

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»**

(Финансовый университет)

Краснодарский филиал Финуниверситета

Кафедра «Математика и информатика»

СОГЛАСОВАНО

ООО «Портал-Юг»
Генеральный директор



Е.В. Мостовой

«20» февраля 2024 г.

УТВЕРЖДАЮ

Краснодарский филиал
Финуниверситета

Директор



Э.В.Соболев

«20» февраля 2024 г.

Хроль Е.В.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

студентов, обучающихся по направлению подготовки

38.03.05 Бизнес-информатика

в соответствии с образовательными стандартами Краснодарского филиала

Финансового университета

(программа подготовки бакалавров)

*Рекомендовано Ученым советом Краснодарского филиала Финуниверситета
(протокол № 12 от 20.02.2024)*

*Одобрено кафедрой «Математика и информатика»
(протокол № 13 от 27.02.2024)*

Краснодар 2024

УДК: 330.131.52:004(075.8)

ББК:65:32.81я73

Д30, Х94

Рецензенты: В.А. Кирий кандидат физико-математических наук, доцент кафедры «Математика и информатика» Краснодарского филиала Финуниверситета. Н.Г. Пьянкова - доцент кафедры «Математика и информатика» Краснодарского филиала Финуниверситета.

Хроль Е.В. «Управление информационной безопасностью». Рабочая программа дисциплины для студентов, обучающихся по направлению подготовки 38.03.05 «Бизнес-информатика» – Краснодар: Краснодарский филиал Финуниверситета, кафедра «Математика и информатика», 2024 г.

Дисциплина Управление информационной безопасностью относится к общепрофессиональному модулю по направлению подготовки 38.03.05 Бизнес-информатика.

В рабочей программе дисциплины определены ее цель, требования к результатам освоения дисциплины, содержание программы, тематика аудиторных занятий, формы самостоятельной работы, оценочные средства для текущего контроля и промежуточной аттестации, учебно-методическое и информационное обеспечение.

Рабочая программа дисциплины

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебное издание

Формат 60X90/16. Гарнитура Times New Roman

Усл. п.л. 4,6. Изд. № _____ от _____. Тираж 100 экз. Заказ № _____

Отпечатано в Краснодарском филиале Финуниверситета

© Хроль Е.В.
© Краснодарский филиал Финуниверситета, 2024

СОДЕРЖАНИЕ

1.Наименование дисциплины	4
2.Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине	4
3.Место дисциплины в структуре образовательной программы.....	5
4.Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	6
5.Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	6
5.1.Содержание тем дисциплины	6
5.2.Учебно-тематический план.....	9
5.3.Содержание семинаров, практических занятий	10
6.Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	11
6.1.Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	11
6.2.Перечень вопросов, заданий, тем для подготовки к текущему контролю	11
7.Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	13
7.1.Описание показателей и критериев оценивания компетенций	13
7.2.Вопросы для оценки знаний и умений, характеризующих формирование компетенций	19
7.3.Тесты	Error! Bookmark not defined.
8.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	24
9.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	24
10.Методические материалы, определяющие процедуры оценивания знаний и умений, характеризующих степень сформированности компетенций	25
11.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем.....	27
11.1.Комплект лицензионного программного обеспечения:	27
11.2.Современные профессиональные базы данных и информационные справочные системы:	27
11.3.Сертифицированные программные и аппаратные средства защиты информации:.....	27
12.Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	27

1.Наименование дисциплины

Б1.О.03.08 «Управление информационной безопасностью».

2.Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине

Дисциплина «Управление информационной безопасностью» обеспечивает формирование следующих компетенций: ПКН-12, УК-7.

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПКН-12	Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1.Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Знать: анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Уметь: проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных
		2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Знать: основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Уметь: консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных
УК-7	Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого	1.Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Знать: основные требования к технике безопасности на рабочем месте, безопасным условиям труда Уметь: выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
	развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	Знать: основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах Уметь: осуществлять выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах
		3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества	Знать: пути решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества Уметь: находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества
		4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Знать: основные способы выживания в экстремальных и чрезвычайных ситуациях Уметь: действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания

3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к Общепрофессиональному модулю учебного плана направления подготовки бакалавриата 38.03.05 Бизнес-информатика, образовательной программы «Цифровая трансформация управления бизнесом».

4.Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Очно - заочная форма обучения.

