Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

Институт международной экономики, лидерства и менеджмента

УТВЕРЖДАЮ
Директор института
международной экономики,
лидерства и менеджмента
_____ А.А. Панарин
«04» октября 2024 г.

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Направление подготовки 38.03.01 Экономика
(уровень бакалавриат)

Направленность (профиль):
« Финансовая разведка и экономическая безопасность»

Форма обучения: очная

Москва

Рабочая программа дисциплины «Информационная безопасность в экономических системах». Направление подготовки 38.03.01 Экономика, направленность (профиль): «Финансовая разведка и экономическая безопасность» / Т.В. Новикова.– М.: ИМПЭ им. А.С. Грибоедова. – 21 с.

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 38.03.01 Экономика, утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 № 922 (с изменениями и дополнениями) и Профессиональным стандартом «Программист», Утверждённым приказом Министерства труда и социальной защиты Российской Федерации от 20 июля 2022 № 424н (регистрационный номер 4).

Разработчики: кандидат экономических наук, доцент, Т.В. Новикова

Ответственный рецензент: М. К. Чистякова, кандидат экономических наук, доцент, декан экономического факультета ОАНО ВО «Московский психолого-социального университета»

(Ф.И.О., уч. степень, уч. звание, должность)

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры аудита, финансов и кредита 04.10.2024г., протокол №2

Заведующий кафедрой _____/Т.В. Новикова, к. э. н., доцент

Согласовано от Библиотеки _____/О.Е. Стёпкина

Раздел 1. Цели и задачи освоения дисциплины

Целью освоения дисциплины является формирование обучающимися основных принципов, моделей и методов защиты информации; овладение методами организационного и правового обеспечения безопасности информационных систем и данных; приобретение навыков и основных приемов защиты информации от утечки и несанкционированного доступа, антивирусной борьбы; применение криптографических методов защиты.

Задачи дисциплины:

– изучить характерные свойства защищаемой информации, основные информационные угрозы, существующие направления защиты;

– получить теоретические знания в области защиты информации;

– ознакомиться с требованиями российских и международных стандартов в области информационной безопасности;

– научиться применять современные программно-аппаратные средства защиты на практике.

Раздел 2. Планирование результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код компетенции	**Формулировка компетенции**	**Индикаторы достижения компетенции** (для планирования результатов обучения по элементам образовательной программы и соответствующих оценочных средств)
ОПК-5	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	**ИОПК-5.1. Знает** современные информационные технологии и программные средства при решении профессиональных задач **ИОПК-5.2. Умеет** использовать современные информационные технологии и программные средства при решении профессиональных задач. **ИОПК-5.3. Владеет** навыками применения современных информационных технологий и программных средств при решении профессиональных задач.
ОПК-6	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	**ИОПК-6.1. Знает** принципы работы современных информационных технологий **ИОПК-6.2. Умеет** использовать их для решения задач профессиональной деятельности **ИОПК-6.3. Владеет** использования современных информационных технологий для решения задач профессиональной деятельности

Раздел 3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» изучается в шестом семестре, относится к Б1.О.1 Обязательной части учебного плана Блока 1 «Дисциплины (модули)».

Раздел 4. Объем (трудоемкость) дисциплины (общая, по видам учебной работы, видам промежуточной аттестации)

Трудоемкость дисциплины и виды учебной нагрузки

на очной форме обучения

Семестр 4										
з.е.	Итого	Лекции	Лабораторные занятия	Практические занятия	Семинары	Курсовое проектирование	Самостоятельная работа под руководством преподавателя	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация
3	108	16		16				72		4 зачет

на заочной форме обучения

Семестр 4										
з.е.	Итого	Лекции	Лабораторные занятия	Практические занятия	Семинары	Курсовое проектирование	Самостоятельная работа под руководством преподавателя	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация
3	108	4		6				94		4 зачет

Тематический план дисциплины

Очная форма обучения

Разделы / Темы	Лекции	Лабораторные занятия	Практические занятия	Семинары	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация	Всего часов
6 семестр								
Тема 1. Введение в информационную безопасность	**2**		**2**		**7**			**10**
Тема 2. Законодательный	**2**		**2**		**7**			**10**

уровень информационной безопасности								
Тема 3. Стандарты и спецификации в области информационной безопасности	**2**		**2**		**7**			**10**
Тема 4. Административный уровень информационной безопасности	**2**		**2**		**7**			**10**
Тема 5. Процедурный уровень информационной безопасности	**2**		**2**		**7**			**10**
Тема 6. Идентификация и аутентификация	**1**		**1**		**7**			**9**
Тема 7. Управление доступом. Протоколирование и аудит	**1**		**1**		**6**			**9**
Тема 8. Криптографические методы защиты	**1**		**1**		**6**			**9**
Тема 9. Контроль целостности	**1**		**1**		**6**			**9**
Тема 10. Экранирование. Тунелирование	**1**		**1**		**6**			**9**
Тема 11.	**1**		**1**		**6**			**9**

