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

УТВЕРЖДАЮ
Начальник отдела лицензирования и аккредитации
_____Чаленко К.Н.
«30» августа 2021 г.

Рабочая программа дисциплины
Основы информационной безопасности

по профессионально-образовательной программе направления
01.03.05 «Статистика» профиль 01.03.05.01 «Анализ больших данных»

Для набора ___2021___ года

Квалификация
Бакалавр

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	76	76	76	76
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 30.08.2021, протокол № 1.

Программу составил(и): к.т.н., доцент Серпенинов О.В. _____

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. _____

Методическим советом направления: к.э.н., доцент Кислая И.А. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	приобретение знаний в области информационной безопасности и защиты информации по организационно- правовой защите коммерческой, служебной, профессиональной тайны, персональных данных; формирование умений и практических навыков по правовому, организационному и техническому обеспечению защиты информации при решении задач профессиональной деятельности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-2:Способен решать задачи профессиональной деятельности с использованием информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

В результате освоения дисциплины обучающийся должен:
Знать:
способы решения стандартных задач профессиональной деятельности в области информационной безопасности на основе организации процесса сбора, анализа и систематизации информации по формированию системы защиты информации с применением информационно-коммуникационных технологий
Уметь:
решать стандартные задачи профессиональной деятельности с учетом требований информационной безопасности на основе анализа требований нормативно-правовых актов в области информационной безопасности
Владеть:
методологией по разработке комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты на основе анализа нормативно-правовых актов в области информационной безопасности при решении задач профессиональной деятельности

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Правовое и организационное обеспечение информационной безопасности				
1.1	Тема 1."Правовое обеспечение информационной безопасности в системе национальной безопасности РФ". Основные направления обеспечения информационной безопасности и защиты информации в РФ. /Лек/	1	2	ПК-2	Л1.3 Л1.4 Л1.2Л2.5 Л2.4
1.2	Тема 1."Правовое обеспечение информационной безопасности в системе национальной безопасности РФ". Работа с СПС "Консультант Плюс": Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования. /Пр/	1	2	ПК-2	Л1.4 Л1.2Л2.5 Л2.4
1.3	Тема 1."Правовое обеспечение информационной безопасности в системе национальной безопасности РФ". Работа с СПС Консультант+, ФСТЭК России/fstec.ru, ЭБС «IPR Books» http://www.iprbookshop.ru/, Библиоклуб.ру http://biblioclub.ru/ : Организация работы со сведениями, отнесенные к государственной тайне и конфиденциальной информации. /Ср/	1	4	ПК-2	Л1.3 Л1.4 Л1.2Л2.5 Л2.4
	Раздел 2. Техническая защита информации				
2.1	Тема 1. «Угрозы утечки информации по техническим каналам». Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок, Угрозы утечки акустической (речевой) информации. Угрозы утечки видовой информации. /Лек/	1	2	ПК-2	Л1.3 Л1.4 Л1.2Л2.5 Л2.4
2.2	Тема 1. «Угрозы утечки информации по техническим каналам». Работа с СПС Консультант+, ФСТЭК России/fstec.ru, ЭБС «IPR Books» http://www.iprbookshop.ru/, Библиоклуб.ру http://biblioclub.ru/ : Формы защищаемой информации. Объекты защиты. Физические основы возникновения ТКУИ. Классификация ТСР. /Пр/	1	4	ПК-2	Л1.3 Л1.4 Л1.2Л2.5 Л2.4

