

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

Факультет
Кафедра

Математики и информационных технологий
Математического моделирования

Аннотация рабочей программы дисциплины (модуля)

дисциплина

Б1.В.ДВ.05.01 Защита персональных данных

часть, формируемая участниками образовательных отношений

Направление

10.03.01

код

Информационная безопасность

наименование направления

Программа

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

Форма обучения

Очно-заочная

Для поступивших на обучение в
2021 г.

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)
ПК-2. Способен использовать инструментальные средства и технологии администрирования средств защиты информации в компьютерных системах и сетях	ПК-2.1. Понимает угрозы безопасности, режимы противодействия.	разрабатывать модели угроз для информационных систем с учетом их назначения, условий и особенностей функционирования
	ПК-2.2. Способен определять состав и порядок администрирования подсистемы информационной безопасности.	Обучающийся должен: знать подходы к правовой защите информации, к организации контроля над возможными каналами их утечки
	ПК-2.3. Обладает навыками мониторинга функционирования подсистемы информационной безопасности.	Обучающийся должен: навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных

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

Цели изучения дисциплины:

Целью освоения дисциплины является подготовка бакалавров к будущей профессиональной деятельности на основе обучения основным принципам работы с персональными данными и методам их защиты.

Дисциплина реализуется в рамках части, формируемой участниками образовательных отношений. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Правовые основы профессиональной деятельности», «Теория информации», «Основы информационной безопасности»,

«Организационное и правовое обеспечение информационной безопасности», «Цифровая экономика», «Теоретические основы защиты информации», «Сети и системы передачи информации», «Техническая защита информации», «Электронный бизнес».

Дисциплина изучается на 4 курсе в 8 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 3 зач. ед., 108 акад. ч.

Объем дисциплины	Всего часов
	Очно-заочная обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	16
практических (семинарских)	32
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	59,8

Формы контроля	Семестры
зачет	8

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	Защита персональных данных	16	32	0	59,8
1.1	Правовое обеспечение защиты персональных данных	2	2	0	6
1.2	Система государственного контроля и надзора за обеспечением безопасности персональных данных	2	2	0	6
1.3	Обязанности и ответственность операторов персональных данных	2	2	0	6
1.4	Угрозы безопасности персональных данных	2	2	0	6
1.5	Классификация информационных систем персональных данных	2	4	0	6
1.6	Обработка персональных данных без	2	4	0	6

	использования средств автоматизации				
1.7	Мероприятия по защите персональных данных при их обработке в информационных системах	2	4	0	6
1.8	Организационные и технические меры безопасности при Присвоение материальному носителю идентификационного номера. Учет экземпляров материальных носителей. Идентификации информационной системы персональных данных и оператора персональных данных. Регистрация фактов несанкционированной хранение персональных данных на носителях	2	4	0	6
1.10	Разработка документов регламентирующих работу с персональными данными	0	4	0	5,8
1.9	Документальное обеспечение деятельности оператора персональных данных	0	4	0	6
	Итого	16	32	0	59,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Защита персональных данных	
1.1	Правовое обеспечение защиты персональных данных	Лабораторная работа №1
1.2	Система государственного контроля и надзора за обеспечением безопасности персональных данных	Лабораторная работа №2
1.3	Обязанности и ответственность операторов персональных данных	Лабораторная работа №3
1.4	Угрозы безопасности персональных данных	Лабораторная работа №4
1.5	Классификация информационных систем персональных данных	Лабораторная работа №5
1.6	Обработка персональных данных без использования средств автоматизации	Лабораторная работа №6
1.7	Мероприятия по защите персональных данных при их обработке в информационных системах	Лабораторная работа №7
1.8	Организационные и технические меры безопасности при Присвоение материальному носителю идентификационного номера. Учет экземпляров материальных носителей. Идентификации информационной системы персональных данных и оператора персональных данных. Регистрация фактов несанкционированной хранение персональных данных на носителях	Лабораторная работа №8
1.10	Разработка документов регламентирующих работу с персональными данными	Лабораторная работа №10
1.9	Документальное обеспечение деятельности оператора персональных данных	Лабораторная работа №9

