Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт национальной и мировой экономики

Кафедра Прикладной информатики

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 10 от 22 мая 2025 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.О.20 Основы информационной безопасности

Основная профессиональная образовательная программа 01.03.05 Статистика программа Информационные системы на финансовых рынках

Квалификация (степень) выпускника бакалавр

Самара 2025

Содержание (рабочая программа)

Стр.

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Основы информационной безопасности входит в обязательную часть блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Основы алгоритмизации и программирования

Последующие дисциплины по связям компетенций: Пакеты прикладных статистических программ, Современные технологии и языки программирования, Управление информационными сервисами и контентом информационных ресурсов организации, Кибербезопасность

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Основы информационной безопасности в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Общепрофессиональные компетенции (ОПК):

ОПК-4 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ОПК-4	ОПК-4.1: Знать:	ОПК-4.2: Уметь:	ОПК-4.3: Владеть (иметь навыки):
	основные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	основными методами, способами и средствами получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных

ОПКЭ-6 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ОПКЭ-6	ОПКЭ-6.1: Знать:	ОПКЭ-6.2: Уметь:	ОПКЭ-6.3: Владеть (иметь навыки):
	основные методы, способы и средства	осуществлять поиск, накопление и обработку	основными методами, способами и средствами

	получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 3
Контактная работа, в том числе:	54.15/1.5
Занятия лекционного типа	18/0.5
Занятия семинарского типа	36/1
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	35.85/1
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	108 3

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Основы информационной безопасности представлен в таблице.

Разделы, темы дисциплины и виды занятий
Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа	ИКР	ГКР		
			Практич. занятия				
1.	Стандарты, нормативные документы по современным информационным технологиям	9	18	0.7		17	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПКЭ-6.1, ОПКЭ-6.2, ОПКЭ-6.3

	регламентирующие понятия и классификацию угроз						
2.	Принципы организации работы с информационными технологиями для защиты автоматизированных систем от угроз информационной безопасности	9	18	0.8		18.85	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПКЭ-6.1, ОПКЭ-6.2, ОПКЭ-6.3
	Контроль	18					
	Итого	**18**	**36**	**0.15**		**35.85**	

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Стандарты, нормативные документы регламентирующие понятия и классификацию угроз автоматизированных систем в КФС	лекция	Понятие информации и информационной безопасности. ГОСТы на АС.
		лекция	Типовые виды структуры АС. Угрозы безопасности АС и их классификация
		лекция	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информационных технологий.
		лекция	Сущность функционирования системы защиты информации в КФС
		лекция	Целостность, доступность и конфиденциальность информации.
2.	Способы защиты автоматизированных систем КФС от угроз информационной безопасности	лекция	Определение, классификация и общая характеристика технических каналов утечки информации.(ТКУИ). Понятие контролируемой зоны и методы определения ее размеров.
		лекция	Визуальные и акустические каналы. Защита информации в телефонных каналах.
		лекция	Защита от побочных электромагнитных излучений и наводок (ПЭМИН).
		лекция	Технические закладки. Способы обнаружения ТКУИ. Способы и методы перекрытия ТКУИ.

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Стандарты, нормативные документы регламентирующие понятия и классификацию угроз	практическое занятие	Установка виртуальной машины Oracle VM
		практическое занятие	Захват пакетов и создание IP фильтра
		практическое занятие	Исследование фрагментированных пакетов
		практическое занятие	Анализ IP заголовков и трафика

	автоматизированных систем в КФС	практическое занятие	Исследование маршрутов прохождения пакетов в эмуляторе
		практическое занятие	Исследование резервного маршрута прохождения пакетов в эмуляторе АС
		практическое занятие	Исследование реализации угроз в беспроводных WiFi сетях
		практическое занятие	Средства технических разведок (СТР)
		практическое занятие	Стационарная и носимая аппаратура СТР
2.	Способы защиты автоматизированных систем КФС от угроз информационной безопасности	практическое занятие	Акустический канал утечки информации. Схема.
		практическое занятие	Вибрационный канал утечки информации. Схема.
		практическое занятие	Проводной канал утечки информации. Схема.
		практическое занятие	Электромагнитный канал утечки информации. Схема.
		практическое занятие	Визуальный канал утечки информации. Схема.
		практическое занятие	Электросетевой канал утечки информации. Схема.
		практическое занятие	Средства съема информации.
		практическое занятие	Аппаратура защиты информации в сетях связи
		практическое занятие	Схема организации закрытого канала связи.

