Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ
Декан, председатель совета факультета КТВТиЭ
_____ **Ш.А. Юсуфов**
24.09 **2018**

УТВЕРЖДАЮ
Проректор по учебной работе, председатель методического совета ДГТУ
_____ **Н.С. Суракатов**
26.09 **2018**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Б1.В.ДВ.4 «Информационная безопасность»
наименование дисциплины по ООП и код по ФГОС

для направления 01.03.02 – «Прикладная математика и информатика»
шифр и полное наименование направления

по профилю Системное программирование и компьютерные технологии

факультет компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационных технологий и прикладной информатики в экономике
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника Бакалавр
бакалавр

Форма обучения очная, курс 4 семестр (ы) 7.
очная, заочная, др.

Всего трудоемкость в зачетных единицах (часах) 4 ЗЕТ (144 ч.):

лекции 17 (час); экзамен 7 - 1 ЗЕТ(36 ч.);
(семестр)

практические (семинарские) занятия - (час); зачет -
(семестр)

лабораторные занятия 34 (час); самостоятельная работа 57 (час);

курсовой проект (работа, РГР) - (семестр).

Зав. кафедрой _____ А.М. Абдулгалимов
подпись ФИО

Начальник УО _____ Э.В. Магомаева
подпись ФИО

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению 01.03.02 – «Прикладная математика и информатика», профилю подготовки: «Системное программирование и компьютерные технологии»

Программа одобрена на заседании выпускающей кафедры прикладной математики и информатики (ПМиИ). Протокол № 1 от 20.09.2018 г.

Зав. выпускающей кафедрой по данному направлению Т.И. Исабекова

ОДОБРЕНО:

Методической комиссией по укрупненной группе специальностей и направлений подготовки 01.00.00 – «Прикладная математика и информатика»

Председатель МК

Т.И. Исабекова

подпись ФИО

20.09 2018

АВТОРЫ(Ы) ПРОГРАММЫ:

А.М. Абдулгалимов, д.э.н., профессор, зав. каф. ИТиПИвЭ
С.Т. Ахмедханова, к.э.н., доцент кафедры ИТиПИвЭ

Ф.И.О, уч. степень, ученое звание, подпись

1. Цель и задачи освоения дисциплины.

Цель изучения дисциплины: обучение студентов основам защиты информации в информационных системах и формирование у них навыков использования существующих пакетов программ и технических средств по информационной безопасности в их дальнейшей деятельности.

Задачи изучения дисциплины: приобретение студентами прочных знаний и практических навыков в области, определяемой целью курса.

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Информационная безопасность» в учебном процессе подготовки бакалавров направления 01.03.02 – «Прикладная математика и информатика» по профилю «Системное программирование и компьютерные технологии» относится к дисциплинам по выбору Блока 1 рабочего учебного плана. Знания, полученные в результате изучения этой дисциплины, будут использоваться студентом в своей дальнейшей учебе и практической деятельности, так как ему придется работать в условиях жесткой рыночной конкуренции и практически постоянных попыток злоумышленников получить несанкционированный доступ к конфиденциальной информации.

Изучение дисциплины предполагает наличие у студентов школьных знаний, а также знаний по курсам: «Математика», «Информатика», «Операционные системы», «Вычислительные методы», «Вычислительные системы, сети и телекоммуникации», «Разработка и стандартизация программных средств и информационных технологий», «Основы сайтостроения и Web-дизайн».

Основными видами занятий являются лекции и лабораторные занятия. Для освоения дисциплины наряду с проработкой лекционного материала необходимо проведение самостоятельной работы.

Основными видами текущего контроля знаний являются контрольные и лабораторные работы по каждой теме.

Основным видом рубежного контроля знаний является экзамен.