2.3	Тема 1. «Угрозы утечки информации по техническим каналам». Работа с СПС Консультант+, ФСТЭК России/fstec.ru, ЭБС «IPR Books» http://www.iprbookshop.ru/, Библиоклуб.ру http://biblioclub.ru/ : Оценка возможностей технических средств разведки. /Ср/	1	10	ПК-2	Л1.3 Л1.4 Л1.2Л2.5 Л2.4
2.4	Тема 2. «Способы и средства технической защиты информации». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Средства защиты объектов от утечки информации за счет ПЭМИ и наводок. /Ср/	1	4	ПК-2	Л1.3 Л1.4 Л1.2Л2.5 Л2.4
2.5	Тема 2. «Способы и средства технической защиты информации». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Предотвращение утечки информации по цепям электропитания и заземления. Средства звукоизоляции и звукопоглощения акустического сигнала, оценка их эффективности. Средства поиска средств негласного съема информации. /Ср/	1	4	ПК-2	Л1.3 Л1.4 Л1.2Л2.5 Л2.4
	Раздел 3. Организация защиты информации в информационной системе				
3.1	Тема 1. «Угрозы несанкционированного доступа к информации в информационной системе». Выявление источников и угроз несанкционированного доступа в информационной системе. Определение типов нарушителей. Выявление носителей вредоносных программ. /Лек/	1	2	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.3 Л2.5 Л2.4 Л2.2
3.2	Тема 1. «Угрозы несанкционированного доступа к информации в информационной системе». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Угрозы непосредственного доступа в операционную среду информационной системы. /Ср/	1	8	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.3 Л2.5 Л2.4 Л2.2
3.3	Тема 1. «Угрозы несанкционированного доступа к информации в информационной системе». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Работа с СПС Консультант+, ФСТЭК России/fstec.ru Угрозы безопасности информации, реализуемых с использованием протоколов межсетевого взаимодействия. /Ср/	1	4	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.3 Л2.5 Л2.4 Л2.2 Л2.1
3.4	Тема 1. «Угрозы несанкционированного доступа к информации в информационной системе». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Угрозы программно-математических воздействий. /Ср/	1	8	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.3 Л2.5 Л2.4 Л2.2 Л2.1
3.5	Тема 1. «Угрозы несанкционированного доступа к информации в информационной системе». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах. /Пр/	1	4	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.3 Л2.5 Л2.4 Л2.2 Л2.1
3.6	Тема 2. «Требования к организации защиты информации в информационной системе». Работа с СПС ФСТЭК России/fstec.ru: Разработка требований к мерам защиты информации, содержащейся в информационной системе. /Ср/	1	4	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.3 Л2.5 Л2.4 Л2.2 Л2.1
3.7	Тема 2. «Требования к организации защиты информации в информационной системе». Работа с СПС ФСТЭК России/fstec.ru: Обеспечение защиты информации в ходе эксплуатации информационной системы. Тема 2. «Требования к организации защиты информации в информационной системе». Обеспечение защиты информации в ходе эксплуатации информационной системы. /Ср/	1	4	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.3 Л2.5 Л2.4 Л2.2 Л2.1
	Раздел 4. Методы и средства криптографический защиты				
4.1	Тема 1. «Симметричные криптосистемы». Принцип функционирования симметричных криптосистем. Функциональная схема взаимодействия участников симметричного криптографического обмена. /Лек/	1	2	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4 Л2.2
4.2	Тема 1. «Симметричные криптосистемы». Система шифрования Цезаря. Шифры перестановки. Оформление работы в MS Word. /Пр/	1	2	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4 Л2.2

4.3	Тема 1. «Симметричные криптосистемы». Шифр Гронсфельда. Шифры многоалфавитной замены. /Ср/	1	2	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4 Л2.2
4.4	Тема 2.«Асимметричные криптосистемы». Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана. Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA. /Пр/	1	2	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4 Л2.2
4.5	Тема 2.«Асимметричные криптосистемы». Основные математические соотношения, используемые в алгоритме RSA. Технология взлома шифра методом полного перебора. /Ср/	1	2	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4 Л2.2
4.6	Тема 2.«Асимметричные криптосистемы». Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Целостность передаваемых данных. Авторство сообщений. Оформление работы в MS Word. /Ср/	1	2	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4 Л2.2
	Раздел 5. Лицензирование и сертификация в области защиты информации				
5.1	Тема 1. «Правовые основы лицензирования в области защиты информации». Структура системы государственного лицензирования. Порядок проведения лицензирования. /Лек/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4
5.2	Тема 1. «Правовые основы лицензирования в области защиты информации». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Организация лицензирования в области защиты информации. Основные лицензионные требования и условия в области защиты информации. /Ср/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.5 Л2.4
5.3	Тема 2. «Правовые основы сертификации в РФ». Работа с СПС Консультант+, ФСТЭК России/fstec.ru:Порядок проведения сертификации средств защиты информации. /Ср/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
	Раздел 6. Основы защиты коммерческой тайны и конфиденциальной информации				
6.1	Тема 1. «Правовые основы защиты коммерческой тайны». Сущность и содержание коммерческой тайны. Правовое обеспечение защиты коммерческой тайны. Сведения, составляющие коммерческую тайну. /Лек/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
6.2	Тема 1. «Правовые основы защиты коммерческой тайны». Порядок отнесения информации к коммерческой тайне. /Пр/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
6.3	Тема 1. «Правовые основы защиты коммерческой тайны». Права обладателя коммерческой тайны. /Ср/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
6.4	Тема 2. «Правовые основы защиты конфиденциальной информации». Права и обязанности работника и работодателя по защите конфиденциальной информации. /Ср/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
	Раздел 7. Правовые основы защиты персональных данных				
7.1	Тема 1. «Сущность и содержание обработки и защиты персональных данных». Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные. /Лек/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
7.2	Тема 1. «Сущность и содержание обработки и защиты персональных данных». Организация защиты персональных данных в организации. Положение об обработке и защите персональных данных в организации. /Ср/	1	4	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
	Раздел 8. Организация контроля за состоянием защиты конфиденциальной информации на предприятии				