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 4 (в часах)
Общая трудоемкость дисциплины	4/108	108
Контактная работа - Аудиторные занятия	20	20
Лекции	8	8
Семинары, практические занятия	12	12
Самостоятельная работа	88	88
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет

5.Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1.Содержание тем дисциплины

Тема 1. Общие вопросы управления ИБ организации

Основные понятия, связанные с управлением ИБ Понятия: информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии и их роль в процессах управления ИБ. Угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ. Сущность управления ИБ организации Необходимость управления обеспечением ИБ организации. Процессный подход к управлению ИБ. Системный подход к управлению ИБ. Управление обеспечением ИБ организации как процесс. Циклическая модель PDCA применительно к управлению ИБ. Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Международная организация по стандартизации (ИСО, ISO). Международная электротехническая комиссия (МЭК, Национальные органы по стандартизации: Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Британский институт стандартов (BSI), Национальный институт стандартов и технологий США (NIST), Федеральное ведомство по безопасности информационных технологий (BSI, Германия). Общие сведения о стандартах США, Великобритании и Германии, касающихся вопросов управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Нормы и правила менеджмента ИБ. Цели и меры управления. Организация обеспечения информационной безопасности. Области контроля. Международные стандарты по общим вопросам управления ИБ (ISO 27001, ISO 27002, ISO 27003) и гармонизированные с ними

российские национальные стандарты.

Тема 2. Специальные вопросы управления ИБ организации

Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО БР ИББС. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и вопросы его использования. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Менеджмент риска информационной безопасности. Менеджмент инцидентов информационной безопасности. Обеспечение непрерывности деятельности и восстановления после прерываний. Обеспечение ИБ на стадиях жизненного цикла автоматизированных систем. Критерии оценки безопасности информационных технологий и автоматизированных систем.

Тема 3. Реализация системы управления ИБ организации.

Планирование в управлении ИБ

Определение приоритетов организации для разработки системы управления ИБ организации. Определение области действия системы управления ИБ организации. Определение защищаемых активов информационной инфраструктуры организации, их классификация. Разработка политики системы управления ИБ организации на основе характеристик бизнеса, организации, ее размещения, активов и технологий. Определение подхода к оценке риска в организации. Анализ и оценка рисков. Определение и оценка различных вариантов обработки рисков. Выбор целей и мер управления для обработки рисков.

Внедрение системы управления информационной безопасностью

Разработка плана обработки рисков. Реализация плана обработки рисков для достижения намеченных целей управления. Внедрение мер управления, выбранные на стадии планирования, для достижения целей управления. Определение способа измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления. Реализация программы по обучению и повышению квалификации сотрудников. Управление работой системой управления ИБ организации. Управление ресурсами системы управления ИБ организации. Внедрение процедур и других мер управления, обеспечивающих быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

Анализ системы управления ИБ организации. Выполнение процедуры мониторинга и анализа.

Совершенствование системы управления ИБ организации.

Выявление возможностей улучшения системы управления ИБ организации. Выполнение необходимых корректирующих и предупреждающих действий. Передача подробной информации о действиях по улучшению системы управления ИБ организации всем заинтересованным сторонам. Обеспечение внедрения улучшений системы управления ИБ организации для достижения

запланированных целей.

Тема 4. Внутренние нормативные документы по управлению ИБ организации.

Документационное обеспечение управления информационной безопасностью организации.

Задачи и назначение документационного обеспечения управления информационной безопасностью организации. Иерархия внутренних нормативных документов по управлению информационной безопасностью организации.

Требования к организации документационного обеспечения управления информационной безопасностью организации.

Политика информационной безопасности организации. Роль политики ИБ как основного внутреннего нормативного документа по ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ

Другие документы по управлению ИБ.

Частные политики ИБ, их назначение и состав. Примеры областей обеспечения ИБ, управляемые частными политиками. Документы, содержащие положения ИБ, применяемые к процедурам обеспечения ИБ. Документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ.

