

Министерство просвещения Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт гуманитарного и социально-экономического образования
Кафедра документоведения, права, истории и русского языка

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.01.01 «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»**

Направление подготовки 46.03.02 Документоведение и архивоведение

Профиль программы «Правовое и документационное обеспечение
управления персоналом»

Автор(ы): канд. ист. наук, доцент, М.Б. Ларионова
заведующий кафедрой

Одобрена на заседании кафедры документоведения, права, истории и русского языка.
Протокол от «01» декабря 2022 г. № 4.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией института ГСЭО РГППУ. Протокол от «12» декабря 2022 г. № 4.

Екатеринбург
2022

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Защита персональных данных»: формирование общекультурных, общепрофессиональных и профессиональных компетенций через усвоение студентами знаний с теорией и практикой работы с документами, содержащими персональные данные сотрудников организации.

Задачи:

- изучение состава сведений, содержащих персональные данные работников;
- дать студентам представление о составе и содержании нормативно-правовых актов, регламентирующих работу с персональными данными;
- обучение студентов организации делопроизводства, обеспечивающего сохранность и учёт персональных данных работников;
- изучение современных технологий в работе с документами, содержащими персональными данными.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Защита персональных данных» относится к части учебного плана, формируемого участниками образовательных отношений.

Для изучения учебной дисциплины необходимы знания, умения и владения, формируемые следующими дисциплинами:

1. Организация и технология документационного обеспечения управления.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
- ПКС-1 Способен осуществлять организационное, документационное и информационное обеспечение деятельности организации;
- ПКС-3 Способен использовать законодательную и нормативно-методическую базу информационно-документационного обеспечения управления и архивного дела;
- ПКС-4 Способен осуществлять администрирование и документационное обеспечение процессов по управлению персоналом.

В результате освоения дисциплины (модуля) обучающийся должен:
Знать:



31. Основные понятия и определения в области документационного обеспечения управления информацией, ограниченного доступа;

32. Нормативно-методическую базу управления документами, содержащими информацию, ограниченного доступа;

33. Правила создания и оформления различных локальных документов нормативного характера для защиты конфиденциальной информации;

34. Принципы организации работы с документами, содержащими информацию ограниченного доступа.

Уметь:

У1. Использовать нормативные правовые документы в своей деятельности;

У2. Обобщать, анализировать, воспринимать информацию;

У3. Применять научные методы при исследовании объектов профессиональной деятельности;

У4. Анализировать ценность документов, содержащих персональные данные, с целью их хранения;

У5. Разрабатывать локальные нормативные акты и нормативно-методические документы по ведению информационно-документационного обеспечения управления;

У6. Обеспечивать защиту персональных данных работников и конфиденциальной информации, в том числе при организации, осуществлении и документировании процессов оценки, аттестации и развития персонала.

Владеть:

В1. Культурой мышления, способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения;

В2. Основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией;

В3. Знаниями в области права (административное, гражданское, трудовое, специальное);

В4. Навыками самостоятельной работы с различными источниками информации;

В5. Способностью вести научно-методическую работу в архивах организаций по вопросу защиты персональных данных;

В6. Способностью разрабатывать локальные нормативные акты и нормативно-методические документы (положения, инструкции и др.) по ведению документационного обеспечения управления и архивного дела;

В7. Законодательной и нормативно-методической базой документационного обеспечения управления и архивного дела; ориентируется в правовой базе смежных областей;

В8. знаниями требований к организации кадрового делопроизводства и документированию трудовых отношений, хранению документов по личному составу;



В9. Принципами, методами и нормами организации, хранения, комплектования, учета и использования архивных документов, в том числе документов личного происхождения;

В10. Навыками работы с документами, содержащими персональные данные сотрудников организации;

В11. Методами защиты информации;

В12. Тенденциями развития информационно-документационного и обеспечения управления;

В13. Принципами и методами создания справочно-информационных средств к документам.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 час.), семестр изучения – 6, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоемкости дисциплины по видам работ

Вид работы	Форма обучения
	очная
	Семестр изучения
	6 сем.
	Кол-во часов
Общая трудоемкость дисциплины по учебному плану	108
Контактная работа, в том числе:	52
Лекции	16
Практические занятия	18
Текущее консультирование	18
Самостоятельная работа студента	56
Промежуточная аттестация, в том числе:	
Зачет с оценкой	6 сем.

