Образовательная автономная некоммерческая организация
высшего образования
«Московский психолого-социальный университет»

Принято:
Решение Ученого совета
От «22» марта 2022 г.
Протокол №5

Факультет экономики и права

Рабочая программа учебной дисциплины

Информационная безопасность

Направление подготовки
38.03.04 Государственное, муниципальное и корпоративное управление

Направленность (профиль) подготовки
Региональное управление

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная, очно-заочная, заочная

Составитель программы:

Судариков Г.В., к.э.н., доцент
кафедры гуманитарных и естественнонаучных дисциплин

Москва, 2022

СОДЕРЖАНИЕ

Программа составлена

1. Аннотация к дисциплине

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.04 Государственное, муниципальное и корпоративное управление (уровень бакалавриата), утвержденного приказом Министерства науки и высшего образования РФ от 12.08. 2020 г. N 954.

Рабочая программа содержит обязательные для изучения темы по дисциплине «Информационная безопасность». Дисциплина дает целостное представление о навыках сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций, основах криптографии и основных алгоритмов шифрования, использовании алгоритмов шифрования для информационной безопасности.

Место дисциплины в структуре основной профессиональной образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока1 учебных планов по направлению подготовки 38.03.04 Государственное, муниципальное и корпоративное управление, уровень бакалавриата.

Дисциплина изучается на 1 курсе, в 1 семестре очной, очно-заочной и заочной форм обучения, форма контроля – зачет.

Цель изучения дисциплины:

Владеть навыками анализа социально значимых проблем и процессов в сфере управления, техникой принятия управленческих решений и действий с позиции социальной ответственности

Задачи:

- Основы криптографии и основных алгоритмов шифрования;
- Использовать алгоритмы шифрования для информационной безопасности;
- навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

ОПК-5 - Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг;.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Процесс изучения дисциплины направлен на формирование компетенций, предусмотренных ФГОС ВО по направлению подготовки 38.03.04 Государственное, муниципальное и корпоративное управление (уровень бакалавриата) и на основе профессионального стандарта «Специалист по Государственному, муниципальному и корпоративному управлению», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 18 августа 2018 г. N 544н, соотнесённого

с федеральным государственным образовательным стандартом по указанному направлению подготовки.

Код компетенции	Результаты освоения ОПОП (содержание компетенций)	Индикаторы достижения компетенций	Формы образовательной деятельности, способствующие формированию и развитию компетенции
ОПК-5	Способность на основе сбора и анализа исходных данных, описание экономических процессов и явлений рассчитать основные социально-экономические показатели на макро - и микроуровне, строить стандартные теоретические и эконометрические модели.	**ОПК-5.1 Знает** источники, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов	Контактная работа: Лекции Практические занятия Контрольная работа
		ОПК-5.2. Знает Законодательные и правовые основы защиты компьютерной информации информационных технологий.	
		ОПК-5.3. Умеет выполнять операции над многочленами. Деление многочленов. Наибольший общий делитель двух многочленов. Алгоритм Евклида. Корни многочлена.	
		ОПК-5.4. Умеет применять криптографические модели.	
		ОПК-5.5. Умеет использовать **с**имметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ	
		ОПК-5.6. Владеет стандартными алгоритмы шифрования.	
		ОПК-5.7. Владеет методами идентификации и проверки подлинности пользователей компьютерных систем	

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины (модуля) составляет 2 зачетные единицы, 72 часа.

3.1. Объем учебной дисциплины по видам учебных занятий (в часах)

Объём дисциплины	Всего часов		
	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость дисциплины	72	72	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий)	32	20	8
Аудиторная работа (всего):	32	20	8
в том числе:			
лекции	8	8	4
лабораторные работы			
семинары, практические занятия	24	12	4
Внеаудиторная работа (всего):			
Самостоятельная работа обучающихся (всего)	40	52	60
Вид промежуточной аттестации обучающегося (зачёт, контрольная работа, экзамен)			4

4. Содержание учебной дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы учебной дисциплины и трудоемкость по видам учебных занятий (в академических часах)

Для очной формы обучения

№ п/п	Разделы и темы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)							Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации *(по семестрам)*
			ВСЕГО	Из них аудиторные занятия			Самостоятельная работа	Контрольная работа	Курсовая работа	
				Лекции	.Практикум. Лаборатор	Практическ.занятия /семинары				
1	Защита информации. Основные понятия и определения	1	8	2		2	4			Опрос, тестирование
2	Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных	1	6			2	4			Опрос, тестирование

	вирусов. Проблемы защиты информации в ИС										
3	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС	1	6			2		4			Опрос, тестирование
4	Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности	1	6			2		4			Опрос, тестирование
5	Криптографически е модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ	1	10	2		4		4			Опрос, тестирование
6	Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем	1	8			4		4			Опрос, тестирование
7	Методы идентификации и проверки подлинности пользователей компьютерных систем	1	8	2		2		4			Опрос, тестирование
8	Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet	1	6			2		4			Опрос, тестирование

9	Защита информации в компьютерных сетях, антивирусная защита	1	8	2		2		4			Опрос, тестирование
10	Требования к системам информационной защиты ИС	1	6			2		4			Опрос, тестирование
	Зачет										Билеты к зачету
	ИТОГО		**72**	**8**		**24**		**40**			**Зачет**

Для очно-заочной формы обучения

№ п/п	**Разделы и темы дисциплины**	**Семестр**	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)**							**Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации** ***(по семестрам)***
			ВСЕГО	**Из них аудиторные занятия**				**Самостоятельная работа**	**Контрольная работа**	**Курсовая работа**	
				Лекции	**.Практикум. Лаборатор**	**Практическ.занятия /семинары**					
1	Защита информации. Основные понятия и определения	1	8	2				6			Опрос, тестирование
2	Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС	1	8			2		6			Опрос, тестирование
3	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание	1	8			2		6			Опрос, тестирование

	основных документов предприятия по обеспечению защиты компьютерной информации в ИС										
4	Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности	1	6			2		4			Опрос, тестирование
5	Криптографически е модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ	1	8	2				6			Опрос, тестирование
6	Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем	1	6			2		4			Опрос, тестирование
7	Методы идентификации и проверки подлинности пользователей компьютерных систем	1	8	2				6			Опрос, тестирование
8	Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet	1	6			2		4			Опрос, тестирование
9	Защита информации в компьютерных сетях, антивирусная защита	1	6	2				4			Опрос, тестирование
10	Требования к системам информационной защиты ИС	1	6			2		4			Опрос, тестирование
	Зачет										Билеты к зачету
	ИТОГО		**72**	**8**		**12**		**52**			**Зачет**

Для заочной формы обучения

№ п/п	Разделы и темы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)							Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации *(по семестрам)*
			ВСЕГО	Из них аудиторные занятия			Самостоятельная работа	Контрольная работа	Курсовая работа	
				Лекции	.Практикум. Лаборатор	Практическ.занятия /семинары				
1	Защита информации. Основные понятия и определения	1	8	2			6			Опрос, тестирование
2	Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС	1	8			2	6			Опрос, тестирование
3	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС	1	6				6			Опрос, тестирование
4	Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности	1	6				6			Опрос, тестирование
5	Криптографически	1	8	2			6			Опрос,

	е модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ										тестирование
6	Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем	1	8			2		6			Опрос, тестирование
7	Методы идентификации и проверки подлинности пользователей компьютерных систем	1	6					6			Опрос, тестирование
8	Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet	1	6					6			Опрос, тестирование
9	Защита информации в компьютерных сетях, антивирусная защита	1	6					6			Опрос, тестирование
10	Требования к системам информационной защиты ИС	1	6					6			Опрос, тестирование
	Зачет		**4**								Билеты к зачету
	ИТОГО		**72**	**4**		**4**		**60**			**Зачет**

4.2 Содержание дисциплины, структурированное по разделам

Тема 1. ***Защита информации. Основные понятия и определения***

Содержание лекционного курса

Информационные ресурсы и документирование информации. Безопасность информационных ресурсов. Государственные информационные ресурсы. Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования. Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

Содержание практических занятий

1. Информационные ресурсы и документирование информации.
2. Государственные информационные ресурсы.
3. Государственные информационные ресурсы.

Тема 2. **Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС**

Содержание лекционного курса

Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС. Классификация угроз и меры по обеспечению сохранности информации в ИС. Классификация рисков и основные задачи обеспечения безопасности информации в ИС. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты.

Содержание практических занятий

1. Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов.
2. Классификация угроз и меры по обеспечению сохранности информации в ИС.
3. Интеграция систем защиты.