8.1	Тема 1. «Деятельность руководства и должностных лиц по проверке состояния защиты конфиденциальной информации». Основные объекты и формы контроля за состоянием защиты информации. Основные задачи и методы контроля. /Лек/	1	2	ПК-2	Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.5 Л2.4
8.2	Тема 1. «Деятельность руководства и должностных лиц по проверке состояния защиты конфиденциальной информации». Организация аудита информационной безопасности. /Ср/	1	8	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.3 Л2.5 Л2.4 Л2.1
8.3	/Зачёт/	1	0	ПК-2	Л1.5 Л1.3 Л1.4 Л1.1 Л1.2Л2.6 Л2.3 Л2.5 Л2.4 Л2.2 Л2.1

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
Л1.1	Шилов, А. К.	Управление информационной безопасностью: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018	http://www.iprbookshop.ru/87643.html неограниченный доступ для зарегистрированных пользователей
Л1.2	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.4	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	http://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей
Л1.5	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.2	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей
Л2.3		Основы информационной безопасности при работе на компьютере	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/52160.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	http://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Рогозин, В. Ю., Галушкин, И. Б., Новиков, В. К., Вепрев, С. Б.	Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»	Москва: ЮНИТИ-ДАНА, 2017	http://www.iprbookshop.ru/72444.html неограниченный доступ для зарегистрированных пользователей
Л2.6		Вестник Института законодательства и правовой информации имени М.М. Сперанского: журнал	Иркутск: Институт законодательства и правовой информации, 2017	https://biblioclub.ru/index.php?page=book&id=457912 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант+

ЭБС «IPR Books» http://www.iprbookshop.ru/

Библиоклуб.ру http://biblioclub.ru/

Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)//fstec.ru

5.4. Перечень программного обеспечения

Microsoft Word

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)

Помещение 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 проводится 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
ПК-2: способен решать задачи профессиональной деятельности с использованием информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
З: способы решения стандартных задач профессиональной деятельности в области информационной безопасности на основе организации процесса сбора, анализа и систематизации информации по формированию системы защиты информации с применением информационно-коммуникационных технологий	знание способов решения стандартных задач профессиональной деятельности в области информационной безопасности при формировании системы защиты информации	полнота и соответствие предлагаемых способов решения стандартных задач профессиональной деятельности в области информационной безопасности требованиям нормативно-правовым актов	О (вопросы 1-57) З (вопросы 1-58)
У: решать стандартные задачи профессиональной деятельности с учетом требований информационной безопасности на основе анализа требований нормативно-правовых актов в области информационной безопасности	качество проведенного анализа состояния системы защиты информации, выявление ее уязвимых мест и определение направления ее совершенствования	соответствие результатов анализа текущему состоянию системы защиты информации	ПЗ (раздел 1, тема 1, практическое задание 1, раздел 2, тема 1, практическое задание 1, раздел 3, тема 1, практическое задание 1, раздел 4, тема 1, практическое задание 1, тема 2, практическое задание 1, раздел 6, тема 1, практическое задание 1, тема 2, практическое задание 1) З (вопросы 59-78)
В: методологией по разработке комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты на основе анализа нормативно-правовых актов в области информационной безопасности при решении задач профессиональной деятельности;	использование методов и средств защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России	соответствие технологического процесса защиты информации требованиям нормативно-методических документов ФСБ России и ФСТЭК России	ПЗ (раздел 1, тема 1, практическое задание 1, раздел 2, тема 1, практическое задание 1, раздел 3, тема 1, практическое задание 1, раздел 4, тема 1, практическое задание 1, тема 2, практическое задание 1, раздел 6, тема 1, практическое задание 1, тема 2, практическое задание 1) З (вопросы 59-78)

О – опрос; ПЗ – практическое задание; З – вопросы к зачету

1.2 Шкалы оценивания:

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

50-100 баллов (оценка «зачет»)

0-49 баллов (оценка «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

В разделе приводятся типовые варианты оценочных средств: вопросы к зачету, практические задания.

