СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Экономический***
Кафедра ***Бухгалтерского учета и аудита***

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Б1.В.14 Информационная безопасность экономических систем***

часть, формируемая участниками образовательных отношений

Специальность

38.05.01	***Экономическая безопасность***
код	наименование специальности

Программа

Экономико-правовое обеспечение экономической безопасности

Форма обучения

Очная

Для поступивших на обучение в
2023 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ПК-1. Способен разработать интегрированную систему управления рисками	ПК-1.1. Применяет современные информационные системы и технологии управления рисками	Обучающийся должен: Знать -источники возникновения информационных угроз; -каналы утечки информации; -направления и средства защиты информации; -принципы национальной безопасности. Уметь - применять правовые, организационные, технические и программные средства защиты информации; - выявлять потенциальные каналы утечки информации и определять их характеристики; - разрабатывать и обосновывать варианты эффективных управленческих решений в области управления рисками. Владеть - навыками противодействия утечке компьютерной информации; - навыками использования электронной цифровой подписи; - навыками проведения аудита локальной политики безопасности, аудита доступа к объектам - навыками профессиональной аргументации при разборе стандартных ситуаций в сфере управления рисками.
	ПК-1.2. Использует программное обеспечение для работы с информацией	Обучающийся должен: Знать - основные функциональные возможности современных программных средств. Уметь - использовать основные функциональные возможности

		современных программных средств. Владеть - навыками использования основных функциональных возможностей современных программных средств поддержки профессиональной деятельности
	ПК-1.3. Осуществляет мониторинг наиболее критичных рисков, их динамики и вырабатывает рекомендаций по дальнейшему развитию системы управления рисками	Обучающийся должен: Знать - порядок проведения мониторинга информационной безопасности объектов и систем Уметь - проводить мониторинг информационной безопасности объектов Владеть - навыками проведения мониторинга информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:
Ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач по сохранности информационных ресурсов, средств и механизмов, методов их применения.
Дисциплина Информационная безопасность экономических систем реализуется в рамках части, формируемой участниками образовательных отношений. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: Экономическая информатика, Информационные технологии и программные средства в экономике.

Дисциплина изучается на 4 курсе в 7 семестре

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

Общая трудоемкость (объем) дисциплины составляет 4 зач. ед., 144 акад. ч.

Объем дисциплины	Всего часов

	Очная форма обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	24
практических (семинарских)	40
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	79,8

Формы контроля	Семестры
дифференцированный зачет	7

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

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

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	**Основы информационной безопасности**	**4**	**8**	**0**	**16**
1.1	Понятие информационной безопасности. Основные составляющие	2	4	0	8
1.2	Наиболее распространенные угрозы информационной безопасности и её составляющие	2	4	0	8
2	**Уровни информационной безопасности**	**10**	**12**	**0**	**24**
2.1	Законодательный уровень информационной безопасности	4	4	0	8
2.2	Административный уровень информационной безопасности	4	4	0	8
2.3	Процедурный уровень информационной безопасности	2	4	0	8
3	**Программно-технические меры по обеспечению информационной безопасности**	**10**	**20**	**0**	**39,8**
3.1	Основные характеристики программно-технических мер	2	4	0	8
3.2	Идентификация и аутентификация	2	4	0	8
3.3	Протоколирование и аудит, шифрование, контроль целостности	2	4	0	8
3.4	Экранирование, анализ защищенности	2	4	0	8

