СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

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

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Защита данных в цифровой экономике***

Блок Б1, вариативная часть, Б1.В.ДВ.03.02
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

38.03.01 ***Экономика***
код наименование направления

Программа

Бухгалтерский учет, анализ и аудит

Форма обучения

Заочная

Для поступивших на обучение в
2020 г.

Стерлитамак 2022

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1)
Способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-8)

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1)	1 этап: Знания	Обучающийся должен знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации;
	2 этап: Умения	Обучающийся должен уметь: пользоваться нормативными документами по противодействию технической разведке;
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методами и средствами технической защиты информации;
Способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-8)	1 этап: Знания	Обучающийся должен знать: возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;
	2 этап: Умения	Обучающийся должен уметь: оценивать качество готового программного обеспечения;
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методами расчета и инструментального контроля показателей технической защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения дисциплины «Экономическая информатика».

Дисциплина изучается на 4, 5 курсах в 8, 9 семестрах

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 108 акад. ч.

Объем дисциплины	**Всего часов**
	Заочная форма обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	8
практических (семинарских)	16
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	3,8
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	80

Формы контроля	**Семестры**
зачет	9

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**	
1.8	Обеспечение режима конфиденциальности при работе с защищаемой информацией	0	2	0	6
1.10	Ответственность за правонарушения информационной безопасности и защиты информации	0	1	0	8
1	**Безымянный**	**8**	**8**	**0**	**80**
1.9	Контроль за соблюдением требований информационной безопасности и защиты информации	2	0	0	6

1.1	Понятие и сущность информационной безопасности и защиты информации	2	0	0	3
1.2	Основные угрозы информационной безопасности	2	0	0	11
1.4	Административн ый уровень обеспечения информационной безопасности	0	2	0	10
1.5	Программнотехнический уровень обеспечения защиты информации	1	0	0	9
1.6	Процедурный уровень информационной безопасности	0	1	0	8
1.7	Система защиты информации	1	0	0	8
1.3	Правовой уровень обеспечения информационной безопасности	0	2	0	11
	Итого	**8**	**8**	**0**	**80**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1.8	Обеспечение режима конфиденциально сти при работе с защищаемой информацией	Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Допуск должностных лиц, работников к конфиденциальной информации Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям
1.10	Ответственность за правонарушения информационной безопасности и защиты информации	Понятие и виды юридической ответственности за нарушение правовых норм по защите информации Меры дисциплинарной ответственности согласно

		Трудового кодекса РФ Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности Уголовная ответственность за правонарушения в области защиты государственной тайны Уголовная ответственность за правонарушения в области конфиденциальной информации
1	**Безымянный**	
1.4	Административн ый уровень обеспечения информационной безопасности	Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики ИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ.
1.6	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня Управление персоналом Физическая защита Поддержание работоспособности Реагирование на нарушения режима безопасности Планирование восстановительных работ
1.3	Правовой уровень обеспечения	Основные федеральные органы,

	информационной безопасности	генеририрующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Степени конфиденциальности сведений, составляющих коммерческую тайну. Методика формирования на фирме перечня сведений, относящихся к коммерческой тайне.

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Безымянный**	
1.9	Контроль за соблюдением требований информационной безопасности и защиты информации	Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные мероприятия по осуществлению контроля. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности.
1.1	Понятие и сущность информационной безопасности и защиты информации	Необходимость и значимость нормативноправового определения основных понятий.

		Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации
1.2	Основные угрозы информационной безопасности	Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воз-действия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.
1.5	Программнотехнический уровень обеспечения защиты информации	Программные сервисы защиты информации в ИС. Идентификация и аутентификация пользователей как передовой рубеж защиты информации. Базовые методы парольной аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности. Базовые методы криптографического преобразования данных. Потоковое и блочное шифрование. Процедура формирования электронной подписи. Экранирование информации в информационнотелекоммуникационных сетях (ИТС). Основные сервисы защиты в ИТС. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с

		ними. Антивирусные программные комплексы.
1.7	Система защиты информации	Процесс развития средств и методов защиты информации Этапы развития системы защиты информации в настоящее время Комплексный подход к построению системы защиты информации Системный подход к построению системы защиты информации Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации