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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Т.К. Платонова
«25» мая 2026 г.

**Рабочая программа дисциплины**
**Средства и методы защиты данных в системе бухгалтерского учета**

Направление подготовки
38.04.01 Экономика

Направленность (профиль) программы магистратуры
38.04.01.11 Бухгалтерский учет и консалтинг в условиях цифровой экономики

Для набора 2026 года

Квалификация
магистр

КАФЕДРА **Информационная безопасность**

**Распределение часов дисциплины по семестрам / курсам**

| Семестр (<Курс>.<Семестр на курсе>) | **1 (1.1)** | | Итого | |
|---|---|---|---|---|
| Недель | 14 | | | |
| Вид занятий | УП | РП | УП | РП |
| Лекции | 8 | 8 | 8 | 8 |
| Лабораторные | 24 | 24 | 24 | 24 |
| Итого ауд. | 32 | 32 | 32 | 32 |
| Контактная работа | 32 | 32 | 32 | 32 |
| Сам. работа | 40 | 40 | 40 | 40 |
| Итого | 72 | 72 | 72 | 72 |

## ОСНОВАНИЕ

Учебный план утвержден учёным советом Университета (протокол № 9 от 03.03.2026 г.).

Программу составил(и): к.ф-м.н., доцент, Карнаухов С.Н.

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

Методический совет направления: д.э.н., доцент Е.М. Евстафьева

Директор института магистратуры: д.э.н., профессор Е.А. Иванова

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| | |
|---|---|
| 1.1 | Освоение дисциплинарных компетенций, связанных с раскрытием основных принципов построения, функционирования и применения методов и средств защиты информации для обеспечения информационной безопасности электронного документооборота |

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий**

**ПК-2. Способен организовать процесс формирования учетно-контрольного обеспечения в области ведения бухгалтерского учета, консалтинговой деятельности, формирования бухгалтерской (финансовой) и нефинансовой отчетности и управлять экономическим субъектом, имеющим обособленные подразделения, в условиях цифровой экономики на основе информации финансового и нефинансового характера**

**В результате освоения дисциплины обучающийся должен:**

**Знать:**

-процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения (соотнесено с индикатором УК-1.1);
- современные методы и средства защиты данных при автоматизированной обработке учетной информации; виды рисков, правила защиты информации в информационных системах бухгалтерского учета, справочно-информационных системах получения информации (соотнесено с индикатором ПК-2.1).

**Уметь:**

- принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий (соотнесено с индикатором УК-1.2);
- использовать методику проведения управленческой бизнес-диагностики в целях выявления имеющихся проблем в области безопасности данных; применять современные программные продукты и технические средства для обеспечения безопасности ведения бухгалтерского учета и формирования отчетности ( соотнесено с индикатором ПК-2.2).

**Владеть:**

- методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях (соотнесено с индикатором УК-1.3);
- методиками контроля состояния защиты данных в системах бухгалтерской службы; методикой осуществления внутреннего контроля безопасности в условиях цифровой экономики; навыками оценки экономической эффективности принятых решений по защите данных в системах бухгалтерской службы с учетом фактора неопределённости (соотнесено с индикатором ПК-2.3).

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### Раздел 1. Организация системы защиты информации экономических данных

