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

УТВЕРЖДАЮ
Директор Института магистратуры
Иванова Е.А.
«01» июня 2023г.

Рабочая программа дисциплины
Организационно-правовые механизмы обеспечения информационной безопасности

Направление 09.04.04 Программная инженерия
магистерская программа 09.04.04.01 "Системное и прикладное программное обеспечение"

Для набора 2023 года

Квалификация
магистр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	15 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	8	8	8	8
Практические	16	16	16	16
Итого ауд.	24	24	24	24
Контактная работа	24	24	24	24
Сам. работа	48	48	48	48
Итого	72	72	72	72

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.03.2023 протокол № 9.

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

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

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	приобретение знаний по организационному обеспечению защиты информации, правовой защите государственной, коммерческой, служебной, профессиональной тайны, персональных данных, видам и условиям применения правовых норм дисциплинарной, гражданско-правовой, административной и уголовной ответственности в области защиты информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
УК-3:Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
ОПК-1:Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте;
ОПК-7:Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях;
ПК-2 :Способен осуществлять контроль взаимодействия программного обеспечения с вычислительной средой на основе современных научных подходов

В результате освоения дисциплины обучающийся должен:
Знать:
Знать методики формирования команд;методы эффективного руководства коллективами (соотнесено с индикатором УК- 3.1). Знать математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности (соотнесено с индикатором ОПК-1.1). Знает методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях (соотнесено с индикатором ОПК-7.1). Знать методологию научной деятельности, технико-экономическое обоснование вариантов архитектуры компонентов, технологии и средства разработки программного обеспечения (соотнесено с индикатором ПК-2.1).
Уметь:
Уметь разрабатывать командную стратегию;организовывать работу коллективов;управлять коллективом;разрабатывать мероприятия по личностному, образовательному и профессиональному росту (соотнесено с индикатором УК-3.2). Уметь решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных социально-экономических и профессиональных знаний (соотнесено с индикатором ОПК-1.2). Умеет применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях (соотнесено с индикатором ОПК- 7.2). Уметь организовывать профессиональную деятельность на основе современных научных подходов, проводить техническое исследование возможных вариантов архитектуры компонентов, проектировать архитектуру, оценивать и корректировать ее компоненты (соотнесено с индикатором ПК-2.2).
Владеть:
Владеть методами организации и управления коллективом, планированием его действий (соотнесено с индикатором (УК- 3.3). Иметь навыки теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте (соотнесено с индикатором ОПК-1.3). Имеет навыки методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях (соотнесено с индикатором ОПК-7.3). Владеть навыками научной деятельности, способами описания архитектуры программного средства, методами контроля согласованности требований архитектуры программного средства (соотнесено с индикатором ПК-2.3).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Основные положения правовой и организационной защиты информации.				

1.1	"Правовое обеспечение информационной безопасности в системе национальной безопасности РФ":основные положения Стратегии национальной безопасности РФ и Доктрины информационной безопасности РФ. /Лек/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.4Л2.1 Л2.3 Л2.4 Л2.5
1.2	Основные направления обеспечения информационной безопасности и защиты информации в РФ. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
1.3	Организация работы со с ведениями, отнесенных к государственной тайне и конфиденциальной информации. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.4Л2.2 Л2.3 Л2.4
1.4	"Политика безопасности предприятия": политика безопасности предприятия как основа организационного управления защитой информации. /Ср/	3	6	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.5	"Структура организационной защиты информации": основные элементы системы защиты информации и их характеристика. /Лек/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.4Л2.3 Л2.4
	Раздел 2. Правовой режим защиты информации ограниченного доступа.				
2.1	"Информация как объект правового регулирования":правовые основы использования конфиденциальной информации. /Лек/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.4Л2.3 Л2.4
2.2	"Источники конфиденциальной информации":организационные каналы утечки конфиденциальной информации. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.4Л2.3 Л2.4
2.3	"Юридическая ответственность за нарушения правового режима защиты информации ограниченного доступа":основные положения Кодекса об административных нарушениях и Уголовного кодекса об юридической ответственности за нарушение режима защиты информации ограниченного доступа. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.4Л2.1 Л2.3 Л2.4
	Раздел 3. Лицензирование и сертификация в области защиты информации				
3.1	"Лицензирование и сертификация в области защиты информации.":основные элементы и системы государственного лицензирования и сертификации. /Лек/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
3.2	Организация проведения аттестации объектов информатизации и оформления ее результатов. /Ср/	3	6	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
	Раздел 4. Допуск и доступ к конфиденциальной информации				
4.1	Задачи режима защиты информации. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3 Л2.4
4.2	"Правовое обеспечение защиты коммерческой тайны":сведения,составляющие коммерческую тайну;требования к обеспечению защиты коммерческой тайны. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.3 Л2.4
4.3	Подбор персонала на должности, связанные с работой с конфиденциальной информацией. /Ср/	3	4	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.3 Л2.4
4.4	Оформление документов при подборе и приеме на должности, связанные с доступом к конфиденциальной информации. /Ср/	3	4	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.3 Л2.4
4.5	"Рассекречивание конфиденциальных сведений, документов и продукции": основные требования при организации рассекречивания конфиденциальных сведений, документов и продукции. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.3 Л2.4

