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

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Рабочая программа дисциплины (модуля)

дисциплина ***Информационная безопасность в профессиональной деятельности***

Блок Б1, базовая часть, Б1.Б.34
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Специальность

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

Программа

специализация N 1 "Экономико-правовое обеспечение экономической безопасности"

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

Разработчик (составитель)
кандидат химических наук, доцент кафедры математического моделирования
Иремадзе Э. О.
ученая степень, должность, ФИО

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 работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)

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 работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)	1 этап: Знания	Обучающийся должен знать: методику определения направленности по назначению режимов обеспечения безопасности; методику выявления угроз информационной безопасности Российской Федерации.
	2 этап: Умения	Обучающийся должен уметь: выявлять обстоятельства, способствующие совершению планирования и осуществления деятельности по предупреждению и профилактике получения, хранения, поиска, систематизации, обработки и передачи информации и фиксировать их в информационных системах.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками анализа и умением работы с различными информационными ресурсами и технологиями.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках базовой части.
Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин:
основные знания из общего курса Профессиональная этика и служебный этикет; Экономическая информатика; Методология научных исследований; Экономика и организация предприятия.. Их наличие позволит понять принципы действия криптографических средств защиты информации, средств технической защиты информации, а также цифровых стенографических систем.

Дисциплина изучается на 1, 2 курсах в 4 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 5 зач. ед., 180 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	180
Учебных часов на контактную работу с преподавателем:	
лекций	18
практических (семинарских)	30
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	96

Формы контроля	**Семестры**
экзамен	4

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**	
1.2	Значение информационной безопасности и ее место в системе профессиональной безопасности. Классификация видов профессиональной безопасности	1	1	0	9
1.1	Понятие цифровой экономики и компетенции цифровой эпохи	1	3	0	9
3	**Способы и методы защиты информации**	**8**	**16**	**0**	**41**
1	**Организационные и правовые основы информационной безопасности**	**6**	**10**	**0**	**37**
1.3	Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности	2	1	0	9
1.4	Государственные органы в области защиты информации	2	5	0	10
2	**Угрозы информационной безопасности**	**4**	**4**	**0**	**18**

2.1	Угрозы Информационной безопасности	2	2	0	9
3.4	Подходы к реализации и этапы построения систем защиты информации	3	4	0	14
3.3	Классификация автоматизированных систем	2	4	0	9
3.2	Модели информационной безопасности	2	5	0	9
3.1	Способы и методы защиты информации	1	3	0	9
2.2	Виды атак на информационную систему	2	2	0	9
	Итого	**18**	**30**	**0**	**96**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1.2	Значение информационной безопасности и ее место в системе профессиональной безопасности. Классификация видов профессиональной безопасности	Принципы обеспечения информационной безопасности.Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.
1.1	Понятие цифровой экономики и компетенции цифровой эпохи	Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятияь «информационная безопасность». Значение информационной безопасности для субъектов информационных отношений.
3	**Способы и методы защиты информации**	
1	**Организационные и правовые основы информационной безопасности**	
1.3	Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности	Характеристика стандартов в области информационной безопасности
1.4	Государственные органы в области защиты информации	Основные объекты профессиональной тайны. Государственные органы в области защиты информации. Система безопасности РФ. Характеристика деятельности федеральных служб – основных государственных регуляторов в области информационной безопасности.
2	**Угрозы информационной безопасности**	
2.1	Угрозы Информационной безопасности	Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.
3.4	Подходы к реализации и этапы построения систем защиты информации	Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. Основные меры и архитектурные принципы обеспечения обслуживаемости информационных систем.
3.3	Классификация	Классификация автоматизированных систем и

	автоматизированных систем	требования к обеспечению безопасности различных классов.
3.2	Модели информационной безопасности	Обеспечение безопасности состоит в достижении трех взаимосвязанных целей: конфиденциальность, целостность и доступность.
3.1	Способы и методы защиты информации	Защита от разглашения. Защитные действия от утечки и от несанкционированных действий (НСД) к конфиденциальной информации. Мероприятия по технической защите информации.
2.2	Виды атак на информационную систему	Методы, используемые злоумышленниками для получения доступа к конфиденциальной информации либо вывода из строя информационной системы.

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1.2	Значение информационной безопасности и ее место в системе профессиональной безопасности. Классификация видов профессиональной безопасности	Понятие и современная концепция профессиональной безопасности. Место информационной безопасности в системе профессиональной безопасности. Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.
1.1	Понятие цифровой экономики и компетенции цифровой эпохи	Тенденции современного общества, критичные с точки зрения информационной безопасности. Становление и развитие понятия «информационная безопасность». Современные подходы к определению понятия. Сущность информационной безопасности. Объекты информационной безопасности.
3	**Способы и методы защиты информации**	
1	**Организационные и правовые основы информационной безопасности**	
1.3	Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности	Обзор законодательства России как основы для обеспечения интересов личности, общества и государства в информационной сфере.
1.4	Государственные органы в области защиты информации	Свойства информации как предмета защиты. Источник конфиденциальной информации. Сведения, которые могут быть отнесены к

