Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Директор Таганрогского института
имени А. П. Чехова (филиала)
РГЭУ (РИНХ)
_____ С. А. Петрушенко
«20» мая 2025 г.

Рабочая программа дисциплины
Информационная безопасность

Направление подготовки
09.03.03 Прикладная информатика

Направленность (профиль) программы бакалавриата
09.03.03.02 Разработка программного обеспечения

Для набора 2025 года

Квалификация
Бакалавр

КАФЕДРА **информатики**

Распределение часов дисциплины по семестрам / курсам

Курс	4		5		Итого	
Вид занятий	УП	РП	УП	РП		
Лекции	4	4	4	4	8	8
Лабораторные	6	6	6	6	12	12
Итого ауд.	10	10	10	10	20	20
Контактная работа	10	10	10	10	20	20
Сам. работа	134	134	53	53	187	187
Часы на контроль			9	9	9	9
Итого	144	144	72	72	216	216

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.02.2025 протокол № 9.

Программу составил(и): канд. техн. наук, Доц., Усенко Ольга Александровна

Зав. кафедрой: Тюшнякова И.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью освоения дисциплины «Информационная безопасность» является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
ОПК-2:	Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
ОПК-2.1:	Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
ОПК-2.2:	Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
ОПК-2.3:	Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
ОПК-3:	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.1:	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.2:	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.3:	Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

правовые понятия и нормы Российского законодательства, иметь представление о системе норм Российского законодательства, о структуре Российского законодательства, видах правовых отраслей и особенностях их регулирования, понимать сущность, характер и взаимодействие правовых явлений, видеть их взаимосвязь в целостной системе знаний и значений реализации права; (соотнесено с индикатором ОПК - 2.1)

- правовое обеспечение информационной безопасности переработки информации в ИС; организационно-правовые основы защиты информационных ресурсов предприятия; (соотнесено с индикатором ОПК - 2.1)

-теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи; (соотнесено с индикатором ОПК - 2.1)

нормативно-правовые документы в области информационных систем и технологий; (соотнесено с индикатором ОПК - 3.1)

методы и алгоритмы решения стандартных задач в своей профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. (соотнесено с индикатором ОПК - 3.1)

Уметь:

анализировать и оценивать нормативно-правовую информацию; (соотнесено с индикатором ОПК - 2.2)

планировать и осуществлять свою деятельность с учётом результатов этого анализа; (соотнесено с индикатором ОПК - 2.2)

- использовать и составлять нормативно-правовые документы, относящиеся к будущей профессиональной деятельности; (соотнесено с индикатором ОПК - 2.2)

- находить нужную статью в законе;(соотнесено с индикатором ОПК - 2.2)

-самостоятельно анализировать правовую и научную литературу и делать обоснованные выводы; (соотнесено с индикатором ОПК - 2.2)

- организовывать защиту информации в ИС; (соотнесено с индикатором ОПК - 2.2)

- применять действующую законодательную базу в области информационной безопасности; (соотнесено с индикатором ОПК - 3.2)

- разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации; (соотнесено с индикатором ОПК - 3.2)

-применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы; (соотнесено с индикатором ОПК - 3.2)

-решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования. (соотнесено с индикатором ОПК - 3.2)

Владеть:
способностью использовать основы правовых знаний в различных сферах деятельности; навыками по предоставлению и улучшению проведения мер по обеспечению безопасности; (соотнесено с индикатором ОПК - 2.3) - правовыми средствами обеспечения информационной безопасности; (соотнесено с индикатором ОПК - 2.3) навыками работы с нормативно-правовыми документами и стандартами в области информационных систем и технологий, обеспечения требований информационной безопасности; (соотнесено с индикатором ОПК - 3.3) навыками применения моделей и методов расчета надежности и безопасности информационных систем при различных видах угроз и моделей поведения нарушителя. (соотнесено с индикатором ОПК - 3.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы информационной безопасности и защиты информации

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Введение в дисциплину. Основные понятия и определения информационной безопасности. Информация и информационная безопасность. Основные составляющие информационной безопасности. Объекты защиты. Категории и носители информации. Средства защиты информации. Способы передачи конфиденциальной информации на расстоянии.	Лекционные занятия	4	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.2	Виды угроз информационной безопасности. Модель нарушителя информационной безопасности.	Лекционные занятия	4	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.3	Принципы построения системы защиты информации. Методы защиты.	Самостоятельная работа	4	6	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.4	Методы и средства защиты информации от шпионажа и несанкционированного доступа.	Самостоятельная работа	4	14	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.5	Изучение содержания и последовательности работ по защите информации.	Лабораторные занятия	4	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.6	Изучение методов комплексного исследования объекта информатизации.	Лабораторные занятия	4	4	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.7	Изучение методов построения систем обеспечения информационной безопасности на основе нормативных актов. Изучение правовой стороны информационной безопасности, идея сертификации и электронной подписи.	Самостоятельная работа	4	14	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3