5.2. Учебно-тематический план

№ п/ п	Наименование темы (раздела) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа - Аудиторная работа			Самостоят ельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практические занятия		
1	Общие вопросы управления ИБ организации	26	4	1	3	22	Доклады, презентации и дискуссии
2	Специальные вопросы управления ИБ организации	27	5	2	3	22	
3	Реализация системы управления ИБ организации	27	5	2	3	22	
4	Внутренние нормативные документы по управлению ИБ организации	28	6	3	3	22	
В целом по дисциплине		108	20	8	12	88	Контрольная работа

5.3.Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Общие вопросы управления ИБ организации	Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Источники: 8.1,8.2,8.3	Групповые дискуссии презентация основных подходов. Учебное задание: сравнение подходов к управлению ИБ в ISO, России, США и Германии
Специальные вопросы управления ИБ организации	Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО и РС БР ИББС. ГОСТ Р 57580.1 и 57580.2. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний. Источники: 8.2,8.3, 8.4	Групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики ГОСТ Р 57580.2
Реализация системы управления ИБ организации	Планирование в управлении ИБ. Внедрение системы управления ИБ. Анализ системы управления ИБ. Совершенствование системы управления ИБ организации. Источники: 8.2,8.3, 8.5	Групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики оценки модели угроз
Внутренние нормативные документы по управлению ИБ организации	Иерархия внутренних нормативных документов по управлению информационной безопасностью. Требования к организации документационного обеспечения управления информационной безопасностью. Политика информационной безопасности организации. Другие документы по управлению ИБ. Источники: 8.1,8.2,8.5	Групповые дискуссии презентация основных подходов. Учебное задание: Пример составления частных политик

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

6.1.Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Общие вопросы Управления ИБ организации	Стандарты систем менеджмента качества в управлении ИБ	<ul style="list-style-type: none"> - работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Специальные вопросы управления ИБ организации	Положения ГОСТ Р 57580.1 в документах Банка России. Менеджмент инцидентов ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний.	<ul style="list-style-type: none"> - работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Реализация системы управления ИБ организации	Определение подхода к оценке риска в организации. Управление ресурсами системы управления ИБ организации. Измерение результативности мер управления для проверки соответствия требованиям ИБ.	<ul style="list-style-type: none"> - работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Внутренние нормативные документы по управлению ИБ организации	Частные политики ИБ, их назначение и состав.	<ul style="list-style-type: none"> - работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания

6.2.Перечень вопросов, заданий, тем для подготовки к текущему контролю

Основные формы текущего контроля:

- участие в дискуссиях по проблемным темам дисциплины;
- выступление с докладом по проблемным темам дисциплины;
- собеседование по теоретическим вопросам;
- выполнение аудиторных самостоятельных работ, письменных работ, обсуждение и анализ их результатов.

Примерный перечень тем контрольных работ:

1. Виды информации, подлежащей защите в РФ.
2. Оценка соответствия требованиям ИБ в КФО.
3. Профили защиты.
4. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций
5. Ключевые требования к защите информации при осуществлении переводов денежных средств.
6. Методика оценки модели угроз и ее применение.
7. Ключевые субъекты НПС.

Примерный перечень вопросов для дискуссий:

1. Национальная платежная система, ее участники и требования к обеспечению ИБ .
2. Менеджмент инцидентов ИБ.
3. Управление в инфраструктуре открытых ключей.
4. Мошеннические операции в кредитно-финансовой сфере.
5. Аудит ИБ

Примерный перечень тем докладов с презентациями

1. Международные и национальные российские стандарты по информационной безопасности.
2. Международные и национальные российские стандарты по управлению информационной безопасностью.
3. Регулирование ИБ международных карточных платежных систем.
4. Требования к обеспечению ИБ в РФ.
5. Требования к обеспечению ИБ в финансовых организациях РФ.

В течение семестра студент может набрать максимальное количество баллов равное 40. На промежуточную аттестацию (экзамен) отводится 60 баллов. Распределение баллов по видам работ, формирующих текущий контроль успеваемости по дисциплине, отражает качество подготовки обучающихся к занятиям семинарского типа и выполнение различных видов самостоятельной работы.

Критерии балльной оценки различных форм текущего контроля успеваемости

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры «Математика и информатика» Краснодарского филиала Финансового университета.

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

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Управление информационной безопасностью» текущего контроля и промежуточной аттестации.

7.1. Описание показателей и критериев оценивания компетенций

Планируемые результаты освоения компетенции (индикатора достижения компетенции)	Уровень освоения				Оценочное средство
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»	
ПKN-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных					
Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных					
Знать: Анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Фрагментарное представление об анализе рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Неполное представление об анализе рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Сформированные, но содержащие отдельные пробелы представления об анализе рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Сформированные систематические представления об анализе рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Вопросы для оценки знаний и умений, тестовые задания.
Уметь: Проводить анализ рынка вычислительного оборудования, систем хранения	Фрагментарное умение проводить анализ рынка вычислительного оборудования, систем хранения	Несистематическое умение проводить анализ рынка вычислительного оборудования, систем хранения	В целом успешное, но содержащее отдельные пробелы умение проводить анализ рынка вычислительного	Сформированное умение проводить анализ рынка вычислительного оборудования, систем хранения	Вопросы для оценки знаний и умений, тестовые задания.