Анализ защищенности								
Текущий контроль								
Зачет							**4**	**4**
Итого за семестр	**16**		**16**		**72**		**4**	**108**

Заочная форма обучения

Разделы / Темы	Лекции	Лабораторные занятия	Практические занятия	Семинары	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация	Всего часов
6 семестр								
Тема 1. Введение в информационную безопасность	**1**		**1**		**9**			**10**
Тема 2. Законодательный уровень информационной безопасности			**1**		**9**			**10**
Тема 3. Стандарты и спецификации в области информационной безопасности	**1**		**1**		**9**			**10**
Тема 4. Административный уровень информационной безопасности			**1**		**9**			**10**
Тема 5. Процедурный уровень информационной безопасности			**1**		**9**			**10**
Тема 6. Идентификация и			**1**		**9**			**9**

аутентификация								
Тема 7. Управление доступом. Протоколирование и аудит	**1**				**8**			**9**
Тема 8. Криптографические методы защиты					**8**			**9**
Тема 9. Контроль целостности					**8**			**9**
Тема 10. Экранирование. Тунелирование	**1**				**8**			**9**
Тема 11. Анализ защищенности					**8**			**9**
Зачет							**4**	**4**
Итого	**4**		**6**		**94**		**4**	**108**

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ п/п	**Наименование разделов и тем дисциплины**	**Содержание темы**
1	Тема 1.1 Введение в информационную безопасность	Изучаемые вопросы: 1. Понятие информационной безопасности. 2. Основные составляющие информационной безопасности: доступность, целостность и конфиденциальность. 3. Угрозы информационной безопасности. 4. Задачи системы информационной безопасности. 5. Меры противодействия угрозам безопасности. 6. Основные принципы построения систем защиты АИС. Вопросы для самостоятельного изучения: 1. Информационная безопасность на уровне государства. Концепция безопасности РФ. 2. Важность проблемы информационной безопасности. Примеры нарушений информационной безопасности.
2	Тема 1.2 Законодательный уровень информационной безопасности	Изучаемые вопросы: 1. Понятие и важность законодательного уровня информационной безопасности. 2. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной без-

№ п/п	Наименование разделов и тем дисциплины	Содержание темы
		опасности. 3. Закон `Об информации, информационных технологиях и о защите информации`. 4. Закон `Об электронной подписи`. 5. Закон `О персональных данных`. 6. Защита авторского права на программные продукты. Вопросы для самостоятельного изучения: 1. Обзор международного законодательства в области информационной безопасности. 2. Федеральный закон `О государственной тайне`.
3	Тема 1.3 Стандарты и спецификации в области информационной безопасности	Изучаемые вопросы: 1. Оценочные стандарты и технические спецификации. 2. Оценочный стандарт ГОСТ Р ИСО/МЭК 15408 `Общие критерии оценки безопасности информационных технологий`. Введение и общая модель. Функциональные компоненты безопасности. Компоненты доверия к безопасности. 3. Сопутствующие документы. Управленческие стандарты информационной безопасности. ГОСТ Р ИСО/МЭК 17799 `Информационные технологии. Практические правила управления информационной безопасностью`. ГОСТ Р ИСО/МЭК 27001 `Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования`. Вопросы для самостоятельного изучения: 1. Руководящие документы Гостехкомиссии России.
4	Тема 1.4 Административный уровень информационной безопасности	Изучаемые вопросы: 1. Основные понятия. 2. Политика безопасности. 3. Программа безопасности. 4. Синхронизация программы безопасности с жизненным циклом систем Вопросы для самостоятельного изучения: 1. Примеры типовых политик безопасности организации.
5	Тема 1.5 Процедурный уровень информационной безопасности	Изучаемые вопросы: 1. Основные классы мер процедурного уровня. 2. Управление персоналом. 3. Физическая защита. 4. Поддержка работоспособности 5. Реагирование на нарушение режима безопасности. 6. Планирование восстановительных работ. Вопросы для самостоятельного изучения: 1. План восстановительных работ.
6	Тема 2.1 Идентификация и аутентификация	Изучаемые вопросы: 1. Определение идентификации и аутентификации. 2. Парольная аутентификация. Требования к паролям. 3. Одноразовые пароли. 4. Сервер аутентификации Kerberos. 5. Идентификация/аутентификация с помощью биометрических данных. Вопросы для самостоятельного изучения: 1. Алгоритмы создания одноразовых паролей.

