Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки	Экономика
Код	38.03.01
Направленность (профиль)	Бухгалтерский учет, анализ и аудит
Квалификация выпускника	бакалавр

Москва
2025

1. Перечень кодов компетенций, формируемых дисциплиной в процессе освоения образовательной программы

Группа компетенций	Категория компетенций	Код
Профессиональные компетенции	-	ПК-19

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-19	Способен к выработке мероприятий по воздействию на риск в разрезе отдельных видов и проводить анализ и оценку рисков	ПК-19.1 Применяет в профессиональной деятельности современные методики анализа и оценки рисков ПК-19.3 Владеет конкретными способами предупреждения рисков и управления рисками в организации

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

Планируемые результаты обучения по дисциплине представлены дескрипторами (знания, умения, навыки).

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-19**		
Способен к выработке мероприятий по воздействию на риск в разрезе отдельных видов и проводить анализ и оценку рисков	– содержание проблемы информационной безопасности в условиях широкого применения и использование информационных компьютерных систем и вычислительных сетей;	– применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий.	– основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером; – основными понятиями и методами информационной безопасности

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений учебного плана ОПОП.

Данная дисциплина взаимосвязана с другими дисциплинами: «Информационные технологии в экономике», «Электронный бизнес и Интернет-технологии».

В рамках освоения программы бакалавриата выпускники готовятся к решению задач профессиональной деятельности следующих типов: аналитической, организационно-управленческой, расчетно-экономической.

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников: Бухгалтерский учет, анализ и аудит.

5. Объем дисциплины

Виды учебной работы	***Формы обучения***	
	Очно-заочная	***Очно-заочная с применением ДОТ***
Общая трудоемкость: зачетные единицы/часы	2/72	2/72
Контактная работа:		
Занятия лекционного типа	16	2
Занятия семинарского типа	16	4
Промежуточная аттестация: **зачет**	0,1	0,1
Самостоятельная работа (СРС)	39,9	65,9

6. Содержание дисциплины (модуля), структурированное по темам / разделам с указанием отведенного на них количества академических часов и видов учебных занятий

6.1. Распределение часов по разделам/темам и видам работы

6.1.1. Очно-заочная форма обучения

№ п/п	**Раздел/тема**	**Виды учебной работы (в часах)**						
		Контактная работа						**Самостоятельная работа**
		Занятия лекционного типа		**Занятия семинарского типа**				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные*	
1	Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	5		5				13,9
2	Защита информации.	5		5				13
3	Комплексная система защиты информации	6		6				13

	Промежуточная аттестация	**0,1**						
	Итого:	**16**		**16**				**39.9**

6.1.2. Очно-заочная форма обучения с применением ДОТ

№ п/п	Раздел/тема	Виды учебной работы (в часах)						
		Контактная работа						Самостоятельная работа
		Занятия лекционного типа		Занятия семинарского типа				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные*	
1.	Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	1		1				22,3
2	Защита информации.	1		1				22,3
3	Комплексная система защиты информации			2				21,3
	Промежуточная аттестация	**0,1**						
	Итого	**2**		**4**				**65,9**

6.1. Программа дисциплины, структурированная по темам / разделам

6.2.1. Содержание лекционного курса

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционного занятия
1.	Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	Защита информации как объективная закономерность эволюции постиндустриального общества. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Системный анализ угроз безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации. Организационно-правовое обеспечение защиты информации. Уязвимость информации и ее оценка. Виды, происхождение, предпосылки появления и источники угроз информационной безопасности. Последствия таких угроз. Случайные угрозы: отказы, сбои, ошибки, аварийные ситуации,

		побочные влияния внешней среды. Преднамеренные угрозы, злоумышленные действия людей. Модель нарушителя информационной безопасности. Несанкционированная модификация структур КС в процессе эксплуатации. Традиционные методы промышленного шпионажа. Утечка информации по техническим каналам.
2.	Защита информации.	Защита информации в компьютерных системах от случайных угроз. Защита информации от утечки по техническим каналам. Защита информации от побочных электромагнитных излучений и наводок. Блокировка ошибочных операций. Защита информации в компьютерных системах от несанкционированного вмешательства. Криптографические методы защиты. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.

6.2.2. Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	*Содержание практического занятия*
1.	Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	№1. Найти кодовое слово, если дан код (7, 4), порожденный многочленом g(x) = x^3 + x^2 +1, а информационным сообщением является вектор a = 1011. №2. Пусть (7,4)-код порожден многочленом g(x) = x^3 + x^2 +1 и принято слово 1110111. Была ли ошибка при передаче информационного сообщения 1011?
2.	Защита информации.	№1Оцените время раскрытия пароля, если число символов в сообщении, передаваемом в систему при попытке получить доступ к ней, равно 20, 600 сим в/мин – скорость передачи символов, длина пароля равна 6, число символов в алфавите – 26. Ответ дать в месяцах. № 2 Выберите необходимую длину пароля, чтобы вероятность его отгадывания не превышала 0.001 за 3 месяца. На одну попытку посылается 20 символов, скорость передачи данных равна 600 символов в минуту. №3 Зашифровать с помощью алгоритма RSA сообщение на русском языке «РИМ».
3.	Комплексная система защиты информации	№ 1 Поясните сущность эвристического анализа, применяемого для удаления вирусов. № 2 . Рассмотрите механизм заражения файловыми вирусами. Какими особенностями обладают макровирусы.

6.2.3. Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	*Содержание самостоятельной работы*
1.	Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	Защита информации как объективная закономерность эволюции постиндустриального общества. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Системный анализ угроз безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации. Организационно-правовое обеспечение защиты информации. Уязвимость информации и ее оценка. Виды, происхождение, предпосылки появления и источники угроз информационной безопасности. Последствия таких угроз. Случайные угрозы: отказы, сбои, ошибки, аварийные ситуации, побочные влияния внешней среды. Преднамеренные угрозы, злоумышленные действия людей. Модель нарушителя информационной безопасности. Несанкционированная модификация структур КС в процессе эксплуатации. Традиционные методы промышленного шпионажа. Утечка информации по техническим каналам.
2.	Защита информации.	Защита информации в компьютерных системах от случайных угроз. Защита информации от утечки по техническим каналам. Защита информации от побочных электромагнитных излучений и наводок. Блокировка ошибочных операций. Защита информации в компьютерных системах от несанкционированного вмешательства. Криптографические методы защиты. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.
3.	Комплексная система защиты информации	Компьютерные вирусы и антивирусные программные средства. Модели распространения вирусных программ. Классификация компьютерных вирусов. Комплексная система защиты информации в компьютерных системах. Контроль сбоев и отказов в работе оборудования. Резервирование технических средств. Помехоустойчивое кодирование. Коды, обнаруживающие и исправляющие ошибки. Код Хэмминга. Дублирование информации. Технология RAID.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Предусмотрены следующие виды контроля качества освоения конкретной дисциплины:

- текущий контроль успеваемости
- промежуточная аттестация обучающихся по дисциплине

Фонд оценочных средств для проведения промежуточной аттестации обучающихся

по дисциплине оформлен в **ПРИЛОЖЕНИИ** к РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины в процессе обучения.

7.1. Паспорт фонда оценочных средств для проведения текущей аттестации по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы)	Наименование оценочного средства
1.	Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	Опрос, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.
2.	Защита информации.	Опрос, проблемно-аналитическое задание, исследовательский проект, творческий проект, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
3.	Комплексная система защиты информации	Опрос, исследовательский проект, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи

7.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе текущего контроля

Типовые вопросы

1. Основные понятия, термины и определения в области защиты информации
2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.
3. Законодательная и нормативная база правового регулирования вопросов защиты информации.
4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.
5. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии
6. Меры и средства защиты информации
7. Применения криптографических методов защиты информации при работе в сетях.
8. Аудит информационной безопасности.

Типовые проблемно-аналитические задания

1. *Проблемно-аналитическое задание:*

1. **Задача 1.** После соревнований бегунов на табло появилась надпись:
• Рустам не был вторым.

•Эдуард отстал от Рустама на два места.• Яков не был первым.
• Галина не была не первой ни последней.• Карина финишировала сразу за Яковом.
Кто же победил в этих соревнованиях? Каково было распределение бегунов на финише?
Решение:
Рисуем таблицу, где столбцы –имена детей, а строки – номера мест. Читаем задачу, пошагово анализируем условие и ставим в таблицу «+», если соответствие установлено и «–», если точно соответствия нет.
Так как Рустам не был вторым и Эдуард отстал от Рустама на два места, то Эдуард не может быть ни первым, ни вторым, ни четвёртым.

	Рустам	Эдуард	Карина	Галина	Яков
1		–			
2	–	–			
3					
4		–			
5					

Яков не был первым и Галина не была не первой ни последней и так как Карина финишировала сразу за Яковом то она не могла быть ни первой ни второй.

