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.
«29» августа 2022 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 2022 года

Квалификация
магистр

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
Недель	15 2/6			
Вид занятий	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 22.02.2022 протокол № 7.

Программу составил(и): к.э.н., доцент Шарыпова Т.Н. _____

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

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Общие вопросы информационной безопасности				
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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
1.3	Тема 1 "Введение в информационную безопасность". Правовая защита информации. /Ср/	1	4	УК-2 ОПК-7	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2

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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
1.6	Тема 2 «Санкционированный и несанкционированный доступ». Административная защита информации. /Ср/	1	4	УК-2 ОПК-7	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
	Раздел 2. Технологии организации работы с информацией				
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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
2.3	Тема 3 «Понятие угрозы, уязвимости, риска». Уязвимость компьютерных систем. /Ср/	1	4	УК-2 ОПК-7	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
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	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
2.6	Тема 5 «Парольные системы идентификации и аутентификации пользователей». Защита электронной почты. /Ср/	1	8	УК-2 ОПК-7	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2
2.7	/Зачёт/	1	0	УК-2 ОПК-7	Л1.3 Л1.2 Л1.1 Л1.5 Л1.4Л2.5 Л2.4 Л2.3 Л2.1 Л2.2

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

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.2	Артемов, А. В.	Информационная безопасность: курс лекций	Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014	http://www.iprbookshop.ru/33430.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.4	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л1.5	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
5.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	http://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	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	http://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2017	http://www.iprbookshop.ru/63594.html неограниченный доступ для зарегистрированных пользователей
Л2.5		Вестник Института законодательства и правовой информации имени М.М. Сперанского: журнал	Иркутск: Институт законодательства и правовой информации, 2017	https://biblioclub.ru/index.php?page=book&id=457912 неограниченный доступ для зарегистрированных пользователей
5.3 Профессиональные базы данных и информационные справочные системы				
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.

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-2 – способен управлять проектом на всех этапах его жизненного цикла			
З: структуру жизненного цикла программного обеспечения, модели и стандарты его описания	формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления при подготовке к тестированию и зачету	сформировавшееся систематическое знание проблемы проектной задачи и способов ее решения через реализацию проектного управления при ответе на вопросы тестирования и зачета	Т (тесты Раздел 1 тема 1, тема 2) З (вопросы 1-13)
У: оперировать стандартами и моделями жизненного цикла при разработке программного обеспечения	разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения при подготовке к тестированию и зачету	сформировавшееся умение разработки концепции проекта в рамках обозначенной проблемы: формулировки цели, задачи, обоснования актуальности, значимости, ожидаемых результатов и возможных сфер их применения при подготовке к тестированию и зачету	ЛЗ (Раздел 1: ЛЗ 1); *ПОЗЗ* (раздел 1 задание1-2)
В: техническими и программными средствами определения стандартных показателей программного обеспечения	осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта при подготовке к тестированию и зачету	корректность мониторинга хода реализации проекта, внесения дополнительных изменений в план реализации проекта, зоны ответственности участников проекта при ответе на вопросы тестирования и зачета	ЛЗ (Раздел 1: ЛЗ 2); *ПОЗЗ* (раздел 2 задание1-2)
ОПК-7 – способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности			