Список дисциплин, для которых освоение данной дисциплины необходимо как предшествующее: «Моделирование рисковых ситуаций», «Стандартизация, сертификация, и управление качеством программного обеспечения», «Прикладные задачи системного анализа», «Поддержка приложений в пользовательских операционных системах», «Имитационное моделирование», «Математическое моделирование на ЭВМ», «Объектно-ориентированное моделирование» и дальнейшее обучение в магистратуре по направлению 09.04.03 - «Прикладная информатика».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Компьтерные сети и информационная безопасность в сети»

В результате освоения дисциплины «Информационная безопасность» обучающийся по направлению подготовки 01.03.02 – «Прикладная математика и информатика» по профилю «Системное программирование и компьютерные технологии» в соответствии с ФГОС ВО должен обладать следующими компетенциями:

способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой (ОПК-1);
способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии (ОПК-2);
способностью к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям (ОПК-3);
способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4).
способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям (ПК-1);
способностью работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности (ПК-4);
способностью формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций (ПК-6);
способностью составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы (ПК-9);

В результате изучения дисциплины студенты должны:

В результате изучения дисциплины студент должен:

***знать*:**

виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них;

аппаратные и программные средства резервного копирования данных;

методы обеспечения защиты компьютерных сетей от несанкционированного доступа;

специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами;

состав мероприятий по защите персональных данных общие основы решения практических задач по созданию резервных копий БД;

специальные знания по работе с установленной БД;

общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных;

основы управления учетными записями пользователей;

общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети;

архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети;

инструкции по установке администрируемых сетевых устройств;

инструкции по эксплуатации администрируемых сетевых устройств;

инструкции по установке администрируемого программного обеспечения;

инструкции по эксплуатации администрируемого программного обеспечения;

протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем;

модель ISO для управления сетевым трафиком;

модели IEEE;

инструкции по установке операционных систем;

***уметь*:**

обеспечивать резервное копирование данных;

осуществлять меры по защите компьютерных сетей от несанкционированного доступа;

применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами;

осуществлять мероприятия по защите персональных данных;

вести отчетную и техническую документацию;

выбирать способ действия из известных: контролировать, оценивать и корректировать свои действия;

выполнять регламентные процедуры по восстановлению и проверке корректности восстановленных данных;

выполнять специальные процедуры управления правами доступа пользователей;

применять специальные процедуры управления правами доступа пользователей;

работать с официальными сайтами организаций – разработчиков компонентов администрируемой сети;

работать с официальными рассылками изменений к компонентам администрируемой сети;

пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

владеть:

навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем;

правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных.

4. Структура и содержание дисциплины «Информационная безопасность»

Общая трудоемкость дисциплины составляет 5 зачетных единиц – 144 часов, в том числе – лекционные – 17 часов, лабораторные - 34 часа, СРС – 57 часов, форма контроля 7 семестр – экзамен (36 часов (1ЗЕТ)).

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины **Тема лекции и вопросы**	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по срокам текущих аттестаций в семестре)* Форма промежуточной аттестации *(по семестрам)*
				ЛК	ПЗ	ЛР	СР	
1.	Лекция 1. Тема 1. «Введение в информационную безопасность». 1. Принципы организации информационной среды. 2. Понятие информационной безопасности (две трактовки). 3. Ответственность специалиста в области безопасности информации и его функции. 4. Современное состояние информационной безопасности. 5. Наступательные и оборонительные составляющие «информационной войны». 6. Анализ компьютерных преступлений. *	7	1-2	2		4	6	Входная контрольная работа
2.	Лекция 2. Тема 2. «Анализ способов нарушений информационной безопасности». 1. Понятие угрозы и характеристика угроз безопасности информации. 2. Несанкционированный доступ (НСД) к информации и его цели. 3. Способы НСД к информации. 4. Три вида возможных нарушений информационной системы: раскрытие,		3-4	2		4	6	

