

## Аннотация рабочей программы дисциплины (модуля)

### Защита персональных данных в организации

#### Цели дисциплины

Целью освоения дисциплины «Защита персональных данных в организации» является подготовка бакалавров к будущей профессиональной деятельности на основе обучения основным принципам работы с персональными данными и методам их защиты.

#### Задачи дисциплины

Задачами освоения дисциплины «Защита персональных данных в организации» являются:

- овладеть теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;
- изучить методы защиты персональных данных; – изучить процесс работы с персональными данными в организации;
- научить разработке документов, регламентирующих работу с персональными данными в организации

#### Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий	ПКС-1.1 - Знает виды моделей бизнес-процессов, требования к информационной системе, виды архитектур ИС; технологии программирования, тестирования и внедрения ИС; ПКС-1.2 - Умеет разрабатывать модели бизнес-процессов, требования к информационной системе, архитектуру ИС, применять технологии программирования, тестирования и внедрения ИС; ПКС-1.3 – Владеет методами разработки модели бизнес-процессов, требований к информационной системе, архитектур ИС, технологиями программирования, тестирования и внедрения ИС
ПКС-3	Способен осуществлять организацию взаимодействия с заказчиком, планирования проекта ИС; руководить разработкой программного кода, верификацией и тестированием ИС	ПКС-3.1 - Знает методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.2 - Умеет применять методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.3 - Владеет методами организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС.

#### Содержание разделов дисциплины

##### Тема 1 Правовое обеспечение защиты персональных данных. Перечень сведений конфиденциального характера.

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.

## **Тема 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 6 содержание проверок.

## **Тема 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

## **Тема 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

## **Тема 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 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. Таблица классификации типовой информационной системы персональных данных

## **Тема 6. Обработка персональных данных без использования средств автоматизации**

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

## **Тема 7. Мероприятия по защите персональных данных при их обработке в информационных системах. Рекомендации по обеспечению безопасности персональных данных при их обработке.**

Организационно-административные меры защиты: формирование системы управления персональными данными; 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

## **Тема 8. Организационные и технические меры безопасности при хранении персональных данных на носителях**

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

## **Тема 9. Документальное обеспечение деятельности оператора персональных данных** Локальные акты, регламентирующие работу с персональными данными в организации

## **Тема 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.