№ п/п	Наименование разделов и тем дисциплины	Содержание темы
		2. Социальный инжиниринг.
7	Тема 2.2 Управление доступом. Протоколирование и аудит	Изучаемые вопросы: 1. Понятие управления доступом. 2. Модели безопасности: модель дискреционного доступа; модель Белла-ЛаПадулы; ролевая модель управления доступом. 3. Понятие протоколирования и аудита. 4. Активный аудит. Вопросы для самостоятельного изучения: 1. Системы разграничения доступа. 2. Функциональные компоненты архитектуры.
8	Тема 2.3 Криптографические методы защиты	Изучаемые вопросы: 1. Введение в криптографию. Основные термины и понятия криптографии. Типы криптографических систем. 2. Шифры подстановки и перестановки. 3. Блочные шифры. Сеть Фейштеля. 4. Симметричные алгоритмы шифрования. Алгоритмы DES, ГОСТ 34.12-2015, AES. 5. Асимметричные алгоритмы шифрования. Алгоритм RSA. Вопросы для самостоятельного изучения: 1. Режимы шифрования блочных шифров 2. Потоковые шифры 3. Обмен ключами Диффи-Хелмана. 4. Шифросистема Эль-Гамаля. 5. Стандарт ГОСТ Р 34.10-2012.
9	Тема 2.4 Контроль целостности	Изучаемые вопросы: 1. Определение функции хеширования. Требования к хеш-фукнциям. Функции Хеширования. 2. Электронная цифровая подпись. Цифровые сертификаты. Вопросы для самостоятельного изучения: 1. Деятельность удостоверяющих центров. 2. Функция хеширования MD5.
10	Тема 2.5 Экранирование. Тунелирование	Изучаемые вопросы: 1. Понятие экранирования. Межсетевые экраны. Классификация межсетевых экранов. Виды межсетевых экранов. 2. Понятие тунелирования. Виртуальные частные сети. Вопросы для самостоятельного изучения: 1. VPN IPsec, PPTP. 2. Разработка конфигурации межсетевого экрана.
11	Тема 2.6 Анализ защищенности	Изучаемые вопросы: 1. Понятие анализа защищенности. 2. Сетевые сканеры. 3. Антивирусная защита. Классификация вирусов. Признаки присутствия на компьютере вредоносных программ. 4. Методы защиты от вредоносных программ. Основы работы антивирусных программ. Вопросы для самостоятельного изучения:

№ п/п	Наименование разделов и тем дисциплины	Содержание темы
		1. Антивирусная защита компьютерной сети.

Занятия семинарского типа
(Лабораторные занятия)

Общие рекомендации по подготовке к лабораторным занятиям. При подготовке к работе во время проведения занятий лабораторного типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний. Предварительная подготовка к учебному занятию лабораторного типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия. Работа во время проведения занятия лабораторного типа включает несколько моментов: а) консультирование обучающихся преподавателями с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, б) самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности»

Лабораторная работа 1. Обзора российского законодательства в области информационной безопасности (4 ч.).

Лабораторная работа 2. Разработка политики безопасности организации (4 ч.).

Лабораторная работа 3. Анализ рисков информационной безопасности организации (4 ч.).

Раздел №2 «Программно-технический уровень информационной безопасности»

Лабораторная работа 4. Защита информации в компьютерной системе от случайных угроз. Создание и управление учетными записями пользователей (4 ч.).

Лабораторная работа 5. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS. Аудит ресурсов и событий системы защиты (4 ч.).

Лабораторная работа 6. Настройка системных параметров безопасности (4 ч.).

Лабораторная работа 7. Настройка параметров безопасности подключения к Интернет (4 ч.).

Лабораторная работа 8. Разработка алгоритмов криптографической защиты (4 ч.).

Раздел 5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Наряду с чтением лекций и проведением семинарских занятий неотъемлемым элементом учебного процесса является *самостоятельная работа.* При самостоятельной работе достигается конкретное усвоение учебного материала, развиваются теоретические способности, столь важные для успешной подготовки и защиты выпускной работы бакалавра. Формы самостоятельной работы, обучаемых могут быть разнообразными. Самостоятельная работа включает: изучение литературы, веб-ресурсов, оценку, обсуждение и рецензирование публикуемых статей; ответы на контрольные вопросы; решение задач; самотестирование. Выполнение всех видов самостоятельной работы увязывается с изучением конкретных тем.