| № | Наименование темы, краткое содержание | Вид занятия / работы / форма ПА | Семестр / Курс | Количество часов | Компетенции |
|---|---|---|---|---|---|
| 1.1 | Тема 1.1. Теоретические аспекты информационной безопасности экономических систем. Основные понятия. Экономическая информация как объект безопасности. Государственное регулирование информационной безопасности | Лекционные занятия | 1 | 2 | УК-1 ПК-2 |
| 1.2 | Лабораторная работа 1.1 Организация защиты документов средствами пакета LibreOffice. | Лабораторные занятия | 1 | 2 | УК-1 ПК-2 |
| 1.3 | Лабораторная работа 1.2. "Работа в системе Консультант плюс". Изучение нормативно-правовых актов, регламентирующих информационную безопасность экономических данных. | Лабораторные занятия | 1 | 2 | УК-1 ПК-2 |
| 1.4 | Тема 1.2 Организация системы защиты информации экономических систем. Подходы, принципы, методы и средства обеспечения безопасности. Организационно-техническое обеспечение компьютерной безопасности. Защита от компьютерных вирусов. Электронная цифровая подпись и особенности ее применения | Лекционные занятия | 1 | 2 | УК-1 ПК-2 |
| 1.5 | Лабораторная работа 1.3 «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. | Лабораторные занятия | 1 | 4 | УК-1 ПК-2 |
| 1.6 | Лабораторная работа 1.4. "Изучение методов восстановления файлов". Восстановление файлов посредством анализа информации о файлах и папках | Лабораторные занятия | 1 | 4 | УК-1 ПК-2 |
| 1.7 | Вопросы для самостоятельного изучения. Правовые основы | Самостоятельная | 1 | 20 | УК-1 |

| | | | | | |
|---|---|---|---|---|---|
| | лицензирования в области защиты информации. Сущность и содержание сертификации в области защиты информации. Правовые основы защиты коммерческой тайны. Правовые основы защиты конфиденциальной информации. 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. Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации. Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей. Защита электронной почты. | работа | | | ПК-2 |

**Раздел 2. Методы и средства защиты данных в системе бухгалтерского учета**

| № | Наименование темы, краткое содержание | Вид занятия / работы / форма ПА | Семестр / Курс | Количество часов | Компетенции |
|---|---|---|---|---|---|
| 2.1 | Тема 2.1. «Принципы криптографической защиты информации». Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем. | Лекционные занятия | 1 | 2 | УК-1 ПК-2 |
| 2.2 | Лабораторная работа 2.1. «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера.Система шифрования Цезаря. Шифры перестановки | Лабораторные занятия | 1 | 4 | УК-1 ПК-2 |
| 2.3 | Тема 2.2 "Информационная безопасность отдельных экономических систем". Обеспечение информационной безопасности автоматизированных бухгалтерских и консалтинговых систем.Информационная безопасность электронной коммерции | Лекционные занятия | 1 | 2 | УК-1 ПК-2 |
| 2.4 | Лабораторная работа 2.2. "Защита информации от несанкционированного доступа в системе 1С" Изучение механизмов аутентификации. Настройки входа в Программу. Обеспечение защиты персональных данных | Лабораторные занятия | 1 | 4 | УК-1 ПК-2 |
| 2.5 | Лабораторная работа 2.3. "Изучение механизмов защиты данных в облачных хранилищах". | Лабораторные занятия | 1 | 4 | УК-1 ПК-2 |
| 2.6 | Вопросы для самостоятельного изучения: Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для криптографической защиты информации.Особенности использования вычислительной техники в криптографии. Принцип функционирования симметричных криптосистем. Функциональная схема взаимодействия участников симметричного криптографического обмена. Недостатки симметричных криптосистем. Основные виды симметричных шифров.Принцип функционирования асимметричных криптосистем, Функциональная схема взаимодействия участников асимметричного криптографического обмена. Достоинства и недостатки асимметричных криптосистем. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана. Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность. Безопасность в интернет.Безопасность хранения данных в облачных сервисах | Самостоятельная работа | 1 | 20 | УК-1 ПК-2 |
| 2.7 | Подготовка к промежуточной аттестации | Зачет | 1 | 0 | УК-1 ПК-2 |

## 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Учебные, научные и методические издания

| | Авторы, составители | Заглавие | Издательство, год | Библиотека / Количество |
|---|---|---|---|---|
| 1 | | Информационная безопасность: журнал | Москва: Гротек, 2014 | ЭБС «Университетская библиотека онлайн» |
| 2 | Прохорова О. В. | Информационная безопасность и защита информации: учебник | Самара: Самарский государственный архитектурно-строительный университет, 2014 | ЭБС «Университетская библиотека онлайн» |
| 3 | Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А. | Информационная безопасность: лабораторный практикум | Пермь: Пермский государственный гуманитарно-педагогический университет, 2018 | ЭБС «IPR SMART» |
| 4 | Ищейнов В. Я. | Информационная безопасность и защита информации: теория и практика: учебное пособие | Москва, Берлин: Директ-Медиа, 2020 | ЭБС «Университетская библиотека онлайн» |

