторизация субъектов доступа в операционной системе. Разграничение доступа к объектам операционной системы. Аудит. Требования к

		аудиту. Политика аудита. Защита в операционной системе UNIX. Средства безопасности OCWINDOWSXP-Professional, OCWINDOWS 7.
6	Основы факторизации натуральных чисел	Решето Эратосфена и критерии простоты. Метод пробных делений. Решето Аткина. Тест Поклингтона. Генерация простых чисел. Расширенный алгоритм Евклида. Символ Лежандра. Метод Ферма. Метод Полларда. Метод Вильямса. Метод Полларда для вычисления дискретного логарифма. Факторизация с использованием непрерывных дробей. Факторизация с использованием квадратичных форм.
7	Аппаратно ориентированные алгоритмы факторизации	Наиболее популярные на сегодняшний день алгоритмы факторизации целых чисел, варианты их параллельной реализации в кластерных вычислительных системах. Получение сравнительных оценок для каждого метода на различном числе параллельных процессов. Выводы об эффективности использования алгоритмов.
8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.
9	Проектирование систем защиты информации	Основы теории защиты информации. Моделирование процессов защиты информации. Угрозы и оценка уязвимости информации. Модели оценки ущерба от реализации угроз безопасности информации. Определение, типизация и стандартизация систем защиты информации. Система защиты информации как многокритериальный развивающийся объект. Проектирование систем защиты информации. Управление процессами функционирования систем защиты.

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	Проблемы информационной безопасности сетей	2
2	Политика безопасности	2
3	Криптографическая защита информации	2
4	Технологии аутентификации	2
5	Модели безопасности операционных систем	2

6	Основы факторизации натуральных чисел	2
7	Аппаратно ориентированные алгоритмы факторизации	2
8	Требования к системам защиты информации	2
9	Проектирование систем защиты информации	2
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	Проблемы информационной безопасности сетей	1-2 недели	8
2	Политика безопасности	3-4 недели	8
3	Криптографическая защита информации	5-7 недели	8
4	Технологии аутентификации	8-9 недели	8
5	Модели безопасности операционных систем	10-11 недели	8
6	Основы факторизации натуральных чисел	12-13 недели	8
7	Аппаратно ориентированные алгоритмы факторизации	14-15 недели	8
8	Требования к системам защиты информации	16-17 недели	8
9	Проектирование систем защиты информации	18 неделя	8
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 «Проблемы информационной безопасности сетей»	Компьютерная презентация	2
2	Семинар на тему «Технологии аутентификации»	Компьютерная презентация	2
3	Семинар на тему «Модели безопасности операци-	Компьютерная	2

	онных систем»	презентация	
4	Практическое занятие «Факторизация натуральных чисел»	Разбор конкретных ситуаций	2
5	Практическое занятие «Аппаратно ориентированные методы факторизации»	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
ПК-1 - способность к решению научных и технических проблем разработки новых и совершенствования имеющихся методов и средств защиты информации и обеспечения информационной безопасности объектов	Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.2 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)
ПК-3 – способность анализировать степень защищенности и совершенствовать системы документооборота и средства защиты циркулирующей в них информации	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
УК-1 - анализу и оценке современных научных достиже-	Б1.Б.1 История и философия науки Б1.В.ОД.1 Методология науки и образовательной деятель-

ний, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	ности 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)
УК-6 - способность планировать и решать задачи собственного профессионального и личностного развития	Б1.Б.1 История и философия науки Б1.В.ОД.3 Психология и педагогика Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации ассиметричного шифрования Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.1Педагогическая 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.