Самостоятельная работа

Наименование разделов/тем	Виды занятий для самостоятельной работы
Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности	- усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции; - выполнение устных упражнений; - выполнение письменных упражнений и практических работ; - выполнение творческих работ; - участие в проведении научных экспериментов, исследований; - выполнение лабораторных работ; - работа в помещениях, оснащенных специальным лабораторным и иным оборудованием, компьютерами и иным оборудованием
Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ защищенности	- усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции; - выполнение устных упражнений; - выполнение письменных упражнений и практических работ; - выполнение творческих работ; - участие в проведении научных экспериментов, исследований; - выполнение лабораторных работ; - работа в помещениях, оснащенных специальным лабораторным и иным оборудованием, компьютерами и иным оборудованием

Примерные задания для самостоятельной работы

1. (Кейс-задание). Расчет рисков информационной безопасности

Описание ситуации:

Например, информационная система Компании состоит из двух ресурсов: сервера и рабочей станции, которые находятся в одной сетевой группе, т.е. физически связанны между собой.

На сервере хранятся виды информации: бухгалтерский отчет и база клиентов Компании.

На рабочей станции расположена база данных наименований товаров Компании с описанием. К серверу локальный доступ имеет группа пользователей (к первой информации – бухгалтерский отчет):

 главный бухгалтер.

К серверу удаленный доступ имеют группы пользователей (ко второй информации – база клиентов Компании):

 бухгалтер (с рабочей станции);

 финансовый директор (через глобальную сеть Интернет).

К рабочей станции локальный доступ имеет группа пользователей (к базе данных наименований товаров Компании с описанием):

 бухгалтер.

По правилам работы модели бухгалтер при удаленном доступе к серверу является группой обычных пользователей, а финансовый директор – группой авторизованных пользователей. Причем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Задание: Рассчитать риски информационной безопасности на основе модели информационных потоков.

2. (Кейс-задание).

Описание ситуации:

В одной из компаний сотрудник хранил на мобильном компьютере кон-фидуциальные сведения компании без применения средств шифрования. После работы он забрал компьютер домой и забыл его в машине, которую оставил под окнами дома, а ночью машину взломали, и компьютер был украден. Злоумышленники получили доступ к конфиденциальной информации компании и могли продать ее конкурентам. Кроме этого, на компьютере хранилась ценная информация, которая не была зарезервирована на другом носителе.

Задание.

1. Определите возможные причины инцидента и степень ответственности сотрудника.
2. Определите меры, направленные на предотвращение повторных инцидентов.

3. (Кейс-задание).

Описание ситуации.

В одной из компаний клиентке вместе со счетом на оплату выдали список других клиентов. В списке были указаны фамилии, имена, даты рождения, домашние адреса и паспортные данные.

Задание.

1. Определите возможные причины инцидента и степень ответственности сотрудника.
2. Определите меры, направленные на предотвращение повторных инцидентов.

4. Выполните следующие практическое задание:

1. Создайте точку восстановления.
2. Создайте 2-х пользователей User-1(администратор компьютера), User-2 (ограниченная запись). Для каждого пользователя потребуйте смену пароля при первом входе в систему.
3. Создайте группу Test и добавьте в нее созданных пользователей.
4. Создайте папку Test в которой разместите три файла text1.txt, text2.txt, text3.txt. Владельцем файла text1.txt сделайте пользователя User-1.
5. Для файла text2.txt настройте следующие права для пользователей и групп:

User-1 – чтение, запись, удаление, чтение разрешений, смена разрешений

User-2 – чтение и выполнение

Группа Test – изменение и запись

5. Выполните следующее практическое задание:

1. Создайте резервную копию системной информации.
2. Создайте 2-х пользователей User-1(администратор компьютера), User-2 (ограниченная запись). Для каждого пользователя потребуйте смену пароля при первом входе в систему.
3. Задайте системные параметры безопасности. Учетная запись пользователя блокируется после 3 неверных попыток ввода пароля.
4. Настройте аудит безопасности. Просмотрите журнал событий для пользователя User-2.
5. Создайте и зашифруйте файла text.txt

Раздел 6. Оценочные и методические материалы по образовательной программе (фонд оценочных средств) для проведения текущего контроля успеваемости и промежуточной аттестации

6.1. Форма промежуточной аттестации обучающегося по учебной дисциплине

В процессе освоения учебной дисциплины для оценивания сформированности требуемых компетенций используются оценочные материалы (фонды оценочных средств), представленные в таблице

Планируемые результаты, характеризующие этапы формирования компетенции	Содержание учебного материала	Примеры контрольных вопросов и заданий для оценки знаний, умений, владений
УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности		
ИУК-10.1	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ИУК-10.2	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ИУК-10.3	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
ИОПК-3.1.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ИОПК-3.2.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ИОПК-3.3.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины

6.2. Типовые вопросы и задания

Перечень вопросов

1. Основы информационной безопасности: понятие, цели и задачи.
2. Угрозы информационной безопасности и их классификация.
3. Методы и средства защиты информации.
4. Криптографические методы защиты информации.
5. Сетевые технологии и информационная безопасность.
6. Безопасность операционных систем и приложений.
7. Антивирусная защита и её роль в обеспечении информационной безопасности.
8. Управление доступом и аутентификация пользователей.
9. Резервное копирование и восстановление данных.
10. Законодательство и стандарты в области информационной безопасности.

