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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Теория информационной безопасности и методология защиты информации

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	48	48	48	48
Практические	32	32	32	32
Итого ауд.	112	112	112	112
Контактная работа	112	112	112	112
Сам. работа	32	32	32	32
Часы на контроль	36	36	36	36
Итого	180	180	180	180

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.т.н., доцент, Лапсарь А. П.

Зав. кафедрой: к.э.н.,доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	изучение и последующее освоение современных технологий обеспечения информационной безопасности объектов; получение навыков планирования мероприятий по обеспечению информационной безопасности объектов; освоение современных технологий обеспечения информационной безопасности объектов;анализ и синтез систем информационной безопасности объектов.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3: способен проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям стандартов в области информационной безопасности

ПК-5: способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять защитой объектов информатизации

В результате освоения дисциплины обучающийся должен:

Знать:

требования нормативных правовых актов и стандартов в области информационной безопасности (соотнесено с индикатором ПК- 3.1);
объем и содержание комплекса мер по обеспечению информационной безопасности, методы управления защитой объектов информатизации (соотнесено с индикатором ПК- 5.1)

Уметь:

проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям нормативных правовых актов и стандартов в области информационной безопасности (соотнесено с индикатором ПК- 3.2);
способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять защитой объектов информатизации (соотнесено с индикатором ПК- 5.2)

Владеть:

проведения анализа информационной безопасности объектов и автоматизированных систем на соответствие требованиям нормативных правовых актов и стандартов в области информационной безопасности, подготовки предложений по совершенствованию системы защиты информации (соотнесено с индикатором ПК- 3.3);
планирования, организации и выполнения комплекса мер по обеспечению информационной безопасности и управления защитой объектов информатизации (соотнесено с индикатором ПК- 5.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Общие сведения о современных технологиях защиты информации.

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Тема 1 "Общие сведения о современных технологиях защиты информации". Классификация технологий обеспечения информационной безопасности.Технические методы защиты информации. Организационные методы защиты информации / Лек /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.2	Тема 1 Классификация технологий обеспечения информационной безопасности.Технические методы защиты информации. Организационные методы защиты информации / Пр /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.3	Тема 1 "Общие сведения о современных технологиях защиты информации". Исследование систем информационной безопасности, встроенных в среду LibreOffice / Лаб /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.4	Тема 1 "Общие сведения о современных технологиях защиты информации". Требования к технологиям обеспечения информационной безопасности объектов защиты. Методы анализа информационной системы для выбора технологий обеспечения информационной безопасности объектов. / Ср /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.5	Тема 2 "Объекты и субъекты информационной безопасности". Информационная система. Техническая и антропогенная составляющие информационной системы Объект информатизации. Информация как объект защиты. машинные норсители информации / Лек /	5	0	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.6	Тема 2 "Объекты и субъекты информационной безопасности". Информационная система. Техническая и антропогенная составляющие информационной системы Объект информатизации. Информация как объект защиты. машинные норсители информации / Пр /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4