	Рустам	Эдуард	Карина	Галина	Яков
1		–	–	–	–
2	–	–	–		
3					
4		–			
5				–	

Отсюда видно, что Рустам был первым тогда Эдуард (по условию 2) был третьим.

	Рустам	Эдуард	Карина	Галина	Яков
1	+	–	–	–	–
2	–	–	–	+	–
3	–	+	–	–	–
4	–	–	–	–	+
5	–	–	+	–	–

Так как Карина финишировала сразу за Яковом, то очевидно, что Яков был четвёртым, а Карина последней и тогда Галина была второй.

Итак, можно выделить
Пять простых шагов на пути поиска решения логических задач.
1. Составляйте таблицу, так как в таблице удаётся учесть все возможные варианты.
2. Внимательно читайте каждое утверждение, так как в каждом содержится что-то такое, что позволит вам исключить хотя бы один из вариантов.
3. Старайтесь отыскать ключевое утверждение, оно поможет развязать весь клубок.
4. После того как вы сравнили все утверждения и исключили из них те, невероятность которых была на поверхности, сравните утверждения между собой, установите связи и противоречия.
5. Решение можно найти простым методом последовательных исключений.

Чем больше будете тренироваться, тем лучше у вас это будет получаться. А теперь за дело.

Задача 2.

В субботний вечер Семен, Коля и Витя решили развлечься. У них был выбор: кино, рок-концерт или танцы

•Семён любит кино, но к танцам менее нетерпим, чем к рок-музыке.

• Коля любит танцевать, но готов пойти в кино скорее, чем на рок концерт.

• Витя любит рок-музыку меньше чем танцы, но кино ему всё-таки не так неприятно, как танцы или концерт.

Поскольку вопрос решатся большинством голосов, то куда, на ваш взгляд отправились эти ребята?

Задача 3.

Трое мальчиков Костя, Фома и Марат дружили с тремя девочками – Женей, Светой и Мариной. Но вскоре компания разделилась на пары, потому, что оказалось:

•Света ненавидит ходить на лыжах

•Костя, Женин брат часто катается со своей подружкой на лыжах

•А Фома теперь бежит на свидание к Костиной сестре.

С кем же проводит время Марат?

Темы исследовательских, творческих проектов

Подготовка исследовательских проектов по темам:

1. Сравнительный анализ современных информационных систем.
2. Робототехника в юриспруденции.
3. История развития Интернета
4. Блог как средство массовой информации.
5. Менеджмент веб-проектов.

Информационный проект

Подготовьте информационный проект (презентацию) по теме:

1. Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней.
2. Законодательство РФ в области информационной безопасности.
3. Информационная безопасность объекта при осуществлении международного сотрудничества. Виды угроз информационной безопасности.
4. Угрозы конституционным правам и свободам гражданина в области информационной деятельности.
5. Угрозы информационному обеспечению государственной политики Российской Федерации.

Творческое задание (с элементами эссе)

Напишите эссе по теме:

1. Угрозы безопасности информационных и телекоммуникационных средств и систем.
2. Внешние и внутренние источники угроз информационной безопасности.
3. История развития поисковых систем.
4. Проблема общественного прогресса в истории информатики.

Творческое задание (с элементами эссе)

1. Информация как объект правового регулирования.

2. Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней.
3. Законодательство РФ в области информационной безопасности.
4. Информационная безопасность объекта при осуществлении международного сотрудничества.
5. Виды угроз информационной безопасности.
6. Угрозы конституционным правам и свободам гражданина в области информационной деятельности.
7. Угрозы информационному обеспечению государственной политики Российской Федерации.
8. Угрозы безопасности информационных и телекоммуникационных средств и систем.
9. Внешние и внутренние источники угроз информационной безопасности.
10. Основные виды угроз безопасности субъектов информационных отношений.
11. Основные непреднамеренные и преднамеренные искусственные угрозы.
12. Основные преднамеренные искусственные угрозы.
13. Закон РФ от 21.09.93 "О государственной тайне".
14. Закон РФ от 09.07.2004г. «О коммерческой тайне».
15. Закон РФ от 08.07.2006г. «О персональных данных».
16. «Концепция защиты СВТ и АС от НСД», предназначение, основные понятия и направления.
17. Основные принципы защиты от НСД, изложенные в нормативных документах концепции защиты СВТ и АС.
18. Свойства защищенных автоматизированных систем обработки информации.
19. Специфика возникновения угроз и рисков в открытых сетях.
20. Что понимается под уязвимостью защищенных компьютерных систем?
21.Основные направления обеспечения информационной безопасности в компьютерных системах.
22.Основные понятия безопасности компьютерных систем.
23.Что понимается под лицензированием деятельности в области защиты информации?
24.Перечислить основные мероприятия, позволяющие решить задачу построения системы защиты рабочей станции.
25.Для чего используются системы многоуровневой защиты?
26.Какие вы знаете аспекты защиты информации в системе с разграничением полномочий?
27.Перечислите и дайте характеристику основным методам построения систем защиты с многоуровневым доступом.
28.Какое место занимает механизм подотчетности в политике безопасности и, на какие категории делятся средства подотчетности?
29.Какие проблемы возникают при использовании защиты информации путем ограничения доступа?
30.Какие принципы положены в концепцию построения защищенных систем?
31.Перечислить и дать характеристику основным компонентам технологии построения защищенной компьютерной системы.
32.Каким способом происходит интеграция средств защиты и распространенных приложений в защищенной компьютерной системе?
33.Что понимается под несанкционированным доступом к информации. 34.Перечислить и дать характеристику обобщенным методам защиты от НСД. 35.Что понимается под стойкостью системы идентификации?
36.Что является интегральной характеристикой защищенной системы? 37.Понятие политики безопасности и её основные базовые представления.

38.В каких случаях используют модели безопасности производители защищенных компьютерных систем?
39.Из каких частей состоит ГОСТ Р 15408? 4
40.На каких базовых представлениях основаны модели безопасности?
41.Какие элементы должна включать в себя политика безопасности организации?
42. В чем различие субъекта компьютерной системы от человека-пользователя?
43.Какими качествами должен обладать монитор обращений?
44.Как определяется доверенная система в ГОСТ Р 15408, и по каким критериям

Типовые задания к интерактивным занятиям

1.Сформировать список документов по тематике: Гражданское право — Интеллектуальная собственность – Авторское право.
2. Выделить несколько документов из списка.
3. Занести документы в созданную папку.
4. Удалить один документ из созданной папки.
5. Выбрать несколько документов из списка и занести в файл.
6. Выделить один документ. Занести его в новую папку: "Авторское право".
7. Создать папку "Патентное законодательство" и занести туда Патентный Закон РФ.
8. Сформировать документ Word, содержащий определения следующих понятий: «информация», «информатизация», «документированная информация», «программа для ЭВМ», «автор», «СМИ», «реклама», «документы», «обязательный экземпляр документа», «архивный документ», «безопасность», «государственная тайна». Название документа: "Терминология, используемая в учебной дисциплине Информационное право"
9. Сделать закладки в документах на эти определения.
10. Создать папку "Информационное право", содержащую законы, в которых определяются данные понятия.
11. Найти изображение Государственного флага РФ.
12. Найти текст Государственного гимна РФ.
13. Сколько графических объектов содержится в приказе Госстандарта России от 26 ноября 2001 г. № 477? Сохраните эти объекты в MS Word.
14. Постойте список материалов судебной практики к статье 151 Гражданского кодекса РФ.
15. Найти постановления Пленума Верховного Суда России, которые в своих текстах ссылаются на статью 139 Уголовного кодекса РФ.
16. Найти приказы Минфина России начиная с 2010года.
17. Найти письмо ГТК России от 6 мая 2010г.
18. Найти документы, зарегистрированные в Минюсте России, но не вступившие в силу.
19. Найти ПБУ 6/01 «Учет основных средств».
20. Найти федеральные законы и законы Вашего региона о государственной гражданской и муниципальной службе, имеющей статус действующей.
21. Найти нормативные акты, регулирующие вопросы деятельности обществ с ограниченной ответственностью. В полученном списке документов найти и открыть Гражданский кодекс РФ.
22. Найти федеральный закон, устанавливающий замену основной части натуральных льгот ежемесячными денежными компенсациями.

Подготовка и проведение диспут-игры

Диспут-игра по теме – взаимодействие информационных систем. Студенты делятся на две группы, каждая из которых защищает свой тезис:

1) Тезис 1 команды – интеграция двух информационных систем возможна только после проектирования и тестирования.

2) Тезис 2 команды - интеграцию двух информационных систем возможно осуществить используя старые возможности каждой из ИС, минуя новые этапы проектирования и тестирования. Каждая команда старается максимально полно аргументировать свою точку зрения, опровергая утверждения и доводы другой команды.