		государственной тайне. Политический и экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну. Основные виды конфиденциальной информации, нуждающейся в защите. Коммерческая тайна. Банковская тайна.
2	**Угрозы информационной безопасности**	
2.1	Угрозы Информационной безопасности	Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.
3.4	Подходы к реализации и этапы построения систем защиты информации	Реализация системы защиты информации на основе встраиваемых и встроенных средств защиты. Организация безопасной среды для работы обработки конфиденциальной информации. Этапы проектирования и реализации систем защиты конфиденциальной информации.
3.3	Классификация автоматизированных систем	Понятие автоматизированной системы. Цели классификации автоматизированных систем. Подходы к классификации автоматизированных систем.
3.2	Модели информационной безопасности	Основными структурными элементами информационной безопасности компьютерных систем в данной модели являются: 1. Цели защиты информации. 2. Субъекты, участвующие в процессах информационного обмена. 3. Угрозы безопасности информационных систем. 4. Уровни уязвимости информации и информационной инфраструктуры.
3.1	Способы и методы защиты информации	Способы предупреждения возможных угроз. Способы обнаружения угроз. Способы пресечения или локализации угроз. Основные способы ликвидации последствий. Основные защитные действия при реализации способов защиты информации.
2.2	Виды атак на информационную систему	Основные способы несанкционированного доступа к конфиденциальной информации.

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

Методические указания для обучающихся по освоению дисциплины При изучении дисциплины необходимо обратить внимание на то, что составление плана работы производить кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий осуществляется с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям: информация, информационные технологии, эволюция ИТ, классификация ИТ, средства и методы ИТ, поколения ЭВМ, архитектура ЭВМ, внешние и внутренние устройства ПК, компьютерная сеть, программное обеспечение, операционная система, прикладное программное обеспечение, информатизация общества, информационная деятельность, информационная культура, понятие информационных и коммуникационных технологий, средств информационных и коммуникационных технологий, мультимедиа, технология телекоммуникации, электронные средства учебного назначения, электронные учебники, базы данных и базы знаний, экспертные обучающие системы, интеллектуальные обучающие системы, образовательные порталы и сайты, электронный портфолио, дистанционное обучение и др. При выполнении и защите лабораторных работ следует руководствоваться учебно-методическими указаниями преподавателя и рекомендованными практикумами, которые отражают технологическую составляющую дисциплины. Они помогут получить навыки работы на персональном компьютере в программных продуктах, изучение которых предусмотрено программой. Практикумы можно использовать как самоучители, с помощью которых можно самостоятельно освоить базовые компьютерные технологии. Изучение практикумов принесет максимальную пользу, если учащиеся будут читать его, одновременно выполняя предлагаемые в книгах задания. Благодаря такой методике начинают действовать средства самоконтроля: инструментарий программной среды осваивается не просто в процессе чтения, а в ходе решения практических задач. Рекомендуется сначала выполнить простые задания для освоения базовой (типовой) технологии. По мере освоения программной среды ставятся все более сложные задачи, при решении которых будут активизироваться знания дополнительных возможностей данной среды. Итак, переходя от простых заданий к более сложным, будет освоена большая часть технологических операций в конкретной программной среде и достигнут достаточно высокий профессиональный уровень. Сдача и защита лабораторной работы включает проверку электронных файлов и ответы на контрольные вопросы, которые должны продемонстрировать теоретические и практические знания, умения и навыки по соответствующей теме.

Перечень вопросов для самостоятельного изучения:

1. Назначение и структура обеспечения информационной безопасности
2. Основы регулирования отношений в информационной сфере
3. Основные нормы в сфере обеспечения информационной безопасности
4. Основы защиты тайны и персональных данных
5. История и современные направления развития информационной безопасности
6. Система организационно-правового обеспечения информационной безопасности
7. Основа информационной безопасности
8. Источники угроз защищаемой информации
9. Общая характеристика способов получения защищаемой информации
10. Принципы защиты информации.

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

6.1. Перечень учебной литературы, необходимой для освоения дисциплины

Основная учебная литература:

1. Озерский С. В., Попов И. В., Рычаго М. Е., Улендеева Н. И. Информационная безопасность https://znanium.com/catalog/document?id=358668 (дата обращения: (20.06.2021).
2. Федотова Елена Леонидовна Информационные технологии в профессиональной деятельности https://znanium.com/catalog/document?id=379718 (дата обращения: (20.06.2021).
3. Федотова Е. Л. Информационные технологии и системы https://znanium.com/catalog/document?id=386738 (дата обращения: (20.06.2021).

Дополнительная учебная литература:

1. Вдовенко Л.А. Информационная система предприятия: учеб. пособие. 2- е изд., пераб. и доп. М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. 304 с. URL: http://znanium.com/catalog.php?bookinfo=501089 (дата обращения: (20.06.2021).
2. Гришина Н.В. Информационная безопасность предприятия: учеб. пособие. 2-е изд., доп. М.: ФОРУМ: ИНФРА-М, 2017. 239 с. URL: http://znanium.com/catalog.php?bookinfo=612572 (дата обращения: (20.06.2021).

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

№ п/п	Наименование документа с указанием реквизитов