1.7	Тема 2 "Объекты и субъекты информационной безопасности". Информационная система. Техническая и антропогенная составляющие информационной системы Объект информатизации. Информация как объект защиты. машинные норсители информации / Лаб /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.8	Тема 3 "Угрозы информационной безопасности". 1. Информационные угрозы, их виды, причины. 2. Вредоносные программы, их виды. 3. Компьютерные преступления, их виды. / Лек /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.9	Тема 3 "Угрозы информационной безопасности". 1. Информационные угрозы, их виды, причины. 2. Вредоносные программы, их виды. 3. Компьютерные преступления, их виды. / Пр /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.10	Тема 3 "Угрозы информационной безопасности". 1. Информационные угрозы, их виды, причины. 2. Вредоносные программы, их виды. 3. Компьютерные преступления, их виды. / Лаб /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.11	Тема 4 "Объектовые технологии обеспечения информационной безопасности". Объекты и субъекты защиты. Разграничение доступа. Физическая защита объекта. Показатели защищенности информации. / Лек /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.12	Тема 4 "Объектовые технологии обеспечения информационной безопасности". Объекты и субъекты защиты. Разграничение доступа. Физическая защита объекта. Показатели защищенности информации. / Пр /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.13	Тема 4 "Объектовые технологии обеспечения информационной безопасности". Объекты и субъекты защиты. Разграничение доступа. Физическая защита объекта. Показатели защищенности информации. / Лаб /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.14	Тема 4 "Объектовые технологии обеспечения информационной безопасности". Концептуальные основы защиты информации. Система документов по технической защите информации. Концептуальные основы защиты информации. Законодательные и иные правовые акты в области технической защиты информации. Органы по технической защите информации в РФ. / Ср /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.15	Тема 5 "Периметровые технологии обеспечения информационной безопасности". Территория с ограниченным доступом. Контролируемая зона. Разделение территории на режимную и нережимную. Показатели защищенности информации. / Лек /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.16	Тема 5 "Периметровые технологии обеспечения информационной безопасности". Территория с ограниченным доступом. Контролируемая зона. Разделение территории на режимную и нережимную. Показатели защищенности информации / Пр /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.17	Тема 5 "Периметровые технологии обеспечения информационной безопасности". Исследование показателей защищенности информациив в РЕД ОС / Лаб /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.18	Тема 5 "Периметровые технологии обеспечения информационной безопасности". Технологии зашиты информации от утечки по каналам ПЭМИН. / Ср /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.19	Тема 6 "Технологии формирования доверенной среды". Понятие доверенной среды. Формирование доверенных сред. Доверенные объекты и доверенные субъекты. Доверенные коммуникации. Межсетевые экраны. / Лек /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.20	Тема 6 "Технологии формирования доверенной среды". Понятие доверенной среды. Формирование доверенных сред. Доверенные объекты и доверенные субъекты. Доверенные коммуникации. Межсетевые экраны. / Пр /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.21	Тема 6 "Технологии формирования доверенной среды". Исследование межсетевых экранов. / Лаб /	5	6	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
1.22	Тема 6 "Технологии формирования доверенной среды". Доверенные технические средства. Доверенное программное обеспечение. Средства доверенной загрузки. Системы обнаружения вторжений, средства антивирусной защиты. / Ср /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
Раздел 2. Базовые технологии обеспечения информационной безопасности объектов на различных этапах их жизненного цикла					

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Тема 1. "Технологии обеспечения защиты от несанкционированного доступа". классификация технологий защиты от НСД. Технологии межсетевоно экранирования. Технологии обраружения вторжений. тезнологии антивирусной защиты. Перспективы развития технологий защиты от несанкционированного доступа / Лек /	5	6	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.2	Тема 1. "Технологии обеспечения защиты от несанкционированного доступа". классификация технологий защиты от НСД. Технологии межсетевоно экранирования. Технологии обраружения вторжений. тезнологии антивирусной защиты. Перспективы развития технологий защиты от несанкционированного доступа / Лаб /	5	8	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.3	Тема 1. "Технологии обеспечения защиты от несанкционированного доступа". классификация технологий защиты от НСД. Технологии межсетевоно экранирования. Технологии обраружения вторжений. тезнологии антивирусной защиты. Перспективы развития технологий защиты от несанкционированного доступа / Пр /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.4	Тема 2 "Облачные технологии обработки информации". Обеспечение информационной безопасности при облачных технологиях обработки информации. / Лек /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.5	Тема 2 "Облачные технологии обработки информации". Обеспечение информационной безопасности при вводе объектов в эксплуатацию. / Пр /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.6	Тема 2 "Облачные технологии обработки информации". Обеспечение информационной безопасности при вводе объектов в эксплуатацию. / Лаб /	5	6	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.7	Тема 2 " Облачные технологии обработки информации". Облачные Web-сервисы для автоматизации прикладных и информационных процессов. Архитектура WEB-сервисов. Стандарты Webсервисы .NET. Основные принципы. NET и общая система типов. NET Основные виды запросов к Web-сервису. / Ср /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.8	Тема 3 "Гармонизация обеспечения информационной безопасности". Основные технологии обеспечения информационной безопасности в США и странах Евросоюза. Стандарты информационной безопасности ISO. Аудит информационной безопасности. / Лек /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.9	Тема 3 "Гармонизация обеспечения информационной безопасности". Основные технологии обеспечения информационной безопасности в США и странах Евросоюза. Стандарты информационной безопасности ISO. Аудит информационной безопасности. / Пр /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.10	Тема 3 "Гармонизация обеспечения информационной безопасности". Технологии зашиты видовой информации от утечки. / Лаб /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.11	Тема 4 "Технологии защиты информации при проектировании объектов информатизации". Обоснование степени информационной безопасности проектируемых объектов информатизации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию, проверки. Специальные проверки и специальные исследования. / Лек /	5	2	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.12	Тема 4 "Технологии защиты информации при проектировании объектов информатизации". Обоснование степени информационной безопасности проектируемых объектов информатизации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию, проверки. Специальные проверки и специальные исследования. / Пр /	5	4	ПК-3, ПК-5	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.13	Тема 4 "Технологии защиты информации при проектировании объектов информатизации". Специальные проверки и специальные исследования объекта защиты. / Лаб /	5	6	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.14	Курсовое проектирование. Перечень тем представлен в	5	20	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3,

	приложении 1 к рабочей программе дисциплины / Ср /				Л1.4, Л2.1, Л2.2, Л2.3, Л2.4
2.15	/ Экзамен /	5	36	ПК-3, ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4

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,	Заглавие	Издательство, год	Колич-во
Л1.1	Загинайлов Ю. Н.	Теория информационной безопасности и методология защиты информации: учебное пособие	Москва, Берлин: Директ-Медиа, 2015	https://biblioclub.ru/index.php?page=book&id=276557 неограниченный доступ для зарегистрированных пользователей
Л1.2	Аверченков, В. И., Рытов, М. Ю.	Организационная защита информации: учебное пособие для вузов	Брянск: Брянский государственный технический университет, 2012	https://www.iprbookshop.ru/7002.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Бахаров, Л. Е.	Информационная безопасность и защита информации: сборник тестов	Москва: Издательский Дом МИСиС, 2015	http://www.iprbookshop.ru/98858.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	https://biblioclub.ru/index.php?page=book&id=576726 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2014	https://biblioclub.ru/index.php?page=book&id=238446 неограниченный доступ для зарегистрированных пользователей
Л2.2	Аверченков, В. И., Рытов, М. Ю., Кувыклин, А. В., Гайнулин, Т. Р.	Разработка системы технической защиты информации: учебное пособие	Брянск: Брянский государственный технический университет, 2012	https://www.iprbookshop.ru/7005.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Титов, А. А.	Технические средства защиты информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	https://www.iprbookshop.ru/13989.html неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.4	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва, Берлин: Директ-Медиа, 2020	https://biblioclub.ru/index.php?page=book&id=571485 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Информационная справочная система "КонсультантПлюс"
База данных Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/
База данных действующих стандартов по направлению "Информационная Безопасность" https://www.gost.ru/portal/gost/home/standarts/InformationSecurity

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

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

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 программными средствами и выходом в Интернет.

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
ПК-3: способен проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям стандартов в области информационной безопасности			
З. требования нормативных правовых актов и стандартов в области информационной безопасности	подбор и изучение нормативных правовых актов и стандартов, основной и дополнительной литературы при подготовке к экзамену, тестированию	полнота и содержательность ответа умение приводить примеры на экзамене, тестировании	Т (1-21), Э (1-12)
У. проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям нормативных правовых актов и стандартов в области информационной безопасности	поиск и сбор необходимой литературы, нормативных правовых актов и стандартов, анализ фундаментальных и прикладных проблем информационной безопасности при выполнении лабораторных работ, в курсовом проекте	полнота и содержательность ответа умение приводить примеры, умение самостоятельно находить решение поставленных задач в курсовом проекте	ЛЗ (1-5) ПЗ (1-4) ПОЗЭ (1-4) КП (1-15)
В. навыками проведения анализа информационной безопасности объектов и автоматизированных систем на соответствие требованиям нормативных правовых актов и стандартов в области информационной безопасности, подготовки предложений по совершенствованию системы защиты информации	использование требований нормативных правовых актов и стандартов, информационно-коммуникационных технологий и глобальных информационных ресурсов при выполнении лабораторных работ, в курсовом проекте	полнота и содержательность ответа, его обоснованность, умение приводить примеры умение самостоятельно находить решение поставленных задач в курсовом проекте	ЛЗ (1-5) ПЗ (1-4) ПОЗЭ (1-4) КП (1-15)
ПК-5: способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять защитой объектов информатизации			
З. объем и содержание комплекса мер по обеспечению информационной безопасности, методы управления защитой объектов информатизации	поиск и анализ необходимой литературы, содержание организационных мер и технических средств обеспечения информационной безопасности при подготовке к экзамену, тестированию	полнота и содержательность ответа умение приводить примеры на экзамене, тестировании	Т (1-21), Э (13-47)
У. способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять защитой объектов информатизации	использование требований нормативных актов и методических документов в области информационной безопасности при выполнении лабораторных работ, в курсовом проекте	полнота и содержательность ответа умение приводить примеры, умение самостоятельно находить решение поставленных задач в курсовом проекте	ЛЗ (4-10) ПЗ (5-10) ПОЗЭ (1-4) КП (1-15)
В. навыками планирования, организации и выполнения комплекса мер по обеспечению информационной безопасности и управления защитой объектов информатизации	уверенное применение требований нормативных актов и методических документов в области информационной безопасности при выполнении лабораторных работ, в курсовом проекте	полнота и содержательность ответа умение приводить примеры, умение самостоятельно находить решение поставленных задач в курсовом проекте	ЛЗ (4-10) ПЗ (5-10) ПОЗЭ (1-4) КП (1-15)