З: информационные технологии, программные средства, требования информационной безопасности	знает основные информационные технологии, программные средства и требования информационной безопасности, а также основные методы хранения и обработки информации и методы ее трансляции при подготовке к тестированию и зачету	сформировавшееся систематическое знание основных информационных технологий, программных средств и требований информационной безопасности, а также основных методов хранения и обработки информации и методов ее трансляции при ответе на вопросы тестирования и зачета	Т (тесты Раздел 2 тема 3, тема 4), З (14-26)
У: решать стандартные задачи профессиональной деятельности с применением информационных технологий	умеет находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять уровень достоверности источников информации и давать ей критическую оценку с учетом основных требований информационной безопасности для решения лабораторных и практико-ориентированных заданий	сформировавшееся систематическое умение находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять уровень достоверности источников информации и давать ей критическую оценку с учетом основных требований информационной безопасности при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (Раздел 2: ЛЗ 1); ПОЗЗ (раздел 1 задание 3-5)
В: информационными технологиями и правовыми базами данных для решения задач профессиональной деятельности	обладает навыками поиска, обработки и фиксации результатов аналитической обработки информации с использованием общего и профессионального программного обеспечения персонального компьютера с учетом требований информационной безопасности для решения лабораторных и практико-ориентированных заданий	сформировавшееся систематическое владение навыками поиска, обработки и фиксации результатов аналитической обработки информации с использованием общего и профессионального программного обеспечения персонального компьютера с учетом требований информационной безопасности при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (Раздел 2: ЛЗ 2); ПОЗЗ (раздел 2 задание 3-5)

ЛЗ – лабораторные задания, Т – тест, ПОЗЗ - практико-ориентированные задания к зачету; З – вопросы к зачету

1.2 Шкалы оценивания:

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

- 50-100 баллов (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

Вопросы к зачету

1. Понятие информации, защиты информации, информационной системы, информационной безопасности.
2. Цель защиты информации.
3. Базовые свойства информации: конфиденциальность, целостность, доступность.
4. Нормативно-правовая база функционирования систем защиты информации.
5. Российское законодательство по защите информационных технологий.
6. Правовая защита программного обеспечения авторским правом.
7. Компьютерные преступления и особенности их расследования с использованием текстового редактора.
8. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
9. Неформальная модель нарушителя.
10. Причины несанкционированного доступа к информации.
11. Последствия несанкционированного доступа к информации.
12. Несанкционированный доступ к информации (НСД).
13. Идентификация.
14. Аутентификация.
15. Понятие угрозы, классификация угроз.
16. Понятие уязвимости, атаки на компьютерную систему.
17. Понятие риска.
18. Виды утечки информации в юриспруденции.
19. Понятие канала утечки информации, основные каналы утечки информации.
20. Классификация злоумышленников.
21. Уязвимость компьютерных систем.
22. Архиваторы. Архивы.
23. Методы сжатия архиваторов.
24. Сегментирование.
25. Возможности ОС по созданию учетной записи пользователя с ограниченными правами.

26.Порядок удаления ограниченной учетной записи.

Типовые практико-ориентированные задания к зачету

Раздел 1 «Общие вопросы информационной безопасности»

1. Добавить пользователей в компьютер.
2. Создать учетную запись локального пользователя.
3. Измените учетную запись локального пользователя на учетную запись администратора.
4. Выполнить настройку учетной записи с ограниченными правами.
5. Выполнить добавление учетных записей, используемых приложениями.

Раздел 2 «Технологии организации работы с информацией»

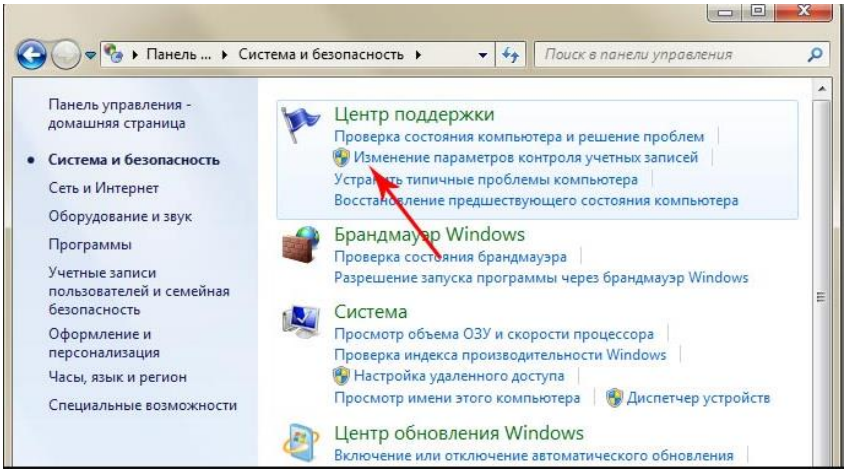
1. Выполнить удаление ограниченной учетной записи.
2. Выполнить установку паролей.
3. Выполнить сегментирование.
4. Выполнить защиту электронной почты.
5. Выполнить установку антивирусной программы.