Тема 3. **Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС**

Содержание лекционного курса

Законодательная, нормативно-методическая и научная база систем защиты информации. Требования к содержанию нормативно-методических документов по защите информации. Российское законодательство по защите информационных технологий. Политика безопасности. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС.

Содержание практических занятий

1. Требования к содержанию нормативно-методических документов по защите информации.
2. Политика безопасности. Политика информационной безопасности..
3. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС.

Тема 4. **Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности**

Содержание лекционного курса

Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Доктрина информационной безопасности Российской Федерации. Классификация защищенности средств вычислительной техники. Международные стандарты по защите информации. Стандарты безопасности в Интернете.

Содержание практических занятий

1. Доктрина информационной безопасности Российской Федерации.
2. Классификация защищенности средств вычислительной техники.
3. Международные стандарты по защите информации.

Тема 5. **Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ**.

Содержание лекционного курса

Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Методы генерации псевдослучайных последовательностей чисел.

Содержание практических занятий

1. Криптографические модели.
2. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС.

Тема 6. **Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем.**

Содержание лекционного курса

Стандартные алгоритмы шифрования. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов. Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных К5А Безопасность и быстродействие криптосистемы К5А, Изучение американского стандарта шифрования данных ОЕ5. Основные режимы работы алгоритма ВЕ5. Отечественный стандарт шифрования данных.

Содержание практических занятий

1. Стандартные алгоритмы шифрования.
2. Концепция криптосистемы с открытым ключом.

Тема 7. **Методы идентификации и проверки подлинности пользователей компьютерных систем**.

Содержание лекционного курса

Основные понятия и концепции идентификации и проверки подлинности пользователей компьютерных систем. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы цифровой подписи. Отечественный стандарт цифровой подписи. Биометрические средства идентификации пользователей.

Содержание практических занятий

1. Идентификация и механизмы подтверждения подлинности пользователя.
2. Взаимная проверка подлинности пользователей.

Тема 8. **Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet**.

Содержание лекционного курса

Многоуровневая защита корпоративных сетей. Режим функционирования

межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Internet.

Содержание практических занятий

1. Многоуровневая защита корпоративных сетей.
2. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы.

Тема 9. **Защита информации в компьютерных сетях, антивирусная защита.**

Содержание лекционного курса

Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействия. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации Internet.

Содержание практических занятий

1. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки.
2. Методы перехвата и навязывания информации. Методы внедрения программных закладок.

Тема 10. **Требования к системам информационной защиты ИС**

Содержание лекционного курса

Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита информационной безопасности ИС и предприятия в целом.

Содержание практических занятий

1. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.
2. Требования по применению способов, методов и средств защиты информации.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающихся при изучении курса «Информационная безопасность» предполагает, в первую очередь, работу с основной и дополнительной литературой. Результатами этой работы становятся выступления на практических занятиях, участие в обсуждении.

Методика самостоятельной работы предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей студентов.

Время и место самостоятельной работы выбираются студентами по своему усмотрению с учетом рекомендаций преподавателя.

Самостоятельную работу над дисциплиной «Информационная безопасность» следует начинать с изучения рабочей программы учебной дисциплины, которая содержит основные требования к знаниям, умениям и навыкам обучаемых. Обязательно следует вспомнить рекомендации преподавателя, данные в ходе лекционных и практических занятий. Затем – приступать к изучению отдельных тем в порядке, предусмотренном рабочей программой.

Получив представление об основном содержании раздела, темы, необходимо изучить материал с помощью учебников, указанных в разделе 7 указанной программы. Целесообразно составить краткий конспект или схему, отображающую смысл и связи основных понятий данного раздела и включенных в него тем. Затем, как показывает опыт, полезно изучить выдержки из первоисточников. При желании можно составить их краткий конспект. Обязательно следует записывать возникшие вопросы, на которые не удалось ответить самостоятельно.