Планируемые результаты освоения компетенции (индикатора достижения компетенции)	Уровень освоения				Оценочное средство
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»	
данных и инфраструктурных решений центров обработки данных	данных и инфраструктурных решений центров обработки данных	хранения данных и инфраструктурных решений центров обработки данных	ного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	данных и инфраструктурных решений центров обработки данных	
Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных					
Знать: Основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Фрагментарное представление об основных вариантах использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Неполное представление об основных вариантах использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Сформированные, но содержащие отдельные пробелы представления об основных вариантах использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Сформированные систематические представления об основных вариантах использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Вопросы для оценки знаний и умений, тестовые задания.

Планируемые результаты освоения компетенции (индикатора достижения компетенции)	Уровень освоения				Оценочное средство
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»	
Уметь: Консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Фрагментарное умение консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Несистематическое умение консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	В целом успешное, но содержащее отдельные пробелы умение консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Сформированное умение консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Вопросы для оценки знаний и умений, тестовые задания.
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов					
Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда					
Знать: Основные требования к технике безопасности на рабочем месте, безопасным условиям труда	Фрагментарное представление об основных требованиях к технике безопасности на рабочем месте, безопасным условиям труда	Неполное представление об основных требованиях к технике безопасности на рабочем месте, безопасным условиям труда	Сформированные, но содержащие отдельные пробелы представления об основных требованиях к технике безопасности на рабочем месте, безопасным условиям труда	Сформированные систематические представления об основных требованиях к технике безопасности на рабочем месте, безопасным условиям труда	Вопросы для оценки знаний и умений, тестовые задания.

Планируемые результаты освоения компетенции (индикатора достижения компетенции)	Уровень освоения				Оценочное средство
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»	
Уметь: Выявлять и устранять проблемы, связанные с нарушениями и техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Фрагментарное умение выявлять и устранять проблемы, связанные с нарушениями и техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Несистематическое умение выявлять и устранять проблемы, связанные с нарушениями и техники безопасности на рабочем месте, обеспечивая безопасные условия труда	В целом успешное, но содержащее отдельные пробелы умение выявлять и устранять проблемы, связанные с нарушениями и техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Сформированное умение выявлять и устранять проблемы, связанные с нарушениями и техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Вопросы для оценки знаний и умений, тестовые задания.
Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах					
Знать: Основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	Фрагментарное представление об основных мероприятиях по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	Неполное представление об основных мероприятиях по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	Сформированные, но содержащие отдельные пробелы представления об основных мероприятиях по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	Сформированные систематические представления об основных мероприятиях по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	Вопросы для оценки знаний и умений, тестовые задания.
Уметь: Осуществлять выполнение мероприятий по защите населения и территорий в	Фрагментарное умение осуществлять выполнение мероприятий по защите населения и	Несистематическое умение осуществлять выполнение мероприятий по защите	В целом успешное, но содержащее отдельные пробелы умение осуществлять	Сформированное умение осуществлять выполнение мероприятий по защите населения и	Вопросы для оценки знаний и умений, тестовые задания.

Планируемые результаты освоения компетенции (индикатора достижения компетенции)	Уровень освоения				Оценочное средство
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»	
чрезвычайных ситуациях и военных конфликтах	территорий в чрезвычайных ситуациях и военных конфликтах	населения и территорий в чрезвычайных ситуациях и военных конфликтах	выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	территорий в чрезвычайных ситуациях и военных конфликтах	
Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества					
Знать: Пути решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества	Фрагментарное представление о путях решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества	Неполное представление о путях решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества	Сформированные, но содержащие отдельные пробелы представления о путях решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества	Сформированные систематические представления о путях решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества	Вопросы для оценки знаний и умений, тестовые задания.
Уметь: Находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для	Фрагментарное умение находить пути решения ситуаций, связанных с безопасностью жизнедеятельности	Несистематическое умение находить пути решения ситуаций, связанных с безопасностью жизнедеятельности	В целом успешное, но содержащее отдельные пробелы умение находить пути решения ситуаций, связанных с	Сформированное умение находить пути решения ситуаций, связанных с безопасностью жизнедеятельности	Вопросы для оценки знаний и умений, тестовые задания.

