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)
_____ Голобородько А.Ю.
«____» _____ 20___г.

Рабочая программа дисциплины
Информационная безопасность

направление 09.03.03 Прикладная информатика
направленность (профиль) 09.03.03.01 Прикладная информатика в менеджменте

Для набора _____ года

Квалификация
Бакалавр

КАФЕДРА **информатики**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	60	60	60	60
Итого ауд.	92	92	92	92
Контактная работа	92	92	92	92
Сам. работа	88	88	88	88
Часы на контроль	36	36	36	36
Итого	216	216	216	216

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 29.08.2023 протокол № 1.

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-2.1: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-3.1: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; - правовое обеспечение информационной безопасности переработки информации в ИС; организационно-правовые основы защиты информационных ресурсов предприятия; теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи;
нормативно-правовые документы в области информационных систем и технологий;
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.

Уметь:

анализировать и оценивать нормативно-правовую информацию; планировать и осуществлять свою деятельность с учётом результатов этого анализа; - использовать и составлять нормативно-правовые документы, относящиеся к будущей профессиональной деятельности; - находить нужную статью в законе; -самостоятельно анализировать правовую и научную литературу и делать обоснованные выводы; - организовывать защиту информации в ИС; - применять действующую законодательную базу в области информационной безопасности; - разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации;
применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы;
решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.

Владеть:

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Основы информационной безопасности и защиты информации				

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. /Лек/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.2	Виды угроз информационной безопасности. Модель нарушителя информационной безопасности. /Лек/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.3	Принципы построения системы защиты информации. Методы защиты. /Лек/	7	6	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.4	Методы и средства защиты информации от шпионажа и несанкционированного доступа. /Лек/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.5	Изучение содержания и последовательности работ по защите информации. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.6	Изучение методов комплексного исследования объекта информатизации. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.7	Изучение методов построения систем обеспечения информационной безопасности на основе нормативных актов. Изучение правовой стороны информационной безопасности, идея сертификации и электронной подписи. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.8	Разработка политики информационной безопасности для организации. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.9	Изучение и построение модели нарушителя информационной безопасности. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.10	Изучение основных видов компьютерных вирусов и способы борьбы с ними. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2

1.11	Обеспечение информационной безопасности за счет повышения связности телекоммуникационной сети. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.12	Поиск надежных каналов передачи информации в телекоммуникационных сетях. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.13	Исследование методов выбора рационального варианта системы защиты информации на основе криптографических методов. Шифры замены, перестановки, гаммирования. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.14	Подготовка к тестированию, лабораторным работам. /Ср/	7	44	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
	Раздел 2. Комплексный подход к решению вопросов обеспечения безопасности информационных систем				
2.1	Повышение надежности информационных систем, как средство обеспечения информационной безопасности. /Лек/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.2	Методы управления средствами сетевой безопасности. /Лек/	7	6	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.3	Повышение безопасности и стандарты информационной безопасности. /Лек/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.4	Исследование основных показателей надежности информационных систем. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.5	Расчет надежности аналоговых и цифровых подсистем ИС при различных видах угроз. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.6	Изучение видов резервирования для повышения надежности и безопасности ИС. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2

2.7	Вероятностно-логический метод расчета надежности. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.8	Логико-вероятностный метод расчета надежности. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.9	Модель расчета надежности систем обеспечения информационной безопасности на основе системы дифференциальных уравнений. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.10	Модель расчета надежности систем обеспечения информационной безопасности на основе системы интегральных уравнений. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.11	Оценка надежности восстанавливаемых систем. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.12	Виды и причины отказов программного обеспечения. Оценка последствий для информационной безопасности. /Лаб/	7	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.13	Методы расчета надежности программного обеспечения. /Лаб/	7	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.14	Подготовка к тестированию, лабораторным работам /Ср/	7	44	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
2.15	/Экзамен/	7	36	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Семененко, Вячеслав Алексеевич	Информационная безопасность: учеб. пособие	М.: МГИУ, 2006	2
Л1.2	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие	Томск: Эль Контент, 2011	http://biblioclub.ru/index.php?page=book&id=208694 неограниченный доступ для зарегистрированных пользователей
Л1.3	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 неограниченный доступ для зарегистрированных пользователей
Л1.4	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 неограниченный доступ для зарегистрированных пользователей
Л1.5	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 неограниченный доступ для зарегистрированных пользователей
Л1.6	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	http://biblioclub.ru/index.php?page=book&id=576726 неограниченный доступ для зарегистрированных пользователей
Л1.7	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 неограниченный доступ для зарегистрированных пользователей
Л1.8	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 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	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 неограниченный доступ для зарегистрированных пользователей
Л2.2	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 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