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Учебно-методическое обеспечение	Форма контроля
Тема 1. Защита информации. Основные понятия и определения	Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос
Тема 2. Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС	Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации	Литература к теме, работа с интернет источниками	Тестирование
Тема 3 Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС	Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос
Тема 4. Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности	Международные стандарты по защите информации. Стандарты безопасности в Интернете.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Тестирование
Тема 5. Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ	Блочные и поточные шифры. Методы генерации псевдослучайных последовательностей чисел.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос
Тема 6. Стандартные алгоритмы	Основные режимы работы алгоритма	Работа в библиотеке,	Литература к теме,	Тестирование

шифрования. Безопасность и быстродействие криптосистем.	BE5. Отечественный стандарт шифрования данных.	включая ЭБС. Подготовка доклада-презентации.	работа с интернет источниками	
Тема 7. Методы идентификации и проверки подлинности пользователей компьютерных систем	Отечественный стандарт цифровой подписи. Биометрические средства идентификации пользователей.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос
Тема 8. Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet	Защита компьютерных систем от удаленных атак через сеть Internet.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Тестирование
Тема 9. Защита информации в компьютерных сетях, антивирусная защита	Понятие изолированной программной среды. Рекомендации по защите информации Internet.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос
Тема 10. Требования к системам информационной защиты ИС	Организация аудита информационной безопасности ИС и предприятия в целом.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Тестирование

6. Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине «Линейная алгебра»

6.1. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Шкала и критерии оценки, балл	Критерии оценивания компетенции
1.	Опрос	Сбор первичной информации по выяснению уровня усвоения пройденного материала	«Зачтено» - если обучающийся демонстрирует знание материала по разделу, основанные на знакомстве с обязательной литературой и современными публикациями; дает логичные, аргументированные ответы на поставленные вопросы. Также оценка «зачтено» ставится, если обучающимся допущены незначительные неточности в ответах, которые он исправляет путем наводящих вопросов со стороны преподавателя. «Не зачтено» - имеются существенные пробелы в знании основного материала по разделу, а также допущены принципиальные ошибки при изложении материала.	**ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4, ОПК-5.5, ОПК-5.6, ОПК-5.7**
2	Тестирование	Тестирование можно проводить в форме: • компьютерного тестирования, т.е. компьютер произвольно выбирает вопросы из базы данных по степени сложности; • письменных ответов, т.е. преподаватель задает вопрос и дает несколько вариантов ответа, а студент на отдельном листе записывает номера вопросов и номера соответствующих ответов	«отлично» - процент правильных ответов 80-100%; «хорошо» - процент правильных ответов 65-79,9%; «удовлетворительно» - процент правильных ответов 50-64,9%; «неудовлетворительно» - процент правильных ответов менее 50%.	**ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4, ОПК-5.5, ОПК-5.6, ОПК-5.7**

6.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы освоения дисциплины

№	Форма контроля/ коды оцениваемых компетенций	Процедура оценивания	Шкала и критерии оценки, балл
1.	**Зачёт - ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4, ОПК-5.5, ОПК-5.6, ОПК-5.7**	на устном зачете: правильность ответов на вопросы (верное, четкое, достаточно глубокое изложение идей, понятий, фактов, нормативно-правового материла и т.п.); правильное решение задачи; полнота и лаконичность ответа; степень использования и понимания научных и нормативных источников; умение связывать теорию с практикой; логика и аргументированность изложения материала; грамотное комментирование, приведение примеров, аналогий; культура речи; на письменном зачете (тестирование): правильные ответы на вопросы письменного теста (задания).	«зачтено» - правильность ответов на вопросы билета (верное, четкое, достаточно глубокое изложение идей, понятий, фактов, нормативно-правового материла и т.п.) и правильное разрешение задачи; полнота и лаконичность ответа; степень использования и понимания научных и нормативных источников; умение связывать теорию с практикой; логика и аргументированность изложения материала; грамотное комментирование, приведение примеров, аналогий; культура речи; «не зачтено» предполагает, что обучающимся либо не дан ответ на вопрос и (или) не решена предложенная задача, либо обучающийся не знает основных понятий, не может определить предмет дисциплины.
2.	**Тестирование (на зачёте) - ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4, ОПК-5.5, ОПК-5.6, ОПК-5.7**	Полнота знаний теоретического контролируемого материала. Количество правильных ответов	«отлично» - процент правильных ответов 80-100%; «хорошо» - процент правильных ответов 65-79,9%; «удовлетворительно» - процент правильных ответов 50-64,9%; «неудовлетворительно» - процент правильных ответов менее 50%.