Вопросы к зачету

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведения конфиденциального характера.
8. Организация работы со сведениями, отнесенные к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Угрозы утечки информации по техническим каналам.

11. Формы защищаемой информации.
12. Основные объекты защиты информации.
13. Классификация технических каналов утечки информации.
14. Технические мероприятия по защите информации от утечки по техническим каналам.
15. Организационные мероприятия по защите информации от утечки по техническим каналам.
16. Классификации угроз безопасности информации в информационных системах.
17. Требования к организации защиты информации в информационной системе.
18. Формирование требований к защите информации в информационной системе.
19. Обеспечение защиты информации в ходе эксплуатации информационной системы.
20. Требования к мерам защиты информации, содержащейся в информационной системе.
21. Определение класса защищенности информационной системы.
22. Лицензирование в области защиты информации.
23. Структура системы государственного лицензирования.
24. Порядок проведения лицензирования.
25. Основные лицензионные требования и условия в области защиты информации.
26. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
27. Структура системы сертификации.
28. Порядок проведения сертификации средств защиты информации.
29. Сертификационные испытания средств защиты информации.
30. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
31. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
32. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
33. Права обладателя коммерческой тайны.
34. Организация защиты информации на предприятии.
35. Обеспечение сохранности документов, дел и изданий.
36. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
37. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
38. Обязанности персонала организации по сохранению коммерческой тайны.
39. Политика безопасности предприятия как основа организационного управления защитой информации.
40. Права и обязанности работника и работодателя по защите конфиденциальной информации.
41. Ответственность за нарушение конфиденциальности информации.
42. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
43. Организация защиты персональных данных в организации.
44. Планирование мероприятий по организационной защите информации на предприятии.
45. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
46. Организация аналитической работы в области защиты информации на предприятии.
47. Основные объекты и формы контроля за состоянием защиты информации.
48. Основные задачи и методы контроля.
49. Основные направления аналитической работы.
50. Организация аудита информационной безопасности предприятия.
51. Функции аналитического подразделения в области защиты информации на предприятии.
52. Основные этапы аналитической работы в области защиты информации на предприятии.

53. Содержание и основные виды аналитических отчетов.
54. Классификация методов анализа информации.
55. Компьютерные преступления в электронной коммерции.
56. Информационная безопасность в электронной коммерции.
57. Юридическая ответственность за нарушение правовых норм защиты информации.
58. Обосновать основные направления обеспечения информационной безопасности и защиты информации в РФ.
59. Выявление угроз утечки информации по каналам побочных электромагнитных излучений и наводок.
60. Выявление угроз утечки акустической (речевой) информации.
61. Выявление угроз утечки видовой информации.
62. Сформулировать технические и организационные мероприятия по защите информации от утечки по техническим каналам.
63. Выявление источников и угроз несанкционированного доступа в информационной системе.
64. Определение типов нарушителей.
65. Выявление носителей вредоносных программ.
66. Выявление уязвимостей информационной системы, системного программного обеспечения, прикладного программного обеспечения.
67. Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах.
68. Определение класса защищенности информационной системы.
69. Сформировать требования к защите информации в информационной системе.
70. Разработка требований к мерам защиты информации, содержащейся в информационной системе.
71. Организация лицензирования в области защиты информации.
72. Организация сертификации в области защиты информации.
73. Правовое обеспечение защиты коммерческой тайны на предприятии.
74. Разработка политики безопасности предприятия.
75. Определение прав и обязанностей оператора, обрабатывающего персональные данные.
76. Определение уровня защищенности ИСПДн.
77. Определить основные объекты и формы контроля за состоянием защиты информации.
78. Сформулировать основные задачи и методы контроля.

Критерии оценивания:

- 100-50 (50-20 за ответ на 2 теоретических вопроса, 50-30 за решение 2-х практико-ориентированных задания) баллов («зачет») – 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-ориентированных заданий, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 0-49 (0-19 за ответ на 2 теоретических вопроса, 0-30 за решение 2-х практико-ориентированных заданий) баллов («незачет») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированных заданий, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Перечень теоретических типовых вопросов для опроса