garant.ru

Consultant.ru

5.4. Перечень программного обеспечения
Python
Гарант (учебная версия)
Microsoft Office

5.5. Учебно-методические материалы для студентов 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 (МОДУЛЯ)

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

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
ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности			
З: - 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; - правовое обеспечение информационной безопасности переработки информации в ИС; организационно-правовые основы защиты информационных ресурсов предприятия; теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи.	Осуществление поиска и сбора необходимой литературы, изучение лекционного материала, основной и дополнительной литературы, подготовка к контрольной работе	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	КВ – контрольные вопросы (1-44), Т - тест (1-2)

У: - анализировать и оценивать нормативно-правовую информацию; планировать и осуществлять свою деятельность с учётом результатов этого анализа; - использовать и составлять нормативно-правовые документы, относящиеся к будущей профессиональной деятельности; - находить нужную статью в законе; - самостоятельно анализировать правовую и научную литературу и делать обоснованные выводы; - организовывать защиту информации в ИС; - применять действующую законодательную базу в области информационной безопасности; - разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.	Изучение современных информационно- коммуникационных технологий, прохождение тестов, выполнение контрольных заданий	достоверность решения заданий с помощью программных средств, правильность выполнения тестовых и контрольных заданий	ЛЗ - лабораторные задания (1.1-1.9, 2.1-2.10), КЗ - контрольные задания, Т - тест (1-2)
В: владеет способностью использовать основы правовых знаний в различных сферах деятельности; навыками по предоставлению и улучшению проведения мер по обеспечению безопасности; - правовыми средствами обеспечения информационной безопасности.	Использование современных информационных технологий	достоверность решения заданий с помощью программных средств, правильность выполнения лабораторных и контрольных заданий	ЛЗ - лабораторные задания (1.1-1.9, 2.1-2.10), КЗ- контрольные задания, Т - тест (1-2)
ОПК-1: способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий			
З: ОПК-1: нормативно-правовые документы в области инфор-	Осуществление поиска и сбора необходимой литерату-	соответствие проблеме исследования; полнота и содержательность ответа;	КВ – контрольные вопросы (1-44), Т

мационных систем и технологий.	ры, изучение лекционного материала, основной и дополнительной литературы, подготовка к контрольной работе	умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	- тест (1-2)
У: - применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Изучение современных информационно- коммуникационных технологий, прохождение тестов, выполнение контрольных заданий	достоверность решения заданий с помощью программных средств, правильность выполнения тестовых и контрольных заданий	ЛЗ - лабораторные задания (1.1-1.9, 2.1-2.10), КЗ - контрольные задания, Т - тест (1-2)
В: владеет навыками работы с нормативно-правовыми документами и стандартами в области информационных систем и технологий, обеспечения требований информационной безопасности.	Использование современных информационных технологий	достоверность решения заданий с помощью программных средств, правильность выполнения лабораторных и контрольных заданий	ЛЗ - лабораторные задания (1.1-1.9, 2.1-2.10), КЗ- контрольные задания, Т - тест (1-2)
ОПК-4: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
З: 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.	Осуществление поиска и сбора необходимой литературы, изучение лекционного материала, основной и дополнительной литературы, подготовка к контрольной работе	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	КВ – контрольные вопросы (1-44), Т - тест (1-2)