Типовые тесты

1. **Создание таблиц в текстовом процессоре MS Word возможно в режиме:**
   □ **обычном**
   □ **разметки**
   □ структуры
   □ **Web-документа**
   □ схемы документа
2. **Создание реквизитных элементов оформления печатных страниц в текстовом процессоре MS Word возможно в режиме:**
   □ обычном
   □ **разметки**
   □ структуры
   □ Web-документа
   □ **схемы документа**
3. **К базовым приемам работы с текстами в текстовом процессоре MS Word относятся:**
   □ **создание, сохранение и печать документа**
   □ отправка документа по электронной почте
   □ **ввод и редактирование текста**
   □ **рецензирование текста**
   □ **форматирование текста**
4. **. К специальным средствам ввода текста в текстовом процессоре MS Word относятся:**
   □ **средства отмены и возврата действий**
   □ **расширенный буфер обмена**
   □ **автотекст**
   □ автосуммирование
   □ **автозамена**
5. **К специальным средствам редактирования текста в текстовом процессоре MS Word относятся:**
   □ **режим вставки символов**
   □ **режим замены символов**
   □ рецензирование
   □ **тезаурус**
   □ **автоматизация проверки правописания**
6. **В документ MS Word можно вставить:**
   □ **формулы**
   □ программы
   □ **таблицы**
   □ **диаграммы**
   □ **рисунки**
7. **Новый макрос можно создать следующими способами:**
   □ **автоматически записать последовательность действий**
   □ **вручную написать соответствующую программу на языке VBA**
   □ импортировать из другого файла существующий макрос

□ **импортировать из другого файла существующий макрос и изменить его**
□ **изменить в уже созданный макрос и сохранить под другим именем**

8. **Ссылки на ячейки в таблицах MS Word включают:**
□ **латинские буквы**
□ русские буквы
□ **арабские цифры**
□ римские цифры
□ греческие символы
9. **Для вычисления в таблицах MS Word используются формулы, содержащие:**
□ математические функции
□ **константы**
□ **встроенные функции**
□ **знаки математических операций**
□ ссылки на блоки текста
10. **При слиянии используются следующие документы:**
□ итоговый документ
□ **основной документ**
□ получатель данных
□ **источник данных**
□ исходный документ
11. **Источником данных при слиянии может быть:**
□ **документ MS Word**
□ **документ MS Excel**
□ документ MS WordPad
□ **документ MS Access**
□ документ MS Graph
12. **Ссылки на ячейки в табличном процессоре MS Excel могут быть:**
□ **относительными**
□ процентными
□ **абсолютными**
□ **смешанными**
□ индивидуальными
13. **Ячейка таблицы MS Excel может содержать:**
□ рисунок
□ **текст**
□ **число**
□ **формулу**
□ **дату и время**
14. **Режимы работы табличного процессора MS Excel:**
□ **готовности**
□ **ввода данных**
□ **командный**
□ обычный
□ **редактирования**
15. **Ограничение доступа к электронным таблицам может выполняться на уровне:**
□ **рабочих книг**
□ группы документов
□ формул
□ **рабочих листов**
□ **отдельных ячеек**

16. **Пункт меню Данные табличного процессора MS Excel позволяет:**
□ проводить защиту данных
□ создавать макросы
□ **проводить сортировку данных**
□ **проводить фильтрацию данных**
□ проверять орфографию
17. **Для запуска макроса можно применять:**
□ **комбинацию клавиш клавиатуры**
□ комбинацию клавиш клавиатуры и экранных кнопок
□ **созданные экранные кнопки**
□ **созданные кнопки панели инструментов**
□ текстовую команду
18. **При форматировании диаграммы в табличном процессоре MS Excel можно изменить:**
□ **тип диаграммы**
□ **исходные данные**
□ **формат легенды**
□ **расположение диаграммы**
□ **формат области построения**
19. **В плане счетов для некоторого счета установлено ведение аналитического учета в разрезе двух видов субконто – «Материалы» и «Склады». Тогда в программе 1С бухгалтерские итоги по данному счету могут быть получены:**
□ **отдельно по материалам**
□ **отдельно по складам**
□ по складам в разрезе материалов и складов
□ **по материалам в разрезе складов**
□ **по складам в разрезе материалов**
20. **В шаблоне типовой операции для некоторого реквизита проводки в параметре «Копирование» установлено наименование этого же реквизита. Данный режим в программе 1С предоставляет пользователю возможность:**
□ **принудительно копировать значения указанного реквизита из этой же проводки**
□ принудительно копировать значения указанного реквизита из последующих проводок
□ **принудительно копировать значения указанного реквизита предшествующих проводок**
□ принудительно копировать значения указанного реквизита из журнала операций
□ принудительно копировать значения указанного реквизита журнала проводок
21. **Данный способов подключения к Интернет обеспечивает наибольшие возможности для доступа к информационным ресурсам:**
□ **постоянное соединение по оптоволоконному каналу**
□ удаленный доступ по коммутируемому телефонному каналу
□ постоянное соединение по выделенному телефонному каналу
□ терминальное соединение по коммутируемому телефонному каналу
22. **Модем, передающий информацию со скоростью 28 800 бит/с, может передать две страницы текста (3 600 байт) в течение…**
□ 1 минуты
□ 1 часа
□ **1 секунды**
□ 1 дня
23. **Электронная почта (e-mail) позволяет передавать…**
□ только сообщения

□ только файлы
□ **сообщения и приложенные файлы**
□ видеоизображения

24. **Базовым стеком протоколов в Internet является:**
□ HTTP
□ HTML
□ TCP
□ **TCP/IP**

25. **Компьютер, подключенный к Internet, обязательно имеет:**
□ **IP-адрес**
□ Web-сервер
□ домашнюю web-страницу
□ доменное имя

26. **Гиперссылки на web — странице могут обеспечить переход:**
□ только в пределах данной web – страницы
□ только на web — страницы данного сервера
□ на любую web — страницу данного региона
□ **на любую web — страницу любого сервера Интернет**

27. **Задан адрес электронной почты в сети Internet: user_name@int.glasnet.ru. «Имя» владельца электронного адреса:**
□ int.glasnet.ru
□ **user_name**
□ glasnet.ru
□ ru

28. **Браузеры являются:**
□ серверами Интернет
□ антивирусными программами
□ трансляторами языка программирования
□ **средством просмотра web-страниц**

29. **Web-страницы имеют расширение:**
□ *.txt
□ ***.htm**
□ *.doc
□ *.exe

30. **Модем — это устройство, предназначенное для:**
□ вывода информации на печать
□ хранения информации
□ обработки информации в данный момент времени
□ **передачи информации по каналам связи**

31. **В качестве гипертекстовых ссылок можно использовать:**
□ только слово
□ только картинку
□ любое слово или любую картинку
□ **слово, группу слов или картинку**

32. **Web-страница — это …**
□ **документ специального формата, опубликованный в Internet**
□ документ, в котором хранится вся информация по сети
□ документ, в котором хранится информация пользователя
□ сводка меню программных продуктов

Реализация программы с применением ДОТ:

Типовые ситуационные задачи:

Оцените время раскрытия пароля, если число символов в сообщении, передаваемом в систему при попытке получить доступ к ней, равно 20, 600 симв/мин – скорость передачи символов, длина пароля равна 6, число символов в алфавите – 26. Ответ дать в месяцах.

Типовые проблемные задачи:

№ 1 Выберите необходимую длину пароля, чтобы вероятность его отгадывания не превышала 0.001 за 3 месяца. На одну попытку посылается 20 символов, скорость передачи данных равна 600 символов в минуту.

№2 Зашифровать с помощью алгоритма RSA сообщение на русском языке «РИМ».

Типовые тесты

1. Защита информации – это …
а) комплекс мероприятий, направленных на обеспечение информационной безопасности
б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов
в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям
г) все определения корректны

2. Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:
а) обнаружение угроз
б) пресечения и локализация угроз
в) ликвидация угроз

3. Возможность за приемлемое время получить требуемую информационную услугу называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации

4. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации
г) конфиденциальностью информации

5. Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации
а) доступность информации
б) целостность информации

в) предоставление информации
г) конфиденциальность информации

6. Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:
а) законодательного уровня
б) административного уровня
в) процедурного уровня
г) программно-технического уровня
д) программно-аппаратного уровня

7. Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами. Какая организация НЕ занимается вопросами формирования законодательства в сфере информационных ресурсов?
а) ISO
б) ITU
в) ANSI
г) NIST
д) NASA
е) SWIFT
ж) GISA

8. Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:
а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
б) Федеральная служба безопасности Российской Федерации
в) Служба внешней разведки Российской Федерации

9. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:
а) политикой безопасности
б) методами защиты информации
в) ограничением доступа к информации
учетными записями пользователей

10. Потенциальная возможность определенным образом нарушить информационную безопасность – это ….
а) угроза
б) атака
в) взлом.