	нарушение целостности, отказ в обслуживании. 5. Объекты защиты информации: АС-ВС-АСУ.*							
3.	Лекция 3. Тема 2. «Анализ способов нарушений информационной безопасности». 1. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты. 2. Компьютерные вирусы и их классификация. 3. Антивирусные программы и их классификация. 4. Понятие защиты информации. 5. Методы борьбы с компьютерными вирусами.*		5-6	2		4	6	**Аттестационная контрольная работа №1**
4.	Лекция 4. Тема 3: «Информационная безопасность в условиях функционирования в России глобальных сетей». 1. Информационная безопасность в условиях функционирования в России глобальных сетей. 2. Международные стандарты информационного обмена. 3. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. 4. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 5. Требования к безопасности компьютерных сетей в Российской Федерации. Обзор методов защиты информации: ограничение доступа на физическом уровне; аутентификация и разграничение доступа.*		7-8	2		4	6	
5.	Лекция 5. Тема 4: «Обеспечение безопасности информации в компьютерных сетях и информационных системах». 1. Основные положения теории информационной безопасности корпоративных информационных систем (КИС). 2. Краткая история создания глобальной информационной сети INTERNET.		9-10	2		4	6	**Аттестационная контрольная работа №2**

	3. Злоумышленники (все о них).*							
6.	Лекция 6. Тема 4: «Обеспечение безопасности информации в компьютерных сетях и информационных системах». 1. Стандартные стеки коммуникационных протоколов. 2. Модель и стек протоколов OSI. 3. Обзор коммуникационных протоколов*		11-12	2		4	6	
7.	Лекция 7. Тема 4: «Обеспечение безопасности информации в компьютерных сетях и информационных системах» 1. Стек протоколов TCP/IP. 2. Проблемы безопасности IP-сетей: варианты распространенных атак на IP-сети и основные причины, порождающие возможность атаки на IP-сети. 3. Сравнительный анализ последствий атак на IP-сети.*		13-14	2		4	7	**Аттестационная контрольная работа №3**
8.	Лекция 8. Тема 5: «Модели безопасности и их применение». 1. Причины уязвимости сети Интернет и сетей и компьютеров, имеющих выход в Интернет. 2. Модель корпоративной сети. 3. Причины, способствующие атаке информации в корпоративных сетях. 4. Модель угроз и модель противодействия угрозам безопасности корпоративной сети. 5. Проблемы защиты корпоративных информационных систем.*		15-16	2		4	7	
9.	Лекция 9. Тема 6: «Доктрина информационной безопасности РФ». 1. Место и роль информационной безопасности корпоративных информационных систем (КИС) в национальной безопасности страны. 2. Доктрина информационной безопасности в РФ. 3. Организационно-правовые меры по защите информации.*		17	1		2	7	
	Итого:	**7**	**17**	**17**	**-**	**34**	**57**	**Экзамен – (1 ЗЕТ – 36 часов)**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	2	3	4	5
1	№№ 1-5	**Основы защиты персонального компьютера** 1. Резервное копирование. 2. Проверка того, открывали ли ваш файл, когда вас не было на месте. 3. Зашита файлов и папок от изменения. 4. Невидимые файлы, папки и приложения. 5. Временные файлы - поиск и удаление. 6. Защита паролем BIOS. 7. Система защиты паролями Windows XP/2000/7/8/10.	8	1, 2, 11
2	№№ 3- 6	**Многоуровневая защита персонального компьютера** 1. Способы ограничения доступа к работе компьютера. 2. Способы ограничения доступа к информации в файлах в офисных программах MS Word, MS Excel. 1. Использование системного реестра для защиты информации. 2. Программы администрирования для Windows XP/7/10. 3. Стратегия безопасности Windows XP/7/8/10.	8	1, 2, 11
3	№№ 5- 7	**Компьютерные антивирусные программы** 1. Dr.Web Security Space for Windows: установка, настройка, работа. 2. Антивирус Kaspersky Total Security 3. Диски аварийного восстановления Windows XP/7/10. 4. Антивирус Norton Security (Standard, Deluxe, Premium).	8	1, 2, 4,7
4	№№ 8 - 9	**Безопасность в Internet** 1. Защита в Internet: работа с пакетом программ Kaspersky Internet Security (или Norton Internet Security). 2. Анонимность в Internet. 3. Безопасность электронной почты. 4. Получение адреса отправителя электронной почты.	10	2, 4, 5,6, 7, 8, 12, 16