1.8	Разработка политики информационной безопасности для организации.	Самостоятельная работа	4	24	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.9	Изучение и построение модели нарушителя информационной безопасности.	Самостоятельная работа	4	20	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.10	Изучение основных видов компьютерных вирусов и способы борьбы с ними.	Самостоятельная работа	4	20	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.11	Обеспечение информационной безопасности за счет повышения связности телекоммуникационной сети.	Самостоятельная работа	4	10	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.12	Поиск надежных каналов передачи информации в телекоммуникационных сетях.	Самостоятельная работа	4	10	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.13	Исследование методов выбора рационального варианта системы защиты информации на основе криптографических методов. Шифры замены, перестановки, гаммирования.	Самостоятельная работа	4	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
1.14	Подготовка к тестированию, лабораторным работам.	Самостоятельная работа	5	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3

Раздел 2. Комплексный подход к решению вопросов обеспечения безопасности информационных систем

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
2.1	Повышение надежности информационных систем, как средство обеспечения информационной безопасности.	Лекционные занятия	5	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.2	Методы управления средствами сетевой безопасности.	Лекционные занятия	5	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1

					ОПК-2.2 ОПК-2.3
2.3	Повышение безопасности и стандарты информационной безопасности.	Самостоятельная работа	5	13	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.4	Исследование основных показателей надежности информационных систем.	Самостоятельная работа	5	6	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.5	Расчет надежности аналоговых и цифровых подсистем ИС при различных видах угроз.	Лабораторные занятия	5	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.6	Изучение видов резервирования для повышения надежности и безопасности ИС.	Лабораторные занятия	5	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.7	Вероятностно-логический метод расчета надежности.	Лабораторные занятия	5	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.8	Логико-вероятностный метод расчета надежности.	Самостоятельная работа	5	10	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.9	Модель расчета надежности систем обеспечения информационной безопасности на основе системы дифференциальных уравнений.	Самостоятельная работа	4	6	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.10	Модель расчета надежности систем обеспечения информационной безопасности на основе системы интегральных уравнений.	Самостоятельная работа	4	2	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.11	Оценка надежности восстанавливаемых систем.	Самостоятельная работа	4	4	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.12	Виды и причины отказов программного обеспечения. Оценка последствий для информационной безопасности.	Самостоятельная работа	4	2	ОПК-2 ОПК-3

					ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.13	Методы расчета надежности программного обеспечения.	Самостоятельная работа	5	16	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.14	Подготовка к тестированию, лабораторным работам	Самостоятельная работа	5	6	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3
2.15	Подготовка к промежуточной аттестации	Экзамен	5	9	ОПК-2 ОПК-3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1	Семененко, Вячеслав Алексеевич	Информационная безопасность: учеб. пособие	М.: МГИУ, 2006	2 экз.
2	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие	Томск: Эль Контент, 2011	http://biblioclub.ru/index.php?page=book&id=208694
3	Филиппов Б. И., Шерстнева О. Г.	Информационная безопасность. Основы надежности средств связи: учебник	Москва|Берлин: Директ-Медиа, 2019	http://biblioclub.ru/index.php?page=book&id=499170
4	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	http://biblioclub.ru/index.php?page=book&id=562246
5	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва|Берлин: Директ-Медиа, 2020	http://biblioclub.ru/index.php?page=book&id=571485
6	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	http://biblioclub.ru/index.php?page=book&id=576726
7	Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: учебно-методическое пособие	Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/77317.html

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
8	Фаронов, А. Е.	Основы информационной безопасности при работе на компьютере: учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/89453.html

5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1	Артемов А. В.	Информационная безопасность: курс лекций: курс лекций	Орел: Межрегиональная академия безопасности и выживания, 2014	http://biblioclub.ru/index.php?page=book&id=428605
2	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	http://biblioclub.ru/index.php?page=book&id=438331

