

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования «Ростовский государственный экономический университет (РИНХ)»
Документ подписан в системе «Электронный документооборот»
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 09.09.2024 11:14:08
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

УТВЕРЖДАЮ
Директор Института магистратуры
Иванова Е.А.
01.06.2023 г.

**Рабочая программа дисциплины
Информационная безопасность**

Направление 40.04.01 Юриспруденция
магистерская программа 40.04.01.01 "Цифровое право. Юрист в сфере информационных технологий"

Для набора 2023 года

Квалификация
магистр

КАФЕДРА Информационная безопасность**Распределение часов дисциплины по семестрам**

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
	15 2/6			
Неделя	УП	РП	УП	РП
Лекции	8	8	8	8
Лабораторные	8	8	8	8
Итого ауд.	16	16	16	16
Контактная работа	16	16	16	16
Сам. работа	20	20	20	20
Итого	36	36	36	36

ОСНОВАНИЕ

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

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

Зав. кафедрой: к.э.н.Радченко Ю.В.

Методическим советом направления: д.соц.н., к.ю.н., доцент, Федоренко Н.В.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- 1.1 Знание основ применения инфокоммуникационных технологий для решения задач профессиональной деятельности, основных терминов, понятий, определения в области информационной безопасности; умение защитить компьютерную информацию от несанкционированного разглашения, обеспечивать правовую защиту компьютерной информации в профессиональной деятельности; владеть навыками самостоятельной работы на компьютере и в компьютерных сетях, способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-2:Способен управлять проектом на всех этапах его жизненного цикла

ОПК-7:Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

информационные технологии, правовые базы данных, требования информационной безопасности (соотнесено с индикатором ОПК-7.1);
структуру жизненного цикла программного обеспечения, модели и стандарты его описания (соотнесено с индикатором УК- 2.1).

Уметь:

решать стандартные задачи профессиональной деятельности с применением информационных технологий и учетом основных требований информационной безопасности (соотнесено с индикатором ОПК-7.2);
оперировать стандартами и моделями жизненного цикла при разработке программного обеспечения (соотнесено с индикатором УК-2.2).

Владеть:

информационными технологиями и правовыми базами данных для решения задач профессиональной деятельности с учетом требований информационной безопасности (соотнесено с индикатором ОПК-7.3);
техническими и программными средствами определения стандартных показателей программного обеспечения (соотнесено с индикатором УК-2.3).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Общие вопросы информационной безопасности

№	Наименование темы / Вид занятия	Семе стр	Часов	Компетен- ции	Литература
1.1	Тема 1 «Введение в информационную безопасность». Понятие информации, защиты информации, информационной системы, информационной безопасности. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность. / Лек /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
1.2	Тема 1 «Введение в информационную безопасность». Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования с использованием текстового редактора LibreOffice. / Лаб /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
1.3	Тема 1 "Введение в информационную безопасность". Правовая защита информации. / Ср /	1	4	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
1.4	Тема 2 «Санкционированный и несанкционированный доступ». Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Неформальная модель нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации. / Лек /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
1.5	Тема 2 «Санкционированный и несанкционированный доступ». Несанкционированный доступ к информации (НСД). Идентификация. Аутентификация. Выбор паролей с использованием текстового редактора LibreOffice. / Лаб /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1

1.6	Тема 2 «Санкционированный и несанкционированный доступ». Административная защита информации. / Ср /	1	4	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
Раздел 2. Технологии организации работы с информацией					
№	Наименование темы / Вид занятия	Семестр	Часов	Компетенции	Литература
2.1	Тема 3 «Понятие угрозы, уязвимости, риска». Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Виды утечки информации в юриспруденции. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников. / Лек /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
2.2	Тема 3 «Понятие угрозы, уязвимости, риска». Технологии организации работы с информацией. Поиск, сохранение информации, проверка на вирусы. / Лаб /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
2.3	Тема 3 «Понятие угрозы, уязвимости, риска». Уязвимость компьютерных систем. / Ср /	1	4	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
2.4	Тема 4 «Парольные системы идентификации и аутентификации пользователей». Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей. / Лек /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
2.5	Тема 4 «Парольные системы идентификации и аутентификации пользователей». Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи. / Лаб /	1	2	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
2.6	Тема 5 «Парольные системы идентификации и аутентификации пользователей». Защита электронной почты. / Ср /	1	8	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1
2.7	/ Зачёт /	1	0	УК-2,ОПК- 7	Л1.4, Л1.1, Л1.2, Л1.3, Л1.5, Л2.3, Л2.4, Л2.2, Л2.1

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.2	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
Л1.3	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.4	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.5	Артемов, А. В.	Информационная безопасность: курс лекций	Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014	https://www.iprbookshop.ru/33430.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	https://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей
Л2.2		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей
Л2.3		Вестник Института законодательства и правовой информации имени М.М. Сперанского: журнал	Иркутск: Институт законодательства и правовой информации, 2017	https://biblioclub.ru/index.php?page=book&id=457912 неограниченный доступ для зарегистрированных пользователей
Л2.4	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	https://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Справочная правовая система "Консультант Плюс"