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок. Особенности взаимодействия с программно-аппаратными средствами защиты. Методика применения средств борьбы с вредоносными закладками на этапе эксплуатации систем КФС	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Технологии межсетевых экранов. Функции МЭ. Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ. Персональные и распределенные сетевые экраны. Проблемы безопасности МЭ. Критерии оценки межсетевых экранов.	- подготовка доклада - подготовка электронной презентации - тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

1. Каракеян, В. И. Безопасность жизнедеятельности : учебник и практикум для вузов / В. И. Каракеян, И. М. Никулина. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 313 с. — (Высшее образование). — ISBN 978-5-534-05849-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510519

Дополнительная литература

1. Резчиков, Е. А. Безопасность жизнедеятельности : учебник для вузов / Е. А. Резчиков, А. В. Рязанцева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 639 с. — (Высшее образование). — ISBN 978-5-534-12794-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511426

Литература для самостоятельного изучения

1. Бондарев В.В. Введение в информационную безопасность автоматизированных систем (2-е издание). – М.: МГТУ им. Н.Э. Баумана. 2018. – 252с

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС ; ОС "Альт Рабочая станция" 10; ОС "Альт Образование" 10
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный, МойОфис Стандартный 3, МойОфис Профессиональный 3

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)
2. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)
3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)
4. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. Справочно-правовая система «Консультант Плюс»
2. Справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран

	Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

5.6 Лаборатории и лабораторное оборудование

6. Фонд оценочных средств по дисциплине Основы информационной безопасности:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	**Форма контроля**	**Отметить нужное знаком « + »**
Текущий контроль	Оценка докладов	-
	Устный/письменный опрос	-
	Тестирование	+
	Практические задачи	-
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Общепрофессиональные компетенции (ОПК):

ОПК-4 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Планируемые результаты	**Планируемые результаты обучения по дисциплине**

обучения по программе			
	ОПК-4.1: Знать:	ОПК-4.2: Уметь:	ОПК-4.3: Владеть (иметь навыки):
	основные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	основными методами, способами и средствами получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных
Пороговый	Отрывочные сведения про основные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	Не в полном объеме осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	Не закрепленными навыками и основными методами, способами и средствами получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных
Стандартный (в дополнение к пороговому)	Твердые знания про основные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	В основном самостоятельно осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать	Устойчивыми навыками и основными методами, способами и средствами получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными

		с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	методами обработки больших данных
Повышенный (в дополнение к пороговому, стандартному)	Глубокие знания про основные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	Самостоятельно разрабатывать осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	На творческом уровне владеть навыками и основными методами, способами и средствами получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных

ОПКЭ-6 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ОПКЭ-6.1: Знать:	ОПКЭ-6.2: Уметь:	ОПКЭ-6.3: Владеть (иметь навыки):
	основные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	основными методами, способами и средствами получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных
Пороговый	Иметь общее представление об основных методах, способах и средствах получения, хранения,	Иметь представление как осуществлять поиск, накопление и обработку информации, в т.ч. с использованием	Некоторыми методами, способами и средствами получения, хранения, переработки информации; навыками использования

	переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных
Стандартный (в дополнение к пороговому)	Знать основные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	Самостоятельно осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	Основными методами, способами и средствами получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных
Повышенный (в дополнение к пороговому, стандартному)	Находить оптимальные методы, способы и средства получения, хранения, переработки информации с помощью современных информационных технологий; принципы работы с информацией в глобальных компьютерных сетях	Оптимально осуществлять поиск, накопление и обработку информации, в т.ч. с использованием компьютера и глобальных информационных сетей; применять на практике ключевые методы сбора и обработки информации из различных источников, в том числе сети Интернет; работать с компьютером; эффективно управлять информацией с помощью информационных и сквозных технологий	Набором основных методов, способов и средств получения, хранения, переработки информации; навыками использования современных технических средств и информационных технологий для решения профессиональных задач; цифровыми инструментами коммуникации, инновационными методами обработки больших данных