		5. Индивидуальная защита от спама и почтовых вирусов.		
	Всего:		**34**	

4.4. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля СРС
1	2	3	4	5
1	Анализ компьютерных преступлений. *	3	№№ 1, 5-12	Реферат, статья
2	Объекты защиты информации: АС-ВС-АСУ.*	3	№№ 1-11	Реферат, статья
3	Методы борьбы с компьютерными вирусами.*	3	№№ 1, 6,11,12	Реферат, статья
4	Обзор методов защиты информации: ограничение доступа на физическом уровне; аутентификация и разграничение доступа.*	3	№№1, 5, 11, 17-22	Реферат, статья
5	Злоумышленники (все о них).*	3	№№ 1, 5-12	Реферат, статья
6	Обзор коммуникационных протоколов*	3	№№ 1-11	Реферат, статья
7	Сравнительный анализ последствий атак на IP-сети.*	3	№№ 1, 6,11,12	Реферат, статья
8	Проблемы защиты корпоративных информационных систем.*	3	№№1, 5, 11, 17-22	Реферат, статья
9	Организационно-правовые меры по защите информации.*	3	№№ 1-12	Реферат, статья
10	Концепция построения защищенных виртуальных частных сетей VPN: средства VPN и построение защищенных каналов.*	3	№№ 1, 4, 11	Реферат, статья
11	Концепция построения защищенных виртуальных частных сетей VPN: туннелирование.*	3	№№ 1, 3-9, 12	Реферат, статья
12	Криптографические методы защиты информации: общий обзор.*	3	№№ 1, 5,6,7, 8, 11- 16	Реферат, статья
13	Криптография: обзор программ симметричного шифрования информации.*	3	№№ 1, 5,6,7, 8, 11- 16	Реферат, статья
14	Сравнительный анализ возможностей симметричных алгоритмов шифрования IDEA, RC2, RC5, CAST, Blowfish.*	3	№№ 1, 5,6,7, 8, 11- 16	Реферат, статья

15	Отечественный стандарт ГОСТ 28147-89 в режиме гаммирования.*	3	№№ 1, 5,6,7, 8, 11- 16	Реферат, статья
16	Обзор асимметричных криптоалгоритмов.*	4	№№ 1, 5,6,7, 8, 11- 16	Реферат, статья
17	Алгоритмы электронной цифровой подписи Эль-Гамаля.*	4	№№ 1, 5,6,7, 8, 11- 16	Реферат, статья
18	Проблемы информационной безопасности Российской Федерации.*	4	№№ 1, 5,6,7, 8, 11- 16	Реферат, статья
	Всего:	**57**		

5. Образовательные технологии

Используется технология учебного исследования:

5.1. При проведении лабораторных работ используются пакеты прикладных программ MicroSoft Office 2007/2013/2016 (MS Word, MS Excel, MS PowerPoint), ППП Borland C++,Visual C#, Internet Explorer, Mozilla Firefox, а также ОС Windows XP/7/10. Данные программы позволяют изучить возможности создания криптографических систем защиты информации, разработки электронной цифровой подписи, защиты электронных документов.

5.2. При чтении лекционного материала используются современные технологии проведения занятий, основанные на использовании интерактивной доски, обеспечивающей наглядное представление методического и лекционного материала. При составлении лекционного материала используется пакет прикладных программ презентаций MS Power Point. Использование данной технологии обеспечивает наглядность излагаемого материала, экономит время, затрачиваемое преподавателем на построение графиков, рисунков, таблиц.

В соответствии с требованиями ФГОС ВО по направлению подготовки «Прикладная математика и информатика» реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных занятий, и в целом в учебном процессе они составляют 20% аудиторных занятий или 14 ч.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Задачи
контрольной работы для проверки входных знаний студентов

1. Имеется n значений случайной величины x_1 , x_2 , x_3 ,..., x_n . Вычислить приближенные значения математического ожидания, дисперсии и среднего квадратического отклонения этой случайной величины.

2. Написать блок-схему алгоритма и программу на одном из алгоритмических языков для вычисления значения следующего выражения:

$$S = \sum_{i=1}^{45} x_i + \sum_{i=1}^{20} y_i ,$$

где x_i , y_i - элементы заданных массивов.

1. Общие принципы построения и архитектуры вычислительных машин.
2. Классификация и архитектура вычислительных сетей.
3. Техническое, информационное и программное обеспечение вычислительных сетей.
4. Определение, назначение, состав и функции операционных систем.
5. Локальные и глобальные сети.