**Распределение трудоемкости по видам контактной работы для заочной формы обучения (при наличии) корректируется в соответствии с учебным планом заочной формы обучения.*



4.2 Содержание и тематическое планирование дисциплины

Таблица 2. Тематический план дисциплины

Наименование разделов и тем дисциплины (модуля)	Сем.	Всего, час.	Вид контактной работы, час.			СРС
			Лекции	Практ. занятия	Лаб. работы	
1. Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации	6	10	2	-	-	8
2. Работа с персональными данными на предприятии (в организации)	6	8	2	2	-	4
3. Разработка организационных мер по обеспечению защиты персональных данных	6	8	2	2	-	4
4. Техническая защита персональных данных в информационных системах	6	8	2	2	-	4
5. Формирование модели угроз безопасности персональных данных	6	10	-	2	-	8
6. Разработка (проектирование) системы защиты персональных данных	6	10	-	2	-	8
7. Развертывание, настройка и опытная эксплуатация системы защиты персональных данных в ИСПД	6	8	2	2	-	4
8. Закрытие технических каналов утечки персональных данных в ИСПД	6	8	2	2	-	4
9. Лицензирование деятельности по технической защите конфиденциальной информации	6	8	2	2	-	4
10. Оценка соответствия (аттестация) ИСПД по требованиям безопасности персональных данных	6	10	2	-	-	8

**Распределение часов по разделам (темам) дисциплины для заочной формы обучения осуществляется научно-педагогическим работником, ведущим дисциплину.*

4.3 Содержание разделов (тем) дисциплин

Раздел 1. Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации

Персональные данные в организации (на предприятии). Защита персональных данных как реализация конституционных прав граждан на



неприкосновенность частной жизни. Международное законодательство и национальное законодательство зарубежных стран о защите персональных данных. Персональные данные в системе документооборота предприятия. Персональные данные в автоматизированных системах и приложениях. Основные понятия Федерального закона 152-ФЗ «О персональных данных». Персональные данные в Федеральном законе и Трудовом кодексе РФ. Содержание категории «персональные данные». Область применения закона 152-ФЗ, ограничения. Структура, задачи и основные функции федеральных регулирующих органов, отвечающих за организацию защиты персональных данных в РФ. Требования руководящих документов ФСТЭК и ФСБ по защите персональных данных. Анализ приказа ФСТЭК России от 5.02.2010 N 58. Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение, обновление, изменение, использование, распространение (передача), обезличивание, блокирование, уничтожение. Принципы и условия обработки персональных данных. Права субъектов персональных данных и их соблюдение при обработке. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Прекращение обработки. Обработка биометрических данных. Обработка персональных данных третьим лицом в интересах оператора. Трансграничная передача персональных данных. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных. Специальные категории персональных данных и особенности их обработки. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.

Раздел 2. Работа с персональными данными на предприятии (в организации)

Мероприятия по защите сведений конфиденциального характера, правовые основания обработки персональных данных. Получение согласия субъектов на обработку. Содержание договоров с субъектами в части обработки персональных данных. Формирование перечня персональных данных. Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроль его соблюдения. Организация доступа пользователей к ИСПДн. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие. Общие сведения о конфиденциальном делопроизводстве.

Особенности обработки персональных данных, осуществляемой без использования ИСПДн. Подготовка уведомлений об обработке персональных данных в уполномоченный орган



Раздел 3. Разработка организационных мер по обеспечению защиты персональных данных

Планирование организационных мероприятий по защите персональных данных. Разработка организационно-распорядительной документации, регламентирующей вопросы организации обеспечения безопасности персональных данных и эксплуатации системы защиты персональных данных в ИСПДн. Выявление и расследование инцидентов

Раздел 4. Техническая защита персональных данных в информационных системах

Требования Федерального закона и Постановления Правительства РФ 2007 г. № 781 к обеспечению безопасности персональных данных. Обязательные механизмы защиты. Перечень основных этапов работ и краткий обзор мероприятий, необходимых для приведения ИСПД в соответствие требованиям российского законодательства по защите персональных данных. Обследование информационных систем с целью выявления фактов обработки персональных данных, форм представления персональных данных, целей и законности обработки, способов, сроков и объёмов их обработки, источников получения и др. Формирование перечня персональных данных и выделение сегментов ИСПД. Сбор, анализ и документирование исходных данных по ИСПД, необходимых для: выявления ИСПД; классификации ИСПД; определения исходной защищённости ИСПД; построения модели угроз и определения актуальности угроз; проектирования СЗПД и организации физической защиты. Описание технологии обработки и защиты персональных данных. Классификация ИСПД. Нормативная база классификации ИСПД. Критерии классификации ИСПД. Классы ИСПД. Порядок проведения классификации ИСПД и её документального оформления. Подклассы ИСПД.

Раздел 5. Формирование модели угроз безопасности персональных данных

Базовая модель угроз безопасности персональных данных. Методика определения актуальных угроз безопасности персональных данных в ИСПД. Разработка частной модели угроз безопасности персональных данных в конкретных ИСПД с учётом их назначения, условий и особенностей функционирования. Каналы утечки информации при обработке персональных данных в информационных системах. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в ИСПДн различных классов.

