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

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

Рабочая программа дисциплины (модуля)

дисциплина ***Б1.О.23 Информационная безопасность***

обязательная часть

Направление

44.03.05 ***Педагогическое образование (с двумя профилями подготовки)***
код наименование направления

Программа

Физическая культура, Безопасность жизнедеятельности

Форма обучения

Заочная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
к.ф.-м.н., доцент
Викторов С. В.
ученая степень, должность, ФИО

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)
ОПК-2. Способен участвовать в разработке основных и дополнительных образовательных программ, разрабатывать отдельные их компоненты (в том числе с использованием информационно-коммуникационных технологий)	ОПК-2.1. Показывает пути достижения образовательных результатов в области ИКТ	Обучающийся должен: знать принципы построения и функционирования образовательных систем; закономерности организации образовательного процесса; специфику использования ИКТ в педагогической деятельности с учетом информационной безопасности.
	ОПК-2.2. Способен разрабатывать и применять отдельные компоненты основных и дополнительных образовательных программ в реальной и виртуальной образовательной среде	Обучающийся должен: уметь разрабатывать и отдельные компоненты основных и дополнительных образовательных программ в реальной и виртуальной образовательной среде с учетом информационной безопасности, в том числе с использованием ИКТ.
	ОПК-2.3. Способен осуществлять поиск информации с применением современных технологий	Обучающийся должен: владеть технологиями безопасного поиска, хранения и обработки информации для реализации основных и дополнительных образовательных программ с использованием ИКТ.
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Знать и понимать принципы работы современных информационных технологий	Обучающийся должен: знать принципы работы современных информационных технологий с учетом информационной безопасности
	ОПК-9.2. Уметь использовать принципы работы современных информационных	Обучающийся должен: уметь использовать современные информационные технологии с учетом информационной

	технологий для решения задач профессиональной деятельности	безопасности.
	ОПК-9.3. Владеть навыками использования современных информационных технологий для решения задач профессиональной деятельности	Обучающийся должен: владеть навыками использования современных информационных технологий для решения задач профессиональной деятельности с учетом информационной безопасности

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

Цели изучения дисциплины:
Дисциплина «Информационная безопасность» является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.
Основной задачей преподавания дисциплины является подготовка специалистов, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.
Уровень освоения содержания дисциплины предполагает: - Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности; Уяснение вопросов обеспечения информационной безопасности организации и проблем создания (концептуального проектирования) систем информационной безопасности; - Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ. Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, практических занятий и самостоятельной работы, должны всесторонне использоваться студентами в процессе дальнейшей профессиональной деятельности при решении широкого класса аналитических задач финансово-экономического характера.

Дисциплина изучается на 5 курсе в 9, 10 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 216 акад. ч.

Объем дисциплины	**Всего часов**
	Заочная форма обучения
Общая трудоемкость дисциплины	216
Учебных часов на контактную работу с преподавателем:	
лекций	8

практических (семинарских)	14
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	7,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	185

Формы контроля	Семестры
экзамен	10

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	**Теоретические основы информационной безопасности**	**4**	**6**	**0**	**95**
1.1	Основные понятия теории информационной безопасности	2	2	0	20
1.2	Информация как объект защиты	0	2	0	25
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	0	0	0	25
1.4	Угрозы информационной безопасности	2	2	0	25
2	**Методология защиты информации**	**4**	**8**	**0**	**90**
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	2	2	0	22
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	2	2	0	23
2.3	Политика и модели безопасности	0	2	0	25
2.4	Обзор международных стандартов информационной безопасности	0	2	0	20
	Итого	**8**	**14**	**0**	**185**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия теории информационной безопасности	Систематизация понятий в области защиты информации. Основные термины и определения

		понятий в области информационной защиты информации. Принципы построения систем защиты. Задачи защиты информации. Средства реализации комплексной защиты информации.
1.2	Информация как объект защиты	Уровни представления информации. Виды и формы представления информации. Свойства защищаемой информации. Структура и шкала ценности информации. Классификация информационных ресурсов.
1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.
2	**Методология защиты информации**	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	Методы защиты от несанкционированного доступа. Организационные и инженерно-технические методы защиты от несанкционированного доступа. Построение систем защиты от угрозы утечки по техническим каналам. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности информации.
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Защита целостности информации при хранении, обработке, транспортировке. Построение систем защиты от угрозы отказа доступа к информации. Семантический анализ.
2.3	Политика и модели безопасности	Модели разграничения доступа в рамках политики безопасности. Модели дискреционного доступа. Парольные системы разграничения доступа. Модели тематического разграничения доступа.
2.4	Обзор международных стандартов информационной безопасности	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.

