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
«20» мая 2025 г.

Рабочая программа дисциплины
Защита электронного документооборота 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 2025 года

Квалификация
магистр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам / курсам

Курс	1		Итого	
Вид занятий	УП	РП		
Лекции	4	4	4	4
Лабораторные	8	8	8	8
Итого ауд.	12	12	12	12
Контактная работа	12	12	12	12
Сам. работа	56	56	56	56
Часы на контроль	4	4	4	4
Итого	72	72	72	72

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.02.2025 г. протокол № 9.

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

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 технологии автоматизированной обработки учетной информации; информационные системы в бухгалтерском учете, справочно-информационные системы получения информации, виды рисков, правила защиты информации в информационных системах (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; применять современные программные продукты для ведения бухгалтерского учета и формирования отчетности, позволяющие проанализировать эффективность работы экономического субъекта (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 электронного документооборота бухгалтерской службы; методикой осуществления внутреннего контроля в условиях цифровой экономики; навыками оценки экономической эффективности принятых решений по защите электронного документооборота с учетом фактора неопределённости (соотнесено с индикатором ПК-2.3).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Общие вопросы защиты информации в системах электронного документооборота

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Тема 1.1. "Основные понятия и принципы построения систем защищённого электронного документооборота": Сущность и определение электронного документооборота Задачи, функции и характеристики систем электронного документооборота. Функциональная классификация систем электронного документооборота Основные подходы к построению архитектуры систем электронного документооборота. Требования к инфраструктуре систем электронного документооборота. Классификация защищаемой информации в системе электронного документооборота,	Лекционные занятия	1	2	УК-1 ПК-2
1.2	Лабораторная работа 1.1 "Особенности интерфейса системы Дело": Подсистема протоколирования.Пользователи.Кабинеты.Справочники.	Лабораторные занятия	1	2	УК-1 ПК-2
1.3	Лабораторная работа 1.2 "Особенности интерфейса системы Дело": Конфигурирование подсистемы протоколирования. Интеграция со средствами контроля утечки конфиденциальной информации. Управление конфигурацией средств контроля за утечкой информацией.	Лабораторные занятия	1	2	УК-1 ПК-2
1.4	Вопросы для самостоятельного изучения: Средства антивирусной защиты.	Самостоятельная работа	1	20	УК-1 ПК-2

	Аппаратно-программные средства защиты информации. Средства идентификации и аутентификации субъектов доступа к объектам доступа Автоматизация резервного копирования информации на защищенные носители Криптографические средства защиты информации Организация учета, хранения и эксплуатации ключей шифрования и электронной подписи; Средства контроля утечки конфиденциальной информации из системы электронного документооборота Электронная подпись – определение, классификация и особенности применения. Правовые условия применения электронной подписи.				

Раздел 2. Методы и средства защиты данных в системе бухгалтерского учетадокументооборота

№	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	2	УК-1 ПК-2
2.3	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	2	УК-1 ПК-2
2.4	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	36	УК-1 ПК-2
2.5	Подготовка к промежуточной аттестации	Зачет	1	4	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	Минин И. В., Минин О. В.	Защита конфиденциальной информации при электронном документообороте: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2011	ЭБС «Университетская библиотека онлайн»

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
2		Информационная безопасность: журнал	Москва: Гротек, 2014	ЭБС «Университетская библиотека онлайн»
3	Шибаев, Д. В.	Правовое регулирование электронного документооборота: учебное пособие	Саратов: Вузовское образование, 2016	ЭБС «IPR SMART»
4	Куняев, Н. Н., Дёмушкин, А. С., Фабричнов, А. Г., Кондрашева, Т. В., Куняев, Н. Н.	Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник	Москва: Логос, 2016	ЭБС «IPR SMART»
5	Романенко, М. Г., Шагрова, Г. В.	Анализ систем электронного документооборота: учебное пособие (лабораторный практикум)	Ставрополь: Северо-Кавказский федеральный университет, 2018	ЭБС «IPR SMART»
6	Краснянский, М. Н., Карпушкин, С. В., Обухов, А. Д., Коробова, И. Л., Карпов, С. В.	Основы проектирования систем электронного документооборота: учебное пособие	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2018	ЭБС «IPR SMART»
7	Кузнецова, И. В., Хачатрян, Г. А.	Конфиденциальное делопроизводство и защищенный электронный документооборот: учебное пособие для бакалавров	Москва: Ай Пи Ар Медиа, 2020	ЭБС «IPR SMART»

5.2. Профессиональные базы данных и информационные справочные системы

СПС КонсультантПлюс
ФСТЭК России/fstec.ru
Web of Science apps.webofknowledge.com
ScienceDirect https://www.sciencedirect.com/

5.3. Перечень программного обеспечения

Операционная система РЕД ОС
ДЕЛО – предприятие
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.