ЛЗ – лабораторные задания, ПЗ- практические задания; Т – тест, Э – вопросы к экзамену, ПОЗЭ – практико-ориентированные задания к экзамену, КП – темы курсового проекта

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. Организационные методы защиты информации.
2. Технические методы защиты информации классификация технологий обеспечения информационной безопасности.
3. Требования к технологиям обеспечения информационной безопасности объектов защиты.
4. Методы анализа информационной системы для выбора технологий обеспечения информационной безопасности объектов.
5. Объекты и субъекты защиты.
6. Разграничение доступа.
7. Физическая защита объекта.
8. Показатели защищенности информации.
9. Концептуальные основы защиты информации.
10. Система документов по технической защите информации.
11. Концептуальные основы защиты информации.
12. Законодательные и иные правовые акты в области технической защиты информации.
13. Органы по технической защите информации в РФ.
14. Территория с ограниченным доступом.
15. Контролируемая зона.
16. Разделение территории на режимную и нережимную.
17. Показатели защищенности информации.
18. Технологии зашиты информации от утечки по каналам ПЭМИН.
19. Понятие доверенной среды.
20. Формирование доверенных сред.
21. Доверенные объекты и доверенные субъекты.
22. Доверенные коммуникации.
23. Межсетевые экраны.
24. Доверенные технические средства.
25. Доверенное программное обеспечение.
26. Средства доверенной загрузки.
27. Системы обнаружения вторжений, средства антивирусной защиты.
28. Обеспечение информационной безопасности при облачных технологиях обработки информации.
29. Облачные Web-сервисы для автоматизации прикладных и информационных процессов.
30. Архитектура WEB-сервисов.
31. Стандарты Webсервисы .NET.
32. Основные принципы.
33. NET и общая система типов.
34. NET Основные виды запросов к Web-сервису.
35. Основные технологии обеспечения информационной безопасности в США и странах Евросоюза.
36. Стандарты информационной безопасности ISO.
37. Аудит информационной безопасности.
38. Классы функциональных требований, описывающие элементарные сервисы безопасности.
39. Классы функциональных требований, описывающие производные сервисы безопасности.

40. Защита данных пользователя.
41. Защита функций безопасности объекта оценки.
42. Классы функциональных требований, играющие инфраструктурную роль.
43. Обоснование степени информационной безопасности проектируемых объектов информатизации.
44. Обеспечение информационной безопасности при вводе объектов в эксплуатацию, проверки.
45. Специальные проверки и специальные исследования.
46. Подбор и обоснование технологий обеспечения информационной безопасности в зависимости от характера объекта информатизации.
47. Технологии для формирования проектных решений по защите объектов информатизации

Практико-ориентированные задания к экзамену

1. Виды контроля состояния информационной безопасности объектов. Межведомственный и ведомственный контроль состояния информационной безопасности объектов.
2. Объектовый мониторинг состояния информационной безопасности. Формы представления результатов контроля.
3. Методы оценки эффективности проводимых мероприятий. Экспертные методы оценки эффективности систем информационной безопасности. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.
4. Системы централизованного управления безопасностью. Средства управления безопасностью локальных сетей. Продукты ведущих производителей для управления безопасностью.

