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
Основы информационной безопасности

Направление 38.03.02 "Менеджмент"
Направленность 38.03.02.11 "Финансовый менеджмент"

Для набора 2022 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	2	2	2	2
Лабораторные	4	4	4	4
Итого ауд.	6	6	6	6
Контактная работа	6	6	6	6
Сам. работа	98	98	98	98
Часы на контроль	4	4	4	4
Итого	108	108	108	108

ОСНОВАНИЕ

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

Программу составил(и): к.т.н., доцент, Севастьянов И.Т.

Зав. кафедрой: к.э.н.,доц. Ефимова Е.В.

Методический совет направления: д.э.н., профессор Суржиков М.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

ОПК-5: Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ.

ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

В результате освоения дисциплины обучающийся должен:

Знать:

- современные информационные технологии и программные средства при решении задач обеспечения информационной безопасности
- принципы работы современных технологий обеспечения информационной безопасности при решении задач профессиональной деятельности.

Уметь:

- использовать современные информационные технологии обеспечения информационной безопасности;
- решать стандартные задачи профессиональной деятельности с учетом требований информационной безопасности.

Владеть:

- реализации требований к формирования необходимых информационных технологий по обеспечению информационной безопасности;
- использования способов и средств защиты информации при решении задач профессиональной деятельности.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Правовое и организационное обеспечение информационной безопасности. Техническая защита информации.

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Тема 1. «Правовые и организационные меры обеспечения информационной безопасности. Угрозы утечки информации по техническим каналам». Основные направления обеспечения информационной безопасности и защиты информации в РФ. Основные объекты защиты информации. Правовое обеспечение защиты коммерческой тайны и персональных данных. Технические каналы утечки информации. / Лек /	6	2	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.2	Тема 1. «Правовое обеспечение информационной безопасности. Угрозы утечки информации по техническим каналам». Работа с СПС Консультант+, ФСТЭК России /fstec.ru, Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Физические основы возникновения ТКУИ. Классификация ТСР с использованием LibreOffice. / Лаб /	6	2	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.3	Тема 1. «Правовые и организационные меры обеспечения информационной безопасности. Угрозы утечки информации по техническим каналам».Консультант+, ФСТЭК России/fstec.ru, Организация работы со сведениями, отнесенными к государственной тайне и конфиденциальной информации. / Ср /	6	13	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.4	Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Средства защиты объектов от утечки информации за счет ПЭМИ и наводок. / Ср /	6	14	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
1.5	Тема 1. «Правовые и организационные меры обеспечения информационной безопасности. Угрозы утечки информации по техническим каналам».Консультант+, ФСТЭК России/fstec.ru: Предотвращение утечки информации по цепям электропитания и заземления. Средства звукоизоляции и звукопоглощения акустического сигнала, оценка их эффективности. Средства	6	14	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4

	поиска средств негласного съема информации. / Ср /				
Раздел 2. Правовые основы защиты конфиденциальной информации					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
2.1	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных». Сущность и содержание коммерческой тайны. Сущность и содержание обработки и защиты персональных данных. Организационные мероприятия по обеспечению защиты информации. / Ср /	6	2	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.2	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных». Формирование перечня сведений, составляющих коммерческую тайну. / Лаб /	6	2	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.3	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных». Права обладателя коммерческой тайны. / Ср /	6	13	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.4	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных».Права и обязанности работника и работодателя по защите конфиденциальной информации. / Ср /	6	14	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.5	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных». Организация защиты персональных данных в организации. Положение об обработке и защите персональных данных в организации. / Ср /	6	14	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.6	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных».Организация аудита информационной безопасности. / Ср /	6	14	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4
2.7	/ Зачёт /	6	4	ОПК-5, ОПК-6	Л1.1, Л1.2, Л1.3, 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	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
Л1.2	Сафонова, Л. А.	Экономические аспекты информационной безопасности: учебное пособие	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2019	https://www.iprbookshop.ru/90606.html неограниченный доступ для зарегистрированных пользователей
Л1.3	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

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1		Вестник Института законодательства и правовой информации им. М.М. Сперанского	, 2009	https://www.iprbookshop.ru/6394.html неограниченный доступ для зарегистрированных пользователей
Л2.2	Шилов, А. К.	Управление информационной безопасностью: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018	https://www.iprbookshop.ru/87643.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л2.4		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант+ https://www.cosultant.ru/
Бесплатная база данных ГОСТ. https://docplan.ru/
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)//fstec.ru