5.2. Профессиональные базы данных и информационные справочные системы

garant.ru

Consultant.ru

5.3. Перечень программного обеспечения

Python
Гарант (учебная версия)
OpenOffice

5.4. Учебно-методические материалы для обучающихся с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет, и/или в специализированных лабораториях, предусмотренных образовательной программой.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности			
З. современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	З. Использование новейших информационных технологий и программного обеспечения, включая разработки российских производителей, для выполнения профессиональных задач.	полнота и содержательность ответа умение приводить примеры	Э – вопросы к экзамену (1-25)
У. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	У. Способен осуществлять выбор актуальных информационных технологий и программных инструментов, в том числе разработанных в России, при решении профессиональных задач.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ – лабораторные задания (1-4) ИЗ- индивидуальные задания
В. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	В. Обладает компетенциями в области использования современных информационных технологий и программных продуктов, включая российские аналоги, в процессе выполнения профессиональной деятельности.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ – лабораторные задания (5-10) индивидуальные задания
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и	Обладает пониманием основ и способов решения типовых профессиональных задач, опираясь на информационную и	полнота и содержательность ответа умение приводить примеры	Э – вопросы к экзамену (26-44)

библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	библиографическую компетентность. Использует современные информационно-коммуникационные технологии, принимая во внимание ключевые аспекты информационной безопасности.		
Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Способен находить решения для стандартных задач в рамках профессиональной деятельности, используя информационно-библиографические ресурсы и современные ИКТ. При этом учитываются базовые требования к защите информации.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ – лабораторные задания (10-15)
Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Демонстрирует навыки в подготовке аналитических обзоров, аннотировании, реферировании, создании научных докладов и публикаций, а также составлении библиографических списков по результатам научно-исследовательской работы с соблюдением стандартов информационной безопасности.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ – лабораторные задания (11-19)

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

84-100 баллов (оценка «отлично»);
67-83 баллов (оценка «хорошо»);
50-66 баллов (оценка «удовлетворительно»);
0-49 баллов (оценка «неудовлетворительно»);

2. 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

Вопросы к экзамену

1. Основные понятия защиты информации и информационной безопасности (ИБ) – информация, инфорационная безопасность, защита информации, объект и цель защиты, конфиденциальность данных,

собственник, владелец и пользователь (потребитель) информации, правило доступа к информации (санкционированный и несанкционированный), ущерб, информационная угроза, шифр, шифрование, дешифрование, ключ, криптография, криптоанализ.

2. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна

3. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.

4. Основные составялющие информационной безопасности: обеспечение доступности, целостности и конфиденциальности.

5. Аутентификация, идентификация и авторизация субъекта. В чем их различие? Что такое политика безопасности и как она может быть реализована?

6. Общая схема обеспечения информационной безопасности. Содержание ИБ – предупреждение возможных угроз, выявление и обнаружение угроз, пресечение или локализация угроз, ликвидация последствий.

7. Составляющие ИБ: обеспечение доступности, целостности и конфиденциальности информации.

8. Понятие угрозы информационной безопасности. Классификация угроз (по природе возникновения, по степени преднамеренности проявления, по источнику угроз, по способу доступа к ресурсам).

9. Угрозы нарушения конфиденциальности, целостности, доступности (нарушения работоспособности).

10. Модель нарушителя безопасности.

11. Принципы построения системы защиты информации – системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления и применения, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств.

12. Компьютерные вирусы. Классификация вирусов. Охарактеризуйте каждый тип вирусов. Признаки заражения вирусами, способы борьбы с вирусами и минимизации последствий от их заражения.

13. Жизненный цикл вирусов и признаки их проявления. Охарактеризовать стадии хранения, исполнения (загрузка вируса в память; поиск жертвы; заражение найденной жертвы; выполнение деструктивных функций; передача управления программе-носителю вируса).

14. Какие методы обнаружения компьютерных вирусов существуют? Охарактеризуйте каждый. Какие методы обнаружения вирусов реализованы в антивирусных программах?

15. Оценка устойчивости топологии сети передачи данных к атакам, направленным на нарушение доступности, алгоритм определения связности.

16. Алгоритма Дейкстры для определения кратчайших путей в сети передачи данных.

17. Проблема надежности и значение ее для обеспечения информационной безопасности современных информационных систем (ИС). Что такое надежность ИС? Дайте основные определения теории надежности (самовосстанавливаемость, старение системы, исправность, работоспособность, предельное состояние, наработка, назначенный ресурс, безотказность, сохраняемость, долговечность, ремонтопригодность, безопасность, живучесть).