Перечень

вопросов и задач текущих контрольных работ по дисциплине

"Информационная безопасность"

Аттестационная контрольная работа №1

1. Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки).
3. Ответственность специалиста в области безопасности информации и его функции.
4. Современное состояние информационной безопасности.
5. Понятие угрозы и характеристика угроз безопасности информации.
6. Несанкционированный доступ (НСД) к информации и его цели.
7. Способы НСД к информации.
8. Три вида возможных нарушений информационной системы: раскрытие, нарушение целостности, отказ в обслуживании.
9. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
10. Компьютерные вирусы и их классификация.
11. Антивирусные программы и их классификация.
12. Понятие защиты информации.
13. Информационная безопасность в условиях функционирования в России глобальных сетей.
14. Международные стандарты информационного обмена.
15. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
16. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
17. Требования к безопасности компьютерных сетей в Российской Федерации.
18. Основные положения теории информационной безопасности корпоративных информационных систем (КИС).
19. Краткая история создания глобальной информационной сети INTERNET.
20. Стек протоколов TCP/IP.
21. Проблемы безопасности IP-сетей: варианты распространенных атак на IP-сети и основные причины, порождающие возможность атаки на IP-сети.

Аттестационная контрольная работа №2

1. Причины уязвимости сети Интернет и сетей и компьютеров, имеющих выход в Интернет.
2. Модель корпоративной сети.
3. Причины, способствующие атаке информации в корпоративных сетях.
4. Модель угроз и модель противодействия угрозам безопасности корпоративной сети.
5. Место и роль информационной безопасности корпоративных информационных систем (КИС) в национальной безопасности страны.
6. Концепция информационной безопасности в РФ.
7. Перспективные технологии информационной защиты корпоративных информационных систем (КИС) и концепция построения защищенных виртуальных частных сетей VPN.
8. Функции и компоненты сети VPN и критерии ее безопасности.
9. Классификация виртуальных частных сетей VPN.
10. Применение стека протоколов IPSec для построения защищенных виртуальных сетей VPN(структура IP – пакета, архитектура стека протоколов IPSec).
11. Об истории развития криптографии (шифр «Скитала» в Спарте, шифр Цезаря, квадрат Полибия, шифр Гронсфельда).
12. Основные понятия криптографии.
13. Требования, предъявляемые к криптографическим системам (КС).
14. Основные классы симметричных криптосистем (СКС): моно- и многоалфавитные подстановки, перестановки, блочные шифры, гаммирование.
15. Симметричные алгоритмы шифрования: понятия блочного и поточного шифров.
16. Обобщенная схема работы симметричной криптосистемы.
17. Действия над числами в блочном криптоалгоритме.
18. Симметричный алгоритм шифрования: классическая сеть Фейстеля и ее структурная схема.
19. Симметричный алгоритм шифрования данных DES: общие сведения, обобщенная схема.
20. Симметричные алгоритмы шифрования IDEA, RC2, RC5, CAST, Blowfish: общие сведения.

Аттестационная контрольная работа №3

21. Отечественный стандарт шифрования данных ГОСТ 28147-89: режимы работы, схема реализации шифрования и расшифрования данных в режиме простой замены.
22. Уравнения первого цикла процедуры шифрования 64-х разрядного блока открытых данных T_0 в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
23. Функция шифрования в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
24. Порядок считывания подключей в циклах процедуры шифрования данных в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
25. Общий вид уравнений шифрования данных в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
26. Порядок вывода зашифрованного блока данных $T_ш$ и его вид.
27. Порядок заполнения накопителей N_1 и N_2 зашифрованным текстом $T_ш$ и считывания подключей при расшифровании текста в режиме простой замены в отечественном стандарте ГОСТ 28147-89.