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 (1-36) УО (Раздел 1 вопросы 1-18, 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 (СЭД Дело) для решения практико-ориентированных и лабораторных заданий	правильность применения методов системного подхода для решения практико-ориентированных и лабораторных заданий	ЛЗ (1.1, 1.2, 1.3 2.1, 2.3) 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: применяет разные подходы защиты экономических данных средствами СЭД Дело	полнота и обоснованность выбора методов системного подхода для решения практико-ориентированных и лабораторных заданий	ЛЗ (1.1, 1.2, 1.3, 2.1, 2.3) 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 технологии автоматизированной обработки учетной информации; информационные системы в бухгалтерском учете, справочно-информационные системы получения информации, виды рисков, правила защиты информации в информационных системах	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 (27-36) УО (Раздел 1 вопросы 15-18, Раздел 2 вопросы 1-21)
У: - использовать методику проведения управленческой бизнес-диагностики в целях выявления имеющихся проблем; применять современные программные продукты для ведения бухгалтерского учета и формирования отчетности, позволяющие проанализировать эффективность работы экономического субъекта	решение практико-ориентированных и лабораторных заданий: применяет методы шифрования данных, владеет основами защиты от несанкционированного доступа средствами СЭД Дело, 1С:Предприятие	правильность применения методов системного подхода для решения практико-ориентированных и лабораторных заданий	ЛЗ (1.3, 2.1, 2.2, 2.3) ПОЗ (3,4,5)
В: - методиками контроля состояния электронного документооборота бухгалтерской службы; методикой осуществления внутреннего контроля в условиях цифровой экономики; навыками оценки экономической эффективности принятых решений по защите электронного документооборота с учетом фактора неопределённости	решение практико-ориентированных и лабораторных заданий: применяет разные методы шифрования данных, владеет разными способами защиты от несанкционированного доступа средствами СЭД Дело, 1С:Предприятие	полнота и обоснованность выбора методов системного подхода для решения практико-ориентированных и лабораторных заданий	ЛЗ (1.3, 2.1, 2.2, 2.3) 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. Сущность и определение электронного документооборота
2. Задачи, функции и характеристики систем электронного документооборота.
3. Функциональная классификация систем электронного документооборота
4. Основные подходы к построению архитектуры систем электронного документооборота.
5. Требования к инфраструктуре систем электронного документооборота.
6. Классификация защищаемой информации в системе электронного документооборота
7. Организационные методы обеспечения безопасности информации в системах электронного документооборота.
8. Технические методы обеспечения безопасности информации в системах электронного документооборота.
9. Программные методы обеспечения безопасности информации в системах электронного документооборота
10. Средства антивирусной защиты.
11. Аппаратно-программные средства защиты информации.
12. Средства идентификации и аутентификации субъектов доступа к объектам доступа
13. Автоматизация резервного копирования информации на защищенные носители
14. Криптографические средства защиты информации
15. Организация учета, хранения и эксплуатации ключей шифрования и электронной подписи;
16. Средства контроля утечки конфиденциальной информации из системы электронного документооборота
17. Электронная подпись – определение, классификация и особенности применения.
18. Правовые условия применения электронной подписи.
19. Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма.
20. Классификация криптосистем.
21. Процесс шифрования текста с помощью таблицы Вижинера.
22. Расшифровка текста с помощью таблицы Вижинера.
23. Система шифрования Цезаря.
24. Шифры перестановки.
25. Обеспечение информационной безопасности автоматизированных бухгалтерских систем
26. Обеспечение информационной безопасности консалтинговых систем.
27. Информационная безопасность электронной коммерции
28. Понятие криптоанализа, криптоаналитической атаки.
29. Основные типы криптоаналитических атак, криптостойкость шифра.
30. Требования к шифрам, используемым для криптографической защиты информации.
31. Особенности использования вычислительной техники в криптографии.
32. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
33. Понятие и назначение центра распределения ключей.
34. Оценка эффективности инвестиций в информационную безопасность.
35. Безопасность в интернет.
36. Безопасность хранения данных в облачных сервисах