Раздел 6. Разработка (проектирование) системы защиты персональных данных

Определение структуры, состава и основных функций системы защиты персональных данных. Определение перечня предполагаемых к использованию сертифицированных средств защиты информации и их настроек. Техническая



защита персональных данных. Контроль безопасности обработки персональных данных. Анализ нарушений системы безопасности. Организация контроля обращения с информацией работников предприятия.

Раздел 7. Развертывание, настройка и опытная эксплуатация системы защиты персональных данных в ИСПД

Обеспечение охраны и физической защиты компонентов ИСПД. Организация и проведение работ по развёртыванию системы защиты персональных данных и настройке ее элементов в ИСПД.

Использование криптографических средств защиты информации. Испытания системы защиты персональных данных в процессе развертывания и опытной эксплуатации ИСПД.

Раздел 8. Закрытие технических каналов утечки персональных данных в ИСПД

Технические каналы утечки персональных данных при их обработке. Условия и причины возникновения, особенности проявления, способы и методы защиты. Мероприятия по защите персональных данных от утечки по техническим каналам для различных классов ИСПД.

Раздел 9. Лицензирование деятельности по технической защите конфиденциальной информации

Лицензионные требования. Подготовка документов для получения лицензии. Оценка и управление риском, связанным с отсутствием лицензии на техническую защиту конфиденциальной информации.

Раздел 10. Оценка соответствия (аттестация) ИСПД по требованиям безопасности персональных данных

Требования и порядок подготовки к проведению оценки соответствия (аттестации). Разработка методики сертификационных испытаний. Контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

Достоинства и недостатки аутсорсинга информационной безопасности.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для изучения дисциплины используются различные образовательные технологии:

1. Технологии проведения занятий в форме диалогового общения, которые переводят образовательный процесс в плоскость активного взаимодействия обучающегося и педагога. Обучающийся занимает активную позицию и престаёт быть просто слушателем семинаров или лекций. Технологии представлены: групповыми дискуссиями, конструктивный совместный поиск решения проблемы,



тренинг (микрообучение и др.), ролевые игры (деловые, организационно-деятельностные, инновационные, коммуникативные и др.).

2. Информационно-коммуникационные образовательные технологии, при которых организация образовательного процесса, основывается на применении специализированных программных сред и технических средств работы с информацией. Используются для поддержки самостоятельной работы обучающихся с использованием электронной информационно-образовательной среды (ЭИОС), телекоммуникационных технологий, педагогических программных средств и др.

3. Технология обучения в сотрудничестве применяются при проведении семинарских, практических и лабораторных занятий, нацелены на совместную работу в командах или группах и достижение качественного образовательного результата.

4. При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;

- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) университета, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС университета и других информационно-коммуникационных технологий (видеоконференцсвязь, облачные технологии и сервисы, др.);

- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1 Основная литература

1. Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0334-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/89449.html> (дата обращения: 24.12.2020). — Режим доступа: для авторизир. пользователей



2. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, А. Г. Фабричнов, Т. В. Кондрашева ; под редакцией Н. Н. Куняев. — Москва : Логос, 2016. — 500 с. — ISBN 978-5-98704-711-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/66416.html> (дата обращения: 23.12.2020). — Режим доступа: для авторизир. пользователей

3. Исаев А. С., Хлюпина Е. А. Правовые основы организации защиты персональных данных : учебное пособие. - Санкт-Петербург : Университет ИТМО, 2014. - 106 с. - Режим доступа: <http://www.iprbookshop.ru/67564>.

4. Макаров А. М., Калиберда И. В., Бондаренко К. О. Организация защиты персональных данных : практикум. - Ставрополь : Северо-Кавказский федеральный университет, 2015. - 92 с. - Режим доступа: <http://www.iprbookshop.ru/62971>.

6.2 Дополнительная литература

1. Ковалева Н. Н. Информационное право России (2-е издание) : учебное пособие. - Москва : Дашков и К, 2016. - 352 с. - Режим доступа: <http://www.iprbookshop.ru/57155>.

2. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 с. — 978-5-238-02857-6. — Режим доступа: <http://www.iprbookshop.ru/72444.html>. — ЭБС «IPRbooks»

3. Нестеров С. А. Основы информационной безопасности: учебное пособие / Нестеров С. А. — Санкт-Петербург : Лань, 2018. — 324 с. — Режим доступа: <http://e.lanbook.com/book/103908>.

6.3 Программное обеспечение и Интернет-ресурсы

Интернет-ресурсы:

1. Информационно-правовая система "Консультант-плюс". Режим доступа: <http://www.consultant.ru>

Программное обеспечение:

1. Операционная система Windows.
2. Офисная система Office Professional Plus.

Информационные системы и платформы:

1. Система дистанционного обучения «Moodle».
2. Информационная система «Таймлайн».
3. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».



7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Учебная аудитория для проведения занятий лекционного типа.
2. Учебная аудитория для проведения занятий семинарского (практического) типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации.
3. Помещения для самостоятельной работы.