6.3. Примерные тестовые задания

Полный банк тестовых заданий для проведения компьютерного тестирование находятся в электронной информационной образовательной среде и включает более 60 заданий из которых в случайном порядке формируется тест, состоящий из 20 заданий.

Компетенции	Типовые вопросы и задания
УК-10	1. Что из перечисленного не относится к сфере действия федерального закона «Об информации, информационных технологиях и о защите информации» направлен на? Осуществление права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации. Регулирование требований к работникам служб, работающих с информаций Формирование необходимых норм и правил, связанных с защитой детей от информации 2. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Когда риски не могут быть приняты во внимание по политическим соображениям Когда необходимые защитные меры слишком сложны Когда стоимость контрмер превышает ценность актива и потенциальные потери 3. Что из перечисленного не является целью проведения анализа рисков? Делегирование полномочий Количественная оценка воздействия потенциальных угроз Выявление рисков Определение баланса между воздействием риска и стоимостью необходимых контрмер
ОПК-3	1. В какой модели доступа для каждого объекта существует субъект-владелец, который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа 1) дискреционной модели доступа 2) модели мандатного доступа 3) ролевой модели доступа 4) модели Белла-ЛаПадулы 2. Центральным для программно-технического уровня является понятие Ответ: _____ 3. Установите соответствие описания мер противодействия угрозам безопасности группам мер безопасности А. Действующие в стране нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил.

	Б. Меры организационного характера, регламентирующие процессы функционирования АИС, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. В. Отдельные мероприятия, выполняемые на протяжении всего жизненного цикла АИС. Ориентированы прежде всего на людей, а не на технические средства. Варианты ответов: 1) Административная 2) Законодательная 3) Программно-техническая 4) Процедурная

6.4. Оценочные шкалы

6.4.1. Оценивание текущего контроля

Целью проведения текущего контроля является достижение уровня результатов обучения в соответствии с индикаторами компетенций.

Текущий контроль может представлять собой письменные индивидуальные задания состоящие из 5/3 вопросов или в форме тестовых заданий по изученным темам до проведения промежуточной аттестации. Рекомендованный планируемый период проведения текущего контроля за 6/3 недели до промежуточной аттестации.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

Шкала оценивания при письменной работе

Оценка	Критерии выставления оценки
Зачтено	Обучающийся должен: - продемонстрировать общее знание изучаемого материала; - показать общее владение понятийным аппаратом дисциплины; - уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
Не зачтено	Обучающийся демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу

6.4.2. Оценивание самостоятельной письменной работы (контрольной работы, эссе)

При оценке учитывается:
1. Правильность оформления
2. Уровень сформированности компетенций.

3. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.

4. Уровень знания фактического материала в объеме программы.

5. Логика, структура и грамотность изложения письменной работы.

6. Полнота изложения материала (раскрытие всех вопросов)

7. Использование необходимых источников.

8. Умение связать теорию с практикой.

9. Умение делать обобщения, выводы.

Шкала оценивания контрольной работы и эссе

Оценка	Критерии выставления оценки
Зачтено	Обучающийся должен: - продемонстрировать общее знание изучаемого материала; - показать общее владение понятийным аппаратом дисциплины; - уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
Не зачтено	Обучающийся демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу

6.4.3. Оценивание ответов на вопросы и выполнения заданий промежуточной аттестации

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.

2. Уровень знания фактического материала в объеме программы.

3. Логика, структура и грамотность изложения вопроса.

4. Умение связать теорию с практикой.

5. Умение делать обобщения, выводы.

Шкала оценивания на экзамене, зачете с оценкой

Оценка	Критерии выставления оценки
Отлично	Обучающийся должен: - продемонстрировать глубокое и прочное усвоение знаний программного материала; - исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; - правильно формулировать определения; - продемонстрировать умения самостоятельной работы с литературой; - уметь сделать выводы по излагаемому материалу.
Хорошо	Обучающийся должен: - продемонстрировать достаточно полное знание программного материала; - продемонстрировать знание основных теоретических понятий; - достаточно последовательно, грамотно и логически стройно излагать материал; - продемонстрировать умение ориентироваться в литературе;

	- уметь сделать достаточно обоснованные выводы по излагаемому материалу.
Удовлетворительно	Обучающийся должен: - продемонстрировать общее знание изучаемого материала; - показать общее владение понятийным аппаратом дисциплины; - уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
Неудовлетворительно	Обучающийся демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу.

