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 ***Информационная безопасность в цифровой экономике***

Блок Б1, вариативная часть, Б1.В.ДВ.03.01
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 использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-8)	1 этап: Знания	Обучающийся должен знать: -автоматизированные информационные системы, используемые в экономике; -автоматизированные рабочие места; -современные информационные технологии для поиска и обработки экономической информации.
	2 этап: Умения	Обучающийся должен уметь: -использовать автоматизированные информационные системы -использовать автоматизированные рабочие ме
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: -применять в профессиональной деятельности автоматизированные информационные системы, используемые в экономике - применять в профессиональной деятельности автоматизированные рабочие места

		- проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач
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: -источники возникновения информационных угроз, -каналы утечки информации, -направления и средства защиты информации, -принципы национальной безопасности, -исследования, ведущиеся в области, информационной безопасности,
	2 этап: Умения	Обучающийся должен уметь: - применять правовые, организационные, технически, - выявлять потенциальные каналы утечки информации и определять их характеристики, - разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности, - систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: - навыками противодействия утечке компьютерной информации - навыками использования электронной цифровой подписи, - навыками проведения аудита локальной политики

		безопасности, аудита доступа к объектам, - специальной терминологией, применяемой в процессе защиты информации, - навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности

2. Место дисциплины (модуля) в структуре образовательной программы

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения дисциплины «Информатика» по программе средней школы.

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	
2.3	Процедурный уровень информационной безопасности	1	0	0	10
3	**Раздел 3. Программно-технические меры по обеспечению информационной безопасности**	**3**	**6**	**0**	**34**
3.1	Основные характеристики программно-технических мер. Идентификация и аутентификация	1	4	0	10
3.2	Протоколирование и аудит, шифрование, контроль целостности	1	0	0	10
3.3	Экранирование, анализ защищенности Обеспечение высокой доступности	1	2	0	14
1	**Раздел 1. Основы информационной безопасности**	**2**	**4**	**0**	**20**
1.1	Понятие информационной безопасности. Основные составляющие	1	0	0	10
1.2	Наиболее распространенные угрозы информационной безопасности и её составляющие	1	4	0	10
2	**Раздел 2. Уровни информационной безопасности**	**3**	**2**	**0**	**30**
2.1	Законодательный уровень информационной безопасности	1	2	0	10
2.2	Административный уровень информационной безопасности	1	0	0	10
	Итого	**8**	**12**	**0**	**84**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
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	**Раздел 3. Программно-технические меры по обеспечению информационной безопасности**	

3.1	Основные характеристики программно-технических мер. Идентификация и аутентификация	Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость. Безопасное восстановление. Основные понятия идентификации и аутентификации. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Ролевое управление доступом.
3.2	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.
3.3	Экранирование, анализ защищенности Обеспечение высокой доступности	Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер. Антивирусная защита. Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.
1	**Раздел 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	**Раздел 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.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
3	**Раздел 3. Программно-технические меры по обеспечению информационной безопасности**	

3.1	Основные характеристики программно-технических мер. Идентификация и аутентификация	1.1 Основные понятия программно-технического уровня информационной 1.2 Безопасности 1.3 Объективные причины, затрудняющие обеспечение надежной защиты 1.4 Основные сервисы безопасности 2.1. Понятие идентификация/аутентификация 2.2. Причины возможного снижения надежности идентификации 2.3. Парольная аутентификация 2.4. Проблемы парольной аутентификации 2.5. Характеристики идентификации/аутентификации с помощью биометрических данных 2.6. Каким угрозам подвержена биометрическая аутентификация
3.3	Экранирование, анализ защищенности Обеспечение высокой доступности	1.1 Понятие межсетевого экранирования 1.2. Типы межсетевых экранов, краткая характеристика 1.3. Технология виртуальных частных сетей (VPN). 2.1Основные понятия: • заданный уровень доступности • Эффективности • Время недоступности 2.2 Основные меры обеспечения высокой доступности • Структуризация системы • Высокая отказоустойчивость (резервирование, тиражирование); •Обслуживаемость информационной системы.
1	**Раздел 1. Основы информационной безопасности**	
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	**Раздел 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