Критерии оценивания:
- 84-100 баллов – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированного задания, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 баллов – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целью обучения, правильные действия по применению навыком и умений при решении практико-ориентированного задания, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 баллов – наличие твердых знаний в объеме пройденного курса в соответствии с целью обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению навыком и умений при решении практико-ориентированного задания;
- 0-49 баллов – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированного задания, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Тесты

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
а) сотрудники
б) хакеры
в) атакующие
г) контрагенты (лица, работающие по договору)
2. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
а) владельцы данных
б) пользователи

в) администраторы
г) руководство
3. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
а) поддержка высшего руководства
б) эффективные защитные меры и методы их внедрения
в) актуальные и адекватные политики и процедуры безопасности
г) проведение тренингов по безопасности для всех сотрудников
4. Что такое политики безопасности?
а) инструкции по выполнению задач безопасности
б) общие руководящие требования по достижению определенного уровня безопасности
в) широкие, высокоуровневые заявления руководства
г) детализированные документы по обработке инцидентов безопасности
5. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
а) анализ рисков
б) анализ затрат / выгоды
в) результаты ALE
г) выявление уязвимостей и угроз, являющихся причиной риска
6. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
а) анализ рисков
б) анализ затрат / выгоды
в) результаты ALE
г) выявление уязвимостей и угроз, являющихся причиной риска
7. Емкостные системы обеспечения безопасности объектов информатизации относятся к категории:
а) система охранно-тревожной сигнализации
б) система контроля и управления доступом
в) система пожарной сигнализации и пожаротушения
г) система периметровой охраны
8. В зависимости от физической природы возникновения информационных сигналов, среды их распространения и способов перехвата техническими средствами разведки технические каналы утечки информации для телекоммуникационной информации можно разделить на:
а) электромагнитные
б) электростатические
в) электрические
г) магнитные
д) параметрические
9. Что такое контролируемая зона?
а) зона, в которой возможно появление лиц и транспортных средств, не имеющих постоянных или временных пропусков
б) зона, в которой исключено появление только транспортных средств, не имеющих постоянных или временных пропусков
в) зона, в которой исключено появление лиц и транспортных средств, имеющих только временные пропуска
г)зона, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков
10. В политике безопасности какого уровня описывается отношение к передовым, но еще недостаточно проверенным технологиям защиты информации?
а) правового и административного
б) процедурного
в) аппаратно-программного
11. Что определяет системная информационная политика?
а) принципы, порядок и правила интеграции информационных ресурсов
б) принципы, порядок и правила построения систем защиты информации
в) принципы, порядок и правила разграничения доступа к информационным ресурсам

12. Как называется внешняя или внутренняя по отношению к атакуемой компьютерной системе программа, обладающая определенными деструктивными функциями по отношению к этой системе?
а) компьютерный вирус
б) программная закладка
в) аппаратная закладка
13. Что не может помощник по конфигурированию сети сайта?
а) управлять IP адресами
б) оптимизировать работу интернет сервиса
в) конфигурировать подсеть
г) интегрировать балансировщики нагрузки
14. Какие преимущества несет в себе использование частного облака?
а) независимость и безопасность данных
б) физический контроль
в) интеграция приложений
г) все перечисленное
15 Как для ИТ специалиста изменится реальность с распространением облачных вычислений
а) массовая глобализация на уровне крупных датацентров
б) установка Xbox в серверной и совершенствования в компьютерных играх
в) возможности сделать карьеру в использованием знакомых технологий, которые будут адаптироваться под требования бизнеса
г) придется все изучать с чистого листа
16.Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
а) поддержка
б) выполнение анализа рисков
в) определение цели и границ
г) делегирование полномочий
17. Целостность и наглядность описания предметной области сохраняется в семантических сетях с увеличением размеров и усложнением связей
а) да
б)нет
18.Задачи аппаратного моделирования деятельности человека могут относиться к задачам искусственного интеллекта
а) да
б)нет
19.Принципом информационной безопасности является принцип недопущения:
а) неоправданных ограничений при работе в сети (системе)
б) рисков безопасности сети, системы
в) презумпции секретности
20. 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
21. Наиболее распространены угрозы информационной безопасности сети:
а) распределенный доступ клиент, отказ оборудования
б) моральный износ сети, инсайдерство
в) сбой (отказ) оборудования, нелегальное копирование данных

Инструкция по выполнению

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его взгляд, варианта ответа. Тестовое задание содержит 20 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается.