Шкала оценивания на зачете

Оценка	Критерии выставления оценки
«Зачтено»	Обучающийся должен: уметь строить ответ в соответствии со структурой излагаемого вопроса; продемонстрировать прочное, достаточно полное усвоение знаний программного материала; продемонстрировать знание основных теоретических понятий; правильно формулировать определения; последовательно, грамотно и логически стройно изложить теоретический материал; продемонстрировать умения самостоятельной работы с литературой; уметь сделать достаточно обоснованные выводы по излагаемому материалу.
«Не зачтено»	Обучающийся демонстрирует: незнание значительной части программного материала; не владение понятийным аппаратом дисциплины; существенные ошибки при изложении учебного материала; неумение строить ответ в соответствии со структурой излагаемого вопроса; неумение делать выводы по излагаемому материалу.

6.4.4. Тестирование

Шкала оценивания

Оценка	Критерии выставления оценки
Отлично	Количество верных ответов в интервале: 71-100%
Хорошо	Количество верных ответов в интервале: 56-70%
Удовлетворительно	Количество верных ответов в интервале: 41-55%
Неудовлетворительно	Количество верных ответов в интервале: 0-40%
Зачтено	Количество верных ответов в интервале: 41-100%
Не зачтено	Количество верных ответов в интервале: 0-40%

6.5. Методические материалы, определяющие процедуру оценивания сформированных компетенций в соответствии с ООП

Качество знаний характеризуется способностью обучающегося точно, структурированно и уместно воспроизводить информацию, полученную в процессе освоения дисциплины, в том виде, в котором она была изложена в учебном издании или преподавателем.

Умения, как правило, формируются на занятиях семинарского типа. Задания, направленные на оценку умений, в значительной степени требуют от обучающегося проявления стереотипности мышления, т.е. способности выполнить работу по образцам, с которыми он работал в

процессе обучения. Преподаватель же оценивает своевременность и правильность выполнения задания.

Навыки можно трактовать как автоматизированные умения, развитые и закрепленные осознанным самостоятельным трудом. Навыки формируются при самостоятельном выполнении обучающимися практико-ориентированных заданий, моделирующих решение им производственных и социокультурных задач в соответствующей области профессиональной деятельности, как правило, при выполнении домашних заданий, курсовых проектов (работ), научно-исследовательских работ, прохождении практик, при работе индивидуально или в составе группы и т.д.

Устный опрос – это процедура, организованная как специальная беседа преподавателя с группой обучающихся (фронтальный опрос) или с отдельными обучающимися (индивидуальный опрос) с целью оценки сформированности у них основных понятий и усвоения учебного материала. Устный опрос может использоваться как вид контроля и метод оценивания формируемых компетенций (как и качества их формирования) в рамках самых разных форм контроля, таких как: собеседование, коллоквиум, зачет, экзамен по дисциплине. Устный опрос (УО) позволяет оценить знания и кругозор обучающегося, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. УО обладает большими возможностями воспитательного воздействия преподавателя. Воспитательная функция УО имеет ряд важных аспектов: профессионально-этический и нравственный аспекты, дидактический (систематизация материала при ответе, лучшее запоминание материала при интеллектуальной концентрации), эмоциональный (радость от успешного прохождения собеседования) и др. Обучающая функция УО состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту или экзамену. УО обладает также мотивирующей функцией: правильно организованные собеседование, коллоквиум, зачёт и экзамен могут стимулировать учебную деятельность студента, его участие в научной работе.

Тесты являются простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест может предоставлять возможность выбора из перечня ответов (один или несколько правильных ответов).

Семинарские занятия. Основное назначение семинарских занятий по дисциплине – обеспечить глубокое усвоение обучающимися материалов лекций, прививать навыки самостоятельной работы с литературой, воспитывать умение находить оптимальные решения в условиях изменяющихся отношений, формировать современное профессиональное мышление обучающихся. На семинарских занятиях преподаватель проверяет выполнение самостоятельных заданий и качество усвоения знаний, умений, определяет уровень сформированности компетенций.

Коллоквиум может служить формой не только проверки, но и повышения производительности труда студентов. На коллоквиумах обсуждаются отдельные части, разделы, темы, вопросы изучаемого курса, обычно не включаемые в тематику семинарских и других практических учебных занятий, а также рефераты, проекты и иные работы обучающихся.

Доклад, сообщение – продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Контрольная работа – средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.

Профессионально-ориентированное эссе – это средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной профессионально-ориентированной проблеме.