6.3. Типовые контрольные задания или иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

6.3.1. Типовые задания для проведения текущего контроля обучающихся

6.3.1.1. Задания для устного опроса на семинарских, практических занятиях

1. Информационные ресурсы и документирование информации?
2. Государственные информационные ресурсы?
3. Права на доступ к информации?
4. Вычислительные сети и защита информации?
5. Компьютерные преступления и особенности их расследования?
6. Проблемы защиты информации в ИС?
7. Классификация рисков и основные задачи обеспечения безопасности информации в ИС?
8. Защита локальных сетей и операционных систем?
9. Интеграция систем защиты?
10. Законодательная, нормативно-методическая и научная база систем защиты информации?
11. Российское законодательство по защите информационных технологий?
12. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС?
13. Национальные интересы Российской Федерации в информационной сфере и их обеспечение?
14. Классификация защищенности средств вычислительной техники?
15. Международные стандарты по защите информации?
16. Криптографические модели?
17. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС?
18. Режим простой замены. Режим гаммирования?
19. Блочные и поточные шифры?
20. Шифры перестановки. Шифрующие таблицы?
21. Концепция криптосистемы с открытым ключом?
22. Безопасность и быстродействие криптосистемы К5А?
23. Изучение американского стандарта шифрования данных ОЕ5?
24. Идентификация и механизмы подтверждения подлинности пользователя?
25. Протоколы идентификации с нулевой передачей знаний?
26. Отечественный стандарт цифровой подписи?
27. Маршрутизаторы. Шлюзы сетевого уровня?
28. Программные методы защиты информации?
29. Защита компьютерных систем от удаленных атак через сеть Inertrnet?
30. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению?

6.3.1.2. Типовые виды тестовых вопросов

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
Разработка аппаратных средств обеспечения правовых данных
Разработка и установка во всех компьютерных правовых сетях журналов учета действий
Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы

Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса
сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
Установление регламента, аудит системы, выявление рисков
Установка новых офисных приложений, смена хостинг-компании
Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
Усиления защищенности самого незащищенного звена сети (системы)
Перехода в безопасное состояние работы сети, системы
Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Одноуровневой защиты сети, системы
Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
Компьютерный сбой
Логические закладки («мины»)
Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
Секретность ключа определена секретностью открытого сообщения
Секретность информации определена скоростью передачи данных
Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
Электронно-цифровой преобразователь
Электронно-цифровая подпись
Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
Покупка нелицензионного ПО
Ошибки эксплуатации и неумышленного изменения режима работы системы
Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
Слабый трафик, информационный обман, вирусы в интернет
Вирусы в сети, логические мины (закладки), информационный перехват
Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
Потерей данных в системе
Изменением формы информации
Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении

информационной безопасности являются:
Целостность
Доступность
Актуальность1

23) Угроза информационной системе (компьютерной сети) – это:
Вероятное событие
Детерминированное (всегда определенное) событие
Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
Регламентированной
Правовой
Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:
Программные, технические, организационные, технологические
Серверные, клиентские, спутниковые, наземные
Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
Владелец сети
Администратор сети
Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
Руководств, требований обеспечения необходимого уровня безопасности
Инструкций, алгоритмов поведения пользователя в сети
Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций

6.3.2. Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине «Линейная алгебра» проводится в форме зачета и экзамена.

1. Понятие информации, ее свойства и виды. Правовая информация.
2. Понятие информационной безопасности
3. Компьютерные вирусы. Происхождение, классификация, степень опасности, внешнее проявление заражения.
4. Средства и методы борьбы с компьютерными вирусами: контроль оперативной памяти, носителей информации; восстановление пораженных файлов, резервное копирование данных и программ.

5. Компьютерные вирусы. Меры профилактики и методы борьбы.
6. Программы-антивирусы.
7. Защита документов MS OFFICE при помощи пользовательского пароля.
8. Защита информации в компьютере. Программные и аппаратные средства.
9. Архивация с паролем.
10. Компьютерные сети. Понятие, классификация.
11. Глобальная сеть INTERNET.
12. Аппаратное обеспечение сетевых технологий.
13. Программное обеспечение сетевых технологий.
14. Локальные и глобальные компьютерные сети.
15. Топология локальной сети. Виды топологий.
16. Основные положения доктрины информационной безопасности.
17. Принципы защиты информации.
18. Программные методы защиты информации.
19. Криптографическая защита.
20. Организационно-технические методы защиты информации.
21. Биометрические устройства.
22. Способы и средства сокрытия информации.
23. Поиск информации на магнитных носителях.
24. Классификация средств защиты информации
25. Классы защищенности автоматизированных систем от несанкционированного доступа к информации; тр
26. Классификация автоматизированных систем по условиям функционирования и степени защищенности
27. Содержание и основные этапы проведения работ по защите объектов электронно-вычислительной техники.
28. Аппаратные и программные способы ограничения доступа и защиты информации.