У: - решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.	Изучение современных информационно- коммуникационных технологий, прохождение тестов, выполнение контрольных заданий	достоверность решения заданий с помощью программных средств, правильность выполнения тестовых и контрольных заданий	ЛЗ - лабораторные задания (1.1-1.9, 2.1-2.10), КЗ - контрольные задания, Т - тест (1-2)
В: владеет навыками применения моделей и методов расчета надежности и безопасности информационных систем при различных видах угроз и моделей поведения нарушителя.	Использование современных информационных технологий	достоверность решения заданий с помощью программных средств, правильность выполнения лабораторных и контрольных заданий	ЛЗ - лабораторные задания (1.1-1.9, 2.1-2.10), КЗ- контрольные задания, Т - тест (1-2)

1.2 Шкалы оценивания:

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

50-100 баллов (зачет);

0-49 баллов (незачет).

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

Примеры контрольных работ

Вариант 0

1. Почему алгоритм AES считается очень эффективным? Как реализовать умножение в конечном поле в алгоритме AES?

2. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация сильнее, чем однофакторная?

3. Разработать программный код, выполняющий шифрование методом Гронсфельда с параметром 15.

Вариант 0

1. Назовите набор потенциальных сценариев террористических действий с использованием сетевой среды (Интернет) в самой общей постановке, в качестве взаимодействующих факторов, характеризующих «типовой профиль»? Дайте определения.

2. Опишите атаки CPA, CCA и CCA2. Чем они отличаются?

3. Разработать программный код, выполняющий шифрование методом Вижинера с параметром KEY.

Вариант 0

1. Назовите направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов? Дайте им объяснения?

2. Что обеспечивает стойкость алгоритмов, использующих генератор псевдослучайных чисел Блюма–Блюма–Шаба?

3. Разработать программный код, выполняющий шифрование методом Цезаря со сдвигом на 3.

Вопросы к зачету

по дисциплине *Информационная безопасность*

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.

Критерии оценки:

Оценка	Критерии
Отлично (84–100)	ответы на вопросы четкие, обоснованные и полные, проявлена готовность к дискуссии, студент демонстрирует высокий уровень владения знаниями, умениями и навыками соответствующих компетенций, что позволяет ему решать широкий круг типовых и нетиповых задач.
Хорошо (67–83)	ответы на вопросы преимущественно правильные, но недостаточно четкие, студент способен самостоятельно воспроизводить и применять соответствующие знания, умения и навыки для решения типовых задач дисциплины, может выполнять поиск и использование новой информации для выполнения новых профессиональных действий на основе полностью освоенных знаний, умений и навыков соответствующих компетенций
Удовлетворительно (50-66)	ответы на вопросы не полные, на некоторые ответ не получен, знания, умения, навыки сформированы на базовом уровне, студенты частично, с помощью извне (например, с использованием наводящих вопросов, ассоциативного ряда понятий и т.д.) могут воспроизводить и применять соответствующие знания, умения, навыки
Неудовлетворительно (0-49)	на большую часть вопросов ответы не были получены, либо они показали полную некомпетентность студента в материале дисциплины, студент не способен самостоятельно, без помощи извне, воспроизводить и применять соответствующие знания, умения, навыки или знания, умения и навыки у студента не выявлены

Лабораторные задания

по дисциплине *Информационная безопасность*

1.Тематика лабораторных работ по разделам и темам

1. Основы информационной безопасности и защиты информации 1.1. Изучение содержания и последовательности работ по защите информации. 1.2. Изучение методов комплексного исследования объекта информатизации. 1.3. Изучение методов построения систем обеспечения информационной безопасности на основе нормативных актов. 1.4. Разработка политики информационной безопасности для организации. 1.5. Изучение и построение модели нарушителя информационной безопасности. 1.6. Изучение основных видов компьютерных вирусов и способы борьбы с ними. 1.7. Обеспечение информационной безопасности за счет повышения связности телекоммуникационной сети. 1.8. Поиск надежных каналов передачи информации в телекоммуникационных сетях. 1.9. Исследование методов выбора рационального варианта системы защиты информации на основе криптографических методов.
2. Комплексный подход к решению вопросов обеспечения безопасности информационных систем 2.1. Исследование основных показателей надежности информационных систем. 2.2. Расчет надежности аналоговых и цифровых подсистем ИС при различных видах угроз. 2.3. Изучение видов резервирования для повышения надежности и безопасности ИС. 2.4. Вероятностно-логический метод расчета надежности. 2.5. Логико-вероятностный метод расчета надежности. 2.6. Модель расчета надежности систем обеспечения информационной безопасности на основе системы дифференциальных уравнений. 2.7. Модель расчета надежности систем обеспечения информационной безопасности на основе системы интегральных уравнений. 2.8. Оценка надежности восстанавливаемых систем. 2.9. Виды и причины отказов программного обеспечения. Оценка последствий для информационной безопасности. 2.10. Методы расчета надежности программного обеспечения.