Курс лекционных занятий

№	Наименование раздела /	Содержание

	темы дисциплины	
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия теории информационной безопасности	История становления и предметная информационной безопасности область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации.
1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.
2	**Методология защиты информации**	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности 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 практических 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 контрольной работы включает проверку электронных файлов и ответы на контрольные вопросы, которые должны продемонстрировать теоретические и практические знания, умения и навыки по соответствующей теме.

№ п/п	Тема и содержание	Задания по самостоятельной работе студентов	
		СР	
1	**2**	**6**	**8**
1.	**Модуль 1**	**95**	
1.1.	Основные понятия теории информационной безопасности. Информация как объект защиты	45	подготовка к индивидуальному опросу; подготовка к практическим работам; подготовка к контрольной работе;
1.2.	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности. Угрозы информационной безопасности	50	подготовка к индивидуальному опросу; подготовка к практическим работам; подготовка к контрольной работе;
2.	**Модуль 2**	**90**	
2.1.	Построение систем защиты от угрозы нарушения конфиденциальности. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	45	подготовка к индивидуальному опросу; подготовка к практическим работам;
2.2.	Политика и модели безопасности. Обзор международных стандартов информационной безопасности	45	подготовка к индивидуальному опросу; подготовка к практическим работам; подготовка к тестированию;
	Всего часов:	**185**	

Внеаудиторными формами и инструментами самостоятельной работы студентов по дисциплине являются: работа с конспектом лекций, изучение дополнительного теоретического материала, подготовка к занятиям, тестированию/контрольной работе.

Наименование тем на самостоятельное изучение:

1. Информационные войны и информационное противоборство.
2. Определение и основные виды информационных войн
3. Информационно-техническая война.
4. Информационно-психологическая война.

Вопросы для самоконтроля

1. Чем отличаются понятия «информационная война» и «информационное противоборство»?

2. Чем отличается информационная война от обычного вооруженного конфликта?

3. Какие виды информационных войн Вы можете выделить?

4. Приведите пример межкорпоративной информационной войны.

5. Можно ли рассматривать рекламу как средство ведения информационной борьбы?

6. Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.

7. Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны?

8. Каковы цели информационной войны?

9. Каковы средства и методы защиты от информационно-технического оружия?

10.Каковы особенности информационно-психологической войны?

Рекомендуемая учебно-методическая литература:

1. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации): юридическая ответственность за правонарушения : учебное пособие / В. К. Новиков. – Москва : Горячая линия – Телеком, 2015. – 175 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=457171.

2. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком, 2013. – 244 с. : ил. – (Вопросы управления информационной безопасностью. Вып. 1). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253575.

3. Беляков, С. Л. Основы разработки программ на языке С++ для систем информационной безопасности : учебное пособие : [16+] / С. Л. Беляков, А. В. Боженюк, М. В. Петряева ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 152 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612164.

4. Сычев, Ю. Н. Основы информационной безопасности: учебно-практическое пособие : учебное пособие / Ю. Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90790.

5. Галатенко, В. А. Основы информационной безопасности: Курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=233063.

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

6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. 1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 25.05.2023).
2. 2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729 (дата обращения: 25.05.2023).
3. 3. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=362895 (дата обращения: 25.05.2023).

Дополнительная учебная литература:

1. 1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 25.05.2023).
2. 2. Основы информационной безопасности: учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия – Телеком, 2011. – 558 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253056 (дата обращения: 25.05.2023).