Russian Science Citation Index (RSCI)clarivate.ru

zbMATH zbmath.org

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.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

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-2: Способен управлять проектом на всех этапах его жизненного цикла			
Знать структуру жизненного цикла программного обеспечения, модели и стандарты его описания	Описывает способы решения стандартных задач профессиональной деятельности в области информационной безопасности при формировании системы защиты информации при ответе на вопросы	Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное	Опрос (вопросы 1-57) Вопросы к зачету (вопросы 1-78)
Уметь оперировать стандартами и моделями жизненного цикла при разработке программного обеспечения	Анализирует состояние системы защиты информации, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного и практического задания	Полнота и правильность решения практико-ориентированного задания или практического задания	Лабораторные задания (задания 1-8) Практико-ориентированные задания к зачету (задания 1-9)
Владеть техническими и программными средствами определения стандартных показателей программного обеспечения	Использует методы и средства защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного и практического задания	Обоснованность и правильность обращения к нормативным источникам, методам и средствам при выполнении практико-ориентированного и практического задания	Лабораторные задания (задания 1-8) Практико-ориентированные задания к зачету (задания 1-9)
ОПК-7: Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности			
Знать информационные технологии, правовые базы данных, требования информационной безопасности	изучает принципы конфиденциальности, целостности и доступности данных, различия между техническими и организационными мерами защиты информации для подготовки к зачету, опросу	полнота и соответствие предлагаемых способов решения стандартных задач профессиональной деятельности в области информационной безопасности требованиям	Опрос (вопросы 1-57) Вопросы к зачету (вопросы 1-78)

		нормативно-правовым актов при ответе на опросе, зачете	
Уметь решать стандартные задачи профессиональной деятельности с применением информационных технологий и учетом основных требований информационной безопасности	анализирует и выбирает средства защиты в зависимости от специфики профессиональных задач и угроз при выполнении практико-ориентированного и практического задания	соответствие результатов анализа текущему состоянию системы защиты информации при выполнении практико-ориентированного и практического задания	Лабораторные задания (задания 1-8) Практико-ориентированные задания к зачету (задания 1-9)
Владеть информационными технологиями и правовыми базами данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	использует инструменты для оценки уязвимостей и анализа инцидентов	качество полученных результатов, точность и полнота выявленных уязвимостей в соответствии с поставленными профессиональными задачами	Лабораторные задания (задания 1-8) Практико-ориентированные задания к зачету (задания 1-9)

1.2 Шкалы оценивания:

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

50-100 баллов (зачтено)

0-49 баллов (не зачтено)

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. Классификация угроз безопасности информации в информационных системах.
17. Требования к организации защиты информации в информационной системе.
18. Формирование требований к защите информации в информационной системе.
19. Обеспечение защиты информации в ходе эксплуатации информационной системы.
20. Требования к мерам защиты информации, содержащейся в информационной системе.
21. Определение класса защищенности информационной системы.
22. Лицензирование в области защиты информации.
23. Структура системы государственного лицензирования.
24. Порядок проведения лицензирования.
25. Основные лицензионные требования и условия в области защиты информации.
26. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
27. Структура системы сертификации.
28. Порядок проведения сертификации средств защиты информации.
29. Сертификационные испытания средств защиты информации.
30. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
31. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
32. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
33. Права обладателя коммерческой тайны.
34. Организация защиты информации на предприятии.
35. Обеспечение сохранности документов, дел и изданий.
36. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
37. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
38. Обязанности персонала организации по сохранению коммерческой тайны.
39. Политика безопасности предприятия как основа организационного управления защитой информации.
40. Права и обязанности работника и работодателя по защите конфиденциальной информации.
41. Ответственность за нарушение конфиденциальности информации.
42. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
43. Организация защиты персональных данных в организации.
44. Планирование мероприятий по организационной защите информации на предприятии.
45. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
46. Организация аналитической работы в области защиты информации на предприятии.
47. Основные объекты и формы контроля за состоянием защиты информации.
48. Основные задачи и методы контроля.
49. Основные направления аналитической работы.
50. Организация аудита информационной безопасности предприятия.
51. Функции аналитического подразделения в области защиты информации на предприятии.
52. Основные этапы аналитической работы в области защиты информации на предприятии.
53. Содержание и основные виды аналитических отчетов.
54. Классификация методов анализа информации.
55. Компьютерные преступления в электронной коммерции.
56. Информационная безопасность в электронной коммерции.
57. Юридическая ответственность за нарушение правовых норм защиты информации.
58. Обосновать основные направления обеспечения информационной безопасности и защиты информации в РФ.
59. Выявление угроз утечки информации по каналам побочных электромагнитных излучений и наводок.
60. Выявление угроз утечки акустической (речевой) информации.

