МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. Н.И. ЛОБАЧЕВСКОГО»

АРЗАМАССКИЙ ФИЛИАЛ

СОГЛАСОВАНО
Директор Арзамасского филиала ННГУ

Щелина Т.Т.
«20» октября 2022 г.

УТВЕРЖДЕНО
Ученым советом Арзамасского филиала ННГУ

(протокол от «19» октября 2022 г.№ 8)

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Организация работы и защиты персональных данных в организациях и учреждениях»

72 часа

Руководитель программы: к.п.н., доцент, доцент кафедры экономики, управления и информатики (Статуев А.А.)

Арзамас 2022

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Цель программы

Цель реализации программы – совершенствование компетенций муниципальных служащих и руководителей муниципальных учреждений в области правовой, организационной, технической, программно-аппаратной и других подсистем, методов, способов и средств, обеспечивающих защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки.

1.2. Нормативные документы для разработки программы повышения квалификации:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Федеральный закон от 02.03.2007 N 25-ФЗ (ред. от 26.05.2021) «О муниципальной службе в Российской Федерации» (с изм. и доп., вступ. в силу с 01.07.2021),

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

– Приказ Министерства образования и науки РФ от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Приказ Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 года N 522н « об утверждении – Профессионального стандарта «Специалист по защите информации в автоматизированных системах» ;

– Стандарт ВО по направлению 09.03.03Прикладная информатика Уровень бакалавриата.

1.3. Категории слушателей на обучение которых рассчитана программа повышения квалификации (далее – Программа):

муниципальные служащие и руководители муниципальных учреждений.

1.4. Входные требования к обучающимся (в случае необходимости):

_____

Задаются требования к минимуму компетенций, необходимому для успешного освоения программы.

1.5. Сфера применения слушателями полученных профессиональных компетенций, умений и знаний.

Организационная работа по защите персональных данных

2. ХАРАКТЕРИСТИКА ПОДГОТОВКИ ПО ПРОГРАММЕ

2.1. Нормативный срок освоения программы 72 часа.

2.2. Срок обучения 4 недели

2.3. Общая трудоемкость 2 ЗЕ[1]

2.4. Режим обучения 18 часов в неделю

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Слушатель, освоивший программу, должен:

3.1. обладать профессиональными компетенциями, включающими в себя способность:

ОПК-5. Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг;

3.2. знать:

– знать нормативные правовые акты и нормативно-методические документы в области комплексной защиты информации;

- знать организацию работ по обеспечению комплексной защиты информации;

3.3. уметь:

– разрабатывать необходимые документы в интересах организации работ по защите информации;

- планировать организацию мероприятий по обеспечению защиты информации;

3.4. владеть:

– владеть деятельностью по планированию и организации мероприятий по обеспечению защиты информации

3.5. Сфера применения слушателями полученных профессиональных компетенций, умений и знаний.

Организационная работа по защите персональных данных

4. ТРЕБОВАНИЯ К СТРУКТУРЕ ПРОГРАММЫ

Программа предусматривает изучение следующих модулей:

- .Законодательство о защите персональных данных. Общие понятия.
- Реализация политики защиты персональных данных в управлении персоналом организации
- Методы и средства технической защиты информации в информационных системах персональных данных.

Учебный план программы повышения квалификации представлен в Приложении №1 к программе повышения квалификации.

Календарный учебный график программы повышения квалификации представлен в Приложении №2 к программе повышения квалификации.