Время прохождения тестирования 20 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

Критерии оценивания:
- 0-20 баллов выставляется обучаемому за прохождение теста.
За один правильный ответ обучаемый получает 1 балл.

Практические задания

1. Классификация технологий обеспечения информационной безопасности. Технические методы защиты информации. Организационные методы защиты информации
2 Объекты и субъекты информационной безопасности.
3 Угрозы информационной безопасности.
4 Объектовые технологии обеспечения информационной безопасности. Объекты и субъекты защиты. Разграничение доступа. Физическая защита объекта. Показатели защищенности информации.
5 Периметровые технологии обеспечения информационной безопасности. Территория с ограниченным доступом. Контролируемая зона. Разделение территории на режимную и нережимную. Показатели защищенности информации.
6 Технологии формирования доверенной среды. Понятие доверенной среды. Формирование доверенных сред. Доверенные объекты и доверенные субъекты. Доверенные коммуникации. Межсетевые экраны.
7. Технологии обеспечения защиты от несанкционированного доступа. классификация технологий защиты от НСД. Технологии межсетевого экранирования. Технологии обнаружения вторжений. технологии антивирусной защиты. Перспективы развития технологий защиты от несанкционированного доступ
8 Облачные технологии обработки информации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
9 Гармонизация обеспечения информационной безопасности. Основные технологии обеспечения информационной безопасности в США и странах Евросоюза. Стандарты информационной безопасности ISO. Аудит информационной безопасности.
10 Технологии защиты информации при проектировании объектов информатизации. Обоснование степени информационной безопасности проектируемых объектов информатизации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию, проверки. Специальные проверки и специальные исследования.

Критерии оценивания:
0-4б может получить студент - (для каждого задания): Максимальное количество баллов – 40б
4 б. – задание выполнено верно;
3 б. – при выполнении задания были допущены неточности, не влияющие на результат;
2 б. – при выполнении задания были допущены ошибки;
1 б. – при выполнении задания были допущены существенные ошибки;
0 б. – задание не выполнено.

Лабораторные задания

1 Общие сведения о современных технологиях защиты информации. Исследование систем информационной безопасности, встроенных в среду LibreOffice
2 Объекты и субъекты информационной безопасности.
3 Угрозы информационной безопасности.
4 Объектовые технологии обеспечения информационной безопасности. Объекты и субъекты защиты. Разграничение доступа. Физическая защита объекта. Показатели защищенности информации.
5 Периметровые технологии обеспечения информационной безопасности. Территория с ограниченным доступом. Контролируемая зона. Разделение территории на режимную и нережимную. Показатели защищенности информации

6 Технологии формирования доверенной среды. Понятие доверенной среды. Формирование доверенных сред. Доверенные объекты и доверенные субъекты. Доверенные коммуникации. Межсетевые экраны.
7. Технологии обеспечения защиты от несанкционированного доступа. Классификация технологий защиты от НСД. Технологии межсетевоно экранирования. Технологии обраружения вторжений. тезнологии антивирусной защиты. Перспективы развития технологий защиты от несанкционированного доступ
8 Облачные технологии обработки информации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
9 Гармонизация обеспечения информационной безопасности. Технологии зашиты видовой информации от утечки
10 Технологии защиты информации при проектировании объектов информатизации. Специальные проверки и специальные исследования объекта защиты.

Критерии оценивания:
0-4б может получить студент - (для каждого задания): Максимальное количество баллов – 40б
4 б. – задание выполнено верно;
3 б. – при выполнении задания были допущены неточности, не влияющие на результат;
2 б. – при выполнении задания были допущены ошибки;
1 б. – при выполнении задания были допущены существенные ошибки;
0 б. – задание не выполнено.