61. Выявление угроз утечки видовой информации.
62. Сформулировать технические и организационные мероприятия по защите информации от утечки по техническим каналам.
63. Выявление источников и угроз несанкционированного доступа в информационной системе.
64. Определение типов нарушителей.
65. Выявление носителей вредоносных программ.
66. Выявление уязвимостей информационной системы, системного программного обеспечения, прикладного программного обеспечения.
67. Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах.
68. Определение класса защищенности информационной системы.
69. Сформировать требования к защите информации в информационной системе.
70. Разработка требований к мерам защиты информации, содержащейся в информационной системе.
71. Организация лицензирования в области защиты информации.
72. Организация сертификации в области защиты информации.
73. Правовое обеспечение защиты коммерческой тайны на предприятии.
74. Разработка политики безопасности предприятия.
75. Определение прав и обязанностей оператора, обрабатывающего персональные данные.
76. Определение уровня защищенности ИСПДн.
77. Определить основные объекты и формы контроля за состоянием защиты информации.
78. Сформулировать основные задачи и методы контроля.

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 модели угроз нарушения информационной безопасности системы электронного документооборота
6. Разработка модели нарушителя информационной безопасности системы электронного документооборота
7. Разработка комплекта типовых эксплуатационных документов системы электронного документооборота
8. Подбор и обоснование выбора средств защиты информации и их компонентов на основании модели угроз
9. Проведение аудита защищенности системы электронного документооборота по требованиям контролирующих органов

Зачетное задание включает 2 теоретических вопроса (раздел «Вопросы к зачету») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к зачету»).

Критерии оценивания:

Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:

– 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;

- 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
- 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
- 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:

- 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
- 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
- 11-24 балла выставляется, если задание решено частично.
- 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:

- 50-100 баллов (зачтено);
- 0-49 баллов (не зачтено).

Опрос

Вопросы 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. 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:

Максимальное количество баллов, которые обучающийся может набрать – 20 баллов (за 20 ответов).

Ответ на вопрос оценивается:

- 1 балл – правильный и полный ответ;
- 0 баллов – неправильный ответ или ответ не представлен.

Лабораторные задания

Задание 1.

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

Задание 2

Работа с ИСС «КонсультантПлюс», БД Федеральной службы по техническому и экспортному контролю (ФСТЭК России) <https://fstec.ru/>: Формы защищаемой информации. Объекты защиты. Физические основы возникновения ТКУИ. Классификация ТСП.

Задание 3.

Работа с ИСС «КонсультантПлюс», БД Федеральной службы по техническому и экспортному контролю (ФСТЭК России) <https://fstec.ru/>: Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах.

Задание 4.

Система шифрования Цезаря. Шифры перестановки.

1. Реализовать систему шифрования Цезаря. Система шифрования Цезаря, в котором каждый символ в открытом тексте сдвигается на определенное число позиций вперед или назад. Реализовать функции шифрования и дешифрования текста с использованием системы шифрования Цезаря.
2. Реализовать шифры перестановки, в которых порядок символов в открытом тексте меняется согласно некоторой функции. Реализовать функции шифрования и дешифрования текста с использованием шифров перестановки.
3. Реализовать систему шифрования Цезаря с ключом.
4. Реализовать функции шифрования и дешифрования текста с использованием системы шифрования Цезаря с ключом.

Задание 5.

Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана.

Реализовать функции для генерации простых чисел и вычисления наибольшего общего делителя.

1. Реализовать функции для генерации ключевой пары и обмена ключевой информацией с использованием протокола Диффи-Хеллмана.
2. Реализовать тесты для функций генерации ключевой пары и обмена ключевой информацией.
3. Реализовать тесты для функций генерации ключевой пары и обмена ключевой информацией.

Задание 6.

Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.

1. Реализовать функции для генерации простых чисел, вычисления наибольшего общего делителя, нахождения обратного элемента по модулю.
2. Реализовать функции для генерации ключевой пары и шифрования/дешифрования сообщений с использованием алгоритма RSA.
3. Реализовать тесты для функций генерации ключевой пары и шифрования/дешифрования сообщений.

Задание 7.

Формирование перечня сведений, составляющих коммерческую тайну.

1. Выберите вымышленную компанию, для которой будете формировать перечень сведений, составляющих коммерческую тайну.
2. Опишите виды сведений, которые могут составлять коммерческую тайну для выбранной компании.
3. Составьте перечень сведений, составляющих коммерческую тайну, для выбранной компании.
4. Оформите результаты в виде отчета

Задание 8.

Разработка политики безопасности предприятия.

1. Определите цели и задачи политики безопасности предприятия.
2. Опишите меры по защите информации, собственности и персонала предприятия.
3. Разработайте процедуры ответа на угрозы безопасности предприятия.
4. Оформите результаты в виде документа политики безопасности предприятия.

Критерии оценивания:

Максимальное количество баллов, которые обучающийся может набрать – 80 баллов (за 8 заданий).

Каждое задание оценивается:

- 10 баллов. – задание выполнено верно;
- 9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 6-3 баллов. – при выполнении задания были допущены ошибки;
- - 1 баллов. – при выполнении задания были допущены существенные ошибки;
- 0 баллов. – задание не выполнено.

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 расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

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 практическим 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 практической 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 практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. 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.