11. Источниками угрозы называют …
а) потенциальных злоумышленников
б) компьютерные вирусы
в) глобальную сеть Интернет

12. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется …
а) окном безопасности
б) окном опасности
в) скользящим окном

г) окном угрозы
13. Ошибки программного обеспечения с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы

14. Ошибки администрирования системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы

15. Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы

16. Некоторая уникальная информация, позволяющая различать пользователей называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
8
г) ключ

17. Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ

18. Совокупность идентификатора и пароля пользователя называется:
а) логин пользователя
б) учетная запись пользователя
в) ключ пользователя

19. Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) опознанием пользователя
г) созданием учетной записи пользователя

20. Проверка принадлежности пользователю предъявленного им идентификатора является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) регистрацией пользователя
г) созданием учетной записи пользователя

Типовые вопросы для промежуточной аттестации представлены в приложении к РПД – в ФОС.

7.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Все задания, используемые для текущего контроля формирования компетенций условно можно разделить на две группы:

1. задания, которые в силу своих особенностей могут быть реализованы только в процессе обучения на занятиях (например, дискуссия, круглый стол, диспут, мини-конференция);

2. задания, которые дополняют теоретические вопросы (практические задания, проблемно-аналитические задания, тест).

Выполнение всех заданий является необходимым для формирования и контроля знаний, умений и навыков. Поэтому, в случае невыполнения заданий в процессе обучения, их необходимо «отработать» до зачета (экзамена). Вид заданий, которые необходимо выполнить для ликвидации «задолженности» определяется в индивидуальном порядке, с учетом причин невыполнения.

1. Требование к теоретическому устному ответу

Оценка знаний предполагает дифференцированный подход к студенту, учет его индивидуальных способностей, степень усвоения и систематизации основных понятий и категорий по дисциплине. Кроме того, оценивается не только глубина знаний поставленных вопросов, но и умение использовать в ответе практический материал. Оценивается культура речи, владение навыками ораторского искусства.

Критерии оценивания: последовательность, полнота, логичность изложения, анализ различных точек зрения, самостоятельное обобщение материала, использование профессиональных терминов, культура речи, навыки ораторского искусства. Изложение материала без фактических ошибок.

Оценка *«отлично»* ставится в случае, когда материал излагается исчерпывающе, последовательно, грамотно и логически стройно, при этом раскрываются не только основные понятия, но и анализируются точки зрения различных авторов. Обучающийся не затрудняется с ответом, соблюдает культуру речи.

Оценка *«хорошо»* ставится, если обучающийся твердо знает материал, грамотно и по существу излагает его, знает практическую базу, но при ответе на вопрос допускает несущественные погрешности.

Оценка *«удовлетворительно»* ставится, если обучающийся освоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении материала, затрудняется с ответами, показывает отсутствие должной связи между анализом, аргументацией и выводами.

Оценка *«неудовлетворительно»* ставится, если обучающийся не отвечает на поставленные вопросы.

2. Творческие задания

Эссе – это небольшая по объему письменная работа, сочетающая свободные, субъективные рассуждения по определенной теме с элементами научного анализа. Текст должен быть легко читаем, но необходимо избегать нарочито разговорного стиля, сленга, шаблонных фраз. Объем эссе составляет примерно 2 – 2,5 стр. 12 шрифтом с одинарным интервалом (без учета титульного листа).

Критерии оценивания - оценка учитывает соблюдение жанровой специфики эссе, наличие логической структуры построения текста, наличие авторской позиции, ее научность и связь с современным пониманием вопроса, адекватность аргументов, стиль изложения, оформление работы. Следует помнить, что прямое заимствование (без оформления цитат) текста из Интернета или электронной библиотеки недопустимо.

Оценка *«отлично»* ставится в случае, когда определяется: наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение с выводами, полученными в результате рассуждения); наличие четко определенной личной позиции по теме эссе; адекватность аргументов при обосновании личной позиции, стиль изложения.

Оценка *«хорошо»* ставится, когда в целом определяется: наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение с выводами, полученными в результате рассуждения); но не прослеживается наличие четко определенной личной позиции по теме эссе; не достаточно аргументов при обосновании личной позиции.

Оценка *«удовлетворительно»* ставится, когда в целом определяется: наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение). Но не прослеживаются четкие выводы, нарушается стиль изложения.

Оценка *«неудовлетворительно»* ставится, если не выполнены никакие требования.

3. Требование к решению ситуационной, проблемной задачи (кейс-измерители)

Студент должен уметь выделить основные положения из текста задачи, которые требуют анализа и служат условиями решения. Исходя из поставленного вопроса в задаче, попытаться максимально точно определить проблему и соответственно решить ее.

Задачи должны решаться студентами письменно. При решении задач также важно правильно сформулировать и записать вопросы, начиная с более общих и, кончая частными.

Критерии оценивания – оценка учитывает методы и средства, использованные при решении ситуационной, проблемной задачи.

Оценка *«отлично»* ставится в случае, когда обучающийся выполнил задание (решил задачу), используя в полном объеме теоретические знания и практические навыки, полученные в процессе обучения.

Оценка *«хорошо»* ставится, если обучающийся в целом выполнил все требования, но не совсем четко определяется опора на теоретические положения, изложенные в научной литературе по данному вопросу.

Оценка *«удовлетворительно»* ставится, если обучающийся показал положительные результаты в процессе решения задачи.

Оценка *«неудовлетворительно»* ставится, если обучающийся не выполнил все требования.

При реализации программы с применением ДОТ:

Студент должен уметь выделить основные положения из текста задачи, которые требуют анализа и служат условиями решения. Исходя из поставленного вопроса в задаче, попытаться максимально точно определить проблему и соответственно решить ее.

Задачи должны решаться студентами письменно. При решении задач также важно правильно сформулировать и записать вопросы, начиная с более общих и, кончая частными.

Критерии оценивания – оценка учитывает методы и средства, использованные при решении ситуационной, проблемной задачи.

Оценка «выполнено» ставится в случае, если обучающийся показал положительные результаты в процессе решения задачи, а именно, когда обучающийся в целом выполнил задание (решил задачу), используя в полном объеме теоретические знания и практические навыки, полученные в процессе обучения.

Оценка «не выполнено» ставится, если обучающийся не выполнил все требования.

4. Интерактивные задания

Механизм проведения диспут-игры (ролевой (деловой) игры).

Необходимо разбиться на несколько команд, которые должны поочередно высказать свое мнение по каждому из заданных вопросов. Мнение высказывающейся команды засчитывается, если противоположная команда не опровергнет его контраргументами. Команда, чье мнение засчитано как верное (не получило убедительных контраргументов от противоположных команд), получает один балл. Команда, опровергнувшая мнение противоположной команды своими контраргументами, также получает один балл. Побеждает команда, получившая максимальное количество баллов.

Ролевая игра как правило имеет фабулу (ситуацию, казус), распределяются роли, подготовка осуществляется за 2-3 недели до проведения игры.

Критерии оценивания – оцениваются действия всех участников группы. Понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Соответствие реальной действительности решений, выработанных в ходе игры. Владение терминологией, демонстрация владения учебным материалом по теме игры, владение методами аргументации, умение работать в группе (умение слушать, конструктивно вести беседу, убеждать, управлять временем, бесконфликтно общаться), достижение игровых целей, (соответствие роли – при ролевой игре). Ясность и стиль изложения.

Оценка *«отлично»* ставится в случае, выполнения всех критериев.

Оценка *«хорошо»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Решения, выработанные в ходе игры, полностью соответствуют реальной действительности. Но некоторые объяснения не совсем аргументированы, нарушены нормы общения, нарушены временные рамки, нарушен стиль изложения.

Оценка *«удовлетворительно»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия в целом соответствуют заданным целям. Однако, решения, выработанные в ходе игры, не совсем соответствуют реальной действительности. Некоторые объяснения не совсем аргументированы, нарушены временные рамки, нарушен стиль изложения.

Оценка *«неудовлетворительно»* ставится, если обучающиеся не понимают проблему, их высказывания не соответствуют заданным целям.

5. Комплексное проблемно-аналитическое задание

Задание носит проблемно-аналитический характер и выполняется в три этапа. На первом из них необходимо ознакомиться со специальной литературой.

Целесообразно также повторить учебные материалы лекций и семинарских занятий по темам, в рамках которых предлагается выполнение данного задания.

На втором этапе выполнения работы необходимо сформулировать проблему и изложить авторскую версию ее решения, на основе полученной на первом этапе информации.

Третий этап работы заключается в формулировке собственной точки зрения по проблеме. Результат третьего этапа оформляется в виде аналитической записки (объем: 2-2,5 стр.; 14 шрифт, 1,5 интервал).

Критерий оценивания - оценка учитывает: понимание проблемы, уровень раскрытия поставленной проблемы в плоскости теории изучаемой дисциплины, умение формулировать и аргументировано представлять собственную точку зрения, выполнение всех этапов работы.