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося. Все виды текущего контроля осуществляются на практических занятиях. Исключение составляет устный опрос, который может проводиться в начале или конце лекции в течение 15-20 мин. с целью закрепления знаний терминологии по дисциплине. При оценке компетенций принимается во внимание формирование профессионального мировоззрения, определенного уровня включённости в занятия, рефлексивные навыки, владение изучаемым материалом.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки.

2. Многоступенчатость: оценка (как преподавателем, так и обучающимися группы) и самооценка обучающегося, обсуждение результатов и комплекс мер по устранению недостатков.

3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

4. Соблюдение последовательности проведения оценки.

Текущая аттестация обучающихся. Текущая аттестация обучающихся по дисциплине «Информационная безопасность» проводится в соответствии с локальными

нормативными актами ОАНО ВО МПСУ и является обязательной.

Текущая аттестация по дисциплине «Информационная безопасность» проводится в форме опроса и контрольных мероприятий по оцениванию фактических результатов обучения обучающихся и осуществляется преподавателем дисциплины.

Объектами оценивания выступают:

1. учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);
2. степень усвоения теоретических знаний в качестве «ключей анализа»;
3. уровень овладения практическими умениями и навыками по всем видам учебной работы;
4. результаты самостоятельной работы (изучение книг из списка основной и дополнительной литературы).

Активность обучающегося на занятиях оценивается на основе выполненных обучающимся работ и заданий, предусмотренных данной рабочей программой дисциплины.

Кроме того, оценивание обучающегося проводится на текущем контроле по дисциплине. Оценивание обучающегося на контрольной неделе проводится преподавателем независимо от наличия или отсутствия обучающегося (по уважительной или неуважительной причине) на занятии. Оценка носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период.

Оценивание обучающегося носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период с выставлением оценок в ведомости.

Промежуточная аттестация обучающихся. Промежуточная аттестация обучающихся по дисциплине «Информационная безопасность» проводится в соответствии с локальными нормативными актами ОАНО ВО «МПСУ» и является обязательной.

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в соответствии с учебным планом в 1-м семестре для очной, очно-заочной и заочной форм обучения в виде зачета в 1-м семестре в период зачетно-экзаменационной сессии в соответствии с графиком проведения.

Обучающиеся допускаются к зачету и экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных программой дисциплины.

Оценка знаний обучающегося на зачете определяется его учебными достижениями в семестровый период и результатами текущего контроля знаний и выполнением им заданий.

Знания умения, навыки обучающегося на зачете оцениваются как: «зачтено» / «не зачтено».

Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения учебной дисциплины

а) Основная учебная литература

1. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское

образование, 2018. — 54 c. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/77320.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей

2. 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 c. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей
3. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 c. — ISBN 978-5-906-17271-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/33857.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей
4. Горбенко, А. О. Основы информационной безопасности (введение в профессию) : учебное пособие / А. О. Горбенко. — Санкт-Петербург : Интермедия, 2017. — 335 c. — ISBN 978-5-4383-0136-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/66797.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей
5. Информационная безопасность при управлении техническими системами : учебное пособие / С. А. Баркалов, О. М. Барсуков, В. Е. Белоусов, К. В. Славнов. — Санкт-Петербург : Интермедия, 2017. — 528 c. — ISBN 978-5-4383-0133-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/68589.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей
6. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 82 c. — ISBN 978-5-4487-0300-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/77319.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей

б) Дополнительная учебная литература

1. 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 c. — ISBN 978-5-374-00301-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/10677.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей
2. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-

библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89453.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей
3. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102070.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей
4. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 242 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/62945.html (дата обращения: 08.06.2021). — Режим доступа: для авторизир. пользователей

8. Методические указания для обучающихся по освоению дисциплины

Вид деятельности	Методические указания по организации деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Прослушивание аудио- и видеозаписей по заданной теме, решение расчетно-графических заданий, решение задач по алгоритму и др.
Индивидуальные задания	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.
Самостоятельная работа	Самостоятельная работа проводится с целью: систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; углубления и расширения теоретических знаний студентов; формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования

	профессиональных компетенций; развитию исследовательских умений обучающихся. Формы и виды самостоятельной работы: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; составление аннотаций к прочитанным литературным источникам; составление рецензий и отзывов на прочитанный материал; составление обзора публикаций по теме; составление и разработка терминологического словаря; составление хронологической таблицы; составление библиографии (библиографической картотеки); подготовка к различным формам текущей и промежуточной аттестации (к тестированию, зачету, экзамену); выполнение домашних контрольных работ; самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, тесты; выполнение творческих заданий). Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов образовательного учреждения: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов, лабораторий и зала кодификации; компьютерные классы с возможностью работы в сети Интернет; аудитории (классы) для консультационной деятельности; учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы студентов, и иные методические материалы. Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения обучающимися внеаудиторной самостоятельной работы и при необходимости преподаватель может проводить индивидуальные и групповые консультации. Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся. Контроль самостоятельной работы предусматривает: • соотнесение содержания контроля с целями обучения; объективность контроля; • валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить); • дифференциацию контрольно-измерительных материалов. Формы контроля самостоятельной работы: • просмотр и проверка выполнения самостоятельной работы преподавателем; • организация самопроверки, • взаимопроверки выполненного задания в группе; обсуждение результатов выполненной работы на занятии; • проведение письменного опроса; • проведение устного опроса; • организация и проведение индивидуального собеседования; организация и проведение собеседования с группой; • защита отчетов о проделанной работе.
Опрос	Опрос - это средство контроля, организованное как специальная

	беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выявление объема знаний по определенному разделу, теме, проблеме и т.п. Проблематика, выносимая на опрос определена в заданиях для самостоятельной работы обучающегося, а также может определяться преподавателем, ведущим семинарские занятия. Во время проведения опроса обучающийся должен уметь обсудить с преподавателем соответствующую проблематику на уровне диалога.
Контрольная работа	Контрольная работа – оригинальное сочинение небольшого размера, в котором излагаются конкретные результаты изучения обучающимся дисциплины (результаты собственного исследования по конкретной теме). В ходе написания контрольной работы обучающийся приобретает навыки самостоятельной работы с научной, учебной и специальной литературой, учится анализировать источники и грамотно излагать свои мысли. Выполнение контрольной работы включает ряд этапов: • выбор темы и подбор научных источников; • изучение научной литературы, анализ и обобщение материалов по проблеме исследования; • формулирование основных положений и выводов; • оформление контрольной работы. Оформление является завершающим этапом контрольной работы. Выбор темы и подбор источников должен быть согласован с научным руководителем, ведущим предмет. На основе собранного материала уточняется структура, содержание и объем контрольной работы. Технические требования к работе: объем 10-12 страниц машинописного текста, отпечатанного через 2 интервала (или в рукописной форме – 12-15 страниц). Контрольная работа должна иметь: титульный лист, содержащий: название работы, Ф.И.О. автора и научного руководителя, название факультета, курса, год и место написания, содержание на отдельной странице, нумерацию страниц. Структура контрольной работы включает: заголовок, введение, основную часть (изложение двух вопросов), заключение, список использованной литературы. Заголовок (название) отражает тему данного сочинения и соответствует содержанию. Введение (вводная часть) должно быть кратким и точным. В нем обосновывается выбор темы, формулируется цель работы. Основная часть делится на главы в соответствии с задачами работы. Дается определение понятиям исследуемых явлений и процессов, раскрываются их сущность и особенности. В небольшой работе части могут не выделять, но каждая новая мысль оформляется в новый абзац. Заключение имеет форму выводов, соответствующих этапам исследования, или форму резюме.
Подготовка к зачёту	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рабочую программу дисциплины, нормативную, основную и дополнительную учебную литературу. Основное в подготовке к сдаче зачета - это повторение всего материала дисциплины. При подготовке к сдаче зачета обучающийся весь объем работы должен распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнение намеченной работы. В период подготовки к зачету обучающийся вновь обращается к уже изученному (пройденному) учебному материалу. Подготовка обучающегося к зачету включает в себя три этапа: самостоятельная работа в течение семестра; непосредственная подготовка в дни, предшествующие зачету по темам курса; подготовка к ответу на задания, содержащиеся в вопросах (тестах) зачета. Зачет проводится

	по вопросам (тестам), охватывающим весь пройденный материал дисциплины, включая вопросы, отведенные для самостоятельного изучения.