4.6	"Персонал организации как источник утечки конфиденциальной информации":характеристика основных путей разглашения конфиденциальной информации персоналом организации. /Ср/	3	6	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
4.7	Организация контроля за соблюдением персоналом требований защиты информации. /Ср/	3	6	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4
4.8	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. /Ср/	3	6	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.3 Л2.4
4.9	"Подбор персонала на должности, связанные с работой с конфиденциальной информацией": основные требования при подборе персонала, связанных с работой с конфиденциальной информацией. /Пр/	3	2	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3 Л2.4
4.10	Основные формы обучения и методы контроля знаний персонала по защите информации. /Ср/	3	4	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4
4.11	"Цели и задачи пропускного режима":характеристика целей и задач организации пропускного режима. /Ср/	3	6	УК-3 ОПК-1 ОПК-7 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3 Л2.4
4.12	/Зачёт/	3	0	УК-3 ОПК-1 ОПК-7 ПК-2	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	Кришталюк А. Н.	Правовые аспекты системы безопасности: курс лекций: курс лекций	Орел: Межрегиональная академия безопасности и выживания, 2014	https://biblioclub.ru/index.php?page=book&id=428612 неограниченный доступ для зарегистрированных пользователей
Л1.2	Аверченков В. И.	Аудит информационной безопасности: учебное пособие	Москва: ФЛИНТА, 2021	https://biblioclub.ru/index.php?page=book&id=93245 неограниченный доступ для зарегистрированных пользователей
Л1.3	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
Л1.4	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Смирнов В. И.	Защита информации: лабораторный практикум: практикум	Йошкар-Ола: Поволжский государственный технологический университет, 2017	https://biblioclub.ru/index.php?page=book&id=476512 неограниченный доступ для зарегистрированных пользователей
Л2.2		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
Л2.3	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
Л2.4	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	http://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей
Л2.5		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

Consultant Plus

ФСТЭК России/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 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 (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
УК-3: Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели			
Знать методики формирования команд; методы эффективного руководства коллективами (соотнесено с индикатором УК- 3.1).	поиск и сбор необходимой литературы, использование различных баз данных	полнота и содержательность ответа, умение приводить примеры	О (вопросы 1-9,40-45) З (вопросы 1-9)
Уметь разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту (соотнесено с индикатором УК-3.2).	использование информационных технологий в практической деятельности для приобретения новых знаний и умений	полнота и содержательность ответа, умение приводить примеры и находить решение поставленных задач	ПЗ (раздел 1, практические задания 1,2) ПОЗЗ (1-5)
Владеть методами организации и управления коллективом, планированием его действий (соотнесено с индикатором (УК- 3.3).	использование современных информационно-коммуникационных технологий и различных информационных ресурсов	полнота и содержательность ответа, умение самостоятельно находить решение поставленных задач	ПЗ (раздел 1, тема 1, практические задания 1,2) ПОЗЗ (1-5)
ОПК-1:Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте			
Знать математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности (соотнесено с индикатором ОПК-1.1).	использование современных информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	полнота и содержательность ответа умение приводить примеры	О (вопросы 10-21) З (вопросы 10-21)
Уметь решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в	использование статических и динамических моделей для обеспечения	полнота и содержательность ответа, умение приводить	ПЗ (раздел 2, практические задания 1,2) ПОЗЗ (1-5)