Реферат – продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Ситуационный анализ (кейс) – это комплексный анализ ситуации, имевший место в реальной практике профессиональной деятельности специалистов. Комплексный анализ включает в себя следующие составляющие: причинно-следственный анализ (установление причин, которые привели к возникновению данной ситуации, и следствий ее развертывания), системный анализ (определение сущностных предметно-содержательных характеристик, структуры ситуации, ее функций и др.), ценностно-мотивационный анализ (построение системы оценок ситуации, ее составляющих, выявление мотивов, установок, позиций действующих лиц); прогностический анализ (разработка перспектив развития событий по позитивному и негативному сценарию), рекомендательный анализ (выработка рекомендаций относительно поведения действующих лиц ситуации), программно-целевой анализ (разработка программ деятельности для разрешения данной ситуации).

Творческое задание – это частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения интегрировать знания различных научных областей, аргументировать собственную точку зрения, доказывать правильность своей позиции. Может выполняться в индивидуальном порядке или группой обучающихся.

Деловая и/или ролевая игра – совместная деятельность группы обучающихся и преподавателя под управлением преподавателя с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.

«Круглый стол», дискуссия – интерактивные оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Занятие может проводить по традиционной (контактной) технологии, либо с использованием телекоммуникационных технологий.

Проект – конечный профессионально-ориентированный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.

Раздел 7. Методические указания для обучающихся по основанию дисциплины

Освоение обучающимся учебной дисциплины предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы учебной дисциплины. Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе Университета. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку: знакомит с новым учебным материалом; разъясняет учебные элементы, трудные для понимания; систематизирует учебный материал; ориентирует в учебном процессе.

С этой целью: внимательно прочитайте материал предыдущей лекции; ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции; внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради; запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции; постарайтесь уяснить место изучаемой темы в своей подготовке; узнайте тему предсто-

ящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия.

Самостоятельная работа. Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала.

Подготовка к зачету, экзамену. К зачету, экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты. При подготовке к зачету обратите внимание на защиту практических заданий на основе теоретического материала. При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

7.1. Методические рекомендации по написанию эссе

Эссе (от французского essai – опыт, набросок) – жанр научно-публицистической литературы, сочетающей подчеркнуто-индивидуальную позицию автора по конкретной проблеме.

Главными особенностями, которые характеризуют эссе, являются следующие положения:

- собственная позиция обязательно должна быть аргументирована и подкреплена ссылками на источники, авторитетные точки зрениями и базироваться на фундаментальной науке. Небольшой объем (4–6 страниц), с оформленным списком литературы и сносками на ее использование;
- стиль изложения – научно-исследовательский, требующий четкой, последовательной и логичной системы доказательств; может отличаться образностью, оригинальностью, афористичностью, свободным лексическим составом языка;
- исследование ограничивается четкой, лаконичной проблемой с выявлением противоречий и разрешением этих противоречий в данной работе.

7.2. Методические рекомендации по использованию кейсов

Кейс-метод (Case study) – метод анализа реальной ситуации, описание которой одновременно отражает не только какую-либо практическую проблему, но и актуализирует определенный комплекс знаний, который необходимо усвоить при разрешении данной проблемы. При этом сама проблема не имеет однозначных решений.

Кейс как метод оценки компетенций должен удовлетворять следующим требованиям:

– соответствовать четко поставленной цели создания;

– иметь междисциплинарный характер;

– иметь достаточный объем первичных и статистических данных;

– иметь соответствующий уровень сложности, иллюстрировать типичные ситуации, иметь актуальную проблему, позволяющую применить разнообразные методы анализа при поиске решения, иметь несколько решений.

Кейс-метод оказывает содействие развитию умения решать проблемы с учетом конкретных условий и при наличии фактической информации. Он развивает такие квалификационные характеристики, как способность к проведению анализа и диагностики проблем, умение четко формулировать и высказывать свою позицию, умение общаться, дискутировать, воспринимать и оценивать информацию, которая поступает в вербальной и невербальной форме.

7.3. Требования к компетентностно-ориентированным заданиям для демонстрации выполнения профессиональных задач

Компетентностно-ориентированное задание – это всегда практическое задание, выполнение которого нацелено на демонстрирование доказательств наличия у обучающихся общекультур-

ных, общепрофессиональных и профессиональных компетенций, знаний, умений, необходимых для будущей профессиональной деятельности.

Компетентностно-ориентированные задания бывают разных видов:

- направленные на подготовку конкретного практико-ориентированного продукта (анализ документов, текстов, критика, разработка схем и др.);
- аналитического и диагностического характера, направленные на анализ различных аспектов и проблем;
- связанные с выполнением основных профессиональных функций (выполнение конкретных действий в рамках вида профессиональной деятельности, например, формулирование целей миссии, и т. п.).