**5.2. Профессиональные базы данных и информационные справочные системы**

Справочная правовая система "Консультант Плюс"
ФСТЭК России/fstec.ru
Web of Science apps.webofknowledge.com
ScienceDirect https://www.sciencedirect.com/

**5.3. Перечень программного обеспечения**

Операционная система РЕД ОС
LibreOffice
1С:Предприятие

**5.4. Учебно-методические материалы для обучающихся с ограниченными возможностями здоровья**

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет, и/или в специализированных лабораториях, предусмотренных образовательной программой.
Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

## 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

**Приложение 1**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

| ЗУН, составляющие компетенцию | Показатели оценивания | Критерии оценивания | Средства оценивания |
|---|---|---|---|
| **УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий** | | | |
| З: -процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения | методы анализа проблемных ситуаций на основе системного подхода, и применения их в профессиональных целях, а также при подготовке к зачету | полнота и обоснованность выбора методов системного анализа проблемных ситуаций на основе изученной литературы | З (1-44)<br>УО (Раздел 1 вопросы 1-26, Раздел 2 вопросы 8-11, 19-21) |
| У: - принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий | умеет применять системный подход анализа экономических данных с учетом информационной безопасности и вырабатывать стратегию действий с использованием информационных технологий для решения практико-ориентированных и лабораторных заданий | правильность применения методов системного подхода для решения практико-ориентированных и лабораторных заданий | ЛЗ (1.1, 1.2, 2.1)<br>ПОЗ (1,2,3) |
| В: - методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях | решение практико-ориентированных и лабораторных заданий:<br>применяет разные подходы защиты экономических данных | полнота и обоснованность выбора методов системного подхода для решения практико-ориентированных и лабораторных заданий | ЛЗ (1.1, 1.2, 2.1)<br>ПОЗ (1,2,3) |
| **ПК-2: Способен организовать процесс формирования учетно-контрольного обеспечения в области ведения бухгалтерского учета, консалтинговой деятельности, формирования бухгалтерской (финансовой) и нефинансовой отчетности и управлять экономическим субъектом, имеющим обособленные подразделения, в условиях цифровой экономики на основе информации финансового и нефинансового характера** | | | |
| З: - современные методы и средства защиты данных при автоматизированной обработке учетной информации; виды рисков, правила защиты информации в информационных системах бухгалтерского учета, справочно-информационных системах получения информации | методы и средства защиты данных в области бухгалтерского учета, консалтинговой деятельности в условиях цифровой экономики | полнота и обоснованность выбора методов и средств защиты данных в области бухгалтерского учета, консалтинговой деятельности в условиях цифровой экономики на основе изученной литературы | З (27-44)<br>УО (Раздел 1 вопросы 23-26, Раздел 2 вопросы 1-21) |
| У: - использовать методику проведения управленческой бизнес-диагностики в целях выявления имеющихся проблем в области безопасности данных; применять современные программные продукты и технические средства для обеспечения безопасности ведения бухгалтерского учета и формирования отчетности | решение практико-ориентированных и лабораторных заданий: применяет методы шифрования данных, владеет основами защиты от несанкционированного доступа 1С:Предприятие, а также методами восстановления данных (R-Studio) | правильность применения методов системного подхода для решения практико-ориентированных и лабораторных заданий | ЛЗ (2.1, 2.2)<br>ПОЗ (3,4,5) |
| В: - методиками контроля состояния защиты данных в системах бухгалтерской службы; методикой осуществления внутреннего контроля безопасности в условиях цифровой экономики; навыками оценки экономической эффективности принятых решений по защите данных в системах бухгалтерской службы с учетом фактора неопределённости | решение практико-ориентированных и лабораторных заданий:<br>применяет разные методы шифрования данных, владеет разными способами защиты от несанкционированного доступа 1С:Предприятие, а также методами восстановления данных (R-Studio) | полнота и обоснованность выбора методов системного подхода для решения практико-ориентированных и лабораторных заданий | ЛЗ ( 2.1, 2.2)<br>ПОЗ (3,4,5) |