Планируемые результаты освоения компетенции (индикатора достижения компетенции)	Уровень освоения				Оценочное средство
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»	
сохранения природной среды, обеспечения устойчивого развития общества	людей для сохранения природной среды, обеспечения устойчивого развития общества	людей для сохранения природной среды, обеспечения устойчивого развития общества	безопасность жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества	людей для сохранения природной среды, обеспечения устойчивого развития общества	
Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания					
Знать: Основные способы выживания в экстремальных и чрезвычайных ситуациях	Фрагментарное представление об основных способах выживания в экстремальных и чрезвычайных ситуациях	Неполное представление об основных способах выживания в экстремальных и чрезвычайных ситуациях	Сформированные, но содержащие отдельные пробелы представления об основных способах выживания в экстремальных и чрезвычайных ситуациях	Сформированные систематические представления об основных способах выживания в экстремальных и чрезвычайных ситуациях	Вопросы для оценки знаний и умений, тестовые задания.
Уметь: Действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Фрагментарное умение действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Несистематическое умение действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	В целом успешное, но содержащее отдельные пробелы умение действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Сформированное умение действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Вопросы для оценки знаний и умений, тестовые задания.

7.2. Вопросы для оценки знаний и умений, характеризующих формирование компетенций

Шифр компетенции	Вопросы	Правильный ответ
ПКП-12	1. Какие действия и процессы составляют стадию проверки СУИБ?	Проверка функционирования процедуры системы управления ИБ необходима для того, чтобы гарантировать их правильную и эффективную работу или в случае выявления каких-либо нарушений определить, какие требуются совершенствования. На данном этапе автоматизированное средство может выполнять, например, следующие роли: Ведение статистики и анализ инцидентов. параметрам, помечать объекты, часто фиксируемые в качестве объектов инцидентов. Сбор метрик оценки эффективности И Б
	2. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии разработки технических заданий?	Разработка и внедрение вновь создаваемой АС производится в соответствии с ТЗ на АС, которое является основным документом, определяющим требования, предъявляемые к АС, порядок создания АС и приемку АС при вводе в действие.
	3. Что такое информационная безопасность.	Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.
	4. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии проектирования?	На данном этапе составляется перечень требований, которые должны быть соблюдены при создании системы безопасности. Они зависят от таких факторов, как потребности субъектов, протекающие в системе бизнес-процессы, угрозы (внутренние и внешние) и степень их опасности.

5. На какие категории подразделяются персональные данные?	<ul style="list-style-type: none"> • общедоступные; • биометрические; • специальные; • иные.
6. Что такое банковская тайна?	БТ хранит информацию о клиенте кредитной организации — состояние счета, личные данные и наличие долгов. Сохранять БТ обязана не только финансовая компания как организация, но и ее работники.
7. Какие вопросы защиты информации в негосударственной сфере регулирует ФСТЭК?	ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.
8. Что такое идентификация и аутентификация?	Идентификация - это присвоение объекту уникального имени - идентификатора, и сравнение идентификатора со всем перечнем присвоенных идентификационных имен. Идентификатор должен однозначно характеризовать объект, т.е. у двух разных объектов не должно быть одинаковых идентификаторов. Аутентификация - это процесс проверки подлинности предъявляемого идентификатора, а именно, является ли идентифицирующийся объект тем, за кого себя выдает. Для того, чтобы подтвердить свою подлинность, объекту необходимо предъявить нечто, что может предъявить только обладающий данным идентификатором, и никто другой.
9. В чем заключается процессный подход к управлению ИБ?	Процессный подход к управлению безопасностью, описанный в ISO/IEC 27001:2005, декларирует, что все процедуры обеспечения информационной безопасности - и в итоге весь процесс в целом - должны последовательно проходить четыре этапа: планирование,