18. Понятие отказа системы. Классификация отказов. В чем отличие дефекта от отказа?

19. Приведите основные количественные характеристики надежности невосстанавливаемых и восстанавливаемых систем.

20. Этапы развития криптографии. Охарактеризуйте методы защиты информации, присущие каждому этапу.

21. Классификация шифров.

22. Шифры замены. Классификация и основные методы шифрования.

23. Шифры одинарной перестановки.

24. Шифры множественной перестановки.

25. Шифры гаммирования. Классификация и основные методы шифрования.

26. Способы генерации псевдослучайных последовательностей.

27. Основы квантового шифрования.

28. Шифрование с открытым ключом.

29. Хэш-функции. Основные понятия и разновидности.

30. Криптографические протоколы. Протоколы обмена ключами. Протоколы аутентификации.

31. Протоколы контроля целостности. Биты четности, контрольные цифры и числа.

32. Классическая и компьютерная стеганография.

33. Основные требования, предъявляемые к криптосистемам. Приведите примеры, как они реализованы в известных вам криптосистемах.

34. Методы и средства обеспечения безопасности процессов переработки информации.

35. Общая классификация методов и средств технологий защиты от угроз.

36. Охарактеризуйте основные методы и средства предотвращения несанкционированного доступа в КС.

37. Классификация методов и средств парирования угроз от электромагнитных излучения и наводок.

38. Классификация методов и средств комплексной зашиты КС.

39. Выбор стратегии обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель» (критерии Вальда, Гурвица, крайнего оптимизма, Сэвиджа, Байеса, минимизации средних рисков, Ходжа-Лемана, недостаточного основания Лапласа.

40. Основные элементы организационной основы системы обеспечения информационной безопасности РФ? Для чего они предназначены?

41. Какие виды деятельности в структуре правового обеспечения информационной безопасности вы знаете? В чем они отличаются?

42. Назовите составляющие, входящие в состав нормативного правового обеспечения информационной безопасности РФ? Дайте им полное описание?

43. Какие существуют принципы нормативного правового обеспечения информационной безопасности? Дайте им описание?

44. Что определяет политика безопасности? Назовите четыре необходимых политики безопасности.

Экзаменационное задание включает три вопроса – два теоретических вопроса и одно практическое задание

Пример практического задания

Пример 1.

С помощью шифрующей системы Трисемуса (Тритемия) зашифровать свою Фамилию

Пример 2. С помощью кода Бодо зашифровать свою Фамилию. Таблица Бодо представлена ниже:

Управляющие символы				
Двоичный код	Десятичный код	Назначение		
01000	8	Возврат каретки		
00010	2	Перевод строки		
11111	31	Буквы латинские		
11011	27	Цифры		
00100	4	Пробел		
00000	0	Буквы русские		
Буквы, цифры и остальные символы				
Двоичный код	Десятичный код	Латинская буква	Русская буква	Цифры и прочие символы
00011	3	A	А	-
11001	25	B	Б	?
01110	14	C	Ц	:
01001	9	D	Д	Кто там?

00001	1	E	Е	З
01101	13	F	Ф	Э
11010	26	G	Г	Ш
10100	20	H	Х	Щ
00110	6	I	И	8
01011	11	J	Й	Ю
01111	15	K	К	(
10010	18	L	Л	)
11100	28	M	М	.
01100	12	N	Н	,
11000	24	O	О	9
10110	22	P	П	0
10111	23	Q	Я	1
01010	10	R	Р	4
00101	5	S	С	'
10000	16	T	Т	5
00111	7	U	У	7
11110	30	V	Ж	=
10011	19	W	В	2
11101	29	X	Ь	/
10101	21	Y	Ы	6
10001	17	Z	З	+

Критерии оценивания:

- 84-100 баллов (оценка «отлично») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 баллов (оценка «хорошо») – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 баллов (оценка «удовлетворительно») – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- 0-49 баллов (оценка «неудовлетворительно») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Лабораторные задания

Лабораторное задание 1 Изучение содержания и последовательности работ по защите информации.

Лабораторное задание 2 Изучение методов комплексного исследования объекта информатизации.

Лабораторное задание 3 Изучение методов построения систем обеспечения информационной безопасности на основе нормативных актов. Изучение правовой стороны информационной безопасности, идея сертификации и электронной подписи.

Лабораторное задание 4 Разработка политики информационной безопасности для организации.

Лабораторное задание 5 Изучение и построение модели нарушителя информационной безопасности.