Оценка *«отлично»* ставится в случае, когда обучающийся демонстрирует полное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«хорошо»* ставится, если обучающийся демонстрирует значительное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«удовлетворительно»* ставится, если обучающийся, демонстрирует частичное понимание проблемы, большинство требований, предъявляемых к заданию, выполнены

Оценка *«неудовлетворительно»* ставится, если обучающийся демонстрирует непонимание проблемы, многие требования, предъявляемые к заданию, не выполнены.

При реализации программы с применением ДОТ:

Студент должен уметь выделить основные положения из текста задачи, которые требуют анализа и служат условиями решения. Исходя из поставленного вопроса в задаче, попытаться максимально точно определить проблему и соответственно решить ее.

Задачи должны решаться студентами письменно. При решении задач также важно правильно сформулировать и записать вопросы, начиная с более общих и, кончая частными.

Критерии оценивания – оценка учитывает методы и средства, использованные при решении ситуационной, проблемной задачи.

Оценка «выполнено» ставится в случае, если обучающийся показал положительные результаты в процессе решения задачи, а именно, когда обучающийся в целом выполнил задание (решил задачу), используя в полном объеме теоретические знания и практические навыки, полученные в процессе обучения.

Оценка «не выполнено» ставится, если обучающийся не выполнил все требования.

6. Исследовательский проект

Исследовательский проект **–** проект, структура которого приближена к формату научного исследования и содержит доказательство актуальности избранной темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, историографии, обобщение результатов, выводы.

Результаты выполнения исследовательского проекта оформляется в виде реферата (объем: 12-15 страниц; 14 шрифт, 1,5 интервал).

Критерии оценивания - поскольку структура исследовательского проекта максимально приближена к формату научного исследования, то при выставлении учитывается доказательство актуальности темы исследования, определение научной проблемы, объекта и предмета исследования, целей и задач, источников, методов исследования, выдвижение гипотезы, обобщение результатов и формулирование выводов, обозначение перспектив дальнейшего исследования.

Оценка *«отлично»* ставится в случае, когда обучающийся демонстрирует полное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«хорошо»* ставится, если обучающийся демонстрирует значительное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«удовлетворительно»* ставится, если обучающийся, демонстрирует частичное понимание проблемы, большинство требований, предъявляемых к заданию, выполнены

Оценка *«неудовлетворительно»* ставится, если обучающийся демонстрирует непонимание проблемы, многие требования, предъявляемые к заданию, не выполнены.

7. Информационный проект (презентация):

Информационный проект **–** проект, направленный на стимулирование учебно-познавательной деятельности студента с выраженной эвристической направленностью (поиск, отбор и систематизация информации об объекте, оформление ее для презентации). Итоговым продуктом проекта может быть письменный реферат, электронный реферат с иллюстрациями, слайд-шоу, мини-фильм, презентация и т.д.

Информационный проект отличается от исследовательского проекта, поскольку представляет собой такую форму учебно-познавательной деятельности, которая отличается ярко выраженной эвристической направленностью.

Критерии оценивания - при выставлении оценки учитывается самостоятельный поиск, отбор и систематизация информации, раскрытие вопроса (проблемы), ознакомление студенческой аудитории с этой информацией (представление информации), ее анализ и обобщение, оформление, полные ответы на вопросы аудитории с примерами.

Оценка *«отличн*о» ставится в случае, когда обучающийся полностью раскрывает вопрос (проблему), представляет информацию систематизировано, последовательно, логично, взаимосвязано, использует более 5 профессиональных терминов, широко использует информационные технологии, ошибки в информации отсутствуют, дает полные ответы на вопросы аудитории с примерами.

Оценка *«хорошо»* ставится, если обучающийся раскрывает вопрос (проблему), представляет информацию систематизировано, последовательно, логично, взаимосвязано, использует более 2 профессиональных терминов, достаточно использует информационные технологии, допускает не более 2 ошибок в изложении материала, дает полные или частично полные ответы на вопросы аудитории.

Оценка *«удовлетворительно»* ставится, если обучающийся, раскрывает вопрос (проблему) не полностью, представляет информацию не систематизировано и не совсем последовательно, использует 1-2 профессиональных термина, использует информационные технологии, допускает 3-4 ошибки в изложении материала, отвечает только на элементарные вопросы аудитории без пояснений.

Оценка *«неудовлетворительно»* ставится, если вопрос не раскрыт, представленная информация логически не связана, не используются профессиональные термины, допускает более 4 ошибок в изложении материала, не отвечает на вопросы аудитории.

8. Дискуссионные процедуры

Круглый стол, дискуссия, полемика, диспут, дебаты, мини-конференции являются средствами, позволяющими включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Задание дается заранее, определяется круг вопросов для обсуждения, группы участников этого обсуждения.

Дискуссионные процедуры могут быть использованы для того, чтобы студенты:

– лучше поняли усвояемый материал на фоне разнообразных позиций и мнений, не обязательно достигая общего мнения;

– смогли постичь смысл изучаемого материала, который иногда чувствуют интуитивно, но не могут высказать вербально, четко и ясно, или конструировать новый смысл, новую позицию;

– смогли согласовать свою позицию или действия относительно обсуждаемой проблемы.

Критерии оценивания – оцениваются действия всех участников группы. Понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Соответствие реальной действительности решений, выработанных в ходе игры. Владение

терминологией, демонстрация владения учебным материалом по теме игры, владение методами аргументации, умение работать в группе (умение слушать, конструктивно вести беседу, убеждать, управлять временем, бесконфликтно общаться), достижение игровых целей, (соответствие роли – при ролевой игре). Ясность и стиль изложения.

Оценка *«отлично»* ставится в случае, когда все требования выполнены в полном объеме.

Оценка *«хорошо»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Решения, выработанные в ходе игры, полностью соответствуют реальной действительности. Но некоторые объяснения не совсем аргументированы, нарушены нормы общения, нарушены временные рамки, нарушен стиль изложения.

Оценка *«удовлетворительно»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия в целом соответствуют заданным целям. Однако, решения, выработанные в ходе игры, не совсем соответствуют реальной действительности. Некоторые объяснения не совсем аргументированы, нарушены временные рамки, нарушен стиль изложения.

Оценка *«неудовлетворительно»* ставится, если обучающиеся не понимают проблему, их высказывания не соответствуют заданным целям.

9. Тестирование

Является одним из средств контроля знаний обучающихся по дисциплине.

Критерии оценивания – правильный ответ на вопрос.

Оценка *«отлично»* ставится в случае, если правильно выполнено 90-100% заданий.

Оценка *«хорошо»* ставится, если правильно выполнено 70-89% заданий.

Оценка *«удовлетворительно»* ставится в случае, если правильно выполнено 50-69% заданий.

Оценка *«неудовлетворительно»* ставится, если правильно выполнено менее 50% заданий.

10. Требование к письменному опросу (контрольной работе)

Оценивается не только глубина знаний поставленных вопросов, но и умение изложить письменно.

Критерии оценивания: последовательность, полнота, логичность изложения, анализ различных точек зрения, самостоятельное обобщение материала. Изложение материала без фактических ошибок.

Оценка *«отлично»* ставится в случае, когда соблюдены все критерии.

Оценка *«хорошо»* ставится, если обучающийся твердо знает материал, грамотно и по существу излагает его, знает практическую базу, но допускает несущественные погрешности.

Оценка *«удовлетворительно»* ставится, если обучающийся освоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении материала, затрудняется с ответами, показывает отсутствие должной связи между анализом, аргументацией и выводами.

Оценка *«неудовлетворительно»* ставится, если обучающийся не отвечает на поставленные вопросы.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

8.1. Основная учебная литература:

1. Бондаренко И.С. Информационная безопасность : учебник / Бондаренко И.С.. — Москва : Издательский Дом МИСиС, 2023. — 254 c. — ISBN 978-5-907560-71-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/137525.html

2. Ревнивых А.В. Информационная безопасность в организациях: учебное пособие / Ревнивых А.В. — Москва: Ай Пи Ар Медиа, 2021. — 83 c. — ISBN 978-5-4497-1164-9. — Текст: электронный // IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/108227.html

3. Суворова Г.М. Информационная безопасность: учебное пособие / Суворова Г.М. — Саратов: Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст: электронный // IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/86938.html

8.2 Дополнительная учебная литература:

1. Информационные системы и технологии. Часть 1: монография / В. Д. Колдаев, И. В. Гелета, Ю. А. Бобель, Р. М. Сафина. — Москва: Перо, Центр научной мысли, 2011. — 126 c. — ISBN 978-5-91940-150-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/8982.html

2. Лучанинов, Д. В. Основы разработки web-сайтов образовательного назначения: учебное пособие / Д. В. Лучанинов. — Саратов: Ай Пи Эр Медиа, 2018. — 105 c. — ISBN 978-5-4486-0174-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/70775.html

4. Дементьева, Ю. В. Основы работы с электронными образовательными ресурсами: учебное пособие / Ю. В. Дементьева. — Саратов: Вузовское образование, 2017. — 80 c. — ISBN 978-5-906172-21-1. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/62066.html

8.3. Периодические издания:

1. «Информационные технологии и телекоммуникации» ISSN 2307-1303
2. «Информационные технологии» ISSN 1684-640

9. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины (модуля)

1. Федеральный портал «Российское образование». http://www.edu.ru/
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов». http://school-collection.edu.ru/

10. Методические указания для обучающихся по освоению дисциплины (модуля)

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности – лекций, семинарских занятий, самостоятельной работы. При этом самостоятельную работу следует рассматривать одним из главных звеньев полноценного высшего образования, на которую отводится значительная часть учебного времени.