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.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-5: способен использовать современные информационные технологии и программные средства при решении профессиональных задач			
З: современные информационные технологии и программные средства при решении задач обеспечения информационной безопасности	изучает способы решения стандартных задач профессиональной деятельности в области информационной безопасности при формировании системы защиты информации для подготовки к зачету, опросу	полнота и соответствие предлагаемых способов решения стандартных задач профессиональной деятельности в области информационной безопасности требованиям нормативно-правовым актов при ответе на опросе, зачете	О (вопросы 1-34) З (вопросы 1-45)
У: использовать современные информационные технологии обеспечения информационной безопасности	анализирует состояние системы защиты информации, выявление ее уязвимых мест и определение направления ее совершенствования при выполнении практико-ориентированного и лабораторного задания	соответствие результатов анализа текущему состоянию системы защиты информации при выполнении практико-ориентированного и лабораторного задания	ПОЗЗ (1-6) ЛЗ (1,2)
В: методологией разработки комплекса организационно-технических мер по обеспечению информационной безопасности объекта	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	ПОЗЗ (1-6) ЛЗ (1,2)
ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности			

З: принципы работы современных технологий обеспечения информационной безопасности при решении задач профессиональной деятельности	изучает современные технологии защиты информации при решении стандартных задач профессиональной деятельности для подготовки к зачету, опросу	полнота и соответствие предлагаемых технологий защиты информации при решении стандартных задач профессиональной деятельности требованиям нормативно-правовым актов при ответе на опросе, зачете	О (вопросы 1-34) З (вопросы 1-45)
У: решать стандартные задачи профессиональной деятельности с учетом требований информационной безопасности	анализирует возможности системы защиты информации, выявляет существующие угрозы и определяет требуемый уровень защищённости при выполнении практико-ориентированного и лабораторного задания	соответствие результатов анализа текущему состоянию системы защиты информации при выполнении практико-ориентированного и лабораторного задания	ПОЗЗ (1-6) ЛЗ (1,2)
В: навыками использования способов и средств защиты информации при решении задач профессиональной деятельности	использование способов и средств защиты информации в соответствии с правовыми нормативными актами и методическими документами ФСБ России и ФСТЭК России	соответствие используемых способов и средств защиты информации требованиям нормативно-правовых актов и методических документов ФСБ России и ФСТЭК России	ПОЗЗ (1-6) ЛЗ (1,2)

О – опрос; ПОЗЗ- практико-ориентированные задания к зачету, ЛЗ – лабораторное 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

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 сведений конфиденциального характера.
8. Организация работы со сведениями, отнесенными 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. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
17. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
18. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
19. Права обладателя коммерческой тайны.
20. Организация защиты информации на предприятии.
21. Обеспечение сохранности документов, дел и изданий.
22. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
23. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
24. Обязанности персонала организации по сохранению коммерческой тайны.
25. Политика безопасности предприятия как основа организационного управления защитой информации.
26. Права и обязанности работника и работодателя по защите конфиденциальной информации.
27. Ответственность за нарушение конфиденциальности информации.
28. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
29. Организация защиты персональных данных в организации.
30. Планирование мероприятий по организационной защите информации на предприятии.
31. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
32. Основные объекты и формы контроля за состоянием защиты информации.
33. Основные задачи и методы контроля.
34. Юридическая ответственность за нарушение правовых норм защиты информации.
35. Обосновать основные направления обеспечения информационной безопасности и защиты информации в РФ.
36. Выявление угроз утечки информации по каналам побочных электромагнитных излучений и наводок.
37. Выявление угроз утечки акустической (речевой) информации.
38. Выявление угроз утечки видовой информации.
39. Сформулировать технические и организационные мероприятия по защите информации от утечки по техническим каналам.
40. Правовое обеспечение защиты коммерческой тайны на предприятии.

41. Разработка политики безопасности предприятия.
42. Определение прав и обязанностей оператора, обрабатывающего персональные данные.
43. Определение уровня защищенности ИСПДн.
44. Определить основные объекты и формы контроля за состоянием защиты информации.
45. Сформулировать основные задачи и методы контроля.