*ЛЗ – лабораторные задания, ПОЗ - практико-ориентированные задания к зачету, З – вопросы к зачету, УО- устный опрос*

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, практико-ориентированные задания к зачету, лабораторные задания, вопросы для устного опроса

**Вопросы к зачету**

1. Теоретические аспекты информационной безопасности экономических систем. Основные понятия.
2. Экономическая информация как объект безопасности.
3. Государственное регулирование информационной безопасности
4. Организация системы защиты информации экономических систем.
5. Подходы, принципы, методы и средства обеспечения безопасности.
6. Организационно-техническое обеспечение компьютерной безопасности.
7. Защита от компьютерных вирусов.
8. Электронная цифровая подпись и особенности ее применения
9. Правовые основы лицензирования в области защиты информации.
10. Сущность и содержание сертификации в области защиты информации.
11. Правовые основы защиты коммерческой тайны.
12. Правовые основы защиты конфиденциальной информации.
13. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
14. Неформальная модель нарушителя.
15. Причины несанкционированного доступа к информации.
16. Последствия несанкционированного доступа к информации.
17. Понятие угрозы, классификация угроз.
18. Понятие уязвимости, атаки на компьютерную систему.
19. Понятие риска.
20. Виды утечки информации.
21. Понятие канала утечки информации, основные каналы утечки информации.
22. Классификация злоумышленников.
23. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
24. Особенности парольных систем, основные типы угроз безопасности парольных систем.
25. Требования к выбору и использованию паролей.
26. Защита электронной почты.
27. Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма.
28. Классификация криптосистем.
29. Процесс шифрования текста с помощью таблицы Вижинера.
30. Расшифровка текста с помощью таблицы Вижинера.
31. Система шифрования Цезаря.
32. Шифры перестановки.
33. Обеспечение информационной безопасности автоматизированных бухгалтерских систем
34. Обеспечение информационной безопасности консалтинговых систем.
35. Информационная безопасность электронной коммерции
36. Понятие криптоанализа, криптоаналитической атаки.
37. Основные типы криптоаналитических атак, криптостойкость шифра.
38. Требования к шифрам, используемым для криптографической защиты информации.

39. Особенности использования вычислительной техники в криптографии.
40. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
41. Понятие и назначение центра распределения ключей.
42. Оценка эффективности инвестиций в информационную безопасность.
43. Безопасность в интернет.
44. Безопасность хранения данных в облачных сервисах

**Практико-ориентированные задания к зачету**

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

**Ключ для контроля правильности выполнения практико-ориентированные задания к зачету**

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.

**Критерии оценивания:**

– 50-100 баллов (зачет) – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе; практико-ориентированное задание выполнено правильно и прокомментировано; наличие твердых и достаточно полных знаний, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, неуверенность и неточность ответов на дополнительные и наводящие вопросы; практико-ориентированное задание выполнено правильно, но не прокомментировано; при неполном ответе на вопросы; затрудняется ответить на дополнительные вопросы; практико-ориентированное задание выполнено с ошибками и отсутствуют комментарии;

– 0-49 баллов (незачет) – 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; практико-ориентированное задание не выполнено.

## Лабораторные задания

**Раздел 1 «Организация системы защиты информации экономических данных»**

Лабораторное занятие 1.1. Организация защиты документов средствами пакета LibreOffice

Лабораторное занятие 1.2 . «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.