Ключ для контроля правильности выполнения практико-ориентированные задания к зачету

Раздел 1 «Общие вопросы информационной безопасности»

1. Добавление пользователей в рабочий или учебный компьютер. Выберите параметры > "Пуск" > " Учетные записи > Другие пользователи". В разделе "Рабочие или учебные > добавить рабочую или учебную учетную запись" выберите " Добавить учетную запись". Введите учетную запись этого пользователя, выберите тип учетной записи и нажмите Добавить.
2. Создание учетной записи локального пользователя. Выберите Пуск > Параметры > Учетные записи а затем Семья и другие пользователи. Рядом с пунктом Добавить другого пользователя выберите Добавить учетную запись. Выберите пункт У меня нет учетных данных этого пользователя и на следующей странице нажмите Добавить пользователя без учетной записи Майкрософт. Введите имя пользователя, пароль, подсказку о пароле или выберите секретные вопросы, а затем нажмите Далее.
3. Изменение учетной записи локального пользователя на учетную запись администратора. Выберите Пуск > Параметры > Учетные записи. В разделе Семья и другие пользователи щелкните имя владельца учетной записи (под ним должно быть указано "Локальная учетная запись") и выберите Изменить тип учетной записи. В разделе Тип учетной записи выберите Администратор, и нажмите ОК. Войдите в систему с новой учетной записью администратора.

4.



5.Добавление на компьютер учетной записи, используемой приложениями: Выберите **параметры >** параметров **> учетных** записей **> электронной почты & учетных записей**. Добавление учетной записи, используемой по электронной почте. выберите "Добавить учетную запись" в разделе "Учетные записи", используемые электронной почтой**, календарем и** контактами. Для других приложений выберите "Добавить учетную запись Майкрософт " или "Добавить рабочую или учебную учетную запись". Следуйте инструкциям по добавлению учетной записи.

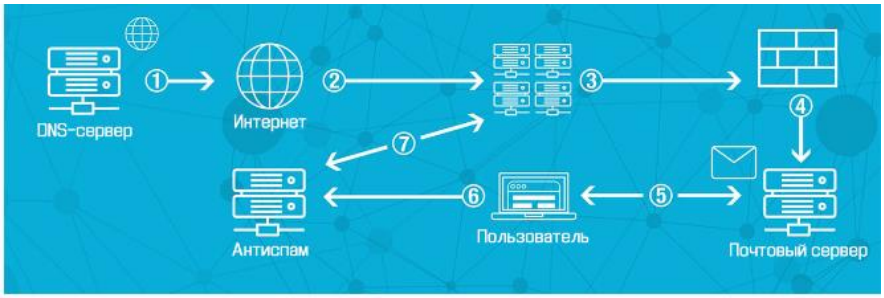
Раздел 2 «Технологии организации работы с информацией»

1. Для удаления данных для входа пользователя с компьютера выберите **параметры > параметров > учетных записей > других пользователей.** Выберите имя пользователя или адрес электронной почты и нажмите **Удалить**. Прочтите уведомление и выберите **Удалить учетную запись и данные**. Обратите внимание, что при этом учетная запись пользователя не будет удалена, но будут удалены его данные для входа и данные учетной записи с вашего компьютера.
2. Нажмите кнопку Параметры, а затем выберите пункт Изменение параметров компьютера. Выберите элемент Учетные записи, а затем Параметры входа. Нажмите или щелкните элемент Изменить **пароль** и следуйте указаниям.

3. <имя сегмента> SEGMENT <параметры>
<предложение>

<предложение>
<имя сегмента> ENDS

4.