5. ТРЕБОВАНИЯ К ОЦЕНКЕ КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

[1] 1 ЗЕ = 36 ак. часов

«Организация работы и защиты персональных данных в организациях и учреждениях»

Программа предусматривает в качестве итоговой аттестации тестирование по следующим вопросам:

1. Вся информация делится на:
- конфиденциальную
- **общедоступную**
- государственную тайну
- **ограниченного доступа**
2. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?
- уязвимость
- слабое место системы
- **угроза**
- атака
3. В отношении информации, доступ к которой ограничен федеральными законами, необходимо соблюдать следующее требование:
- обеспечение доступности
- обеспечение неотказуемости
- **обеспечение конфиденциальности**
- обеспечение целостности
4. К какой категории персональных данных можно отнести сведения о национальной принадлежности человека?
- **специальные**
- биометрические
- общедоступные
- дополнительные
5. Как называется гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных?
- **оператор информационной системы**
- обладатель информации
- субъект информации
- обладатель информационной системы
6. Информация, к которой нельзя ограничить доступ:
- **информация о работе государственных органов**
- **информация об окружающей среде**
- персональные данные субъекта
- информация о здоровье субъекта
7. Как называется попытка реализации угрозы?
- нападение
- уязвимость
- **атака**
- слабое место системы
8. Какой Федеральный закон устанавливает эквивалентность документа, подписанного собственноручно, и электронного сообщения с ЭЦП?
- о персональных данных
- о лицензировании отдельных видов деятельности
- **об информации, информационных технологиях и о защите информации**

- о безопасности

9. На сколько групп подразделяются классы защищенности автоматизированной системы обработки информации?
- 10
- 9
- **3**
- 5

10. Каждый пользователь ЛВС должен иметь:
- **уникальный идентификатор и пароль**
- права доступа, позволяющие настраивать свое рабочее место
- свой съемный накопитель информации
- права доступа, позволяющие настраивать антивирусную защиту

11. Персональные данные, над которыми были произведены действия, в результате которых невозможно определить их принадлежность конкретному субъекту ПД, называются:
- общедоступными
- общеизвестными
- **обезличенными**
- специальными

12. Кто должен своевременно обнаруживать факты несанкционироанного доступа к персональным данным?
- субъект персональных данных
- **оператор персональных данных**
- регулятор
- контролер

13. Выдача одноразового бумажного пропуска на территорию оператора считается:
- **неавтоматизированной обработкой персональных данных**
- запрещенной обработкой персональных данных в соответствии с ФЗ “О персональных данных”
- автоматизированной обработкой персональных данных
- это неавтоматизированная обработка, если количество сотрудников оператора меньше 100 человек

14. Слабое место в системном обеспечении ИСПД, которое может быть использовано для реализации угрозы безопасности персональных данных, называется:

уязвимостью
угрозой
недостатком
брешью

15. Выдача бумажного талончика к врачу считается:
- запрещенной обработкой персональных данных в соответствии с ФЗ “О персональных данных”
- **неавтоматизированной обработкой персональных данных**
- автоматизированной обработкой персональных данных
- это неавтоматизированная обработка, если количество сотрудников больницы меньше 100 человек

16. Какой документ отражает полномочия пользователей по выполнению конкретных действий в отношении конкретных информационных ресурсов ИСПД – чтение, запись, корректировка, удаление?
- список лиц, допущенных к обработке ПД
- **матрица доступа**
- частная модель угроз
- положение по обеспечению безопасности персональных данных

17. При построении сети и конфигурировании коммуникационного оборудования рекомендуется учитывать:
- количество пользователей сети
- **разделение трафика по видам деятельности предприятия**
- **разделение трафика по производственной основе**
- расположение межсетевых экранов

18. К какому типу относится ИСПД, если в ней необходимо обеспечить целостность информации?
- **специальная**
- биометрическая
- типовая
- государственная

19. К какому классу относится ИСПД, если в ней обрабатываются данные 1500 субъектов о состоянии их здоровья?
- 3 класс
- 2 класс
- 4 класс
- **1 класс**

20. Требования к средствам защиты и их выбор в каждом конкретном случае зависит от:

категории персональных данных, обрабатываемых в ИСПД
- решения руководителя
- **класса ИСПД**
- ущерба, который может быть нанесен в результате атаки