Практико-ориентированные задания к зачету

1. Разработка концепции, программы и плана исследования.
2. Выбор метода исследования на различных этапах работы.
3. Получение первичной информации об объекте исследования с использованием инструментальных методов.
4. Обработка первичной информации об объекте исследования.
5. Разработка комплекта типовых эксплуатационных документов системы электронного документооборота
6. Проведение аудита защищенности системы электронного документооборота по требованиям контролирующих органов

Критерии оценивания:

- 50-100 (20-40 за ответ на 2 теоретических вопроса, 30-60 за решение практико-ориентированного задания) баллов («зачет»): – 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;

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

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 сведений конфиденциального характера.
8. Организация работы со сведениями, отнесенными 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. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
17. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
18. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
19. Права обладателя коммерческой тайны.
20. Организация защиты информации на предприятии.
21. Обеспечение сохранности документов, дел и изданий.
22. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
23. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
24. Обязанности персонала организации по сохранению коммерческой тайны.
25. Политика безопасности предприятия как основа организационного управления защитой информации.
26. Права и обязанности работника и работодателя по защите конфиденциальной информации.
27. Ответственность за нарушение конфиденциальности информации.
28. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
29. Организация защиты персональных данных в организации.
30. Планирование мероприятий по организационной защите информации на предприятии.
31. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
32. Основные объекты и формы контроля за состоянием защиты информации.
33. Основные задачи и методы контроля.
34. Юридическая ответственность за нарушение правовых норм защиты информации.

Критерии оценивания*:*
правильный и полный ответ на 1 вопрос – 1 балл;
неправильный ответ на 1 вопрос – 0 баллов.
Количество баллов за семестр – 20 баллов.

Лабораторные задания

Лабораторное задание 1.

Работа с СПС Консультант+, ФСТЭК России /fstec.ru, Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Физические основы возникновения ТКУИ. Классификация ТСР с использованием LibreOffice.

Лабораторное задание 2

Формирование перечня сведений, составляющих коммерческую тайну.

Критерии оценивания:

- (для каждого задания):

10 б. – задание выполнено верно;

9-7 б. – при выполнении задания были допущены неточности, не влияющие на результат;

6-3 б. – при выполнении задания были допущены ошибки;

2 - 1 б. – при выполнении задания были допущены существенные ошибки;

0 б. – задание не выполнено.

Максимальное количество баллов, которые могут быть получены обучающимся - 80.

Тесты для проверки знаний

1. Контролируемая зона:

1. зона, в которой исключено появление посторонних лиц и транспортных средств
2. зона, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков.
3. зона, в которой исключено появление лиц и транспортных средств, не имеющих допуска к защищаемой информации

2. Что входит в технический канал утечки информации? (выберите все правильные *ответы*):

1. Физическая среда распространения информационного сигнала
2. Объект разведки
3. Субъект разведки
4. Техническое средство разведки

3. К ОТСС относятся (*выберите все правильные ответы*):

1.средства изготовления и размножения документов
2.системы охранной сигнализации
3.системы пожарной сигнализации
4.средства и системы открытой телефонной связи;
5.аппаратура звукоусиления в выделенных помещениях

4. К ОТСС относятся технические средства, обрабатывающие:

1.экономическую информацию
2.техническую информацию
3.информацию ограниченного доступа
4.информацию о поставщиках

5. В каком законе определен правовой режим информатизации, правила, процедуры и распределение ответственности в области защиты информации в системах ее обработки, установлен порядок правовой защиты и гарантии реализации прав и ответственности субъектов информационных взаимоотношений:

1. Федеральный закон от 28.12.2010 № 390-ФЗ "О безопасности".
2. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
3. Федеральный закон от 27.12.2002 № 184-ФЗ "О техническом регулировании".
4. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".

6. Свойства информации как объекта защиты (*выберите все правильные ответы*):

1. Конфиденциальность
2. Доступность
3. Модификация.
4. Достоверность
5. Уничтожение.
6. Целостность

7. Перечень сведений конфиденциального характера по видам тайны (*выберите все правильные ответы*):

1. служебные сведения
2. сведения об организационной структуре организации
3. сведения, связанные с коммерческой деятельности
4. сведения, распространение которых нанесут ущерб интересам министерства (ведомства) или отрасли экономики РФ.

8. Что предписано сделать с персональными данными после достижения целей, с которыми они обрабатывались?

