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.
«____» _____ 20___г.

Рабочая программа дисциплины
Информационная безопасность

основная профессиональная образовательная программа по направлению 02.03.02 Фундаментальная информатика и информационные технологии
02.03.02.01 "Теоретические основы информатики и компьютерные науки"

Для набора 2021 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	6	6	6	6
Практические	4	4	4	4
Итого ауд.	10	10	10	10
Контактная работа	10	10	10	10
Сам. работа	125	125	125	125
Часы на контроль	9	9	9	9
Итого	144	144	144	144

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 27.06.2023 г. протокол № 12.

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

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

Методическим советом направления: д.э.н., проф., Тищенко Е.Н. _____

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 инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

современные информационные технологии и программные средства при решении задач обеспечения информационной безопасности

Уметь:

использовать современные информационные технологии обеспечения информационной безопасности

Владеть:

навыками разработки комплекса организационно-технических мер по обеспечению информационной безопасности объекта

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. Техническая защита информации.				
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. Технические каналы утечки информации. /Лек/	7	2	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
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. Выполнение практических заданий с использованием LibreOffice. /Пр/	7	2	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
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/	7	13	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.4	Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Средства защиты объектов от утечки информации за счет ПЭМИ и наводок. /Ср/	7	14	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
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 поиска средств негласного съема информации. /Ср/	7	14	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

1.6	Тема 2. «Организация защиты информации в информационных системах». Источники и виды угроз информации в информационных системах. Структура государственной системы технической защиты информации. Организация защиты информации. Меры защиты информации в информационных системах. /Лек/	7	2	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.7	Тема 2. «Организация защиты информации в информационных системах».Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Угрозы непосредственного доступа в операционную среду информационной системы. /Ср/	7	5	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.8	Тема 2. «Организация защиты информации в информационных системах». 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/	7	5	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.9	Тема 2. «Организация защиты информации в информационных системах». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Угрозы программно-математических воздействий. /Ср/	7	5	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.10	Тема 2. «Организация защиты информации в информационных системах». Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах. /Ср/	7	5	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.11	Тема 2. «Организация защиты информации в информационных системах». Работа с СПС ФСТЭК России/fstec.ru: Разработка требований к мерам защиты информации, содержащейся в информационной системе. /Ср/	7	5	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.12	Тема 2. «Организация защиты информации в информационных системах». Работа с СПС ФСТЭК России/fstec.ru: Обеспечение защиты информации в ходе эксплуатации информационной системы. /Ср/	7	4	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
	Раздел 2. Правовые основы защиты конфиденциальной информации				
2.1	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных». Сущность и содержание коммерческой тайны. Правовое обеспечение защиты коммерческой тайны. Сущность и содержание обработки и защиты персональных данных. Организационные мероприятия по обеспечению защиты информации. /Лек/	7	2	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.2	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных». Формирование перечня сведений, составляющих коммерческую тайну. Выполнение практических заданий с использованием LibreOffice. /Пр/	7	2	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.3	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных». Права обладателя коммерческой тайны. /Ср/	7	13	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.4	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных».Права и обязанности работника и работодателя по защите конфиденциальной информации. /Ср/	7	14	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
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/	7	14	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

2.6	Тема 1. «Правовые основы защиты коммерческой тайны и персональных данных».Организация аудита информационной безопасности. /Ср/	7	14	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.7	/Экзамен/	7	9	ОПК-5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

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	Пакин А. И.	Информационная безопасность информационных систем управления предприятием: учебное пособие	Москва: Альтаир|МГАВТ, 2009	https://biblioclub.ru/index.php?page=book&id=429778 неограниченный доступ для зарегистрированных пользователей
Л1.2		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
Л1.3	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
Л1.4	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

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Теплов, Э. П., Гатчин, Ю. А., Ныркov, А. П., Коробейников, А. Г., Сухостат, В. В.	Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции	Санкт-Петербург: Университет ИТМО, 2016	http://www.iprbookshop.ru/66435.html неограниченный доступ для зарегистрированных пользователей
Л2.2		Вестник Института законодательства и правовой информации им. М.М. Сперанского	, 2009	https://www.iprbookshop.ru/6394.html неограниченный доступ для зарегистрированных пользователей
Л2.3	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

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.4	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л2.5		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

ИСС «КонсультантПлюс»

ИСС «Гарант» http://www.internet.garant.ru/

Бесплатная база данных ГОСТ - https://docplan.ru/

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

5.4. Перечень программного обеспечения

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 (МОДУЛЯ)

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование.

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
ОПК-5: Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности			
З: современные информационные технологии и программные средства при решении задач обеспечения информационной безопасности	знает определения и понятия информационной безопасности, способы ее обеспечения в профессиональной деятельности	полнота и содержательность ответа умение приводить примеры	Т – тест (1-26), Э – вопросы к экзамену (1-45)
У: использовать современные информационные технологии обеспечения информационной безопасности	анализирует состояние системы защиты информации, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практического задания	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ – практические задания (1,2)
В: навыками разработки комплекса организационно-технических мер по обеспечению информационной безопасности объекта	использует методы и средства защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ – практические задания (1,2)

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. 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.

Экзаменационное задание включает три вопроса – два теоретических вопроса и одно практико-ориентированное задание из числа приведенных ниже практических заданий.

Критерии оценивания:

- 84-100 баллов (оценка «отлично») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 баллов (оценка «удовлетворительно») – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (оценка «неудовлетворительно») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Тест

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.

Критерии оценивания:

Из имеющегося банка тестов формируется вариант, содержащий 10 вопросов для одного обучающегося.

17-20 б. – тест пройден на 85-100 %;

7-16 б. – тест пройден на 35-84 %;

0-6 б. – тест пройден на менее, чем 35 %.

Максимальное количество баллов за тест – 20.

Практические задания

Практическое 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.

Практическое задание 2.

Формирование перечня сведений, составляющих коммерческую тайну.

Выполнение заданий с использованием LibreOffice.

Критерии оценивания (для каждого задания):

32-40 б. – задание выполнено верно;

20-31 б. – при выполнении задания были допущены неточности, не влияющие на результат;

10-19 б. – при выполнении задания были допущены ошибки;

0-9 б. – при выполнении задания были допущены существенные ошибки.

Максимальное количество баллов за практические задания – 80 (2 задания по 40 баллов).

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

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

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в устном виде. Количество вопросов в экзаменационном задании – 3 (два теоретических вопроса и одно практико-ориентированное задание). 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.

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

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

При подготовке к практическим занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме.

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

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

Студент должен готовиться к предстоящему практическому 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.