Лабораторное задание 6 Изучение основных видов компьютерных вирусов и способы борьбы с ними.

Самостоятельные задания – Лабораторные задания для самостоятельного изучения:

Лабораторное задание 7 Обеспечение информационной безопасности за счет повышения связности телекоммуникационной сети.

Лабораторное задание 8 Поиск надежных каналов передачи информации в телекоммуникационных сетях.

Лабораторное задание 9 Исследование методов выбора рационального варианта системы защиты информации на основе криптографических методов. Шифры замены, перестановки, гаммирования.

Лабораторное задание 10 Исследование основных показателей надежности информационных систем.

Лабораторное задание 11 Расчет надежности аналоговых и цифровых подсистем ИС при различных видах угроз.

Лабораторное задание 12 Изучение видов резервирования для повышения надежности и безопасности ИС.

Лабораторное задание 13 Вероятностно-логический метод расчета надежности.

Лабораторное задание 14 Логико-вероятностный метод расчета надежности.

Лабораторное задание 15 Модель расчета надежности систем обеспечения информационной безопасности на основе системы дифференциальных уравнений.

Лабораторное задание 16 Модель расчета надежности систем обеспечения информационной безопасности на основе системы интегральных уравнений.

Лабораторное задание 17 Оценка надежности восстанавливаемых систем.

Лабораторное задание 18 Виды и причины отказов программного обеспечения. Оценка последствий для информационной безопасности.

Лабораторное задание 19 Методы расчета надежности программного обеспечения.Критерии оценивания (для каждого задания):

5 б. – лабораторное задание выполнено верно;
3-4 б.– при выполнении лабораторного задания были допущены неточности, не влияющие на результат;
1-2 б. – при выполнении лабораторного задания были допущены ошибки;
0- б. – при выполнении лабораторного задания были допущены существенные ошибки.

Максимальное количество баллов за все лабораторных заданий– 30 (6 заданий по 5 баллов).

Максимальное количество баллов за самостоятельные задания – 65 (13заданий по 5 баллов

Варианты индивидуальных заданий (темы рефератов)

Основные законодательные акты в сфере информационной безопасности и защиты информации.
Электронный документ.
Почтовая бомба.
Понятие и виды защищаемой информации.
Несанкционированный доступ к информации.
Утечка информации.
Угрозы информации.
Документированная информация.
Электронно-цифровая подпись.
Информационные ресурсы.
Электронная почта и угрозы, связанные с ней.
Способы и методы защиты компьютерной информации.
Понятие, принципы и правила архи-вации файлов.
Компьютерные вирусы. Последствия воздействия компьютерного вируса.
Ос-новные методы защиты от компьютерных вирусов.
Классификация антивирусных программных средств по типам и функциональному назначению.
Общее назначение крип-тографической защиты файлов.
Методы частотного криптоанализа.
Ключ шифрования и способы его ввода.
Понятие компьютерных преступлений.
Криминалистическая характеристика компьютерных преступлений.
Типичные орудия подготовки, совершения и сокрытия преступлений в сфере компьютерной информации.
Способы совершения компьютерных преступлений, их классификация.
Перехват информации.
Несанкционированный доступ к средствам компьютерной техники.
Манипуляция данными и управляющими командами.
Моделирование как способ совершения компьютерного преступления.
Преодоление программных средств защиты.
Особенности тактики назначения и проведения экспертиз при расследовании преступлений в сфере компьютерной информации.
Особенности осмотра машинного носителя информации.
Особенности осмотра компьютерной техники.
Правила поведения следователя при обыске и выемке компьютерной техники.

Критерии оценивания (для каждого задания):
5 б. – реферат составлен и представлен в полном объеме;
3-4 б.– реферат составлен и представлен в неполном объеме;
1-2 б. – реферат составлен с допущением ошибок;
0 б. – в реферате существенные ошибки.
Максимальное количество баллов за индивидуальное задание– 5 (1 задание - 5 баллов).

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию промежуточной аттестации. Количество вопросов в задании – 2 (два теоретических вопроса и один практический) Объявление результатов производится в день экзамена. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные работы.

В ходе лекционных занятий рассматриваются основные теоретические вопросы, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки практической работы.

При подготовке к лабораторным каждый студент должен:

– изучить рекомендованную учебную литературу;
– изучить конспекты лекций;
– подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к лабораторным студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях, лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом выполнения лабораторных и индивидуальных заданий. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников, выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лабораторному занятию по всем обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.