21. Ущерб, связанный с причинением физического, морального, финансового или материального вреда непосредственно субъекту ПД, называется:
- **непосредственный ущерб**
- косвенный ущерб
- явный ущерб
- опосредованный ущерб

22. К какой категории относятся персональные данные, позволяющие идентифицировать субъекта?
- 2 категория
- 4 категория
- **3 категория**
- 1 категория

23. В ходе какого этапа построения системы защиты персональных данных определяются основные направления защиты персональных данных, и производится выбор способов защиты?
- **формирование замысла защиты**
- построение частной модели угроз
- оценка обстановки
- решение вопросов управления защитой

24. К какому типу относится ИСПД, если в ней необходимо обеспечить доступность информации?
- биометрическая
- государственная
- **специальная**
- типовая

25. Какое свойство информации требуется обеспечить в типовых информационных системах обработки персональных данных?
- целостность

- аутентичность
- **конфиденциальность**
- доступность

26. Если злоумышленник получил доступ к почтовому ящику человека и рассылает письма от его имени, о каком виде ущерба идет речь?
- опосредованный ущерб
- **непосредственный ущерб**
- нематериальный ущерб
- неявный ущерб

27. На каком этапе построения системы защиты происходит оценка возможного физического доступа к ПД?
- разработка замысла защиты
- реализация замысла защиты
- **оценка обстановки**
- решение вопросов управления защитой

28. Требования по защите от НСД каких классов ИСПД в многопользовательском режиме при разных правах доступа совпадают?
- 1 и 2 классов
- **2 и 3 классов**
- 1 и 3 классов
- 3 и 4 классов

29. В каком законодательном документе определено понятие профиля защиты?
- ФЗ “О персональных данных”
- **ГОСТ “Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий”**
- ФЗ “Об информации, информационных технологиях и о защите информации”
- ФЗ “О безопасности”

30. Наличие межсетевого экрана необходимо при:
- использовании изолированной локальной сети
- **использовании сетей общего пользования**
- использовании почтового ящика в сети Интернет
- использовании автономного автоматизированного рабочего места

31. Если ИСПД подключена к Интернету и в ней используются съемные носители, для защиты от НСД необходимо использование:
- браузера
- защищенных каналов связи
- **антивирусной защиты**
- носителей, открытых на запись

32. В каком документе содержатся состав, содержание и сроки проведения работ по разработке и внедрению СЗПД?
- **в техническом задании СЗПД**
- матрице доступа
- в частной модели угроз
- в проекте СЗПД

33. Какой участник процесса сертификации оформляет экспертное заключение по сертификации средств защиты информации?
- **органы по сертификации средств защиты информации**
- заявитель
- федеральный орган по сертификации
- испытательные лаборатории

34. На каком этапе создания системы защиты персональных данных разрабатывается частная модель угроз?

- ввод в действие
- эксплуатация
- стадия проектирования
- **предпроектная стадия**

35. Сколько органов по сертификации действует в России?
- 3
- **4**
- 5
- 2

36. На каком этапе создания СЗПД производится закупка технических средств защиты?
- эксплуатация
- ввод в действие
- **стадия проектирования**
- предпроектная стадия

37. Какой срок действия у сертификата средства защиты информации?
- 10 лет
- **3 года**
- 5 лет
- 2 года

38. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?
- создание СЗПД
- административное мероприятие
- организационное мероприятие
- **техническое мероприятие**

39. На каком этапе создания СЗПД производится опытная эксплуатация средств защиты?
- эксплуатация
- предпроектная стадия
- стадия проектирования
- **ввод в действие**

40. На каком этапе создания системы защиты персональных данных определяется состав персональных данных и необходимость их обработки?
- эксплуатация
- **предпроектная стадия**
- ввод в действие
- стадия проектирования