междисциплинарном контексте, с применением математических, естественнонаучных социально-экономических и профессиональных знаний (соотнесено с индикатором ОПК-1.2).	информационной безопасности	примеры и находить решение поставленных задач	
Иметь навыки теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте (соотнесено с индикатором ОПК-1.3).	использование математических методов для решения задач защиты информации	полнота и содержательность ответ, умение самостоятельно находить решение поставленных задач	ПЗ (раздел 2, практические задания 1,2) ПОЗЗ (1-5
ОПК-7:Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях			
Знает методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях (соотнесено с индикатором ОПК-7.1).	использование современных информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	полнота и содержательность ответа умение приводить примеры	О (вопросы 22-39) З (вопросы 22-39)
Умеет применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях (соотнесено с индикатором ОПК- 7.2).	использование программ и методик испытаний средств и систем обеспечения информационной безопасности	полнота и содержательность ответа, умение приводить примеры и находить решение поставленных задач	ПЗ (раздел 4, практические задания 1,2) ПОЗЗ (1-5)
Имеет навыки методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях (соотнесено с индикатором ОПК-7.3).	использование программных средств для обеспечения информационной безопасности	полнота и содержательность ответ, умение самостоятельно находить решение поставленных задач	ПЗ (раздел 4, практические задания 1,2) ПОЗЗ (1-5)
ПК-2 :Способен осуществлять контроль взаимодействия программного обеспечения с вычислительной средой на основе современных научных подходов			
Знать методологию научной деятельности, технико-экономическое обоснование вариантов архитектуры компонентов, технологии и средства	использование информационных ресурсов для решения задач по обеспечению информационной	полнота и содержательность ответа умение приводить примеры	О (вопросы 46-57) З (вопросы 46-57)

разработки программного обеспечения (соотнесено с индикатором ПК-2.1).	безопасности		
Уметь организовывать профессиональную деятельность на основе современных научных подходов, проводить техническое исследование возможных вариантов архитектуры компонентов, проектировать архитектуру, оценивать и корректировать ее компоненты (соотнесено с индикатором ПК-2.2).	использование современных информационно-коммуникационных технологий и различных информационных ресурсов	полнота и содержательность ответа, умение приводить примеры и находить решение поставленных задач	ПЗ (раздел 4, практические задания 3,4) ПОЗЗ (1-5)
Владеть навыками научной деятельности, способами описания архитектуры программного средства, методами контроля согласованности требований архитектуры программного средства (соотнесено с индикатором ПК-2.3).	применение компьютерной математики для решения типовых задач	полнота и содержательность ответ, умение самостоятельно находить решение поставленных задач	ПЗ (раздел 4, практические задания 3,4) ПОЗЗ (1-5)

О – опрос; ПЗ – практические задания; З – вопросы к зачету; ПОЗЗ –практико-ориентированные задания 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 (зачет);
- 0-49 баллов (незачет).

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

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

Вопросы к зачету

по дисциплине Организационно-правовые механизмы обеспечения информационной безопасности

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.

Практико-ориентированные задания к зачету

1. Выявление угроз утечки информации по каналам побочных электромагнитных излучений и наводок.
2. Выявление угроз утечки акустической (речевой) информации.
3. Выявление угроз утечки видовой информации.
4. Сформулировать технические и организационные мероприятия по защите информации от утечки по техническим каналам.

5. Выявление источников и угроз несанкционированного доступа в информационной системе.

Ключи для контроля правильности выполнения практико-ориентированного задания к зачету

1. Модель угроз при рассмотрении потенциального риска утечки информации по каналам ПЭМИН должна опираться на действительную ценность охраняемых данных. ФСТЭК РФ делит их на три группы:

- первый класс. Ценность информации определяется ее владельцем самостоятельно;
- второй класс. В ИС обрабатываются информация ограниченного по закону доступа (банковская тайна, врачебная тайна) или персональные данные;
- третий класс. Организация работает со сведениями, составляющими государственную тайну.

Ведомство делит злоумышленников на группы — с низким потенциалом, со средним и с высоким. Реализация угроз утечки по каналам ПЭМИН требует оборудования и навыков злоумышленников на уровне второй и третьей группы — профессионалов в сфере бизнес-шпионажа или иностранных технических разведок.

Соответственно, беспокоиться об утечках по каналам ПЭМИН следует тем организациям, которые работают с ценными данными, интересными этим категориям агентов. На высоком уровне профессионалы не ограничиваются просто снятием имеющихся наводок. Они способны внедрять в компьютер вредоносные программы, находящие нужную информацию и генерирующие дополнительные сигналы в целях их перехвата.