3.5	Обеспечение высокой доступности	2	4	0	7,8
	Итого	**24**	**40**	**0**	**79,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Основы информационной безопасности**	
1.1	Понятие информационной безопасности. Основные составляющие	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
1.2	Наиболее распространенные угрозы информационной безопасности и её составляющие	Основные определения и критерии классификации угроз. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
2	**Уровни информационной безопасности**	
2.1	Законодательный уровень информационной безопасности	Российское законодательство в области информационной безопасности. Стандарты и спецификации в области информационной безопасности.
2.2	Административный уровень информационной безопасности	Основные понятия, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками
2.3	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.
3	**Программно-технические меры по обеспечению информационной безопасности**	
3.1	Основные характеристики программно-технических мер	Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость. Безопасное восстановление.
3.2	Идентификация и аутентификация	Основные понятия. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Ролевое управление доступом.
3.3	Протоколирование и аудит, шифрование, контроль целостности	Основные понятия. Активный аудит. Шифрование. Симметричный метод шифрования. Асимметричный метод шифрования. Секретный и открытый ключ. Криптография. Контроль целостности. Цифровые сертификаты. Электронная цифровая подпись.
3.4	Экранирование, анализ защищенности	Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер. Антивирусная защита.

3.5	Обеспечение высокой доступности	Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Основы информационной безопасности**	
1.1	Понятие информационной безопасности. Основные составляющие	1. Понятие «Информационная безопасность». 2. Место информационной безопасности и Информационной безопасности РФ. 3. Обеспечение информационной безопасности. 4. Обеспечение доступности информации. 5. Обеспечение целостности информации. 6. Обеспечение конфиденциальности информации.
1.2	Наиболее распространенные угрозы информационной безопасности и её составляющие	1. Перечислите виды угроз безопасности информации. 2. Каковы источники угроз безопасности информации? 3. Каковы проблемы защиты электронной информации? 4. Что такое компьютерное преступление? 5. Дайте классификацию компьютерным преступлениям. 6. Правовое обеспечение защиты информации. 7. Опишите механизмы преступлений с использованием пластиковых карт. 8. Опишите мошенничество на Интернет-аукционах. 9. Компьютерные вирусы и средства защиты от них. 10. Троянские программы, использование троянских программ для совершения компьютерных преступлений. 11. Что такое информационная атака? 12. Что такое информационная война? 13. Что такое электронный терроризм?
2	**Уровни информационной безопасности**	
2.1	Законодательный уровень информационной безопасности	1. Задачи Информационной безопасности общества. 2. Законодательно-правовой уровень обеспечения информационной безопасности 3. Ответственность за нарушение в сфере информационной безопасности 4. Стандарты информационной безопасности

2.2	Административный уровень информационной безопасности	1. Цели, задачи и содержание административного уровня. 2. Политика информационной безопасности 3. Содержание политики информационной безопасности фирмы 4. Разработка политики информационной безопасности
2.3	Процедурный уровень информационной безопасности	1. Управление персоналом 2. Поддержание работоспособности 3. Планирование восстановительных работ 4. Физическая защита 5. Реагирование на нарушение безопасного режима
3	**Программно-технические меры по обеспечению информационной безопасности**	
3.1	Основные характеристики программно-технических мер	1. Основные понятия программно-технического уровня информационной безопасности 2. Объективные причины, затрудняющие обеспечение надежной защиты 3. Основные сервисы безопасности
3.2	Идентификация и аутентификация	1. Понятие идентификация/аутентификация 2. Причины возможного снижения надежности идентификации 3. Парольная аутентификация 4. Проблемы парольной аутентификации 5. Характеристики идентификации/аутентификации с помощью биометрических данных 6. Каким угрозам подвержена биометрическая аутентификация
3.3	Протоколирование и аудит, шифрование, контроль целостности	1. Протоколирование и аудит. Основные понятия. 2. Активный аудит. Основные понятия. 3. Функциональные компоненты и архитектура. 4. Шифрование. 5. Контроль целостности.
3.4	Экранирование, анализ защищенности	1. Понятие межсетевого экранирования 2. Типы межсетевых экранов, краткая характеристика. 3. Технология виртуальных частных сетей (VPN)
3.5	Обеспечение высокой доступности	1. Основные понятия: • заданный уровень доступности • эффективности

		• время недоступности 2. Основные меры обеспечения высокой доступности • Структуризация системы • Высокая отказоустойчивость (резервирование, тиражирование); • Обслуживаемость информационной системы.