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведения конфиденциального характера.
8. Организация работы со сведениями, отнесенные к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Угрозы утечки информации по техническим каналам.
11. Формы защищаемой информации.
12. Основные объекты защиты информации.
13. Классификация технических каналов утечки информации.
14. Технические мероприятия по защите информации от утечки по техническим каналам.
15. Организационные мероприятия по защите информации от утечки по техническим каналам.
16. Классификации угроз безопасности информации в информационных системах.
17. Требования к организации защиты информации в информационной системе.
18. Формирование требований к защите информации в информационной системе.
19. Обеспечение защиты информации в ходе эксплуатации информационной системы.
20. Требования к мерам защиты информации, содержащейся в информационной системе.
21. Определение класса защищенности информационной системы.
22. Лицензирование в области защиты информации.
23. Структура системы государственного лицензирования.
24. Порядок проведения лицензирования.
25. Основные лицензионные требования и условия в области защиты информации.
26. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
27. Структура системы сертификации.
28. Порядок проведения сертификации средств защиты информации.
29. Сертификационные испытания средств защиты информации.
30. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
31. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
32. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
33. Права обладателя коммерческой тайны.
34. Организация защиты информации на предприятии.
35. Обеспечение сохранности документов, дел и изданий.
36. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
37. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
38. Обязанности персонала организации по сохранению коммерческой тайны.
39. Политика безопасности предприятия как основа организационного управления защитой информации.
40. Права и обязанности работника и работодателя по защите конфиденциальной информации.
41. Ответственность за нарушение конфиденциальности информации.

42. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
43. Организация защиты персональных данных в организации.
44. Планирование мероприятий по организационной защите информации на предприятии.
45. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
46. Организация аналитической работы в области защиты информации на предприятии.
47. Основные объекты и формы контроля за состоянием защиты информации.
48. Основные задачи и методы контроля.
49. Основные направления аналитической работы.
50. Организация аудита информационной безопасности предприятия.
51. Функции аналитического подразделения в области защиты информации на предприятии.
52. Основные этапы аналитической работы в области защиты информации на предприятии.
53. Содержание и основные виды аналитических отчетов.
54. Классификация методов анализа информации.
55. Компьютерные преступления в электронной коммерции.
56. Информационная безопасность в электронной коммерции.
57. Юридическая ответственность за нарушение правовых норм защиты информации.

Критерии оценивания:

правильный ответ на 1 вопрос – 1 балл;
неправильный ответ на 1 вопрос – 0 баллов.
Количество баллов за семестр – 20 баллов.

Лабораторные задания

1.Тематика лабораторных заданий по разделам и темам

Раздел 1. Правовое и организационное обеспечение информационной безопасности.

Тема 1."Правовое обеспечение информационной безопасности в системе национальной безопасности РФ".

Лабораторная работа 1. Работа с СПС "Консультант Плюс": Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования.

Раздел 2. Техническая защита информации

Тема 1. «Угрозы утечки информации по техническим каналам».

Лабораторная работа 1.Работа с СПС Консультант+, ФСТЭК России/fstec.ru, ЭБС «IPR Books» http://www.iprbookshop.ru/, Библиоклуб.ру http://biblioclub.ru/ : Формы защищаемой информации. Объекты защиты. Физические основы возникновения ТКУИ. Классификация ТСР.

Раздел 3. Организация защиты информации в информационной системе.

Тема 1. «Угрозы несанкционированного доступа к информации в информационной системе».

Лабораторная работа 1. Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах.

Раздел 4. Методы и средства криптографический защиты

Тема 1. «Симметричные криптосистемы».

Лабораторная работа 1. Система шифрования Цезаря. Шифры перестановки. Оформление работы в MS Word.

Тема 2.«Асимметричные криптосистемы».

Лабораторная работа 1. Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана. Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.

Раздел 6. Основы защиты коммерческой тайны и конфиденциальной информации

Тема 1. «Правовые основы защиты коммерческой тайны».

Лабораторная работа 1. Порядок отнесения информации к коммерческой тайне.

Тема 2. «Правовые основы защиты конфиденциальной информации».

Лабораторная работа 1. Разработка политики безопасности предприятия.

Критерии оценивания:

Правильное решение практического задания: раздел 1 – 10 баллов; раздел 2 – 10 баллов; раздел 3 – 15 баллов; раздел 4 – 20 баллов; раздел 6 – 25 баллов.

Неправильное решение практического задания – 0 баллов.

Количество баллов за семестр – 80 баллов.

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

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

Промежуточная аттестация проводится в форме зачета.

Экзамен проводится по окончанию теоретического обучения в соответствии с расписанием. Количество вопросов в задании – 3 (2 теоретических вопроса, 1 - практический). Объявление результатов производится в день зачета. Результаты аттестации заносятся в электронную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы по изучаемой теме.

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практическим занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом устного опроса. 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 источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

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.