**Раздел 2 «Методы и средства защиты данных в системе бухгалтерского учета».**

Лабораторное занятие 2.1. «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. Система шифрования Цезаря. Шифры перестановки

Лабораторное занятие 2.2. "Защита информации от несанкционированного доступа в системе 1С" Изучение механизмов аутентификации. Настройки входа в Программу. Обеспечение защиты персональных данных

*Критерии оценивания (для каждого задания):*

18-20 б. – задание выполнено верно;

13-17 б. – при выполнении задания были допущены неточности, не влияющие на результат;

7-12 б. – при выполнении задания были допущены ошибки;

1-6 б. – при выполнении задания были допущены существенные ошибки.

***Максимальное количество баллов за лабораторные задания – 80 (4 задания по 20 балла).***

## Перечень вопросов для устного опроса

### Раздел 1. Организация системы защиты информации экономических данных

1. Теоретические аспекты информационной безопасности экономических систем. Основные понятия.
2. Экономическая информация как объект безопасности.
3. Государственное регулирование информационной безопасности
4. Организация системы защиты информации экономических систем.
5. Подходы, принципы, методы и средства обеспечения безопасности.
6. Организационно-техническое обеспечение компьютерной безопасности.
7. Защита от компьютерных вирусов.
8. Электронная цифровая подпись и особенности ее применения
9. Правовые основы лицензирования в области защиты информации.
10. Сущность и содержание сертификации в области защиты информации.
11. Правовые основы защиты коммерческой тайны.
12. Правовые основы защиты конфиденциальной информации.
13. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
14. Неформальная модель нарушителя.
15. Причины несанкционированного доступа к информации.
16. Последствия несанкционированного доступа к информации.
17. Понятие угрозы, классификация угроз.
18. Понятие уязвимости, атаки на компьютерную систему.
19. Понятие риска.
20. Виды утечки информации.
21. Понятие канала утечки информации, основные каналы утечки информации.
22. Классификация злоумышленников.
23. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
24. Особенности парольных систем, основные типы угроз безопасности парольных систем.
25. Требования к выбору и использованию паролей.

26. Защита электронной почты.

**Раздел 2. Методы и средства защиты данных в системе бухгалтерского учета**

1. Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма.
2. Принципы функционирования криптографической системы.
3. Классификация криптосистем.
4. Процесс шифрования текста с помощью таблицы Вижинера.
5. Расшифровка текста с помощью таблицы Вижинера.
6. Система шифрования Цезаря.
7. Шифры перестановки.
8. Обеспечение информационной безопасности автоматизированных бухгалтерских систем
9. Обеспечение информационной безопасности консалтинговых систем.
10. Информационная безопасность электронной коммерции
11. Понятие криптоанализа, криптоаналитической атаки.
12. Основные типы криптоаналитических атак, криптостойкость шифра.
13. Требования к шифрам, используемым для криптографической защиты информации.
14. Особенности использования вычислительной техники в криптографии.
15. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
16. Понятие и назначение центра распределения ключей.
17. Требования Диффи и Хеллмана.
18. Алгоритм шифрования RSA.
19. Оценка эффективности инвестиций в информационную безопасность.
20. Безопасность в интернет.
21. Безопасность хранения данных в облачных сервисах

**Критерии оценивания:**

Для каждого вопроса:

– 2 балла дан полный ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;

– 1 балл – в ответе на поставленный вопрос были неточности;

– 0 баллов – обучающийся не владеет материалом по заданному вопросу.

Максимальное количество баллов – 20

## 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 (2 теоретических вопроса и 1 практико-ориентированное задание к зачету). Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке

**Приложение 2**

## МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:
- практические занятия;
- лабораторные занятия;

В ходе лабораторных и практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки применения методов и средств защиты данных с использованием современных различных информационных ресурсов и технологий, применяемых при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности.

При подготовке к практическим и 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 и практическим занятиям студенты могут воспользоваться консультациями преподавателя.

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

Студент должен готовиться к предстоящему лабораторному и практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.