41. Какие подсистемы в рамках СЗПД можно не использовать, если ИСПД является изолированной (локальной)?
- **подсистема безопасности межсетевого взаимодействия**
- подсистема криптографической защиты информации
- **подсистема обнаружения вторжений**
- подсистема обеспечения целостности
- подсистема анализа защищенности
- подсистема управления доступом, регистрации и учета
- подсистема антивирусной защиты

42. Как называются меры защиты, которые создают маскирующие акустические и вибрационные помехи?
- криптографические меры защиты
- **активные меры защиты от утечки по техническим каналам**

- пассивные меры защиты от утечки по техническим каналам
- активные меры защиты от несанкционированного доступа

43. Какая подсистема в рамках СЗПД предназначена для защиты информационной системы от вредоносных программ?
- подсистема обнаружения вторжений
- **подсистема антивирусной защиты**
- подсистема безопасности межсетевого взаимодействия
- подсистема анализа защищенности

44. Что является основанием для включения оператора в ежегодный план проверок ФСТЭК?
- предписание Роскомнадзора
- заявления и обращения граждан
- **истечение 3 лет со дня последней плановой проверки**
- **истечение 3 лет со дня государственной регистрации**

45. Выберите утверждения, характеризующие антивирусы с эвристическим методом обнаружения вирусов:
- не способны находить неизвестные вирусы
- **способны находить неизвестные вирусы**
- гарантированно находят известные вирусы
- **имеют большое количество ложных срабатываний**

46. Процедура фильтрации в межсетевом экране представляет собой:
- анализ доменного имени источника сообщения на предмет совпадения определенным условиям
- помещение всех пакетов в буфер и ожидание решения администратора о легитимности трафика
- **анализ заголовка пакета на предмет совпадения определенным условиям**

47. Какой орган является регулятором в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПД (не криптографическими методами) при их обработке в ИСПД?
- **ФСТЭК**
- Роспотребнадзор
- ФСБ
- Роскомнадзор

48. Какой этап построения системы защиты персональных данных включает в себя анализ уязвимых звеньев и возможных угроз безопасности?
- реализация замысла защиты
- разработка замысла защиты
- решение вопросов управления защитой
- **оценка обстановки**

49. На каком этапе создания СЗПД производится оценка(аттестация) ИСПД требованиям безопасности ПД?
- **ввод в действие**
- стадия проектирования
- предпроектная стадия
- эксплуатация

50. На каком этапе создания СЗПД разрабатывается эксплуатационная документация к ИСПД и средствам защиты информации?
- **стадия проектирования**
- эксплуатация
- предпроектная стадия
- ввод в действие

51. Какой участник процесса сертификации ходатайствует перед федеральным органом по сертификации о приостановке или отмене действия выданных сертификатов?

- заявитель
- **органы по сертификации средств защиты информации**
- испытательные лаборатории
- центральный орган сертификации

Формы и методы контроля и оценки результатов освоения модулей представлены в таблице 1:

Таблица 1

Формы и методы контроля и оценки результатов освоения модулей

№ п/п	Наименование процедуры	Основные показатели оценки	Формы и методы контроля и оценки
	Итоговая аттестация	Тест считается выполненным, если слушатель выполнил более 60% от предложенных заданий.	Тест в электронной форме

6. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Руководитель программы повышения квалификации:

Статуев Алексей Анатольевич к.п.н., доцен, доцент т кафедры экономики, управления и информатики

Разработчики программы повышения квалификации:

Статуев Алексей Анатольевич к.п.н., доцен, доцент т кафедры экономики, управления и информатики

Марина А.В., к.п.н., доцент, руководитель отделения дополнительного образования и профессионального обучения

Составители учебно-тематического плана программы повышения квалификации:

Статуев Алексей Анатольевич к.п.н., доцен, доцент т кафедры экономики, управления и информатики

Марина А.В., к.п.н., доцент, руководитель отделения дополнительного образования и профессионального обучения

Сведения о педагогических (научно-педагогических) работниках, участвующих в реализации программы повышения квалификации, и лицах, привлекаемых к реализации дополнительной образовательной программы на иных условиях, представлены в таблице 2.