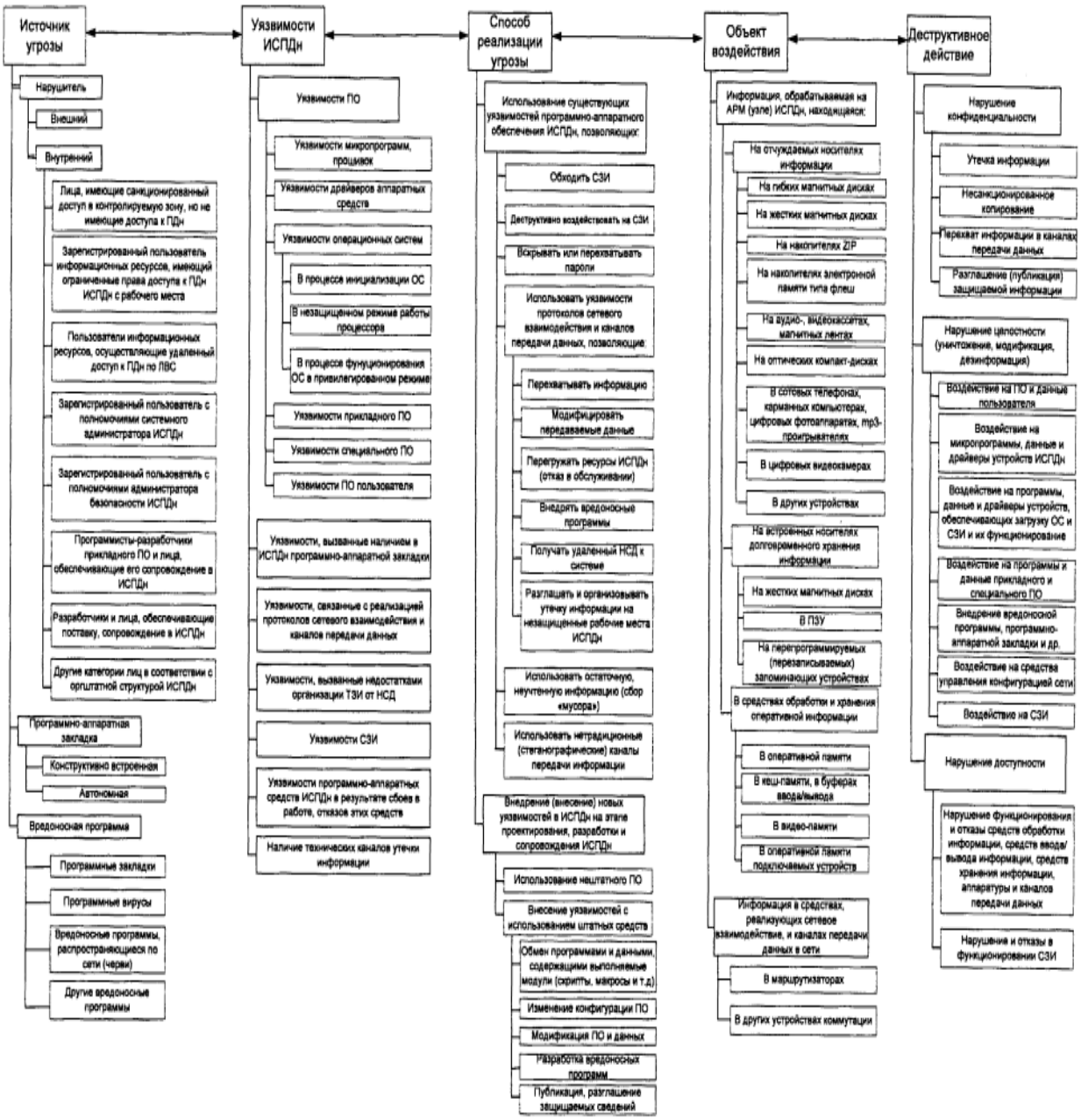
2.

3.