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

№ п/п	Наименование документа с указанием реквизитов
1	Договор на доступ к ЭБС ZNANIUM.COM между БашГУ в лице директора СФ

	БашГУ и ООО «Знаниум»№ 3/22-эбс от 05.07.2022
2	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между БашГУ в лице директора СФ БашГУ и ООО «Электронное издательство ЮРАЙТ» № 1/22-эбс от 04.03.2022
3	Договор на доступ к ЭБС «Университетская библиотека онлайн» между БашГУ и «Нексмедиа» № 223-950 от 05.09.2022
4	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-948 от 05.09.2022
5	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-949 от 05.09.2022
6	Соглашение о сотрудничестве между БашГу и издательством «Лань» № 5 от 05.09.2022
7	ЭБС «ЭБ БашГУ», бессрочный договор между БашГУ и ООО «Открытые библиотечные системы» № 095 от 01.09.2014 г.
8	Договор на БД диссертаций между БашГУ и РГБ № 223-796 от 27.07.2022
9	Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между БашГУ в лице директора СФ БашГУ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019
10	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 1/23-эбс от 03.03.2023

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»)

№ п/п	Адрес (URL)	Описание страницы
1	http://ru.wikipedia.org/wiki/Netiquette	Сетевой этикет — Википедия
2	http://www.content-filtering.ru/	Интернет- СМИ "Ваш личный Интернет" - помощь родителям в организации безопасного доступа детей в сеть Интернет
3	http://internetsecure.ru/	Набор технологий и программ для безопасной работы в сети с компьютером
4	http://www.etika.ru/	Этика — сайт создан специально для пользователей Рунета, которые хотят работать в этичной, корректной и

		безопасной среде и готовы участвовать в создании такой среды
5	http://www.securityportal.ru/	Сайт по защите информации, защите приватности, безопасным сетевым взаимодействиям, криптографии.
6	http://www.oszone.net/6213/	Обеспечение безопасности детей при работе в Интернет (статья, ссылки, материалы)
7	http://www.anti-malware.ru/	Независимый информационно-аналитический портал по безопасности
8	http://www.securitylab.ru/software/1423/	Каталог программ «Защита детей от интернет угроз» (описание, сравнение, оценки)
9	http://download.live.com/familysafety	Семейная безопасность — Windows Live - программа от компании Microsoft
10	http://nicekit.ru/	Программа родительского контроля
11	https://securelist.ru/enciklopediya	Энциклопедия информационной безопасности
12	http://www.citforum.ru/security/	CITFORUM — информационная безопасность (большое количество материалов по теме)

13	http://www.infoforum.ru/	Национальный форум информационной безопасности "ИНФОФОРУМ" — электронное периодическое издание по вопросам информационной безопасности
14	http://saferinternet.ru/	Портал Российского Оргкомитета по проведению Года Безопасного Интернета (ресурсы, ссылки, документы, материалы по проблематике)
15	http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?a id=cs_teach_kids	Вопросы безопасности — сайт от компании Symantec
16	http://www.microsoft.com/rus/protect/default.mspx#	Вопросы обеспечения информационной безопасности от компании Microsoft
17	http://www.itn.ru/communities.aspx?cat_no=71586&tmpl=com	Обеспечение информационной безопасности в учебных заведениях. 4 этапа защиты компьютера — советы от компании Microsoft.
18	http://www.antispam.ru/	Проект Антиспам.Ру
19	http://laste.arvutikaitse.ee/rus/html/etusivu.htm	Основы безопасности в Интернете для молодежи интерактивный курс по

		Интернет-безопасности

6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование программного обеспечения
Kaspersky Endpoint Security
Windows 10
Office Standart 2007 Russian OpenLicensePack NoLevel Acdmc

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Тип учебной аудитории	Оснащенность учебной аудитории
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, учебная мебель, проектор, экран, учебно-наглядные пособия.
Читальный зал: помещение для самостоятельной работы.	Учебная мебель, учебно-наглядные пособия, компьютеры с доступом к сети «Интернет» и ЭИОС Филиала.
Лаборатория технической защиты информации. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
Лаборатория программно-аппаратных средств обеспечения информационной безопасности. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
Лаборатория электричества и магнетизма. Учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультацийю.	Доска, учебная мебель, оборудование для проведения лабораторных работ.