Таблица 2

Преподаватели программы повышения квалификации

«Организация работы и защиты персональных данных в организациях и учреждениях»

п/п	Наименование модулей (тем, разделов)	Фамилия, имя,отчество,	Ученая степень, ученое звание	Основное место работы, должность	Место работы и должность по совместительству (если есть)
1.	Законодательство о защите персональных данных. Общие понятия. Реализация политики защиты персональных данных в управлении персоналом организации	Статуев А.А.	К.п.н., доцент	Кафедра экономики, управления и информатики	
2	Методы и средства технической защиты информации в информационных системах персональных данных.	Киселев С.В.	Ст. преподаватель	Кафедра экономики, управления и информатики	

Учебно-методическое и информационное обеспечение программы, а также материально-технические условия реализации программы представлены в приложении 3 «Рабочая программа модуля (курса)» программы повышения квалификации.

ПРИЛОЖЕНИЕ 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»

УЧЕБНЫЙ ПЛАН

отделение дополнительного образования и профессионального обучения

факультет/институт/филиал

«Организация работы и защиты персональных данных в организациях и учреждениях»

наименование программы повышения квалификации

Наименование учебных предметов, курсов дисциплин (модулей)		Форма аттестации		Зачетные единицы	Часов					
						В том числе				
						В том числе				
		зачет	экзамен	Всего	Всего	Аудиторных	Лекции	Семинары, практические	Самостоятельная работа	Контроль, зачет экзамен
1.	Законодательство о защите персональных данных. Общие понятия.				24	20	12	8	4	
2.	Реализация политики защиты персональных данных в управлении персоналом организации				24	20	12	8	4	
3.	Методы и средства технической защиты информации в информационных системах персональных данных.				20	12	8	4	8	
	Итоговая аттестация				4				4	Тестировани

										e
				2	**72**	**52**	**32**	**20**	**20**	

ПРИЛОЖЕНИЕ 2

Календарный учебный график

Нед	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
I	т	т	т	т																																																	

	Теоретическое обучение
П	Практика
Э	Экзаменационная сессия
Иа	Итоговая аттестация
К	Каникулы
*	Обучение не ведется

Календарный учебный график составляется для программ повышения квалификации и представляет собой график учебного процесса, устанавливающий последовательность и продолжительность теоретического обучения, экзаменационных сессий, практик, стажировок, итоговой аттестации.

ПРИЛОЖЕНИЕ 3

РАБОЧАЯ ПРОГРАММА

модуля (курса)

«Организация работы и защиты персональных данных в организациях и учреждениях»

1. АННОТАЦИЯ

Программа рассматривает основы информационной безопасности, техническую защиту информации.

Существенное внимание уделено вопросам комплексной защиты объектов информатизации.

Программа предназначена для муниципальных служащих и руководителей муниципальных учреждений.

Основной формой итоговой аттестации слушателя при освоении курса является тестирование.

Цель: – совершенствование компетенций муниципальных служащих и руководителей муниципальных учреждений в области правовой, организационной, технической, программно-аппаратной и других подсистем, методов, способов и средств, обеспечивающих защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки.

СОДЕРЖАНИЕ

.Учебная программа по модулю

№ п/п	Наименование модуля, разделов и тем	Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы с указанием кол-ва часов, используемых образовательных технологий и рекомендуемой литературы
1	Законодательство о защите персональных данных. Общие понятия.	Защита персональных данных в международном законодательстве: история вопроса. Развитие современного российского законодательства в сфере защиты персональных данных. Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ (с изм. и доп. от 2 июля 2021 года). Защита персональных данных в трудовом