5. Создать аккаунт. Загрузите антивирус. Сменить авторизацию. Пройдите процесс установки, показанный на экране. Перезагрузите компьютер.

Критерии оценивания:

- 50-100 баллов (оценка «зачтено») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированных заданий, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 0-49 баллов (оценка «не зачтено») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированных заданий, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Тесты письменные

1. Банк тестов по модулям и (или) темам

Раздел 1 «Общие вопросы информационной безопасности»

Тема 1 **«Введение в информационную безопасность».**

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
   a) Разработка аппаратных средств обеспечения правовых данных
   b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
   c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2. Основными источниками угроз информационной безопасности являются все указанное в списке:
   a) Хищение жестких дисков, подключение к сети, инсайдерство
   b) Перехват данных, хищение данных, изменение архитектуры системы
   c) Хищение данных, подкуп системных администраторов, нарушение регламента работы
3. Виды информационной безопасности:
   a) Персональная, корпоративная, государственная
   b) Клиентская, серверная, сетевая
   c) Локальная, глобальная, смешанная
4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
   a) несанкционированного доступа, воздействия в сети
   b) инсайдерства в организации
   c) чрезвычайных ситуаций
5. Основные объекты информационной безопасности:
   a) Компьютерные сети, базы данных
   b) Информационные системы, психологическое состояние пользователей
   c) Бизнес-ориентированные, коммерческие системы

Тема 2 **«Санкционированный и несанкционированный доступ».**

1. Требования к целостности информации для систем, зависящим от данных:
   a) Безопасность пользовательского программного обеспечения;
   b) Безопасная организация работы с данными;

c) Реализация прав граждан на поиск, получение, передачу и потребление информации;

2. Какие существуют методы несанкционированного доступа и перехвата информации?
   a) Уничтожение;
   b) Блокирование;
   c) Модификация;
   d) Копирование;
   e) Нарушение работы ЭВМ;
   f) Закрытие организации.
3. Система защиты информации от несанкционированного доступа - это:
   a) совокупность мер организационного характера и программно-технических СЗИ от НСД;
   b) меры по защите информации;
   c) комплекс мер по защите информации.
4. Формальными информационными моделями называются:
   a) модели, созданные на естественном языке (т.е. на любом языке общения между людьми: английском, русском, китайском, мальтийском и т.п.) в устной или письменной форме;
   b) модели, созданные на формальном языке (т.е. научном, профессиональном или специализированном).
5. На какие классы разделяются вредоносные программы?
   a) Первый;
   b) Второй;
   c) Третий;
   d) Четвертый.

Раздел 2 «Технологии организации работы с информацией»

Тема 3. «**Понятие угрозы, уязвимости, риска»**.

1. Наиболее распространены угрозы информационной безопасности сети:
   a) Распределенный доступ клиент, отказ оборудования
   b) Моральный износ сети, инсайдерство
   c) Сбой (отказ) оборудования, нелегальное копирование данных
2. Наиболее распространены средства воздействия на сеть офиса:
   a) Слабый трафик, информационный обман, вирусы в интернет
   b) Вирусы в сети, логические мины (закладки), информационный перехват
   c) Компьютерные сбои, изменение администрирования, топологии
3. Утечкой информации в системе называется ситуация, характеризуемая:
   a) Потерей данных в системе
   b) Изменением формы информации
   c) Изменением содержания информации
4. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
   a) Целостность
   b) Доступность
   c) Актуальность
5. Угроза информационной системе (компьютерной сети) – это:
   a) Вероятное событие
   b) Детерминированное (всегда определенное) событие
   c) Событие, происходящее периодически

Тема 4. **«Парольные системы идентификации и аутентификации пользователей».**

1. Управление правами доступа включает:
   a) разрешение доступа
   b) запрещение доступа
   c) неявное отклонение доступа

2. К основным средствам защиты информации в базах данных относят следующие:
   a) парольная защита;
   b) защита полей и записей таблиц БД;
   c) установление прав доступа к объектам БД;
   d) шифрование данных и программ
   e) закрытие организаций.