Раздел 8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература[1]

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

2. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/10677.html

Дополнительная литература[2]

3. Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/118458.html

4. Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: интернет-ресурсы, современные профессиональные базы данных, информационные справочные системы

Интернет-ресурсы

URL: https://www.IPRsmart hop.ru/ – электронно-библиотечная система IPRsmart .

Информационно-справочные и поисковые системы

Справочная правовая система «КонсультантПлюс»: http://www.con-sultant.ru

Современные профессиональные базы данных

URL:http://www.edu.ru/ – библиотека федерального портала «Российское образование»

URL:http://www.prlib.ru – Президентская библиотека

URL:http://www.rusneb.ru – Национальная электронная библиотека

URL:http://elibrary.rsl.ru/ – сайт Российской государственной библиотеки (раздел «Электронная библиотека»)

URL:http://elib.gnpbu.ru/ – сайт Научной педагогической электронной библиотеки им. К.Д. Ушинского

---

[1] Из ЭБС

[2] Из ЭБС

Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Комплект лицензионного программного обеспечения

Microsoft Open Value Subscription для решений Education Solutions № Tr000544893 от 21.10.2020 г. MDE Windows, Microsoft Office и Office Web Apps. (срок действия до 01.11.2023 г.)

Антивирусное программное обеспечение ESET NOD32 Antivirus Business Edition договор № ИС00-006348 от 14.10.2022 г. (срок действия до 13.10.2025 г.)

Программное обеспечение «Мираполис» система вебинаров - Лицензионный договор 244/09/16-к от 15.09.2016 (Спецификация к Лицензионному договору 244/09/16-к от 15.09.2016, от 11.05.2022 г.) (срок действия до 10.07.2023 г.)

Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)

Информационная система «ПервыйБит» сублицензионный оговор от 06.11.2015 г. №009/061115/003 (бессрочно)

Система тестирования Indigo лицензионное соглашение (Договор) от 08.11.2018 г. №Д-54792 (бессрочно)

Информационно-поисковая система «Консультант Плюс» - договор об информационно поддержке от 26.12.2014, (бессрочно)

Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2021 г. №8234/21С (срок действия до 31.08.2024 г.)

Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2022 от 12.01.2022 г. (срок действия до 27.01.2024 г.)

Свободно распространяемое программное обеспечение

Комплект онлайн сервисов GNU ImageManipulationProgram, свободно распространяемо программное обеспечение

Веб-браузер, Google Ghrome, свободное ПО, ежегодно обновляемое ПО.

Пакет офисных приложений, Office 2016, лицензионное соглашение - Договор №Tr000544893 от 21/10/2020 – 3 года

Пакет офисных приложений, OpenOffice, свободное ПО, ежегодно обновляемое ПО

Просмотр файлов в формате PDF, Adobe Reader, свободно распространяемое ПО, ежегодно обновляемое ПО

Просмотр файлов в формате DJV, WinDjView, свободное ПО, ежегодно обновляемое ПО

Файловый архиватор, 7 Zip, свободное ПО, ежегодно обновляемое ПО

Файловый менеджер, Far, свободно распространяемое ПО, ежегодно обновляемое ПО

Anaconda: дистрибутив языков программирования Python и R.

Программное обеспечение отечественного производства:

Программное обеспечение «Мираполис» система вебинаров - Лицензионный договор 244/09/16-к от 15.09.2016 (Спецификация к Лицензионному договору 244/09/16-к от 15.09.2016, от 11.05.2022 г.) (срок действия до 10.07.2023 г.)

Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)

Информационная система «ПервыйБит» сублицензионный договор от 06.11.2015 г. №009/061115/003 (бессрочно)

Система тестирования Indigo лицензионное соглашение (Договор) от 08.11.2018 г. №Д-54792 (бессрочно)

Информационно-поисковая система «Консультант Плюс» - договор МИ-ВИП-79717-56/2022 от 23.12.2021 (срок действия до 31.12.2022 г.)

Информационно-поисковая система «Консультант Плюс» - договор об информационно поддержке от 26.12.2014, (бессрочно)

Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2021 г. №8234/21С (срок действия до 31.08.2024 г.)

Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2022 от 12.01.2022 г. (срок действия до 27.01.2024 г.)

Раздел 9. Материально-техническое обеспечение образовательного процесса

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Оборудование: специализированная мебель (мебель аудиторная (11 столов, 11 стульев, доска аудиторная), стол преподавателя, стул преподавателя. Технические средства обучения: персональный компьютер -11; мультимедийное оборудование (проектор, экран).
Помещение для самостоятельной работы	Специализированная мебель (10 столов, 10 стульев), персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета