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 ***Б1.О.13 Основы информационной безопасности***

обязательная часть

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2021 г.

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

Стерлитамак 2022

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-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации.	Обучающийся должен: основные принципы формирования политики информационной безопасности и методы организации работ по реализации политики безопасности.
	ОПК-8.2. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов.	Обучающийся должен: сформировать план мероприятий для обеспечения информационной безопасности объекта защиты.
	ОПК-8.3. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов.	Обучающийся должен: навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты.
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты.	Обучающийся должен: базовый понятийный аппарат в области информационной безопасности и защиты информации; виды и состав угроз информационной безопасности; принципы и общие методы обеспечения информационной безопасности.
	ОПК-10.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной	Обучающийся должен: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе

	безопасности.	анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
	ОПК-10.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.	Обучающийся должен: методами и способами выявления угроз информационной безопасности применительно к объектам защиты с учетом содержания информационных процессов и особенностей их функционирования.

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

Цели изучения дисциплины:
В структуре образовательной программы дисциплина "Основы информационной безопасности" находится в обязательной части

Дисциплина изучается на 1 курсе в 1 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 4 зач. ед., 144 акад. ч.

Объем дисциплины	**Всего часов**
	Очно-заочная обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	16
практических (семинарских)	32
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	60

Формы контроля	**Семестры**
экзамен	1

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	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	2	4	0	5
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	2	4	0	5
2	**Модуль 2**	**8**	**16**	**0**	**30**
1.4	Угрозы информационной безопасности	2	4	0	5
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	2	4	0	10
1.2	Информация как объект защиты	2	4	0	10
1.1	Основные понятия теории информационной безопасности	2	4	0	5
1	**Модуль 1**	**8**	**16**	**0**	**30**
2.3	Политика и модели безопасности	2	4	0	10
2.4	Обзор международных стандартов информационной безопасности	2	4	0	10
	Итого	**16**	**32**	**0**	**60**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
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	**Модуль 2**	
1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные

		направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Роль и место информационной безопасность в системе национальной безопасности РФ. Нормативная деятельность, функции и задачи органов обеспечения информационной безопасности и 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.
1.1	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	**Модуль 1**	
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 / темы дисциплины	Содержание
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.
2	**Модуль 2**	
1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
1.2	Информация как объект защиты	Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.

1.1	Основные понятия теории информационной безопасности	История становления и предметная 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	**Модуль 1**	
2.3	Политика и модели безопасности	Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.
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.

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

№ п/п	Тема и содержание	Задания по самостоятельной работе студентов	
		СР	
1	**2**	**6**	**8**
1.	**Модуль 1.**	**30**	
1.1.	Основные понятия теории информационной безопасности	5	подготовка к индивидуальному опросу;
1.2.	Информация как объект защиты	10	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
1.3.	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	10	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
1.4.	Угрозы информационной безопасности	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
2.	**Модуль 2.**	**30**	
2.1.	Построение систем защиты от угрозы нарушения конфиденциальности	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам;
2.2.	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	5	подготовка к индивидуальному опросу; подготовка к лабораторным работам;
2.3.	Политика и модели безопасности	10	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к тестированию;

2.4.	Обзор международных стандартов информационной безопасности	10	подготовка к индивидуальному опросу; подготовка к лабораторным работам;
	Всего часов:	**60**	

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

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 (дата обращения: 20.06.2021).

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 (дата обращения: 20.06.2021).

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 (дата обращения: 20.06.2021).

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 (дата обращения: 20.06.2021).

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 (дата обращения: 20.06.2021).

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

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

Основная учебная литература:

1. 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: 20.06.2021).
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: 20.06.2021).
3. 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: 20.06.2021).

Дополнительная учебная литература:

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: 20.06.2021).
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: 20.06.2021).

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

№ п/п	Наименование документа с указанием реквизитов