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые	Вид контроля/используемые оценочные средства

		результаты обучения в соотношении с результатами обучения по программе	Текущий	Промежуточный
1.	Стандарты, нормативные документы регламентирующие понятия и классификацию угроз автоматизированных систем в КФС	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПКЭ-6.1, ОПКЭ-6.2, ОПКЭ-6.3	Тестирование	Зачет
2.	Способы защиты автоматизированных систем КФС от угроз информационной безопасности	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПКЭ-6.1, ОПКЭ-6.2, ОПКЭ-6.3	Тестирование	Зачет

6.4.Оценочные материалы для текущего контроля

Практические задачи для тестирования

№ п.п	Задание	Ключ к заданию \Эталонный ответ
1	Определите какая угроза информационной безопасности является пассивной при решении задач профессиональной деятельности: 1. Копирование секретных данных. 2. Внедрение вредоносного программного обеспечения. 3. Кража носителей информации. 4. Удаление файла.	1
2	Политика безопасности организации при решении задач профессиональной деятельности: 1. Совокупность документированных управленческих решений, направленных на защиту информации. 2. Совокупность юридических законов в информации. 3. Процедура безопасности. 4. Руководство по архитектуре безопасности.	1
3	При реализации современных информационных технологий для проверки электронной цифровой подписи необходим: 1. Открытый ключ отправителя. 2. Секретный ключ отправителя. 3. Два ключа отправителя: секретный и открытый. 4. Не требуется знания никаких ключей.	1
4	Реализация современных информационных требует следующие виды систем идентификации и аутентификации: 1. Электронные и биометрические. 2. Электронные, биометрические и механические. 3. Электронные, биометрические и криптографические. 4. Электронные, биометрические и комбинированные	4

<table>
<tr><td>5</td><td>Осуществляя профессиональную деятельность, определите какую функцию не может выполнять межсетевой экран?
1. Регистрация событий.
2. Лечение файлов, зараженных вирусами.
3. Фильтрация трафика.
4. Трансляция сетевых адресов.</td><td>2</td></tr>
<tr><td>6.</td><td>Какая профессиональная деятельность требует лицензирования:
1. передача секретных данных
2. продажа секретных данных
3. продажа шифровальных устройств.</td><td>3</td></tr>
<tr><td>7.</td><td>Современные информационные технологии определяют ЭЦП как:
1. электронно-цифровой преобразователь
2. электронно-цифровая подпись
3. электронно-цифровой процессор</td><td>2</td></tr>
<tr><td>8.</td><td>Реализуя свою профессиональную деятельность укажите черты организационной защиты информации:<table><tr><td>1.Правовые методы</td><td>А. Невозможности миновать защитные средства сети (системы)</td></tr><tr><td>2. Политика ИБ</td><td>Б. Аудит, анализ уязвимостей</td></tr><tr><td>3. Защитные меры политики безопасности</td><td>В. Разработка и конкретизация правовых нормативных актов обеспечения безопасности</td></tr></table></td><td>1 - В
2 - А
3 - Б</td></tr>
<tr><td>9.</td><td>Реализуя свою профессиональную деятельность укажите характерные черты пользователей информации ограниченного доступа<table><tr><td>1. Ответственным за определение уровня классификации информации?</td><td>А. Сотрудник</td></tr><tr><td>2. Какая фигура категория является наиболее рискованной для компании</td><td>Б. Руководитель</td></tr><tr><td>3. Кто несет ответственность за то, что данные классифицированы и защищены?</td><td>В. Владелец</td></tr></table></td><td>1 - В
2 - А
3 - Б</td></tr>
<tr><td>10.</td><td>Современные информационные технологии к внутренним нарушителям информационной безопасности относят</td><td>Сотрудников организации</td></tr>
<tr><td>11.</td><td>Под угрозой безопасности информации при создании информационной системы понимается</td><td>Потенциально возможное событие, действие (воздействие), процесс или явление, которые</td></tr>
</table>