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Защита персональных данных	
1.1	Правовое обеспечение защиты персональных	Основные нормативно-

	данных	<p>правовые акты в области защиты персональных данных. Требования ФЗ «О персональных данных». Понятийный аппарат. Обеспечение конфиденциальности персональных данных. Специальные категории персональных данных. Право субъекта персональных данных на доступ к своим персональным данным. Принципы обработки и хранения персональных данных. Условия обработки персональных данных: согласие субъекта на обработку, обрабатываемые без уведомления персональных данных. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных</p>
1.2	Система государственного контроля и надзора за обеспечением безопасности персональных данных	<p>Федеральные органы, уполномоченные в области регуляторы. Сфера деятельности регуляторов. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций. О Федеральной службе технического и экспортного контроля. О Федеральной службе безопасности. Методические документы регуляторов. Типы, основание, порядок, сроки и содержание проверок</p>
1.3	Обязанности и ответственность операторов персональных данных	<p>Обязанности операторов персональных данных: уведомление об обработке персональных данных, по устранению нарушений, при достижении целей обработки, при отзыве согласия субъекта. Ответственность оператора в</p>

		<p>области защиты персональных данных: гражданская, уголовная, административная, дисциплинарная</p>
1.4	Угрозы безопасности персональных данных	<p>Классификация угроз безопасности персональных данных. Анализ и характеристики угроз возможной утечки информации по техническим каналам. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена. Формирование перечня актуальных угроз безопасности персональным данным</p>
1.5	Классификация информационных систем персональных данных	<p>Понятие информационной системы персональных данных. Типовые и специальные информационные системы персональных данных. Структура информационной системы персональных данных. Критерии классификации типовых информационных систем персональных данных: категория обрабатываемых данных, объем обрабатываемых данных, характеристики безопасности персональных данных с учетом подключений к</p>

		<p>Интернету, режима обработки персональных данных, режима разграничения прав доступа пользователей, местонахождения технических средств.</p> <p>Таблица классификации типовой информационной системы персональных данных</p>
1.6	Обработка персональных данных без использования средств автоматизации	<p>Правовые меры защиты: распределение полномочий между субъектами; нормативно-правовой контроль использования персональных данных Назначение ответственного за защиту информации, содержащей персональных данных; правовая регламентация порядка сбора, использования, предоставления и уничтожения персональных данных</p>
1.7	Мероприятия по защите персональных данных при их обработке в информационных системах	<p>Организационно-административные меры защиты: формирование системы управления персональных данных; регламентация деятельности персонала по использованию персональных данных; регламентация порядка взаимодействия пользователей и администраторов информационных систем персональных данных; контроль над деятельностью персонала. Технические меры защиты от НСД в информационных системах персональных данных различного класса: защита от вредоносных программ и средства защиты от вторжений; идентификация и аутентификация</p>

		<p>пользователей; разграничение и контроль доступа к персональным данным; обеспечение целостности персональных данных; регистрация событий безопасности; защита каналов передачи персональных данных</p>
1.8	<p>Организационные и технические меры безопасности при Присвоение материальному носителю идентификационного номера. Учет экземпляров материальных носителей. Идентификации информационной системы персональных данных и оператора персональных данных. Регистрация фактов несанкционированной хранение персональных данных на носителях</p>	<p>Присвоение материальному носителю идентификационного номера. Учет экземпляров материальных носителей. Идентификации информационной системы персональных данных и оператора персональных данных. Регистрация фактов несанкционированной повторной и дополнительной записи информации. Применение средств электронной цифровой подписи для сохранения целостности и неизменности персональных данных. Процедура уничтожения персональных данных</p>