За выполнение всех лабораторных работ курса запланирован максимум в 40 баллов, если студент в ходе защиты показал наличие твердых знаний по

материалу лабораторной работы, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике. В случае частичного выполнения работ, баллы уменьшаются пропорционально количеству защищенных работ.

Тесты письменные и/или компьютерные*

по дисциплине *Информационная безопасность*

ВАРИАНТ 1

1. Под информационной безопасностью понимается…

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;

б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;

в) нет правильного ответа.

2. Защита информации – это…

а) комплекс мероприятий, направленных на обеспечение информационной безопасности;

б) процесс разработки структуры базы данных в соответствии с требованиями пользователей;

в) небольшая программа для выполнения определенной задачи.

3. От чего зависит информационная безопасность?

а) от компьютеров;

б) от поддерживающей инфраструктуры;

в) от информации.

4. Основные составляющие информационной безопасности:

а) целостность;

б) достоверность;

в) конфиденциальность.

5. Доступность – это…

а) возможность за приемлемое время получить требуемую информационную услугу;

б) логическая независимость;

в) нет правильного ответа.

6. Целостность – это…

а) целостность информации;

б) непротиворечивость информации;

в) защищенность от разрушения.

7. Конфиденциальность – это…

а) защита от несанкционированного доступа к информации;

б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов;

в) описание процедур.

8. Для чего создаются информационные системы?

а) получения определенных информационных услуг;

б) обработки информации;

в) все ответы правильные.

9. Целостность можно подразделить:

а) статическую;

б) динамичную;

в) структурную.

10. Где применяются средства контроля динамической целостности?

а) при анализе потока финансовых сообщений;

б) обработке данных;

в) при выявлении кражи, дублирования отдельных сообщений.

11. Какие трудности возникают в информационных системах при конфиденциальности?

а) сведения о технических каналах утечки информации являются закрытыми;

б) на пути пользовательской криптографии стоят многочисленные технические проблемы;

в) все ответы правильные.

12. Угроза – это…

а) потенциальная возможность определенным образом нарушить информационную безопасность;

б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;

в) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.

13. Атака – это…

а) попытка реализации угрозы;

б) потенциальная возможность определенным образом нарушить информационную безопасность;

в) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это…

а) потенциальный злоумышленник;

б) злоумышленник;

в) нет правильного ответа.

15. Окно опасности – это…

а) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется;

б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области;

в) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере.

16. Какие события должны произойти за время существования окна опасности?

а) должно стать известно о средствах использования пробелов в защите;

б) должны быть выпущены соответствующие заплаты;

в) заплаты должны быть установлены в защищаемой ИС.

17. Угрозы можно классифицировать по нескольким критериям:

а) по спектру ИБ;

б) по способу осуществления;

в) по компонентам ИС.

18. По каким компонентам классифицируется угрозы доступности:

а) отказ пользователей;

б) отказ поддерживающей инфраструктуры;

в) ошибка в программе.

19. Основными источниками внутренних отказов являются:

а) отступление от установленных правил эксплуатации;

б) разрушение данных;

в) все ответы правильные.

20. Основными источниками внутренних отказов являются:

а) ошибки при конфигурировании системы;

б) отказы программного или аппаратного обеспечения;

в) выход системы из штатного режима эксплуатации.

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности;

б) обрабатывать большой объем программной информации;

в) нет правильного ответа.