		могут привести к нанесению ущерба информации
12.	Современные технологии позволяют использовать электронную подпись для	Подтверждения подлинности электронного документа
13.	Ответственным за определение уровня классификации информации при осуществлении профессиональной деятельности является	Владелец информации
14.	Зачем современные информационные технологии предусматривают создание системы контроля управления доступом	Для контроля и управления посещением отдельных помещений, а также оперативного контроля за персоналом и временем его нахождения на территории объекта
15.	Осуществляя свою профессиональную деятельность, администратор случайно обнаруживает в логах сервера странные записи, указывающие на попытку SQL- инъекции в форме авторизации корпоративного портала. Каковы ваши первые шаги в течение следующих 30 минут	Остановить атаку — заблокировать IP- адрес злоумышленника на межсетевом экране
16.	Решая задачи администрирования сети обнаруживаете, что политика паролей в компании устарела и имеет следующие требования: 1. Минимальная длина пароля: 6 символов. 2. Обязательный набор символов: не регламентирован (можно использовать только цифры). Ваши действия	Увеличить длину пароля: минимальная длина должна быть увеличена до не менее 12 символов с использованием символов верхнего, нижнего регистров и цифр
17.	СКУД блокирует доступ при предъявлении пропуска штатному сотруднику организации в серверную комнату для осуществления им своей профессиональной деятельности	Не пропускать сотрудника, зафиксировать попытку доступа, сообщить руководству
18.	Сотрудником при решении поставленной задачи в начале рабочего дня регистрируется жалоба 1.Необъяснимо медленную работу компьютеров. 2.Появление всплывающих окон с рекламой (в том числе на русском языке, предлагающие установить какие-то "утилиты для очистки"). 3.Самопроизвольное изменение домашней страницы в браузере на неизвестный поисковый портал.	Администратору компьютерной сети немедленно отключить пораженный компьютер от локальной сети. Проверить журналы антивируса.

19.	Во время осуществления своей профессиональной деятельности сотрудник обратился в отдел ИБ в связи с тем, что часть файлов оказалась зашифрована.	Администратору сети изолировать рабочее место от сети. Оповестить руководителя. Сохранить доказательства. Восстановить данные из резервной копии.
20.	Используя информационные технологии получаете электронное письмо от якобы службы поддержки популярного облачного сервиса, которым вы пользуетесь. Письмо выглядит срочным: «Ваша учетная запись будет заблокирована в течение 24 часов!». В письме есть кнопка «Восстановить доступ»	Нельзя нажимать на ссылку и открывать вложения, если они есть. Внимательно изучить адрес отправителя. Немедленно переслать это письмо в IT-отдел или службу информационной безопасности.
21.	Осуществляя профессиональную деятельность в качестве администратора сети необходимо новому сотруднику дать доступ к корпоративным ресурсам	Получить официальную заявку от начальника функционального отдела куда устраивается сотрудник: 1. Должность и конкретные обязанности. 2. Точный список необходимых систем, программ и прав доступа. В службе каталогов создать учетную запись пользователя по утвержденному шаблону

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Стандарты, нормативные документы регламентирующие понятия и классификацию угроз автоматизированных	1. Информационные технологии требуют идентификация и аутентификация пользователей 2. При работе с информационными технологиями сталкиваются с несанкционированным доступом 3. При использовании информационных технологий необходима физическая защита компьютеров 4. Осуществляя профессиональную деятельность, необходимо классифицировать компьютерные вирусы.

систем в КФС	5. Лицензирование и в области защиты персональных данных при реализации информационных технологий 6. Российская Федерация, используя информационные технологии, подвергается угрозам 7. Для решения профессиональной задачи необходимо определить требования к построению систем безопасности предприятия 8. Современные информационные технологии подвергаются угрозам информационной безопасности
Способы защиты автоматизированных систем КФС от угроз информационной безопасности	9. Для решения поставленной задачи по защите данных какие использовать методы обеспечения информационной безопасности Российской Федерации 10. Профессиональные организации составляющие силы обеспечения информационной безопасности Российской Федерации 11. Современные технологии базируются на модели информационной безопасности 12. Профессиональная деятельность ФСТЭК при сертификации СЗИ 13. Для решения задачи подготовки ИСПДн к сертификации определить 14. Для решения задачи организации защиты коммерческой тайны 15. Пи реализации технологии электронного документооборота определить угрозы электронной почты

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	**Критерии оценивания для мероприятий контроля с применением 2-х балльной системы**
«зачтено»	ОПК-4, ОПКЭ-6
«не зачтено»	Результаты обучения не сформированы на пороговом уровне