3.Как может быть обеспечена подлинность сеанса связи между пользователями компьютерной сети {несколько верных ответов):
   a) можно использовать механизм запроса-ответа;
   b) можно использовать механизм электронной подписи;
   c) можно использовать механизм отметки времени.

4. При принятии решения о предоставлении доступа обычно анализируется следующая информация {несколько верных ответов):
   a) электронная подпись субъекта, для которой ключ проверки электронной подписи указан в квалифицированном сертификате;
   b) идентификатор субъекта (например, идентификатор пользователя, сетевой адрес компьютера);
   c) атрибуты субъекта (например, метка безопасности, группа пользователя).

5. Какие меры позволяют повысить надежность парольной защиты {несколько верных ответов):
   a) наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры и т.п.);
   b) управление сроком действия паролей, их периодическая смена;
   c) ограничение доступа к файлу паролей;
   d) неиспользование программных генераторов паролей;
   e) ограничение числа неудачных попыток входа в систему; обучение пользователей.

2. Инструкция по выполнению

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его взгляд, варианта ответа. Тестовое задание содержит 20 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается. Время прохождения тестирования 20 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

Ключ для контроля правильности выполнения теста

№ задания	Правильный ответ

Раздел 1	
Тема 1	
вопрос 1	c)
вопрос 2	a)
вопрос 3	a)
вопрос 4	a)
вопрос 5	a)
Тема 2	
вопрос 1	a) b)
вопрос 2	a) b) c) d) e)
вопрос 3	a)
вопрос 4	b)
вопрос 5	a) b) c)
Раздел 2	
Тема 1	
вопрос 1	c)
вопрос 2	b)
вопрос 3	a)
вопрос 4	a)
вопрос 5	a)
Тема 2	
вопрос 1	a) b) c)
вопрос 2	a) b) c) d)
вопрос 3	a) c)
вопрос 4	b) c)
вопрос 5	a) b) c) e)

3. Критерии оценки:

Максимальное количество баллов – 40 баллов.

- 1-40 баллов выставляется обучаемому в зависимости от правильного ответа на вопросы теста.

За один правильный ответ обучаемый получает 2 балла;

За неправильный ответ – 0 баллов.

Лабораторные задания

1.Тематика лабораторных заданий по разделам и темам

Раздел 1 «**Общие вопросы информационной безопасности»**

Тема 1 **«Введение в информационную безопасность»**

Лабораторное задание 1 **«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.

Тема 2 **«Санкционированный и несанкционированный доступ».**

Лабораторное задание 2 **«Несанкционированный доступ к информации (НСД)».** Идентификация. Аутентификация. Выбор паролей с использованием текстового редактора LibreOffice.

Раздел 2 «**Технологии организации работы с информацией»**

Тема 3 **«Понятие угрозы, уязвимости, риска».**

Лабораторное задание 1 **«Технологии организации работы с информацией»**. Поиск, сохранение информации, проверка на вирусы.

Тема 4 **«Парольные системы идентификации и аутентификации пользователей».**

Лабораторное задание 2 **«**Архиваторы». Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи.

2. Критерии оценки:

Максимальное количество баллов – 60 баллов.

(для каждого задания):

15 б. – задание выполнено верно;

14-10 б. – при выполнении задания были допущены неточности, не влияющие на результат;

9-3 б. – при выполнении задания были допущены ошибки;

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

0 б. – 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.

Зачет проводится по расписанию **промежуточной аттестации**.

Количество вопросов в задании – 3: два теоретических вопроса и одно практико-ориентированное задание. Объявление результатов производится в день зачета. Результаты аттестации заносятся в 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;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются информационные технологии и программные средства в управлении проекта, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки управления проектом.

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме.

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

Вопросы, не рассмотренные на лекциях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий. 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 лабораторному 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.