Темы курсовых проектов

1. Внедрение средств межсетевого экранирования в информационную инфраструктуру онлайн-кинотеатра с использованием методов генеративного проектирования.
2. Внедрение системы предотвращения вторжений в УК ЖКХ с использованием методов генеративного проектирования.
3. Внедрение системы сбора и корреляции событий безопасности в корпоративную информационную систему с использованием методов генеративного проектирования.
4. Внедрение единой среды управления безопасностью личных и корпоративных устройств в организации с использованием методов генеративного проектирования.
5. Внедрение средств межсетевого экранирования в информационную систему сетевого ритейлера электроники с использованием методов генеративного проектирования.
6. Внедрение средств антивирусной защиты в информационную систему образовательного учреждения с использованием методов генеративного проектирования.
7. Внедрение средств обнаружения и предотвращения вторжений IDS/IPS в информационную систему организации с использованием методов генеративного проектирования.
8. Внедрение комплексного программного средства защиты от несанкционированного доступа в медицинской организации с использованием методов генеративного проектирования.
9. Внедрение средства контроля за утечкой информации в туристической компании с использованием методов генеративного проектирования.
10. Внедрение средств межсетевого экранирования в офисе с использованием методов генеративного проектирования.
11. Разработка комплекса мероприятий по защите корпоративной информационной системы от атак методами социальной инженерии с использованием методов генеративного проектирования.
12. Внедрение средств антивирусной защиты в кредитно-финансовом учреждении с использованием методов генеративного проектирования.
13. Внедрение средства обнаружения и предотвращения вторжений IDPS в компании по разработке мобильного ПО с использованием методов генеративного проектирования.
14. Внедрение средств межсетевого экранирования в высшем учебном заведении с использованием методов генеративного проектирования.
15. Внедрение средств антивирусной защиты в муниципальной поликлинике с использованием методов генеративного проектирования.

Требования к оформлению курсового проекта приведены в Приложении 2.

Критерии оценивания:
- 84-100 (оценка «отлично») – изложенный материал в курсовом проекте фактически верен, тема раскрыта; текстовый материал в полном объеме, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 (оценка «хорошо») – изложенный материал в курсовом проекте в основном верен, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 (оценка «удовлетворительно») – изложенный материал в курсовом проекте не в полном объеме ,тема раскрыта не полностью, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов;
- 0-49 (оценка «неудовлетворительно») – изложенный материал в курсовом проекте не в полном объеме ,тема не раскрыта, ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого материала, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

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, защиты курсового проекта.

Экзамен проводится по расписанию промежуточной аттестации в письменном виде. Количество вопросов в экзаменационном задании – 3. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную 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

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются теоретические вопросы с учетом практико-ориентированности изучаемой дисциплины, 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 работы с компьютером, применения методов и технологий защиты информации.

При подготовке к лабораторным занятиям каждый обучающийся должен:

– изучить рекомендованную учебную литературу;

– изучить практические примеры, рассмотренные на лекциях;

– подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к лабораторным занятиям 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 посредством выполнения лабораторных заданий с учетом индивидуальности и творческого решения. 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.

Методические рекомендации по оформлению курсового проекта

Проект должен включать следующие разделы.

1. Содержание, включающее наименование всех разделов и пунктов с указанием номеров страниц.
2. Введение.

2.1 Дается характеристика предметной области, к которой относится решаемая задача и обосновывается ее актуальность.

2.2 Цель работы.

Формулируется цель выполнения задания на курсовой проект.

2.3 Постановка задач.

В этом разделе требуется формализовать задачи, указать возможные ограничения на их решение, ИТ-технологии и т.п.

3. Техническое задание

В соответствии с вариантом формулируется задание по курсовому проекту.

4. Теоретическая часть, освещающую теоретические аспекты темы;
5. Выводы.
6. Список использованных источников.

Таблицы, рисунки, формулы оформляются в соответствии с внутривузовским изданием для нормоконтроля. На все таблицы, рисунки, литературные источники, приложения в тексте должны быть ссылки.

Оформление курсового проекта должно соответствовать требованиям государственных стандартов, в т.ч. и методических рекомендаций вуза (кафедры). Текст работы должен быть набран на белой бумаге формата А4 с одной стороны листа. Размер шрифта: 12, интервал: 1,5. Поля: левое – 30 мм, правое – 10 мм, верхнее – 20 мм, нижнее – 20 мм. Объём курсового проекта 30-40 л.