22. Какие существуют грани вредоносного ПО?

а) вредоносная функция;

б) внешнее представление;

в) способ распространения.

23. По механизму распространения П.О. различают:

а) вирусы;

б) черви;

в) все ответы правильные.

24. Вирус – это…

а) код, обладающий способностью к распространению путем внедрения в другие программы;

б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов;

в) небольшая программа для выполнения определенной задачи.

25. Черви – это…

а) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения;

б) код обладающий способностью к распространению путем внедрения в другие программы;В) программа действий над объектом или его свойствами

26. Конфиденциальную информацию можно разделить:

а) предметную;

б) служебную;

в) глобальную.

27. Природа происхождения угроз:

а) случайные;

б) преднамеренные;

в) природные.

28. Предпосылки появления угроз:

а) объективные;

б) субъективные;

в) преднамеренные.

29. К какому виду угроз относится присвоение чужого права?

а) нарушение права собственности;

б) нарушение содержания;

в) внешняя среда.

30. Отказ, ошибки, сбой – это:

а) случайные угрозы;

б) преднамеренные угрозы;

в) природные угрозы.

31. Отказ - это…

а) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций;

б) некоторая последовательность действий, необходимых для выполнения конкретного задания;

в) структура, определяющая последовательность выполнения и взаимосвязи процессов.

32. Ошибка – это…

а) неправильное выполнение элементом одной или нескольких функций, происходящее вследствие специфического состояния;

б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций;

в) негативное воздействие на программу.

33. Сбой – это…

а) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент;

б) неправильное выполнение элементом одной или нескольких функций, происходящее вследствие специфического состояния;

в) объект-метод.

34. Побочное влияние – это…

а) негативное воздействие на систему в целом или отдельные элементы;

б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент;

в) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций.

35. СЗИ (система защиты информации) делится:

а) ресурсы автоматизированных систем;

б) организационно-правовое обеспечение;

в) человеческий компонент.

36. Что относится к человеческому компоненту СЗИ?

а) системные порты;

б) администрация;

в) программное обеспечение.

37. Что относится к ресурсам автоматизированной СЗИ?

а) лингвистическое обеспечение;
б) техническое обеспечение;
в) все ответы правильные.

38. По уровню обеспеченной защиты все системы делят:
а) сильной защиты;
б) особой защиты;
в) слабой защиты.

39. По активности реагирования СЗИ системы делят:
а) пассивные;
б) активные;
в) полупассивные.

40. Правовое обеспечение безопасности информации – это…
а) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации;
б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;
в) нет правильного ответа.

ВАРИАНТ 2

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
а) разработка аппаратных средств обеспечения правовых данных;
б) разработка и установка во всех компьютерных правовых сетях журналов учета действий;
в) разработка и конкретизация правовых нормативных актов обеспечения безопасности.

2. Основными источниками угроз информационной безопасности являются все указанное в списке:
а) хищение жестких дисков, подключение к сети, инсайдерство;
б) перехват данных, хищение данных, изменение архитектуры системы;
в) хищение данных, подкуп системных администраторов, нарушение регламента работы.

3. Виды информационной безопасности:
а) персональная, корпоративная, государственная;
б) клиентская, серверная, сетевая;
в) локальная, глобальная, смешанная.

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:

а) несанкционированного доступа, воздействия в сети;

б) инсайдерства в организации;

в) чрезвычайных ситуаций.

5. Основные объекты информационной безопасности:

а) компьютерные сети, базы данных;

б) информационные системы, психологическое состояние пользователей;

в) бизнес-ориентированные, коммерческие системы.

6. Основными рисками информационной безопасности являются:

а) искажение, уменьшение объема, перекодировка информации;

б) техническое вмешательство, выведение из строя оборудования сети;

в) потеря, искажение, утечка информации.

7. К основным принципам обеспечения информационной безопасности относится:

а) экономической эффективности системы безопасности;

б) многоплатформенной реализации системы;

в) усиления защищенности всех звеньев системы.

