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 2022г.

УТВЕРЖДЕНО
Ученым советом Арзамасского филиала ННГУ

(протокол от «19» октября 2022 г.№ 8)

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Комплексная защита информации»

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:

- Основы информационной безопасности.
- Техническая защита информации.
- Комплексная защита объектов информатизации.

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 «Комплексная защита информации»

[1] 1 ЗЕ = 36 ак. часов

Программа предусматривает в качестве итоговой аттестации тестирование по следующим вопросам:

1. Какой из компонентов подсистемы безопасности Windows предназначен для контроля за доступом к объектам?
- Encrypted File System
- NT File System
- Security Account Manager
- **Security Reference Monitor**

2. К какому типу протоколов относится протокол SSL?
- К протоколам прямой аутентификаци
- **К протоколам автономной аутентификации**
- К протоколам установления защищенной связи на сетевом уровне
- К протоколам непрямой аутентификации

3. В чем сущность комплексного подхода к защите информации?
- В использовании комплексных систем защиты информации
- В привлечении к защите информации коллектива квалифицированных экспертов
- В использовании комплекса защитных мер
- **Защита информации ? это постоянный процесс, проводимый с использованием всех существующих методов и средств**

4. Что не относится к динамическим (поведенческим) биометрическим характеристикам?
- **Термограмма лица, шеи и верхней части груди**
- Клавиатурный "почерк"
- Тембр голоса
- Рукописная подпись

5. Что такое информационная безопасность?
- **Состояние защищенности информационной среды объекта**
- Деятельность по созданию безопасных информационных систем
- Деятельность по обеспечению защищенности информации
- Деятельность по предотвращению утечки информации, непреднамеренного и несанкционированного воздействия на информацию

6. Что понимается под затенением файла с паролями пользователей?
- **Запрет доступа к файлу для непривилегированных пользователей**
- Перенос на защищенный от несанкционированного чтения носитель
- Замена * символов паролей
- Запрет доступа к файлу для любых процессов

7. Какая из криптосистем не используется в системах электронной подписи?
- Эллиптических кривых
- **Диффи-Хеллмана**
- Эль-Гамаля
- RSA

8. В каком из симметричных криптоалгоритмов может потребоваться расширение открытого текста?
- Одноалфавитная подстановка
- Гаммирование

- Многоалфавитная подстановка
- **Перестановка**

9. Что относится к локальному уровню правового регулирования информационной безопасности?
- Принятие государственных стандартов
- Принятие постановлений правительства
- **Утверждение перечня сведений, составляющих коммерческую тайну**
- Принятие федеральных законов

10. Какие виды антивирусных программ принципиально могут обнаруживать только уже известные вредоносные программы?
- Эвристические анализаторы
- Инспекторы (ревизоры)
- **Сканеры**
- Мониторы (сторожа)
- Вакцины

11. Какой из режимов криптосистемы DES может использоваться для проверки целостности шифра?
- Электронной кодовой книги
- **Сцепления блоков шифра**
- Обратной связи по выходу
- Выработки имитовставки

12. Что не относится к аппаратным средствам защиты информации?
- **Средства контроля и управления доступом**
- Устройства криптографической защиты данных
- Устройства хранения данных для аутентификации пользователей
- Устройства стирания информации на магнитных дисках

13. Что не может использоваться при биометрической аутентификации?
- Отпечатки пальцев
- **Температура тела**
- Геометрическая форма руки
- Тембр голоса
- Все указанные параметры могут использоваться

14. На чем основана возможность внедрения вирусов в документы Microsoft Office?
- На недокументированности формата документов
- **На возможности добавления к документу автоматически выполняющихся макросов**
- На возможности включения в документ объектов
- На возможности включения в состав документа макросов

15. Какие вычеты по модулю n входят в приведенный набор вычетов по модулю n?
- Не являющиеся взаимно простыми с n
- **Являющиеся взаимно простыми с n**
- Являющиеся простыми
- Все вычеты по модулю n входят в приведенный набор вычетов

16. На каком уровне модели OSI обеспечивается защита сообщений в протоколе SSL?

- На прикладном
- На канальном
- **На сеансовом**
- На сетевом

17. Что нельзя отнести к свойствам вредоносных программ?
- Ассоциация себя с другими файлами
- Изменение кода других программ в оперативной памяти
- Скрытие признаков своего присутствия
- **Копирование файлов**

18. Для чего предназначена программа syskey в ОС Windows?
- Для генерации системного ключа
- Для шифрования файла SAM
- **Для шифрования хешей паролей пользователей**
- Для выбора способа шифрования паролей пользователей

19. Какой из криптоалгоритмов является алгоритмом потокового шифрования?
- AES
- DES
- **RC4**
- RC2

20. Что относится к косвенным каналам утечки информации?
- Внедрение вредоносных программ
- Подключение к линии передачи данных для перехвата информации
- Вход в систему под чужим именем
- **Перехват информации по каналу ПЭМИН**

21. Какой протокол относится к протоколам прямой аутентификации?
- Kerberos
- **CHAP**
- SSL
- RADIUS

22. Что не относится к функциям хеширования?
- MD5
- **ГОСТ Р 34.10-2012**
- ГОСТ Р 34.11-2012
- SHA-1

23. Как генерируется ключ шифрования файла в шифрующей файловой системе Windows?
- Ключ выводится из идентификатора безопасности пользователя (SID)
- Ключ выводится из пароля пользователя
- **Ключ генерируется случайно**
- Ключ выводится из пароля и идентификатора безопасности пользователя (SID)