28. Уравнения расшифрования в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
29. Порядок вывода расшифрованного блока данных T_0 и его вид.
30. Основные свойства асимметричных криптосистем.
31. Однонаправленные функции.
32. Алгоритм шифрования RSA.
33. Комбинированные криптосистемы.
34. Понятие хэш-функции и ее свойства.
35. Хэш-функции MD4, MD5 и американский стандарт хеширования SHA.
36. Отечественный стандарт хэш-функции.
37. Понятие электронной цифровой подписи и ее цель
38. Процедура формирования и проверки ЭЦП.
39. Алгоритмы электронной цифровой подписи – RSA: основные сведения.
40. Отечественный стандарт ЭЦП.
41. Место и роль информационной безопасности корпоративных информационных систем (КИС) в национальной безопасности страны.

Перечень
экзаменационных вопросов по дисциплине
«Информационная безопасность»

1. Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки).
3. Ответственность специалиста в области безопасности информации и его функции.
4. Современное состояние информационной безопасности.
5. Понятие угрозы и характеристика угроз безопасности информации.
6. Несанкционированный доступ (НСД) к информации и его цели.
7. Способы НСД к информации.
8. Три вида возможных нарушений информационной системы: раскрытие, нарушение целостности, отказ в обслуживании.
9. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
10. Компьютерные вирусы и их классификация.
11. Антивирусные программы и их классификация.
12. Понятие защиты информации.
13. Информационная безопасность в условиях функционирования в России глобальных сетей.
14. Международные стандарты информационного обмена.
15. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
16. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
17. Требования к безопасности компьютерных сетей в Российской Федерации.
18. Основные положения теории информационной безопасности корпоративных информационных систем (КИС).
19. Краткая история создания глобальной информационной сети INTERNET.
20. Стек протоколов TCP/IP.
21. Проблемы безопасности IP-сетей: варианты распространенных атак на IP-сети и основные причины, порождающие возможность атаки на IP-сети.
22. Причины уязвимости сети Интернет и сетей и компьютеров, имеющих выход в Интернет.
23. Модель корпоративной сети.

24. Причины, способствующие атаке информации в корпоративных сетях.
25. Модель угроз и модель противодействия угрозам безопасности корпоративной сети.
26. Место и роль информационной безопасности корпоративных информационных систем (КИС) в национальной безопасности страны.
27. Концепция информационной безопасности в РФ.
28. Перспективные технологии информационной защиты корпоративных информационных систем (КИС) и концепция построения защищенных виртуальных частных сетей VPN.
29. Функции и компоненты сети VPN и критерии ее безопасности.
30. Классификация виртуальных частных сетей VPN.
31. Применение стека протоколов IPSec для построения защищенных виртуальных сетей VPN(структура IP – пакета, архитектура стека протоколов IPSec).
32. Об истории развития криптографии (шифр «Скитала» в Спарте, шифр Цезаря, квадрат Полибия, шифр Гронсфельда).
33. Основные понятия криптографии.
34. Требования, предъявляемые к криптографическим системам (КС).
35. Основные классы симметричных криптосистем (СКС): моно- и многоалфавитные подстановки, перестановки, блочные шифры, гаммирование.
36. Симметричные алгоритмы шифрования: понятия блочного и поточного шифров.
37. Обобщенная схема работы симметричной криптосистемы.
38. Действия над числами в блочном криптоалгоритме.
39. Симметричный алгоритм шифрования: классическая сеть Фейстеля и ее структурная схема.
40. Симметричный алгоритм шифрования данных DES: общие сведения, обобщенная схема.
41. Симметричные алгоритмы шифрования IDEA, RC2, RC5, CAST, Blowfish: общие сведения.
42. Отечественный стандарт шифрования данных ГОСТ 28147-89: режимы работы, схема реализации шифрования и расшифрования данных в режиме простой замены.
43. Уравнения первого цикла процедуры шифрования 64-х разрядного блока открытых данных T_0 в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
44. Функция шифрования в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
45. Порядок считывания подключей в циклах процедуры шифрования данных в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
46. Общий вид уравнений шифрования данных в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
47. Порядок вывода зашифрованного блока данных $T_ш$ и его вид.
48. Порядок заполнения накопителей N_1 и N_2 зашифрованным текстом $T_ш$ и считывания подключей при расшифровании текста в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
49. Уравнения расшифрования в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
50. Порядок вывода расшифрованного блока данных T_0 и его вид.
51. Основные свойства асимметричных криптосистем.
52. Однонаправленные функции.
53. Алгоритм шифрования RSA.
54. Комбинированные криптосистемы.
55. Понятие хэш-функции и ее свойства.