Угрозы утечки информации по техническим каналам и за счёт НСД	Уровень исходной защищённости (Y1)	Вероятность реализации угрозы (Y2)				Коэффициент реализуемости угрозы Y=(Y1+Y2)/20	Показатель опасности угрозы *(определяется на основе опроса специалистов в области ЗИ)*			Вывод об актуальности угрозы
		Малая вероятность (0)	Низкая вероятность (2)	Средняя вероятность (5)	Высокая вероятность (10)	Возможность реализации угрозы	Низкая опасность	Средняя опасность	Высокая опасность	
Утечка информации по каналу ПЭМИН	5		2			0,35 средняя	да			нет
Утечка речевой информации	5	0				0.25 низкая	да			нет
перехват паролей (идентификаторов)	5			5		0,5 средняя			да	да

4. Существует комплекс мероприятий, изменяющих параметры электромагнитного поля и снижающих риск утечки данных по каналам. Существуют многочисленные способы активного подавления электромагнитных излучений:

- метод «синфазной» низкочастотной маскирующей помехи — в провод по определенному временному алгоритму подаются сигналы маскирующего низкочастотного шума. Уровень сигнала в разы превосходит передаваемый, и снятие данных становится невозможным;
- использование высокочастотной маскирующей помехи. Низкочастотный сигнал подавляет речевой при передаче по линии. Для маскировки применяются широкополосные аналоговые сигналы типа «белого шума» или дискретные сигналы типа псевдослучайной последовательности электромагнитных импульсов;
- применение ультразвуковой маскирующей помехи. Принцип работы аналогичен предыдущему, создавать ультразвуковые помехи проще, но качество маскировки снижается;
- использование низкочастотной маскирующей помехи. Способ рассчитан на подавление работы подключенных диктофонов, вместо речи на них записывается «белый шум»;
- повышение напряжения. Оно переводит закладки в нелинейный режим работы, ЗУ с параллельным подключением отключаются;
- понижение напряжения. Оно также подавляет работу устройств съема информации;
- компенсационный способ, на линию подается чистый шум;
- метод «выжигания». На линию направляются высоковольтные импульсы, выжигающие входные каналы ЗУ.



5.

Критерии оценивания*:*

- оценка «зачет» (50-100 баллов) – изложенный материал верен, наличие знаний в объеме пройденного курса в соответствии с поставленными программой курса целями и задачами обучения; правильные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- оценка «незачет» (0-49 баллов) – 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.

Содержание 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.

Практические задания

1.Тематика практических заданий по разделам и темам

Раздел 1. Основные положения правовой и организационной защиты информации.

Практическое задание 1. Основные направления обеспечения информационной безопасности и защиты информации в РФ.

Практическое задание 2. Организация работы со с ведениями, отнесенные к государственной тайне и конфиденциальной информации.

Раздел 2. Правовой режим защиты информации ограниченного доступа.

Практическое задание 1. "Источники конфиденциальной информации": организационные каналы утечки конфиденциальной информации.

Практическое задание 2. "Юридическая ответственность за нарушения правового режима защиты информации ограниченного доступа": основные положения Кодекса об административных нарушениях и Уголовного кодекса о юридической ответственности за нарушение режима защиты информации ограниченного доступа.

Раздел 4. Допуск и доступ к конфиденциальной информации

Практическое задание 1. Задачи режима защиты информации.

Практическое задание 2. "Правовое обеспечение защиты коммерческой тайны": сведения, составляющие коммерческую тайну; требования к обеспечению защиты коммерческой тайны.

Практическое задание 3. "Рассекречивание конфиденциальных сведений, документов и продукции": основные требования при организации рассекречивания конфиденциальных сведений, документов и продукции.

Практическое задание 4. "Подбор персонала на должности, связанные с работой с конфиденциальной информацией": основные требования при подборе персонала, связанных с работой с конфиденциальной информацией.

Критерии оценивания*:*

Правильное решение практического задания – 10 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.

Зачет проводится по окончанию теоретического обучения в соответствии с расписанием. Количество вопросов в задании – 3. 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 вопросы методологии научных исследований в области информационной безопасности, методы анализа информации об объектах информационной безопасности, математические методы исследований в области информационной безопасности, даются рекомендации для самостоятельной работы и подготовке к практическим и лабораторным занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по вопросам технической защиты информации и организации защиты информации в информационных системах, по методологии защиты коммерческой тайны и конфиденциальной информации, по правовым основам защиты персональных данных, организации контроля за состоянием защиты конфиденциальной информации на предприятии, а также даются рекомендации для самостоятельной работы.

При подготовке к практическим занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

- подготовить ответы на все вопросы по изучаемой теме.

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

Вопросы, не рассмотренные на практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме. Выделить непонятные термины, найти их значение в энциклопедических словарях и используя профессиональную базу данных Консультант+.

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.