1. хранить в течение установленного срока

2. передать в уполномоченный орган по защите прав субъектов персональных данных
3. уничтожить
4. опубликовать
5. блокировать

9. Для ИСПДн актуальны угрозы, связанные с наличием недекларированных возможностей в прикладном программном обеспечении. Это угрозы:

1. 1-го типа
2. 2-го типа
3. 3-го типа

10. При обработке персональных данных, касающиеся политических взглядов, она относится к ИСПДн, обрабатывающей:

1. биометрические персональные данные
2. общедоступные персональные данные
3. специальные категории персональных данных
4. иные категории персональных данных

11. Контроль за выполнением требований к защите персональных данных в ИСПДн проводится:

1. не реже 1 раза в течение года
2. не реже 1 раза в 2 года
3. не реже 1 раза в 3 года

12 В каком документе приведен перечень мер, направленных на обеспечение выполнения обязанностей операторами, являющимися государственными или муниципальными органами, по защите персональных данных:

1. Федеральный закон от 27.07.2006 № 152-ФЗ.
2. Постановление Правительства РФ от 01.11.2012 №1119.
3. Постановление Правительства РФ от 21.03.2012 №211.
4. Постановление Правительства РФ от 15.09.2008 №687.
5. Приказ ФСТЭК от 18.02.2013 №21.

13. В каком документе приведен состав и содержание организационных и технических мер, направленных на обеспечение безопасности персональных данных при их обработке в ИСПДн:

1. Федеральный закон от 27.07.2006 № 152-ФЗ.
2. Постановление Правительства РФ от 01.11.2012 №1119.
3. Постановление Правительства РФ от 21.03.2012 №211.
4. Постановление Правительства РФ от 15.09.2008 №687.
5. Приказ ФСТЭК от 18.02.2013 №21.

14. К конфиденциальным документам можно отнести:

1.Учредительные документы, уставы
2. Документы, содержащие персональные данные
3.Документы, составляющие служебную тайну

15. Виды электронных подписей:

1.простая
2.усиленная неквалифицированная
3.квалифицированная
4.все варианты верны

16. Срок действия электронной подписи:

1.1 год
2. 5 лет
3. 10 лет
4. бессрочный

17. Каким документом регулируются отношения в области использования электронных подписей:

1. Федеральный закон от 6.04.2011 №63-ФЗ
2. Федеральный закон от 27.07.2010 №210-ФЗ
3. Федеральный закон от 10.01.2002 №1-ФЗ
4. все варианты верны

18. Какая ограничительная пометка ставится на документе, содержащем служебную тайну?

1.Конфиденциально
2.Для служебного пользования

19. Где можно обсуждать служебную информацию?

1.В кабинете руководителя
2.В режимном помещении
3.В защищаемом помещении
4.В любом помещении при отсутствии посторонних лиц

20. В каком документе определены требования к мерам защиты информации, не составляющей государственную тайну, содержащейся в информационной системе?

1.СТР-К
2.Федеральный закон от 06.04.2011 N 63-ФЗ
3.Федеральный закон от 27.07.2006 N 152-ФЗ
4.Приказ ФСТЭК №17

21 Для информационной системы регионального масштаба с УЗ 1 устанавливается класс защищенности:

1.К1
2.К2
3.К3

22. Технические каналы утечки информации ограниченного доступа, обрабатываемой в информационной системе (*выберите все правильные ответы*):

1.электрический
2.электромагнитный
3.индукционный
4.виброакустический

23. Источники ПЭМИН (*выберите все правильные ответы*):

1. Вычислительная техника
2. Вибрация оконных стёкол
3. Средства изготовления и размножения документов.
4. Проводка электропитания

24. Технические каналы утечки акустической речевой информации (*выберите все правильные ответы*):

1.оптико-электронный
2.электромагнитный
3.индукционный
4.виброакустический
5.электрический

25. Зона 2 – пространство вокруг ОТСС:

1.на границе и за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.

2.за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.

3. в пределах которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.

26. Зона 1 – пространство вокруг ОТСС:

1. на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, не превышает нормированного значения.

2. за пределами которого уровень наведенного от ОТСС информативного сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения.

3.на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения.

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.

Зачет проводится по окончании теоретического обучения до начала экзаменационной сессии. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Проверка ответов и объявление результатов производится в день зачета. 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

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные 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 подготовки к лабораторным занятиям.

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

При подготовке к лабораторным 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 лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется методом 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.