		законодательстве Российской Федерации 12 часов
2	Реализация политики защиты персональных данных в управлении персоналом организации	Политика организации в области защиты персональных данных. Документы, регламентирующие защиту персональных данных кандидатов и работников в процессе хранения, обработки и передачи их третьим лицам. Процедуры и регламенты работы кадровой службы в рамках соблюдения законодательства о защите персональных данных. Государственный контроль и надзор за обеспечением выполнения требований ФЗ «О персональных данных». 12 часов
3	Методы и средства технической защиты информации в информационных системах персональных данных.	Угрозы безопасности персональным данным при их обработке в информационных системах персональных данных. Модель угроз безопасности персональным данным. 8 часов
	Лабораторные работы	–
	Практические занятия (семинары)	20 часов Законодательство о защите персональных данных. Общие понятия. Реализация политики защиты персональных данных в управлении персоналом организации Методы и средства технической защиты информации в информационных системах персональных данных.
	Стажировка	-
	Самостоятельная работа	-

2. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ МОДУЛЯ

(формы аттестации, оценочные и методические материалы)

Программа предусматривает проведение итогового тестирования

Формы и методы контроля и оценки результатов освоения модуля

№ п/п	Наименование модуля	Основные показатели оценки	Формы и методы контроля и оценки
	Итоговая аттестация	Тестирование	Оценка «отлично» 80 – 100 % правильных ответов; Оценка «хорошо» 60 – 79 % правильных ответов; Оценка «удовлетворительно» 40 – 59% правильных ответов. Оценка «неудовлетворительно» менее 40 % правильных ответов.

Шкала оценивания сформированности компетенции

Уровень сформированности компетенции (индикатора достижения компетенции)				
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
	не зачтено	**зачтено**		
Знания	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок.	Уровень знаний в объеме, соответствующем требованиям программы подготовки, без ошибок.
Умения	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме.	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме.

Навыки	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МОДУЛЯ

4.1. Учебно-методическое и информационное обеспечение программы:

Для реализации ДПОП ПК «Организация работы и защиты персональных данных в организациях и учреждениях» имеется учебно-методическая литература, электронные ресурсы.

Реализация ДПОП ПК «Организация работы и защиты персональных данных в организациях и учреждениях»» осуществляется информационно-библиотечным ресурсом: учебно-методической литературой. Есть доступ к электронно- библиотечной системе (ЭБС), которая обеспечивает доступ к учебной, учебно-методической и научной литературе по всем отраслям знаний ведущих российских издательств.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам «ZNANIUM.COM», «Юрайт», «Консультант студента», «Лань» и к электронной информационно-образовательной среде университета. Электронно-библиотечные системы и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети Интернет как на территории вуза, так и вне ее.

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

4.2. Используемые образовательные технологии.

Программа реализуется с использованием дистанционных образовательных технологий. Для каждой темы разработаны учебно-методические и оценочные материалы, размещенные в системе дистанционного обучения, которые позволяют слушателям самостоятельно осваивать содержание программы.

В процессе реализации программы используются: проблемная лекция, дискуссии, практические занятия (практикумы), техники технологий проблемно- и проектно-ориентированного обучения.

4.3. Литература.

Основная

1. Кузнецов, И. Н. Документационное обеспечение управления. Документооборот и делопроизводство : учебник и практикум для вузов / И. Н. Кузнецов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 461 с. — (Высшее образование). — ISBN 978-5-534-04275-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488697
2. Доронина, Л. А. Организация и технология документационного обеспечения управления : учебник и практикум для вузов / Л. А. Доронина, В. С. Иритикова. — Москва : Издательство Юрайт, 2022. — 233 с. — (Высшее образование). —