При реализации программы с применением ДОТ:

Все виды занятий проводятся в форме онлайн-вебинаров с использованием современных компьютерных технологий (наличие презентации и форума для обсуждения).

В процессе изучения дисциплины студенты выполняют практические задания и промежуточные тесты. Консультирование по изучаемым темам проводится в онлайнрежиме во время проведения вебинаров и на форуме для консультаций.

Самостоятельная работа студентов складывается из следующих составляющих:

1. работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;

2. внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;

3. выполнение самостоятельных практических работ;

4. подготовка к экзаменам (зачетам) непосредственно перед ними.

Для правильной организации работы необходимо учитывать порядок изучения разделов курса, находящихся в строгой логической последовательности. Поэтому хорошее усвоение одной части дисциплины является предпосылкой для успешного перехода к следующей. Задания, проблемные вопросы, предложенные для изучения дисциплины, в том числе и для самостоятельного выполнения, носят междисциплинарный характер и базируются, прежде всего, на причинно-следственных связях между компонентами окружающего нас мира. В течение семестра, необходимо подготовить рефераты (проекты) с использованием рекомендуемой основной и дополнительной литературы и сдать рефераты для проверки преподавателю. Важным составляющим в изучении данного курса является решение ситуационных задач и работа над проблемно-аналитическими заданиями, что предполагает знание соответствующей научной терминологии и т.д.

Для лучшего запоминания материала целесообразно использовать индивидуальные особенности и разные виды памяти: зрительную, слуховую, ассоциативную. Успешному запоминанию также способствует приведение ярких свидетельств и наглядных примеров. Учебный материал должен постоянно повторяться и закрепляться.

При выполнении докладов, творческих, информационных, исследовательских проектов особое внимание следует обращать на подбор источников информации и методику работы с ними.

Для успешной сдачи экзамена (зачета) рекомендуется соблюдать следующие правила:

1. Подготовка к экзамену (зачету) должна проводиться систематически, в течение всего семестра.
2. Интенсивная подготовка должна начаться не позднее, чем за месяц до экзамена.
3. Время непосредственно перед экзаменом (зачетом) лучше использовать таким образом, чтобы оставить последний день свободным для повторения курса в целом, для систематизации материала и доработки отдельных вопросов.

На экзамене высокую оценку получают студенты, использующие данные, полученные в процессе выполнения самостоятельных работ, а также использующие собственные выводы на основе изученного материала.

Учитывая значительный объем теоретического материала, студентам рекомендуется регулярное посещение и подробное конспектирование лекций.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Microsoft Windows Server;
2. Семейство ОС Microsoft Windows;
3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом;
4. Информационно-справочная система: Система КонсультантПлюс (КонсультантПлюс);
5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (Система ГАРАНТ);
6. Электронная информационно-образовательная система ММУ: https://elearn.mmu.ru/

Перечень используемого программного обеспечения указан в п.12 данной рабочей программы дисциплины.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

12.1. Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения.

Специализированная мебель:

Комплект учебной мебели (стол, стул) по количеству обучающихся; комплект мебели для преподавателя; доска (маркерная).

Технические средства обучения:

Компьютер в сборе для преподавателя, проектор, экран, колонки

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

Windows 10, КонсультантПлюс, Система ГАРАНТ, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Adobe Acrobat Reader DC, Google Chrome, LibreOffice, Skype, Zoom.

Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду ММУ.

12.2. Помещение для самостоятельной работы обучающихся.

Специализированная мебель:

Комплект учебной мебели (стол, стул) по количеству обучающихся; комплект мебели для преподавателя; доска (маркерная).

Технические средства обучения:

Компьютер в сборе для преподавателя; компьютеры в сборе для обучающихся; колонки; проектор, экран.

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

Windows Server 2016, Windows 10, Microsoft Office, КонсультантПлюс, Система ГАРАНТ, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Adobe Acrobat Reader DC, Google Chrome, LibreOffice, Skype, Zoom, Gimp, Paint.net, AnyLogic, Inkscape.

13.Образовательные технологии, используемые при освоении дисциплины

Для освоения дисциплины используются как традиционные формы занятий – лекции (типы лекций – установочная, вводная, текущая, заключительная, обзорная; виды лекций – проблемная, визуальная, лекция конференция, лекция консультация); и семинарские (практические) занятия, так и активные и интерактивные формы занятий - деловые и ролевые игры, решение ситуационных задач и разбор конкретных ситуаций.

На учебных занятиях используются технические средства обучения мультимедийной аудитории: компьютер, монитор, колонки, настенный экран, проектор, микрофон, пакет программ Microsoft Office для демонстрации презентаций и медиафайлов, видеопроектор для демонстрации слайдов, видеосюжетов и др. Тестирование обучаемых может осуществляться с использованием компьютерного оборудования университета.

При реализации программы с применением ДОТ:

Все виды занятий проводятся в форме онлайн-вебинаров с использованием современных компьютерных технологий (наличие презентации и форума для обсуждения).

В процессе изучения дисциплины студенты выполняют практические задания и промежуточные тесты. Консультирование по изучаемым темам проводится в онлайнрежиме во время проведения вебинаров и на форуме для консультаций.

13.1. В освоении учебной дисциплины используются следующие традиционные образовательные технологии:

- чтение проблемно-информационных лекций с использованием доски и видеоматериалов;
- семинарские занятия для обсуждения, дискуссий и обмена мнениями;
- контрольные опросы;
- консультации;
- самостоятельная работа студентов с учебной литературой и первоисточниками;
- подготовка и обсуждение рефератов (проектов), презентаций (научно-исследовательская работа);
- тестирование по основным темам дисциплины.

13.2. Активные и интерактивные методы и формы обучения

Из перечня видов: («*мозговой штурм», анализ НПА, анализ проблемных ситуаций, анализ конкретных ситуаций, инциденты, имитация коллективной профессиональной деятельности, разыгрывание ролей, творческая работа, связанная с освоением дисциплины, ролевая игра, круглый стол, диспут, беседа, дискуссия, мини-конференция и др.*) используются следующие:

- *диспут*
- *анализ проблемных, творческих заданий, ситуационных задач*
- *ролевая игра;*
- *круглый стол;*
- *мини-конференция*
- *дискуссия*
- *беседа.*

13.3. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

При организации обучения по дисциплине учитываются особенности организации взаимодействия с инвалидами и лицами с ограниченными возможностями здоровья (далее – инвалиды и лица с ОВЗ) с целью обеспечения их прав. При обучении учитываются особенности их психофизического развития, индивидуальные возможности и при необходимости обеспечивается коррекция нарушений развития и социальная адаптация указанных лиц.

Выбор методов обучения определяется содержанием обучения, уровнем методического и материально-технического обеспечения, особенностями восприятия учебной информации студентов-инвалидов и студентов с ограниченными возможностями здоровья и т.д. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Приложение

Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Информационная безопасность

Направление подготовки	**Экономика**
Код	38.03.01
Направленность (профиль)	Бухгалтерский учет, анализ и аудит
Квалификация выпускника	бакалавр

Москва
2025 г.

1. Перечень кодов компетенций, формируемых дисциплиной в процессе освоения образовательной программы

Группа компетенций	Категория компетенций	Код
Профессиональные компетенции	-	ПК-19

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-19	Способен к выработке мероприятий по воздействию на риск в разрезе отдельных видов и проводить анализ и оценку рисков	ПК-19.1 Применяет в профессиональной деятельности современные методики анализа и оценки рисков ПК-19.3 Владеет конкретными способами предупреждения рисков и управления рисками в организации

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

Планируемые результаты обучения по дисциплине представлены дескрипторами (знания, умения, навыки).

