

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 22.08.2023 10:52:49
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad36

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

Факультет Математики и информационных технологий
Кафедра Математического моделирования

Аннотация рабочей программы дисциплины (модуля)

дисциплина Защита персональных данных

Блок Б1, вариативная часть, Б1.В.ДВ.06.01

цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01

Информационная безопасность

код

наименование направления

Программа

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

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

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 участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)

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 участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)	1 этап: Знания	Обучающийся должен знать: подходы к правовой защите информации, к организации контроля над возможными каналами их утечки
	2 этап: Умения	Обучающийся должен уметь: разрабатывать модели угроз для информационных систем с учетом их назначения, условий и особенностей функционирования
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках вариативной части. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «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 7 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
	Очная форма обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	12
практических (семинарских)	18
лабораторных	18
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	7

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	12	18	18	59,8
1.1	Правовое обеспечение защиты персональных данных	2	0	2	6
1.2	Система государственного контроля и надзора за обеспечением безопасности персональных данных	2	0	2	6
1.3	Обязанности и ответственность операторов персональных данных	2	0	2	6
1.4	Угрозы безопасности персональных данных	2	0	2	6
1.5	Классификация информационных систем персональных данных	2	0	2	6
1.6	Обработка персональных данных без использования средств автоматизации	2	2	0	6
1.7	Мероприятия по защите персональных данных при их обработке в информационных системах	0	4	2	6
1.8	Организационные и технические меры безопасности при Присвоение материальному носителю идентификационного номера. Учет	0	4	2	6

	экземпляров материальных носителей. Идентификации информационной системы персональных данных и оператора персональных данных. Регистрация фактов несанкционированной хранения персональных данных на носителях				
1.9	Документальное обеспечение деятельности оператора персональных данных	0	4	2	6
1.10	Разработка документов регламентирующих работу с персональными данными	0	4	2	5,8
	Итого	12	18	18	59,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Защита персональных данных	
1.6	Обработка персональных данных без использования средств автоматизации	Назначение ответственного за защиту информации, содержащей персональных данных; правовая регламентация порядка сбора, использования, предоставления и уничтожения персональных данных Лабораторная работа №6
1.7	Мероприятия по защите персональных данных при их обработке в информационных системах	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 пользователей; разграничение и контроль доступа к персональным данным; обеспечение целостности персональных данных; регистрация событий безопасности; защита каналов передачи персональных данных
1.8	Организационные и технические меры безопасности при Присвоение материальному носителю	Присвоение материальному носителю идентификационного номера. Учет экземпляров материальных носителей.

	идентификационного номера. Учет экземпляров материальных носителей. Идентификации информационной системы персональных данных и оператора персональных данных. Регистрация фактов несанкционированной хранения персональных данных на носителях	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
1.9	Документальное обеспечение деятельности оператора персональных данных	Локальные акты, регламентирующие работу с персональными данными в организации
1.10	Разработка документов регламентирующих работу с персональными данными	Проектирование локальных актов регламентирующих персональных данных без использования средств автоматизации. Разработка документов регулирующих защиту персональных данных в автоматизированных информационных системах.

Курс лабораторных 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
1.7	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 хранения персональных данных на носителях	Лабораторная работа №8
1.9	Документальное обеспечение деятельности оператора персональных данных	Лабораторная работа №9
1.10	Разработка документов регламентирующих работу с персональными данными	Лабораторная работа №10

Курс лекционных занятий

№	Наименование раздела /	Содержание
---	------------------------	------------

	темы дисциплины	
1	Защита персональных данных	
1.1	Правовое обеспечение защиты персональных данных	Основные нормативно-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
1.2	Система государственного контроля и надзора за обеспечением безопасности персональных данных	Федеральные органы, уполномоченные в области обеспечения безопасности персональных данных □ 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
1.3	Обязанности и ответственность операторов персональных данных	Обязанности операторов персональных данных: уведомление об обработке персональных данных, по устранению нарушений, при достижении целей обработки, при отзыве согласия субъекта. Ответственность оператора в области защиты персональных данных: гражданская, уголовная, административная, дисциплинарная
1.4	Угрозы безопасности персональных данных	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
1.5	Классификация информационных систем персональных данных	Понятие информационной системы персональных данных. Типовые и специальные информационные системы персональных данных. Структура информационной системы персональных данных. Критерии классификации типовых информационных

		<p>систем персональных данных: категория обрабатываемых данных, объем обрабатываемых данных, характеристики безопасности персональных данных с учетом подключений к 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</p>