ISBN 978-5-534-04568-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489555
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469235
4. Терещенко, Л. К. Модернизация информационных отношений и информационного законодательства : монография / Л.К. Терещенко. — Москва: Институт законодательства и сравнительного правоведения при Правительстве РФ : ИНФРА-М, 2020. — 227 с. - ISBN 978-5-16-006123-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1095734
5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/113790
6. Государственная и муниципальная служба: учебник для вузов / Е. В. Охотский [и др.] ; под общей редакцией Е. В. Охотского. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 409 с. — (Высшее образование). — ISBN 978-5-534-07946-3. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469072
7. Государственная и муниципальная служба : учебник для вузов / С. И. Журавлев [и др.] ; под редакцией С. И. Журавлева, В. И. Петрова, Ю. Н. Туганова. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 305 с. — (Высшее образование). — ISBN 978-5-534-13270-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/468771

Дополнительная

1. Знаменский, Д. Ю. Государственная и муниципальная служба : учебник для вузов / Д. Ю. Знаменский ; ответственный редактор Н. А. Омельченко. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 414 с. — (Высшее образование). — ISBN 978-5-534-09076-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/468756
2. Абуладзе, Д. Г. Документационное обеспечение управления персоналом : учебник и практикум для вузов / Д. Г. Абуладзе, И. Б. Выпряжкина, В. М. Маслова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 370 с. — (Высшее образование). — ISBN 978-5-534-14486-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477699
3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326
4. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2021. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189342
5. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее

образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523
6. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364
7. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022
8. Никитина, А. С. Управление человеческими ресурсами в государственном и муниципальном управлении : учебное пособие для вузов / А. С. Никитина, Н. Г. Чевтаева. — 2-е изд. — Москва : Издательство Юрайт, 2021. — 187 с. — (Высшее образование). — ISBN 978-5-534-12784-3. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/476846
9. Омельченко, Н. А. Этика государственной и муниципальной службы : учебник и практикум для вузов / Н. А. Омельченко. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 316 с. — (Высшее образование). — ISBN 978-5-534-01329-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450055
10. Васильев, В. П. Государственное и муниципальное управление : учебник и практикум для вузов / В. П. Васильев, Н. Г. Деханова, Ю. А. Холоденко. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 307 с. — (Высшее образование). — ISBN 978-5-534-13886-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467191
11. Конталев В.А. Государственная и муниципальная служба Российской Федерации [Электронный ресурс] : Учебное пособие / В. А. Конталев. М.: МГАВТ, 2009. 264 с. //ЭБС «Znanium»: [Электронный ресурс]: - URL:http://znanium.com/catalog.php?bookinfo=402773

Нормативные документы

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (с изм. и доп. от 2 июля 2021 года)
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
3. Федеральный закон от 02.03.2007 N 25-ФЗ (ред. от 26.05.2021) «О муниципальной службе в Российской Федерации» (с изм. и доп., вступ. в силу с 01.07.2021)
4. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
5. Постановление Правительства Российской Федерации от 26.02.2010 № 96 «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов».
6. Указ Президента Российской Федерации от 10.03.2009 № 261 «Об утверждении федеральной программы «Реформирование и развитие системы государственной службы Российской Федерации (2009 – 2013 годы)».

Интернет-ресурсы

1. http://www.garant.ru - ГАРАНТ. Информационно-правовой портал
4. http://www.consultant.ru - «КонсультантПлюс». Справочно-правовая система
5. http://www.fz131.minregion.ru - Система подготовки кадров поддержка и сопровождения органов местного самоуправления
6. http://www.government.ru/ - Интернет-портал Правительства РФ
7. http://emsu.ru/ms/ - Журнал «Муниципальная служба» (электронная версия)

4.4. Материально-технические условия реализации программы:

Материально-техническая база

№ п.п.	Наименование модуля (тем, разделов)	Материально-технические условия для реализации программ (наличие лабораторий, производственных участков и т.п. по профилю программы повышения квалификации)
1.	Законодательство о защите персональных данных. Общие понятия.	Компьютер, проектор
2.	Реализация политики защиты персональных данных в управлении персоналом организации	Компьютер, проектор
3.	Методы и средства технической защиты информации в информационных системах персональных данных.	Компьютер, проектор