Практико-ориентированные задания к зачету

Задание 1. (Дело). "Управление документами в системе Дело":
Выполнить следующие действия:
- Регистрация документа.
- Исполнение документа.
- Контроль исполнения.
- Гриф доступа.

Задание 2 (Дело). Выполнить следующие действия:
- Регистрация документа в системе Дело.
- Обеспечение юридической значимости электронного документооборота.
- Архивное хранение документов, обеспеченных средствами защиты от нарушения целостности информации

Задание 3. С помощью алгоритма RSA зашифровать слово БАЛАНС (6. 5. 1). Для реализации алгоритма использовать числа p=11, q=13.

Задание 4. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: АКТИВ – ЮЛОУЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Задание 5. (1С: Предприятие)
Создать нового пользователя. Сформировать пароль и обосновать его сложность. Установить:
- настройки пользователей и прав.
- Ограничение входа для пользователей

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

1.Тематика лабораторных заданий по разделам и темам

Раздел 1 «Общие вопросы защиты информации в системах электронного документооборота»

Лабораторное занятие 1.1. "Особенности интерфейса системы Дело": Подсистема протоколирования. Пользователи. Кабинеты. Справочники

Лабораторное занятие 1.2 . «Особенности интерфейса системы Дело": Конфигурирование подсистемы протоколирования. Интеграция со средствами контроля утечки конфиденциальной информации. Управление конфигурацией средств контроля за утечкой информацией

Лабораторное занятие 1.3 . «Управление документами в системе защищенного электронного документооборота Дело». Регистрация документа в системе Дело". Обеспечение юридической значимости электронного документооборота. Архивное хранение документов, обеспеченных средствами защиты от нарушения целостности информации

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

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

Лабораторное занятие 2.3. "Изучение механизмов защиты данных в облачных хранилищах".

Критерии оценивания:
10 б. – задание выполнено верно;
7-9 б. – при выполнении задания были допущены неточности, не влияющие на результат;
4-6 б. – при выполнении задания были допущены ошибки;
1-3 б. – при выполнении задания были допущены существенные ошибки.
Максимальное количество баллов по лабораторным заданиям – 60

Перечень вопросов для устного опроса

Раздел 1. Общие вопросы защиты информации в системах электронного документооборота

1. Сущность и определение электронного документооборота
2. Задачи, функции и характеристики систем электронного документооборота.
3. Функциональная классификация систем электронного документооборота
4. Основные подходы к построению архитектуры систем электронного документооборота.
5. Требования к инфраструктуре систем электронного документооборота.
6. Классификация защищаемой информации в системе электронного документооборота
7. Организационные методы обеспечения безопасности информации в системах электронного документооборота.
8. Технические методы обеспечения безопасности информации в системах электронного документооборота.
9. Программные методы обеспечения безопасности информации в системах электронного документооборота
10. Средства антивирусной защиты.
11. Аппаратно-программные средства защиты информации.
12. Средства идентификации и аутентификации субъектов доступа к объектам доступа
13. Автоматизация резервного копирования информации на защищенные носители
14. Криптографические средства защиты информации
15. Организация учета, хранения и эксплуатации ключей шифрования и электронной подписи;
16. Средства контроля утечки конфиденциальной информации из системы электронного документооборота
17. Электронная подпись – определение, классификация и особенности применения.
18. Правовые условия применения электронной подписи.

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

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:
– 4 балла дан полный ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;
– 2-3 балл – в ответе на поставленный вопрос были неточности;
– 1 балл – обучающийся не владеет материалом по заданному вопросу.
Максимальное количество баллов – 40

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:
- лекции;
- лабораторные занятия;

В ходе лекционных занятий рассматриваются вопросы информационной защиты экономических данных, 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 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 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 занятиях 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 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.