		внедрение, проверку и внесение изменений. Такой подход гарантирует непрерывное совершенствование процесса обеспечения безопасности.
	10. Какие действия и процессы составляют стадию планирования СУИБ?	Процесс планирования включает следующие этапы: 1. Определение перечня информационных ресурсов компании. 2. Оценка критичности видов информации. 3. Оценка защищенности информационной системы (ИС), то есть выявление угроз и уязвимостей информационных ресурсов. 4. Определение информационных рисков, используя имеющиеся данные об информационной системе. 5. Выбор стратегии обработки рисков, определение мер по снижению рисков.
УК-7	1. Что такое угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ?	Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации.
	2. Что такое циклическая модель PDCA применительно к управлению ИБ?	подход к управлению для тестирования изменений и устранения проблем. PDCA расшифровывается как Plan, Do, Check, Act — «планируй, делай, проверяй, действуй». Цель PDCA — постоянное совершенствование процессов организации с течением времени, в т. ч. в управлении ИБ.
	3. Что включает выбор и применение финансовой организацией мер ЗИ согласно ГОСТ Р 57580.1-2017?	Выбор и применение финансовой организацией мер защиты информации включает: - выбор мер защиты информации, требования к

		<p>содержанию базового состава которых установлены в разделе 7 настоящего стандарта;</p> <p>- адаптацию (уточнение) при необходимости выбранного состава и содержания мер защиты информации с учетом модели угроз и нарушителей безопасности информации финансовой организации и структурно-функциональных характеристик объектов информатизации, в том числе АС, включаемых в область применения настоящего стандарта;</p> <p>- исключение из базового состава мер, не связанных с используемыми информационными технологиями;</p> <p>- дополнение при необходимости адаптированного (уточненного) состава и содержания мер защиты информации мерами, обеспечивающими выполнение требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации;</p> <p>- применение для конкретной области адаптированного (уточненного) и дополненного состава мер защиты информации в соответствии с положениями разделов 8 и 9 настоящего стандарта.</p>
	4. В каких случаях, согласно ГОСТ Р 57580.1-2017, возможно использование	При невозможности технической реализации

	компенсирующих мер ЗИ?	отдельных выбранных мер защиты информации, а также с учетом экономической целесообразности на этапах адаптации (уточнения) базового состава мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности информации, определенных в модели угроз, и нарушителей безопасности информации финансовой организации.
	5. Что такое контур безопасности и уровень защиты информации, согласно ГОСТ Р 57580.1-2017? Кем и на основании чего устанавливается уровень ЗИ финансовой организации для конкретного контура безопасности?	<p>Контур защиты безопасности - совокупность объектов информатизации, определяемая областью применения настоящего стандарта, используемых для реализации бизнес-процессов и (или) технологических процессов финансовой организации единой степени критичности (важности), для которой финансовой организацией применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации)</p> <p>Уровень защиты информации - определенная совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики (режима) защиты информации, соответствующей критичности (важности) защищаемой информации бизнес-процессов и (или) технологических процессов финансовой организации</p>
	6. Укажите стадии жизненного цикла автоматизированных систем.	Можно выделить следующие стадии (этапы) жизненного

		цикла ИС: формирование требований (концепции) на основе анализа предметной области, проектирование, реализация, внедрение (ввод системы в эксплуатацию), эксплуатация (сопровождение проекта).
	7. Назовите основные нормативно правовые документы в области управления информационной безопасности.	Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации Указ Президента Российской Федерации от 03 апреля 1995 г. N 334 Указ Президента Российской Федерации от 17 марта 2008 г. N 351 Постановление Правительства РФ от 26.06.1995 О сертификации средств защиты информации N 608
	8. Какие вопросы защиты информации в негосударственной сфере регулирует ФСБ?	Защита информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
	9. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?	1) Персональные данные гражданина РФ 2) Информация, содержащая гос.тайну
	10. Укажите типы факторов аутентификации.	Факторы аутентификации подразделяются на следующие три категории: - что-то, что субъект или объект доступа знает, например, пароли легальных субъектов доступа, ПИН-коды; - что-то, чем субъект или объект доступа обладает, например, данные, хранимые

		<p>на персональных технических устройствах аутентификации: токенах, смарт-картах и иных носителях;</p> <p>- что-то, что свойственно субъекту или объекту доступа, например, биометрические данные физического лица - легального субъекта доступа.</p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.3 Практико-ориентированные задания