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-19**		
Способен к выработке мероприятий по воздействию на риск в разрезе отдельных видов и проводить анализ и оценку рисков	– содержание проблемы информационной безопасности в условиях широкого применения и использование информационных компьютерных систем и вычислительных сетей;	– применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий.	– основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером; – основными понятиями и методами информационной безопасности

3.2. Критерии оценки результатов обучения по дисциплине

Шкала оценивания	Индикаторы достижения	Показатели оценивания результатов обучения
ОТЛИЧНО	Знает:	- студент глубоко и всесторонне усвоил материал, уверенно, логично, последовательно и грамотно его излагает, опираясь на знания основной и дополнительной литературы, - на основе системных научных знаний делает квалифицированные выводы и обобщения, свободно оперирует категориями и понятиями.
	Умеет:	- студент умеет самостоятельно и правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, используя научные понятия, ссылаясь на нормативную базу.
	Владеет:	- студент владеет рациональными методами (с использованием рациональных методик) решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал навыки - выделения главного, - связкой теоретических положений с требованиями руководящих документов, - изложения мыслей в логической последовательности, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
ХОРОШО	Знает:	- студент твердо усвоил материал, достаточно грамотно его излагает, опираясь на знания основной и дополнительной литературы, - затрудняется в формулировании квалифицированных выводов и обобщений, оперирует категориями и понятиями, но не всегда правильно их верифицирует.
	Умеет:	- студент умеет самостоятельно и в основном правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, не в полной мере используя научные понятия и ссылки на нормативную базу.
	Владеет:	- студент в целом владеет рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении смог продемонстрировать достаточность, но не глубинность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.

УДОВЛЕТВОРИТЕЛЬНО	Знает:	- студент ориентируется в материале, однако затрудняется в его изложении; - показывает недостаточность знаний основной и дополнительной литературы; - слабо аргументирует научные положения; - практически не способен сформулировать выводы и обобщения; - частично владеет системой понятий.
	Умеет:	- студент в основном умеет решить учебно-профессиональную задачу или задание, но допускает ошибки, слабо аргументирует свое решение, недостаточно использует научные понятия и руководящие документы.
	Владеет:	- студент владеет некоторыми рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал недостаточность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
НЕУДОВЛЕТВОРИТЕЛЬНО	Знает:	- студент не усвоил значительной части материала; - не может аргументировать научные положения; - не формулирует квалифицированных выводов и обобщений; - не владеет системой понятий.
	Умеет:	студент не показал умение решать учебно-профессиональную задачу или задание.
	Владеет:	не выполнены требования, предъявляемые к навыкам, оцениваемым «удовлетворительно».

4. Типовые контрольные задания и/или иные материалы для проведения промежуточной аттестации, необходимые для оценки достижения компетенции, соотнесенной с результатами обучения по дисциплине

Типовые контрольные задания для проверки знаний студентов

Тесты

1. Перечислите виды информационной безопасности:
А) Персональная, корпоративная, государственная
Б) Локальная, глобальная, смешенная;
В) Клиентская, серверная, техническая;

2. Дайте определение понятию «Кибербезопасность» …

А) совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры;
Б) область информационных технологий, направленная на получение доступа к персональным, корпоративным и государственным данным;
В)совокупность методов и практик защиты от несанкционированного доступа злоумышленников к компьютерам, серверам, мобильным устройствам, электронным системам, сетям и к данным;

3. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации является:
А) Источником информации;
Б) Носителем информации;
В) Обладателем информации;

4. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:
А) Электронная база данных;
Б) Информационные технологии;
В) Информационно-телекоммуникационная сеть;

5. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это:
А) Доступ к информации;
Б) Шифрование информации;
В) Конфиденциальность информации;

6.Что такое персональные данные?
А) это любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
Б) это определенная информация, не относящаяся к прямо определенному, или определяемому физическому лицу, а также юридическому лицу (субъекту персональных данных) ;
В) частичная информация, относящаяся к прямо определенному, или определяемому физическому лицу и юридическому лицу (субъекту и объекту персональных данных);

7. Что относится к специальным категориям персональных данных?
А) физиологические особенности человека, а также информация о дате и месте рождения;
Б) национальная принадлежность, политические взгляды, религиозные или философские убеждения;
В) личные сведения (паспортные данные, номер телефона, сведения об образовании и профессии;

8. Что такое информационная безопасность?
А) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;
Б) практика предотвращения санкционированного доступа, для использования, раскрытия, искажения, изменения, исследования для передачи информации третьим лицам;

В) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб информационной безопасности;

9. Отношения, связанные с обработкой персональных данных, регулируются законом…
А) Приказом Президента «Об информации, информационных технологиях»;
Б) Федеральным законом «О защите информации»;
В) Федеральным законом «О персональных данных»;

10. Действия с персональными данными (согласно федеральному закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т.д это:
А) «Исправление персональных данных»;
Б) «Работа с персональными данными»;
В) «Обработка персональных данных»;

11. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом называется:
А) Авторизация;
Б) Аутентификация;
В) Идентификация.

12. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:
А) Идентификация;
Б) Аутентификация;
В) Шифрование.

13. В Федеральном законе «О персональных данных» выделяют следующие категории персональных данных:
А) главные, дополнительные, специальные;
Б) личные, публичные, государственные;
В) общедоступные, специальные, биометрические.

14.Что такое «деобезличивание» персональных данных?
А) действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными;
Б) это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному объекту персональных данных возможно определить без дополнительной информации;
В) действия, в результате которых становится невозможным без использования специальной информации определить принадлежность персональных данных конкретному лицу, обладателю персональных данных.

15. Что понимается под «обезличенные персональные данные»?
А) это данные, находящиеся в электронных системах, принадлежность которых конкретному объекту персональных данных возможно определить без дополнительной информации;

Б) это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации;
В) это персональные данные, хранимые в электронных информационных базах, которые принадлежат определенным субъектам персональных данных.

16. Дайте определение понятию «Государственная тайна»…
А) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности;
Б) режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
В) совокупность информационных ресурсов, позволяющие при существующих обстоятельствах с помощью специальных информационных систем безопасности не допустить несанкционированный доступ к сведениям.

17. Что такое «коммерческая тайна»?
А) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности.
Б) совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.
В) режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

18. За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен законодательством РФ:
А). Дисциплинарные взыскания;
Б) Административный ответственность;
В) Смертная казнь.

19. Информационная безопасность обеспечивает…
А) Блокирование информации;
Б) Искажение информации;
В) Сохранность информации;

20. Что такое киберпреступления?
А) преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства;
Б) преступная деятельность, целью которой является передача, сбор, похищение или хранение в целях передачи сведений, составляющих государственную тайну;
В) преступная деятельность, целью которой является правомерное использование компьютера, компьютерной сети или сетевого устройства;

21. Что такое «фишинг»?
А) тип кибератаки, которую злоумышленники используют для взлома системы или сети;
Б) вид интернет-мошенничества, цель которого получить идентификационные данные пользователей;
В) тип кибератаки с помощью заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО;

22. Для защиты от злоумышленников необходимо использовать:
А) Системное программное обеспечение;
Б) Прикладное программное обеспечение;
В) Антивирусные программы;

23. Что такое «ЭЦП»?
А) электронно-цифровой процессор;
Б) электронная цифровая подпись;
В) электронно-цифровой преобразователь.

24. Информация, составляющая государственную тайну не может иметь гриф…
А) «для служебного пользования»;
Б) «секретно»;
В) «совершенно секретно»;

25. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?

А) атака;
Б) угроза;
В) уязвимость.

26. Как называется государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных?

А) субъект персональных данных;
Б)оператор информационной системы;
В) оператор персональных данных.

27. Дайте определение «Оператор персональных данных» по ФЗ «О персональных данных»….

А) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и/или осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
Б) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

В) это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации.

28. Какой подход к обеспечению безопасности имеет место?
А) логический;
Б) математический;
В) комплексный.

29. Основными объектами информационной безопасности являются:
А) Компьютерные сети, базы данных;
Б) Информационные системы, государственные системы;
В) Бизнес-ориентированные, коммерческие системы.

30. Федеральный закон «О персональных данных»

А) ФЗ № 153 от 27.06.2006;
Б) ФЗ № 152 от 27.07.2006;
В) ФЗ № 150 от 27.08.2006.

31. Под информационной безопасностью понимается…
А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
В) нет правильного ответа

32. Защита информации – это..
А) комплекс мероприятий, направленных на обеспечение информационной безопасности.
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

33. От чего зависит информационная безопасность?
А) от компьютеров
Б) от поддерживающей инфраструктуры
В) от информации

34. Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

35. Доступность – это…
А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость
В) нет правильного ответа

36. Целостность – это..
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

37. Конфиденциальность – это..
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

38. Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

39. Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

40. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

41. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

42. Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

43. Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

44. Источник угрозы – это..

А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

45. Окно опасности – это…
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

46. Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

47. Угрозы можно классифицировать по нескольким критериям:
А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам ИС.