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для осуществления образовательного процесса по дисциплине «Информационная безопасность» необходимо использование следующих помещений:

Материально-техническое обеспечение дисциплины включает в себя:
учебная аудитория для проведения учебных занятий, оснащенная оборудованием и техническими средствами обучения (мебель аудиторная (столы, стулья, доска), стол, стул преподавателя) и технические средства обучения (персональный компьютер; мультимедийное оборудование);

помещение для самостоятельной работы обучающихся: специализированная мебель и компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

10.1 Лицензионное программное обеспечение:

1. Операционная система Microsoft Windows XP Professional Russian — OEM-лицензии (поставляются в составе готового компьютера);
2. Операционная система Microsoft Windows 7 Professional — OEM-лицензии (поставляются в составе готового компьютера);
3. Программный пакет Microsoft Office 2007 — лицензия № 45829385 от 26.08.2009;
4. Программный пакет Microsoft Office 2010 Professional — лицензия № 48234688 от 16.03.2011;
5. Программный пакет Microsoft Office 2010 Professional — лицензия № 49261732 от 04.11.2011;
6. Комплексная система антивирусной защиты DrWEB Entrprise Suite — лицензия № 126408928;
7. 1С: Бухгалтерия 8 учебная версия — лицензионный договор № 01/200213 от 20.02.2013;
8. Программный комплекс IBM SPSS Statistic BASE — лицензионный договор № 20130218-1 от 12.03.2013;
9. Программный пакет LibreOffice — свободная лицензия Lesser General Public License
10. Корпоративная платформа Microsoft Teams. Проприетарная лицензия.

10.2. Электронно-библиотечная система:

Электронная библиотечная система (ЭБС): http://www.iprbookshop.ru/

10.3. Современные профессиональные баз данных:

1. Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru
2. Портал "Информационно-коммуникационные технологии в образовании" http://www.ict.edu.ru
3. Научная электронная библиотека http://www.elibrary.ru/
4. Национальная электронная библиотека http://www.nns.ru/
5. Электронные ресурсы Российской государственной библиотеки http://www.rsl.ru/ru/root3489/all
6. Web of Science Core Collection — политематическая реферативно-библиографическая и наукомтрическая (библиометрическая) база данных — http://webofscience.com
7. Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно-информационного консорциума (НЭИКОН) http://neicon.ru
8. Базы данных издательства Springer https://link.springer.com
9. www.minfin.ru Сайт Министерства финансов РФ
10. http://gks.ru Сайт Федеральной службы государственной статистики
11. www.skrin.ru База данных СКРИН (крупнейшая база данных по российским компаниям, отраслям, регионам РФ)
12. www.cbr.ru Сайт Центрального Банка Российской Федерации
13. http://moex.com/ Сайт Московской биржи
14. www.fcsm.ru Официальный сайт Федеральной службы по финансовым рынкам (ФСФР)
15. www.rbc.ru Сайт РБК («РосБизнесКонсалтинг» - ведущая российская компания, работающая в сферах масс-медиа и информационных технологий)
16. www.expert.ru Электронная версия журнала «Эксперт»
17. http://ecsn.ru/ «Экономические науки»

10.4. Информационные справочные системы:

1. Информационно-правовая система «Консультант+»
2. Информационно-справочная система «LexPro»
3. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru
4. www.garant.ru Информационно-правовая система Гарант

11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья по личному заявлению обучающегося разрабатывается адаптированная образовательная программа, индивидуальный учебный план с учетом

особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья библиотека комплектует фонд основной учебной литературой, адаптированной к ограничению их здоровья, предоставляет возможность удаленного использования электронных образовательных ресурсов, доступ к которым организован в ОАНО ВО «МПСУ». В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале, оборудованные программами невизуального доступа к информации, экранными увеличителями и техническими средствами усиления остаточного зрения: Microsoft Windows 7, Центр специальных возможностей, Экранная лупа; MicrosoftWindows 7, Центр специальных возможностей, Экранный диктор; MicrosoftWindows 7, Центр специальных возможностей, Экранная клавиатура; экранная лупа OneLoupe; речевой синтезатор «Голос».

12.Лист регистрации изменений

Рабочая программа учебной дисциплины обсуждена и утверждена на заседании Ученого совета от «22» марта 2021 г. протокол №5

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.	Утверждена решением Ученого совета на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.01 Экономика (уровень бакалавриата), утвержденного приказом Министерства науки и высшего образования РФ от 12.08.2020 г. N 954.	Протокол заседания Ученого совета от «22» марта 2021 года протокол №5	01.09.2021
2.			
3.			