

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

Факультет
Кафедра

Экономический
Бухгалтерского учета и аудита

Рабочая программа 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

код

Экономика

наименование направления

Программа

Бухгалтерский учет, анализ и аудит

Форма обучения

Заочная

Для поступивших на обучение в
2020 г.

Разработчик (составитель)

кандидат педагогических наук, доцент

Рафикова В. М.

ученая степень, должность, ФИО

Стерлитамак 2022

1. Перечень планируемых результатов обучения по дисциплине (модулю)	3
1.1. Перечень планируемых результатов освоения образовательной программы	3
1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы .	3
2. Место дисциплины (модуля) в структуре образовательной программы	4
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	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	4
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)	4
4.2. Содержание дисциплины, структурированное по разделам (темам)	5
5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....	9
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	10
6.1. Перечень учебной литературы, необходимой для освоения дисциплины	10
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	11

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	Административный уровень обеспечения информационной безопасности	0	2	0	10
1.5	Программотехнический 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 конфиденциальности 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

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

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

Курс лекционных занятий

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

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

		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

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа студентов является одной из форм учебной деятельности и представляет собой систематическую, планомерную, целенаправленную работу студентов по овладению содержания учебного материала, формированию профессиональных умений и навыков. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня. По курсу «Защита данных в цифровой экономике» самостоятельная работа обучаемых предполагает выработку навыков изучения первоисточников и другой литературы во внеаудиторное время.

Самостоятельная работа студентов проводится с целью систематизации и закрепления полученных теоретических знаний и практических умений студентов, формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу и развития познавательных способностей студентов, самостоятельности, ответственности и организованности.

Самостоятельная работа включает в себя:

- самостоятельное изучение источников, в том числе нормативных правовых актов и практики их применения;
- подготовку к практическим занятиям;
- выполнение заданий преподавателя;
- конспектирование материалов по заданию преподавателя, написание рефератов;
- оформление развернутых ответов на вопросы в электронном виде
- подготовку к промежуточному контролю;
- подготовку к зачету.

Темы для самостоятельного изучения

- 1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
- 2 Современные средства защиты информации

- 3 Современные системы компьютерной безопасности
- 4 Современные средства противодействия экономическому шпионажу
- 5 Современные криптографические системы
- 6 Криптоанализ, современное состояние
- 7 Правовые основы защиты информации
- 8 Технические аспекты обеспечения защиты информации. Современное состояние
- 9 Атаки на систему безопасности и современные методы защиты
- 10 Современные пути решения проблемы информационной безопасности РФ

Основная учебная литература

Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — URL : <https://urait.ru/bcode/468273> (дата обращения 21.06.2021)

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — URL : <https://urait.ru/bcode/477968> (дата обращения 21.06.2021)

Дополнительная учебная литература

Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — URL : <https://urait.ru/bcode/469758> (дата обращения 21.06.2021)

Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — URL : <https://urait.ru/bcode/468902> (дата обращения 21.06.2021)

Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — URL : <https://urait.ru/bcode/476798> (дата обращения 21.06.2021)

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1. Перечень учебной литературы, необходимой для освоения дисциплины

Основная учебная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — URL : <https://urait.ru/bcode/468273> (дата обращения 21.06.2021)
2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — URL : <https://urait.ru/bcode/477968> (дата обращения 21.06.2021)

Дополнительная учебная литература:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. —

- 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — URL : <https://urait.ru/bcode/469758> (дата обращения 21.06.2021)
2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — URL : <https://urait.ru/bcode/468902> (дата обращения 21.06.2021)
 3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — URL : <https://urait.ru/bcode/476798> (дата обращения 21.06.2021)

6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование документа с указанием реквизитов
--------------	--