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.23 Основы управления информационной безопасностью***

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
Гнатенко Ю. А.
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-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах.	Обучающийся должен: знать основные принципы политики управления доступом в компьютерных системах.
	ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях.	Обучающийся должен: уметь внедрять средства защиты информации в компьютерных системах и сетях.
	ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.	Обучающийся должен: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем

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

Цели изучения дисциплины:
Цель дисциплины - изучение основных понятий, методологии и применения практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.
Дисциплина реализуется в рамках обязательной части. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Теория информации», «Основы информационной безопасности».

Дисциплина изучается на 2 курсе в 3 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	20
практических (семинарских)	44
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	79,8

Формы контроля	Семестры
зачет	3

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	Протоколирование и аудит, шифрование, контроль целостности	4	6	0	9,8
1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	4	6	0	10
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	2	6	0	10
1.5	Правовые меры обеспечения информационной безопасности.	2	6	0	10
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	2	6	0	10
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security	2	6	0	10
1.2	Оценочные стандарты в информационной безопасности.	2	4	0	10

	Стандарты управления информационной безопасностью.				
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	2	4	0	10
1	**Система управления информационной безопасностью**	**20**	**44**	**0**	**79,8**
	Итого	**20**	**44**	**0**	**79,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1.8	Протоколирование и аудит, шифрование, контроль целостности	Протоколирование и аудит. Шифрование. Цифровые сертификаты.
1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Основные программно-технические меры. Идентификация и аутентификация. Управление доступом.
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	Общие положения организационной защиты. Особенности организационной защиты компьютерных информационных систем и сетей. Служба безопасности предприятия.
1.5	Правовые меры обеспечения информационной безопасности.	Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	Обоснование необходимости инвестиций в информационную безопасность компании.Методика FRAP. Методика OCTAVE (октэйв). Методика RiskWatch (риск вэтч)
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании	Этапы создания системы управления ИБ. Содержание этапов разработки и внедрения

	Digital Security	системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков. Обработка информационных рисков.Внедрение процедур системы управления ИБ. Расчет рисков по угрозе информационной безопасности. Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Роль стандартов ИБ. Оранжевая книга как оценочный стандарт.Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы доступности.Основные угрозы целостности. Вредительские программы
1	**Система управления информационной безопасностью**	

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1.8	Протоколирование и аудит, шифрование, контроль	Организация работы службы

	целостности	безопасности предприятия. Практическая работа №5
1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Проведение внутреннего аудита ИБ. Практическая работа №4
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	Служба безопасности предприятия. Практическая работа №3
1.5	Правовые меры обеспечения информационной безопасности.	Нормативные акты предприятия по информационной безопасности. Практическая работа №2
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	Разработка методики оценки рисков ИБ. Практическая работа №1
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security	Разработка политики ИБ
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Сертификация СУИБ на соответствие ISO 27001.
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	Выбор области действия СУИБ.
1	**Система управления информационной безопасностью**	

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

Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим занятиям, подготовку к докладам, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.

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

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

Основная учебная литература:

1. 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: 21.06.2021). –

Библиогр. в кн. – ISBN 978-5-9912-0271-8. – Текст : электронный.

2. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком, 2013. – 216 с. : ил. – (Вопросы управления информационной безопасностью. Вып. 4). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253578 (дата обращения: 21.06.2021). – Библиогр. в кн. – ISBN 978-5-9912-0274-9. – Текст : электронный.

Дополнительная учебная литература:

1. Кришталюк, А. Н. Правовые аспекты системы безопасности: курс лекций / А. Н. Кришталюк ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 204 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428612 (дата обращения: 21.06.2021). – Библиогр. в кн. – Текст : электронный.

2. Коваленко, Ю. И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю. И. Коваленко. – Москва : Горячая линия – Телеком, 2012. – 140 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253538 (дата обращения: 21.06.2021). – Библиогр. в кн. – ISBN 978-5-9912-0261-9. – Текст : электронный.

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

№ п/п	Наименование документа с указанием реквизитов