56. Хэш-функции MD4, MD5 и американский стандарт хеширования SHA.
57. Отечественный стандарт хэш-функции.
58. Понятие электронной цифровой подписи и ее цель
59. Процедура формирования и проверки ЭЦП.
60. Алгоритмы электронной цифровой подписи – RSA: основные сведения.
61. Отечественный стандарт ЭЦП.
62. Место и роль информационной безопасности корпоративных информационных систем (КИС) в национальной безопасности страны.

Перечень
вопросов для проверки остаточных знаний студентов по дисциплине
«Информационная безопасность»

1. Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки).
3. Понятие угрозы и характеристика угроз безопасности информации.
4. Несанкционированный доступ (НСД) к информации и его цели.
5. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
6. Компьютерные вирусы и их классификация.
7. Антивирусные программы и их классификация.
8. Понятие защиты информации.
9. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
10. Основные положения теории информационной безопасности корпоративных информационных систем (КИС).
11. Стек протоколов TCP/IP.
12. Причины уязвимости сети Интернет и сетей и компьютеров, имеющих выход в Интернет.
13. Модель корпоративной сети.
14. Концепция информационной безопасности в РФ.
15. Перспективные технологии информационной защиты корпоративных информационных систем (КИС) и концепция построения защищенных виртуальных частных сетей VPN.
16. Функции и компоненты сети VPN и критерии ее безопасности.
17. Об истории развития криптографии (шифр «Скитала» в Спарте, шифр Цезаря, квадрат Полибия, шифр Гронсфельда).
18. Основные понятия криптографии.
19. Симметричные алгоритмы шифрования: понятия блочного и поточного шифров.
20. Обобщенная схема работы симметричной криптосистемы.
21. Отечественный стандарт шифрования данных ГОСТ 28147-89: режимы работы, схема реализации шифрования и расшифрования данных в режиме простой замены.
22. Общий вид уравнений шифрования данных в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
23. Уравнения расшифрования в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
24. Основные свойства асимметричных криптосистем.
25. Однонаправленные функции.
26. Алгоритм шифрования RSA.
27. Понятие хэш-функции и ее свойства.
28. Понятие электронной цифровой подписи и ее цель

29. Процедура формирования и проверки ЭЦП.
30. Алгоритмы электронной цифровой подписи – RSA: основные сведения.
31. Отечественный стандарт ЭЦП.

7. Учебно-методическое и информационное обеспечение дисциплины «Информационная безопасность»

Зав. библиотекой

Рекомендуемая литература и источники информации (основная и дополнительная)

№ п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Автор(ы)	Издательство и год издания	Количество изданий	
					В библиотеке	На кафедре
1	2	3	4	5	6	7
ОСНОВНАЯ						
1	Лк, лб, срс	Информационная безопасность: Учебное пособие с грифом УМО	Абдулгалимов А.М. .Оруджев М.И.	Махачкала, ДГТУ, 2011	-	15
2	лк, лб, срс	Проектирование информационных систем: учебник	Белова В.В.	М.: Академия, 2013	30	-
3	Лк, лб, срс	Основы информационной безопасности [Электронный ресурс] Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks»	Галатенко В.А.	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	-	-
4	Лк, лб, срс	Информационная безопасность и защита информации [Электронный ресурс] Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»	Шаньгин В.Ф.	Саратов: Профобразование, 2017	-	-
5	Лк, лб, срс	Введение в информационную безопасность: Учеб. (e.lanbook. com)	Малюк А.А., Горбатов В.С., Королев В.И.	Изд-во "Горячая линия-Телеком" , 2012	-	-
ДОПОЛНИТЕЛЬНАЯ						
6	Лк, лб, срс	Методические указания к выполнению лабораторных работ по дисциплине «Информационная безопасность». Часть 1	Абдулгалимов А.М., Филенко А.Д., Тагиев М.Х., Тагиев Р.Х.	Махачкала, ДГТУ, 2008.	47	12