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	ПК-1	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
2	ПК-3	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.	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

			Владеть: основами 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	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 ин-

				формации
4	УК-6 - способность планировать и решать задачи собственного профессионального и личностного развития	Знать: -методологию исследовательской деятельности, основные проблемы в области информационной безопасности; Уметь: - определять программу проведения исследований, Владеть: - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач	Знать: - основы культуры научного исследования в информационной безопасности, Уметь: - использовать и применять их в современных информационно-коммуникационных технологиях Владеть: - способностью к критическому анализу результатов научного творчества	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;

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	Проблемы информационной безопасности сетей	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	Оценивая ответ, члены комиссии учитывают следующие *основные критерии*: – уровень теоретических знаний (подразумевается не только формальное воспроизведение информации, но и пони-
		ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Собеседование	См. МУ	

2	Политика безопасности	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	мание 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 других факторов. *Критерии оценок:* Оценка *зачтено* – исчерпывающее владение программным материалом, понимание сущности рассматриваемых процессов и явлений, твèрдое 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.
		ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Практическая работа	См. МУ	
3	Криптографическая защита информации	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Практическая работа		
4	Технологии аутентификации	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента Практическая работа	См. МУ	
		ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие			
5	Модели безопасности операционных систем	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
6	Основы факторизации натуральных чисел	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Практическая работа		
7	Основы факторизации натуральных чисел	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Практическая работа		
8	Требования к системам защиты информации	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ПК-1 УК-3 УК-1	Лекция Практическое заня-	Практическая работа		

		УК-6	тие			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..
9	Проектирование систем защиты информации	ПК-1 УК-3 УК-1 УК-6	Лекция Практическое занятие	Сообщение студента	См. МУ	
		ПК-1 УК-3 УК-1 УК-6	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.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная и дополнительная литература

а) Основная литература:

1. Применко, Э. А. Алгебраические основы криптографии [Текст] : учебное пособие / Э. А. Применко. - Москва :Либроком, 2013. - 288 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

б) Дополнительная литература:

1. Рябко, Б. Я. Основы современной криптографии и стенографии [Текст] : монография / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия-Телеком, 2010. - 232 с.
2. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Текст] / М. А. Иванов. - М. : КУДИЦ-ОБРАЗ, 2001. - 368 с.
3. Таранников, Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии [Текст] / Ю. В. Таранников. - М. : МЦНМО, 2011. - 152 с.
4. Алферов, А. П. Основы криптографии [Текст] :учеб.пособие / А. П. Алферов [и др.]. - М. : Гелиос АРВ, 2001. - 480 с.
5. Баричев, С. Г. Основы современной криптографии [Текст] :учеб.курс / В. В. Гончаров, Р. Е. Серов. - 2-е изд., перераб. и доп. - М. : Горячая линия - Телеком, 2002. - 175 с.
6. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Текст] / О. Н. Василенко ; Институт проблем информационной безопасности МГУ. - М. : МЦНМО, 2003. - 328 с.
7. Смарт, Н. Криптография [Текст] / Н. Смарт. - М. :Техносфера, 2005. - 528 с.
8. Фергюсон, Н. Практическая криптография [Текст] / Н. Фергюсон, Б. Шнайер. - М. : Вильямс, 2005. - 424 с.
9. Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с.

7.2 Перечень методических указаний

1. Алгоритмы цифровой подписи [Электронный ресурс] : методические указания по выполнению курсовой работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (782 КБ). - Курск : ЮЗГУ, 2016. - 31 с.

7.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет

2. Корпорация Microsoft [официальный сайт]. Режим доступа: http://www.microsoft.com/
3. Рускоязычный сайт сообщества Ubuntu [сайт]. Режим доступа: http://ubuntu.ru/

7.4 Перечень информационных технологий

Microsoft Office Power Point;
Microsoft Office Excel;
Диспетчер рисунков Microsoft Office: (Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал».)

7.5 Другие учебно-методические материалы

18. Специальные требования и рекомендации по защите информации СТР-К, Государственная техническая комиссия при Президенте Российской Федерации. 2001.
19. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-2002.
20. Гражданский кодекс РФ.
21. ФЗ № 24 от 20.02.95 «Об информации, информатизации и защите информации».
22. ФЗ№ 15 от 20.01.95 «О связи».
23. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

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		4			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		9			1	01.09.17	Приказ № 301 от 05.04.2017 г.
3		23-24			2	13.12.17	Протокол заседания кафедры ИСиТ №10 от 13.12.17