Шифр компетенции	Практико-ориентированные задания	Правильный ответ
ПКП-12	1. Составьте модель угроз нарушения информационной безопасности для автоматизированной банковской системы коммерческого банка.	Проект студента
	2. Составьте проект классификатора инцидентов ИБ.	Проект студента
	3. Переформулируйте требования стандарта PCI DSS в терминах стандарта ГОСТ Р 57580.1	Проект студента
	4. В ходе проведенной службой информационной безопасности банка проверки были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ.	Проект студента
	5. В корпоративной сети кредитной организации выявлено автоматизированное рабочее место, на котором не установлен антивирус. Опишите возможные риски информационной безопасности, которые могут возникнуть.	Проект студента
	6. Составьте развернутый план частной политики менеджмента инцидентов ИБ.	Проект студента
	7. Какие факторы необходимо учитывать при выборе области действия СУИБ?	Проект студента
	8. Входные и выходные данные мониторинга и пересмотра всего процесса управления рисками информационной безопасности.	Проект студента
	9. Изложить варианты сегментации вычислительного оборудования центров обработки данных согласно требованиям к защите информации финансовых организаций.	Проект студента
УК-7	10. Разработать частную политику информационной безопасности. Политика оценки рисков информационной безопасности организации.	Политика оценки рисков информационной безопасности организации.
	11. Разработать частную политику информационной безопасности. Политика аудита информационной безопасности организации.	Политика аудита информационной безопасности организации.
	12. Разработать частную политику информационной безопасности. Политика для пограничных маршрутизаторов интранета в организации	Политика для пограничных маршрутизаторов интранета в организации
	13. Разработать частную политику информационной безопасности.	Политика удаленного доступа к интранету

	Политика удаленного доступа к интранету организации.	организации.
	14. Разработать частную политику информационной безопасности. Политика построения виртуальных частных сетей в организации.	Политика построения виртуальных частных сетей в организации.
	15. Разработать частную политику информационной безопасности. Политика для пограничной демилитаризованной зоны организации.	Политика для пограничной демилитаризованной зоны организации.
	16. Разработать частную политику информационной безопасности. Политика работы с конфиденциальной информацией организации.	Политика работы с конфиденциальной информацией организации.
	17. Разработать частную политику информационной безопасности. Политика работы с конфиденциальной информацией банка.	Политика работы с конфиденциальной информацией банка.
	18. Разработать частную политику информационной безопасности. Политика использования VPN в организации.	Политика использования VPN в организации.

7.4 Тесты

Шифр компетенции	Тестовые задания	Правильный ответ
ПКП-12	<p>1. Основная масса угроз информационной безопасности приходится на:</p> <p>а) Троянские программы б) Шпионские программы в) Черви г) Все перечисленное</p> <p>2. Определите вид идентификации и аутентификации, который получил наибольшее распространение:</p> <p>а) системы PKI б) постоянные пароли в) одноразовые пароли г) Другое (написать ответ)</p> <p>3. Определите системы распространения вирусов, в которых происходит все наиболее динамично:</p> <p>[а) Windows б) Mac OS в) Android г) Все</p> <p>4. Заключительным этапом построения системы защиты является:</p> <p>а) сопровождение б) планирование в) анализ уязвимых мест г) установка антивируса</p>	<p>1. А 2. Б 3. В 4. А 5. В 6. Б</p>

	<p>5. Определите угрозы безопасности информации, которые являются преднамеренными со стороны сотрудника организации:</p> <p>а) ошибки персонала б) открытие электронного письма, содержащего вирус в) не авторизованный доступ г) хакерская атака</p> <p>6. Определите подход к обеспечению безопасности, который имеет место:</p> <p>а) теоретический б) комплексный в) логический г) нет правильных ответов</p>	
УК-7	<p>1. Определите подход к обеспечению безопасности, который имеет место:</p> <p>а) теоретический б) комплексный в) логический г) нет верного ответа</p> <p>2. Системой криптографической защиты информации является:</p> <p>а) VFox Pro б) CAudit Pro в) Крипто г) все перечисленное</p> <p>3. Определите вирусы, которые активизируются в самом начале работы с операционной системой:</p> <p>а) загрузочные вирусы б) троянцы в) черви г) все перечисленное</p> <p>4. Stuxnet – это:</p> <p>а) троянская программа б) макровирус в) промышленный вирус г) антивирус</p> <p>5. Таргетированная атака – это:</p> <p>а) атака на сетевое оборудование б) атака на компьютерную систему крупного предприятия в) атака на конкретный компьютер пользователя г) атака рекламной кампанией, по ссылке которой обнаруживается вирус</p> <p>6. Под информационной безопасностью понимается:</p> <p>а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера,</p>	<p>1. Б 2. В 3. А 4. В 5. Б 6. А</p>

	<p>которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре</p> <p>б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия</p> <p>в) нет верного ответа</p> <p>г) варианты А,Б</p>	
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

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

Основная литература:

1. Мошак, Н. Н. Основы управления информационной безопасностью : учебное пособие / Н. Н. Мошак ; под редакцией В. В. Овчинникова. — Санкт-Петербург : ГУАП, 2022. — 141 с. — ISBN 978-5-8088-1711-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/340967>. — Режим доступа: для авториз. пользователей.

2. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/255569>. — Режим доступа: для авториз. пользователей.

3. Милославская, Н. Г. Управление информационной безопасностью: Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. — Москва : НИЯУ МИФИ, 2020. — 536 с. — ISBN 978-5-7262-2694-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/284378>. — Режим доступа: для авториз. пользователей.

4. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/328889> (дата обращения: 15.07.2024)

Дополнительная литература:

5. Кухарский, А. Н. Информационная безопасность политического процесса в системе государственного и муниципального управления : монография / А. Н. Кухарский. — Чита : ЗабГУ, 2021. — 260 с. — ISBN 978-5-9293-2742-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/271505>. — Режим доступа: для авториз. пользователей.

6. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов. — 4-е изд., стер. — Москва : ФЛИНТА, 2021. — 186 с. : ил., схем. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=93356>. — Библиогр. в кн. — ISBN 978-5-9765-1271-9. — Текст : электронный.

7. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/369482> (дата обращения: 15.07.2024)

9.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>

2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
4. Электронно-библиотечная система Znanium <http://www.znaniy.com>
5. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
6. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>
7. Электронно-библиотечная система издательства Лань <https://e.lanbook.com/>
8. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
9. Электронная библиотека Издательского дома «Гребенников» <https://grebennikon.ru/>

10. Методические материалы, определяющие процедуры оценивания знаний и умений, характеризующих степень сформированности компетенций

Рекомендации по подготовке к лекционным занятиям

Изучение дисциплины требует систематического и последовательного накопления знаний и практических навыков, следовательно, пропуски отдельных лекций необходимо сразу наверстывать посредством самостоятельного изучения пропущенной темы и консультаций с преподавателем, ведущим занятия.

Рекомендации по подготовке к практическим (семинарским) занятиям

Студентам следует на каждое практическое занятие приходить с результатами выполненной домашней работы предыдущего семинара. Такое требование связано с тем, что сложные программы обсуждаются и выполняются несколько семинаров подряд, и для работы по теме текущего семинара используются результаты работы на предыдущем семинаре и соответствующей домашней работы.

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины и приобретение практических навыков по дисциплине Управление информационной безопасностью.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны выполняться самостоятельно. Результатом выполнения задания является контрольная работа. Задание может быть выполнено как на компьютере студента (домашнем или в компьютерном классе), так и на компьютере преподавателя (домашнем или установленном в компьютерном классе).

Студентам следует:

- руководствоваться графиком самостоятельной работы, определенным РПД
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения
- разбирать на семинарах и консультациях ошибки в программах и прочие

непонятные вопросы.

Форма промежуточной аттестации по дисциплине – *зачет*.

Критерии оценивания знаний и умений, характеризующих степень сформированности компетенций:

- оценкой **«зачет»** оценивается полное освоение компетенций по данной дисциплине. Оценка выставляется при получении обучающимся от 50 до 86 и более баллов. При этом он:

знает: анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; основные требования к технике безопасности на рабочем месте, безопасным условиям труда; основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах; пути решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества; основные способы выживания в экстремальных и чрезвычайных ситуациях.

умеет: проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда; осуществлять выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах; находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества; действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания.

- оценка **«не зачет»** выставляется в том случае, если компетенции не освоены, ответы содержат существенные ошибки и обучающимся получено менее 50 баллов. При этом он:

Не знает: анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; основные требования к технике безопасности на рабочем месте, безопасным условиям труда; основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах; пути решения ситуаций, связанных с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества; основные способы выживания в экстремальных и чрезвычайных ситуациях.

Не умеет: проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; консультировать по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда; осуществлять выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах; находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества; действовать в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания.

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

11.1.Комплект лицензионного программного обеспечения:

Пакет офисных программ;
Антивирус Kaspersky.

11.2.Современные профессиональные базы данных и информационные справочные системы:

Информационно-правовая система «Консультант Плюс»;
Информационно-правовая система «Гарант»;
Система комплексного раскрытия информации «СКРИН» -
<http://www.skrin.ru/>

11.3.Сертифицированные программные и аппаратные средства защиты информации:

Не предусмотрены.

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

Лекционные и практические занятия проводятся в мультимедийных компьютерных классах.