7	Лк, лб, срс	Методические указания к выполнению лабораторных работ по дисциплине «Информационная безопасность». Часть 2	Абдулгалимов А.М., Филенко А.Д., Тагиев М.Х., Тагиев Р.Х.	Махачкала, ДГТУ, 2008.	46	-
8	Лк, лб, срс	Информационная безопасность	Башлы П.Н.	Ростов н/Д : Феникс, 2006.	3	-
9	Лк, лб, срс	Руководство по защите от хакеров. : Пер. с англ.	Коул Эрик	М.: Издательский дом «Вильямс», 2002.	-	2
10	Лк, лб, срс	Криптографические методы защиты информации: Учебное пособие	Рябко Б.Я. ,Фионов Н.И.	М.: Горячая Линия – Телеком, 2005.	-	2
11	Лк, лб, срс	Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С.	Брюс Шнайер	М.: Изд-во ТРИУМФ, 2003.	-	2
12	Лк, лб, срс	Защита информации в распределенных корпоративных сетях и системах. (Серия «Администрирование и защита»)	Соколов А.В., Шаньгин В.Ф.	М.: ДМК Пресс, 2002.	-	2
13	Лк, лб, срс	Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. /Под ред. В.А. Васенина.	Андреев О.О. и др.	М.: МЦНМО, 2008	-	2
14	Лк, лб, срс	Защита информации в компьютерных системах.	Мельников В.В.	М., Финансы и статистика, 1997.	1	2
15	Лк, лб, срс	Информационная безопасность и защита информации : учеб. пособие	Мельников В.П.	М.: Академия, 2008.	15	2
16	Лк, лб, срс	Информационная безопасность и защита информации : учеб. пособие	Мельников В.П.	М.: Академия, 2007.	56	-
17	Лк, лб, срс	Основы информационных и телекоммуникационных технологий. Программные средства информационных технологий. Учеб. Пособие.	Попов В.Б.	М.: Финансы и статистика, 2005.	3	1
18	Лк, лб, срс	Криптография: Учебное пособие для вузов.	Алферов А.П., Зубов А.Ю., Кузьмина А.С., Черемушкин Н.В..	М., Гелиос АВР, 2001.	-	1
ИНТЕРНЕТ - РЕСУРСЫ						

19	Лк, лб, срс	http://window.edu.ru– единое окно доступа к образовательным ресурсам				
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ						
20	Лб, срс	ОС Windows XP/ 7 / 8/10				
21	Лк, лб, срс	Microsoft Office 2007/2013/2016				
22	Лб, срс	Borland C++				

8. Материально-техническое обеспечение дисциплины «Информационная безопасность»

Для изучения данной дисциплины материально-техническое обеспечение включает:

- библиотечный фонд (учебная, учебно-методическая, справочная математическая и экономическая литература, математическая научная периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет;
- аудитории, оборудованные проекционной техникой.

Для проведения лекционных занятий используется лекционный зал факультета КТВТиЭ, оборудованный проектором и интерактивной доской.

Для проведения лабораторных работ используются компьютерные классы №317 кафедры прикладной математики и информатики, оборудованные современными персональными компьютерами, характеристики которых приведены ниже:

Процессор Intel (R) Core (TM) i3-3220 CPU @ 3.30 GHz 3.30 GHz;

Установленная память (ОЗУ) - 4 ГБ;

Операционная система - 64 разрядная: Windows 7/8/10;

Монитор BenQ GL2250 с диагональю 21,5" (DVI)

Все персональные компьютеры в количестве 18 штук подключены к сети университета и имеют выход в глобальную сеть Интернет.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 01.03.02 – «Прикладная математика и информатика» с учетом рекомендаций ООП ВО по профилю подготовки бакалавров «Системное программирование и компьютерные технологии».

Рецензент от работодателя по направлению «Прикладная математика и информатика»

Подпись, ФИО

9. Дополнения и изменения в рабочей программе на 20___/____учебный год

В рабочую программу вносятся следующие изменения

Рабочая программа пересмотрена и одобрена на заседании
кафедры "_____"_____20___г.

Заведующий кафедрой_____

Внесенные изменения утверждаю
Проректор по учебной работе (декан)_____

"_____"_____20___г.