8. Основными субъектами информационной безопасности являются:

а) руководители, менеджеры, администраторы компаний;

б) органы права, государства, бизнеса;

в) сетевые базы данных, фаерволлы.

9. К основным функциям системы безопасности можно отнести все перечисленное:

а) установление регламента, аудит системы, выявление рисков;

б) установка новых офисных приложений, смена хостинг-компании;

в) внедрение аутентификации, проверки контактных данных пользователей.

10. Принципом информационной безопасности является принцип недопущения:

а) неоправданных ограничений при работе в сети (системе);

б) рисков безопасности сети, системы;

в) презумпции секретности.

11. Принципом политики информационной безопасности является принцип:

а) невозможности миновать защитные средства сети (системы);

б) усиления основного звена сети, системы;

в) полного блокирования доступа при риск-ситуациях.

12. Принципом политики информационной безопасности является принцип:

а) усиления защищенности самого незащищенного звена сети (системы);

б) перехода в безопасное состояние работы сети, системы;

в) полного доступа пользователей ко всем ресурсам сети, системы.

13. Принципом политики информационной безопасности является принцип:

а) разделения доступа (обязанностей, привилегий) клиентам сети (системы);

б) одноуровневой защиты сети, системы;

в) совместимых, однотипных программно-технических средств сети, системы.

14. К основным типам средств воздействия на компьютерную сеть относится:

а) компьютерный сбой;

б) логические закладки («мины»);

в) аварийное отключение питания.

15. Когда получен спам по e-mail с приложенным файлом, следует:

а) прочитать приложение, если оно не содержит ничего ценного – удалить;

б) сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама;

в) удалить письмо с приложением, не раскрывая (не читая) его.

16. Принцип Кирхгофа:

а) Секретность ключа определена секретностью открытого сообщения;

б) Секретность информации определена скоростью передачи данных;

в) Секретность закрытого сообщения определяется секретностью ключа.

17. ЭЦП – это:

а) электронно-цифровой преобразователь;

б) электронно-цифровая подпись;

в) электронно-цифровой процессор.

18. Наиболее распространены угрозы информационной безопасности корпоративной системы:

а) покупка нелицензионного ПО;

б) ошибки эксплуатации и неумышленного изменения режима работы системы;

в) сознательного внедрения сетевых вирусов.

19. Наиболее распространены угрозы информационной безопасности сети:

а) распределенный доступ клиент, отказ оборудования;

б) моральный износ сети, инсайдерство;

в) сбой (отказ) оборудования, нелегальное копирование данных.

20. Наиболее распространены средства воздействия на сеть офиса:

а) слабый трафик, информационный обман, вирусы в интернет;

б) вирусы в сети, логические мины (закладки), информационный перехват;

в) компьютерные сбои, изменение администрирования, топологии.

21. Утечкой информации в системе называется ситуация, характеризуемая:

а) потерей данных в системе;

б) изменением формы информации;

в) изменением содержания информации.

22. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

а) целостность;

б) доступность;

в) актуальность.

23. Угроза информационной системе (компьютерной сети) – это:

а) вероятное событие;

б) детерминированное (всегда определенное) событие;

в) событие, происходящее периодически.

24. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

а) регламентированной;

б) правовой;

в) защищаемой.

25. Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

а) программные, технические, организационные, технологические;

б) серверные, клиентские, спутниковые, наземные;

в) личные, корпоративные, социальные, национальные.

26. Окончательно, ответственность за защищенность данных в компьютерной сети несет:

а) владелец сети;
б) администратор сети;
в) пользователь сети.

27. Политика безопасности в системе (сети) – это комплекс:

а) руководств, требований обеспечения необходимого уровня безопасности;
б) инструкций, алгоритмов поведения пользователя в сети;
в) нормы информационного права, соблюдаемые в сети.

28. Наиболее важным при реализации защитных мер политики безопасности является:

а) аудит, анализ затрат на проведение защитных мер;
б) аудит, анализ безопасности;
в) аудит, анализ уязвимостей, риск-ситуаций.

29. Программные средства – это…

а) специальные программы и системы защиты информации в информационных системах различного назначения;
б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла;
в) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними.