48. По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

49. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

50. Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

51. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

52. Какие существуют грани вредоносного ПО?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

53. По механизму распространения ПО различают:

А) вирусы
Б) черви
В) все ответы правильные

54. Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

55. Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

56. Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

57. Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

58. Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

59. К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

60. Отказ, ошибки, сбой – это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

61. Отказ - это…
А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

62. Ошибка – это…

А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

63. Сбой – это…
А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

64. Побочное влияние – это…
А) негативное воздействие на систему в целом или отдельные элементы
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

65. СЗИ (система защиты информации) делится:
А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

66. Что относится к человеческому компоненту СЗИ?
А) системные порты
Б) администрация
В) программное обеспечение

67. Что относится к ресурсам АС СЗИ?
А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные

68. По уровню обеспеченной защиты все системы делят:
А) сильной защиты
Б) особой защиты
В) слабой защиты

69. По активности реагирования СЗИ системы делят:
А) пассивные
Б) активные
В) полупассивные

70. Правовое обеспечение безопасности информации – это…
А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

71. Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные

72. Информацию с ограниченным доступом делят:
А) государственную тайну
Б) конфиденциальную информацию
В) достоверную информацию

73. Что относится к государственной тайне?
А) сведения, защищаемые государством в области военной, экономической … деятельности
Б) документированная информация
В) нет правильного ответа

74. Вредоносная программа - это…
А) программа, специально разработанная для нарушения нормального функционирования систем
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

75. Основополагающие документы для обеспечения безопасности внутри организации:
А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

76. К организационно - административному обеспечению информации относится:
А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

77. Что относится к организационным мероприятиям:
А) хранение документов
Б) проведение тестирования средств защиты информации
В) пропускной режим

78. Какие средства используется на инженерных и технических мероприятиях в защите информации:
А) аппаратные
Б) криптографические
В) физические

79. Программные средства – это…
А) специальные программы и системы защиты информации в информационных системах различного назначения
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

80. Криптографические средства – это…
А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего

81. Что такое киберпреступления?
А) преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства;
Б) преступная деятельность, целью которой является передача, сбор, похищение или хранение в целях передачи сведений, составляющих государственную тайну;
В) преступная деятельность, целью которой является правомерное использование компьютера, компьютерной сети или сетевого устройства;

82. Что такое «фишинг»?
А) тип кибератаки, которую злоумышленники используют для взлома системы или сети;
Б) вид интернет-мошенничества, цель которого получить идентификационные данные пользователей;
В) тип кибератаки с помощью заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО;

83. Для защиты от злоумышленников необходимо использовать:
А) Системное программное обеспечение;
Б) Прикладное программное обеспечение;
В) Антивирусные программы;

84. Что такое «ЭЦП»?
А) электронно-цифровой процессор;
Б) электронная цифровая подпись;
В) электронно-цифровой преобразователь.

85. Информация, составляющая государственную тайну не может иметь гриф…
А) «для служебного пользования»;
Б) «секретно»;
В) «совершенно секретно»;

86. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?
А) атака;
Б) угроза;
В) уязвимость.

87. Как называется государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных?
А) субъект персональных данных;
Б)оператор информационной системы;
В) оператор персональных данных.

88. Дайте определение «Оператор персональных данных» по ФЗ «О персональных данных»….

А) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и/или осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
Б) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
В) это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации.

89. Какой подход к обеспечению безопасности имеет место?
А) логический;
Б) математический;
В) комплексный.

90. Основными объектами информационной безопасности являются:
А) Компьютерные сети, базы данных;
Б) Информационные системы, государственные системы;
В) Бизнес-ориентированные, коммерческие системы.

91. Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

92. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

93. Какие существуют грани вредоносного ПО?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

94. По механизму распространения ПО различают:
А) вирусы
Б) черви
В) все ответы правильные

95. Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то

же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

96. Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

97. Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

98. Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

99. Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

100. К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

Типовые проблемные задачи

№1Оцените время раскрытия пароля, если число символов в сообщении, передаваемом в систему при попытке получить доступ к ней, равно 20, 600 симв/мин – скорость передачи символов, длина пароля равна 6, число символов в алфавите – 26. Ответ дать в месяцах.

Типовые ситуационные задачи

№ 1 Выберите необходимую длину пароля, чтобы вероятность его отгадывания не превышала 0.001 за 3 месяца. На одну попытку посылается 20 символов, скорость передачи данных равна 600 символов в минуту.

№ 2 Зашифровать с помощью алгоритма RSA сообщение на русском языке «РИМ».

Примерный перечень вопросов к промежуточной аттестации:

1. Какая информация является объектом права собственности, и какие особенности для нее характерны.
2. Охарактеризуйте избыточное кодирование в целом с точки зрения обнаружения и исправления случайных ошибок.
3. Что определяет при таком кодировании минимальное кодовое расстояние.
4. Дайте общую характеристику кода Хэмминга и равновесного кода.

5. Рассмотрите на примере шифрование аналитическими методами с использованием преобразований матричной алгебры.

6. Что представляют собой односторонние функции?

7. Как используется в алгоритме RSA с открытым ключом разложение больших чисел на простые множители?

8. Приведите классификацию методов шифрования в зависимости от способа преобразования информации.

9. Проанализируйте основные технологические этапы, реализуемые в процессе разработки КСЗИ.

10. Как реализуются резидентные функции загрузочного вируса с точки зрения его распространения.

11. Поясните сущность эвристического анализа, применяемого для удаления вирусов

5. Методические материалы, определяющие процедуры оценивания индикаторов достижения компетенций

Специфика формирования компетенций и их измерение определяется структурированием информации о состоянии уровня подготовки обучающихся.

Алгоритмы отбора и конструирования заданий для оценки достижений в предметной области, техника конструирования заданий, способы организации и проведения стандартизированный оценочных процедур, методика шкалирования и методы обработки и интерпретации результатов оценивания позволяют обучающимся освоить компетентностно-ориентированные программы дисциплин.

Формирование компетенций осуществляется в ходе всех видов занятий, практики, а контроль их сформированности на этапе текущей, промежуточной и итоговой аттестации.

Оценивание знаний, умений и навыков по учебной дисциплине осуществляется посредством использования следующих видов оценочных средств:

- опросы: устный, письменный;
- задания для практических занятий;
- ситуационные задания;
- контрольные работы;
- коллоквиумы;
- написание реферата;
- написание эссе;
- решение тестовых заданий;
- экзамен.

Опросы по вынесенным на обсуждение темам

Устные опросы проводятся во время практических занятий и возможны при проведении аттестации в качестве дополнительного испытания при недостаточности результатов тестирования и решения заданий. Вопросы опроса не должны выходить за рамки объявленной для данного занятия темы. Устные опросы необходимо строить так, чтобы вовлечь в тему обсуждения максимальное количество обучающихся в группе, проводить параллели с уже пройденным учебным материалом данной дисциплины и смежными курсами, находить удачные примеры из современной действительности, что увеличивает эффективность усвоения материала на ассоциациях.

Основные вопросы для устного опроса доводятся до сведения студентов на предыдущем практическом занятии.

Письменные опросы позволяют проверить уровень подготовки к практическому занятию всех обучающихся в группе, при этом оставляя достаточно учебного времени для

иных форм педагогической деятельности в рамках данного занятия. Письменный опрос проводится без предупреждения, что стимулирует обучающихся к систематической подготовке к занятиям. Вопросы для опроса готовятся заранее, формулируются узко, дабы обучающийся имел объективную возможность полноценно его осветить за отведенное время.

Письменные опросы целесообразно применять в целях проверки усвояемости значительного объема учебного материала, например, во время проведения аттестации, когда необходимо проверить знания обучающихся по всему курсу.

При оценке опросов анализу подлежит точность формулировок, связность изложения материала, обоснованность суждений.

Решение заданий (кейс-методы)

Решение кейс-методов осуществляется с целью проверки уровня навыков (владений) обучающегося по применению содержания основных понятий и терминов дисциплины вообще и каждой её темы в частности.

Обучающемуся объявляется условие задания, решение которого он излагает либо устно, либо письменно.

Эффективным интерактивным способом решения задания является сопоставления результатов разрешения одного задания двумя и более малыми группами обучающихся.

Задачи, требующие изучения значительного объема, необходимо относить на самостоятельную работу студентов, с непременным разбором результатов во время практических занятий. В данном случае решение ситуационных задач с глубоким обоснованием должно представляться на проверку в письменном виде.

При оценке решения заданий анализируется понимание обучающимся конкретной ситуации, правильность её понимания в соответствии с изучаемым материалом, способность обоснования выбранной точки зрения, глубина проработки рассматриваемого вопроса, умением выявить основные положения затронутого вопроса.

Решение заданий в тестовой форме

Проводится тестирование в течение изучения дисциплины

Не менее чем за 1 неделю до тестирования, преподаватель должен определить обучающимся исходные данные для подготовки к тестированию: назвать разделы (темы, вопросы), по которым будут задания в тестовой форме, теоретические источники (с точным указанием разделов, тем, статей) для подготовки.

При прохождении тестирования пользоваться конспектами лекций, учебниками, и иными материалами не разрешено.