30. Криптографические средства – это…

а) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования;
б) специальные программы и системы защиты информации в информационных системах различного назначения;
в) механизм, позволяющий получить новый класс на основе существующего.

31. Правовое обеспечение безопасности информации делится:

а) международно-правовые нормы;
б) национально-правовые нормы;
в) все ответы правильные.

32. Информацию с ограниченным доступом делят:

а) государственную тайну;
б) конфиденциальную информацию;
в) достоверную информацию.

33. Что относится к государственной тайне?

а) сведения, защищаемые государством в области военной, экономической и иной деятельности;

б) документированная информация;

в) нет правильного ответа.

34. Вредоносная программа - это…

а) программа, специально разработанная для нарушения нормального функционирования систем;

б) упорядочение абстракций, расположение их по уровням;

в) процесс разделения элементов абстракции, которые образуют ее структуру и поведение.

35. Основополагающие документы для обеспечения безопасности внутри организации:

а) трудовой договор сотрудников;

б) должностные обязанности руководителей;

в) коллективный договор.

36. К организационно - административному обеспечению информации относится:

а) взаимоотношения исполнителей;

б) подбор персонала;

в) регламентация производственной деятельности.

37. Что относится к организационным мероприятиям:

а) хранение документов;

б) проведение тестирования средств защиты информации;

в) пропускной режим.

38. Какие средства используется на инженерных и технических мероприятиях в защите информации:

а) аппаратные;

б) криптографические;

в) физические.

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 зачета, это аттестация, которая проводится в соответствии с действующим в РГЭУ (РИНХ) Положением о курсовых, экзаменах и зачётах.

Зачет проводится в соотвествии с расписанием в компьютерном классе. Количество вопросов контрольном задании – 3. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины адресованы студентам всех форм обучения.

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные работы.

Важным условием успешного освоения дисциплины «Информационная безопасность» является создание системы правильной организации труда, позволяющей распределить учебную нагрузку равномерно в соответствии с графиком образовательного процесса. Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подвести итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине они произошли. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана. Все задания к лабораторным занятиям, а также задания, вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующей темы лекционного курса, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями и навыками.

Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит

больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

В процессе подготовки к лабораторным занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

Изучение дисциплины проходит с акцентом на лабораторные работы. Лабораторные занятия проводятся в компьютерных классах с применением специально разработанных учебно-методических материалов, в которых изложены подробные методические рекомендации по изучению каждой темы и выполнению заданий. Наличие таких учебно-методических и дидактических материалов позволяет каждому студенту работать в своем индивидуальном темпе, а также дополнительно прорабатывать изучаемый материал во время самостоятельных занятий.

Перед выполнением лабораторной работы требуется получить вариант задания. Далее необходимо ознакомиться с заданием. Выполнение лабораторной работы следует

начать с изучения теоретических сведений, которые приводятся в соответствующих методических указаниях. Результаты работы необходимо оформить в виде отчета.

Лабораторная работа считается выполненной, если

- предоставлен отчет о результатах выполнения задания;
- проведена защита проделанной работы.

Защита проводится в два этапа:

1) Демонстрируются результаты выполнения задания.

2) В случае лабораторной работы, предусматривающей разработку программного приложения при помощи тестового примера, доказывается, что результат, получаемый при выполнении программы правильный.

3) Далее требуется ответить на ряд вопросов из перечня контрольных вопросов, который приводится в задании на лабораторную работу.

Вариант задания выдается преподавателем, проводящим лабораторные занятия.

Для успешного овладения предлагаемым курсом студент должен обладать определённой информационной культурой: навыками работы с литературой, умением определять и находить информационные ресурсы, соответствующие целям и задачам образовательного процесса, получать к ним доступ и использовать в целях повышения эффективности своей профессиональной деятельности. При изучении данного курса необходимо максимально использовать компьютер, изучать дополнительные информационные ресурсы.

Подготовка к промежуточной аттестации.

При подготовке к промежуточной аттестации целесообразно:

- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
- составить краткие конспекты ответов (планы ответов).