24. Где хранятся хеши паролей пользователей в современных версиях ОС Unix (например, в Linux)?
- В файле /etc/hash
- В файле /etc/passwd

- В файле /usr/bin/passwd
- **В файле /etc/shadow**

25. Зачем в учетной записи пользователя может храниться случайное значение?
- **Для исключения возможности установления факта совпадения паролей** пользователей с разными правами
- Для упрощения администрирования
- Чтобы нельзя было восстановить пароль
- Для увеличения стойкости функции хеширования

26. Какие из алгоритмов не относятся к симметричным криптоалгоритмам?
- DESX
- **SHA**
- ГОСТ 28147-89
- RC5

27. Что не относится к функциям безопасности программы BIOS Setup?
- Установка пароля на загрузку операционной системы
- **Задание ключа шифрования системной памяти**
- Изменение порядка использования устройств внешней памяти при загрузке ОС
- Установка пароля на изменение настроек BIOS

28. Что является эталонной характеристикой при аутентификации по клавиатурному почерку или "росписи" мышью?
- **Темп ввода**
- Другое
- Время, затраченное на ввод
- Ключевая фраза или рисунок

29. Что не является назначением аудита событий безопасности в компьютерной системе?
- Подтверждение факта, источника и возможной причины нарушения политики безопасности
- **Облегчение администрирования безопасности компьютерной системы**
- Немедленная реакция на совершении критичных для информационной безопасности действий
- Обнаружение подготовки к совершению неправомерных действий нарушителем

30. Для чего используется открытый ключ в асимметричных криптосистемах?
- **Для шифрования данных и проверки электронной подписи**
- Для расшифрования данных и проверки электронной подписи
- Для расшифрования данных и вычисления электронной подписи
- Для шифрования данных и вычисления электронной подписи

31. Если Ek и Dk ? функции шифрования (расшифрования) криптосистемы DES с ключом k, то какая запись соответствует шифрованию в криптосистеме DESX (+ означает операцию сложения по модулю 2, а P ? открытый текст)?
- E(k1+k+k2)(P)
- **k1+Ek(P+k2)**
- Dk2(Ek(Dk1(P)))
- Ek1(Dk(Ek2(P)))

32. Что не относится к требованиям доверия к безопасности?
- Проведение функционального тестирования объекта оценки
- Требования к составу документации
- Требования к качеству проектирования объекта оценки
- **Строгая аутентификация субъекта**

33. Что такое модель "рукопожатия"?
- Аутентификация пользователя, основанная на одноразовых паролях
- Аутентификация пользователя, основанная на биометрии
- **Аутентификация пользователя, основанная на знании им правила выработки ответа** на случайный запрос
- Аутентификация пользователя, основанная на применении элементов аппаратного обеспечения

34. Какие методы и средства защиты информации являются обязательными в любой системе защиты?
- Инженерно-технические
- Криптографические
- **Организационные**
- Программно-аппаратные

35. Что является основным критерием при выборе элемента аппаратного обеспечения для аутентификации пользователей?
- **Сложность копирования**
- Стоимость изготовления
- Скорость считывания ключевой информации
- Объем памяти и наличие микропроцессора

36. В чем разница между протоколами AH и ESP в IPSec?
- Существенного различия нет
- AH предназначен для защиты целостности данных пакета, а ESP - их конфиденциальности
- AH предназначен для защиты конфиденциальности заголовка пакета, а ESP - его данных
- **AH предназначен для защиты целостности адресной части и данных пакета, а ESP - конфиденциальности его данных**

37. Какие требования к значению числа N (в вызове сервера) предъявляются в протоколе CHAP?
- **N должно быть уникальным и непредсказуемым**
- N должно быть непредсказуемым
- N должно быть неповторяющимся
- N должно быть случайным

38. Какой из протоколов не может применяться для построения VPN?
- **PPP**
- L2TP
- IPSec в туннельном режиме
- PPTP

39. Как должны храниться пароли в базе учетных записей?
- В открытом виде

- Защищенные помехоустойчивым кодом
- В зашифрованном виде
- **В хешированном виде**

40. Что не относится к требованиям уровня безопасности С2, в соответствии с "оранжевой книгой"?
- Возможность аудита событий безопасности
- **Мандатное разграничение доступа к объектам**
- Дискреционное разграничение доступа к объектам
- Исключение возможности использования объектов одного процесса со стороны других

41. Что такое удостоверяющий центр?
- Орган, осуществляющий резервное копирование криптографических ключей
- **Орган, выдающий сертификаты открытых ключей пользователей**
- Орган, создающий секретные ключи пользователей
- Орган, занимающийся проверкой электронной подписи под документами

42. Какая модель разграничения доступа к объектам реализована в ОС Windows?
- Смешанная (дискреционная и мандатная)
- Мандатная
- Ролевая
- **Дискреционная**

43. Какое из действий администратора системы является потенциально опасным с точки зрения внедрения вредоносных программ?
- Изменение привилегий пользователя
- Редактирование реестра
- Удаление учетной записи пользователя
- **Работа в Интернете**
- Добавление учетной записи пользователя

44. Что относится к двухфакторной аутентификации?
- **Использование устройства и секрета (PINa) для доступа к этому устройству**
- Аутентификация на основе модели "запрос-отклик"
- Использование двух паролей: одного на вход в систему и другого для доступа к конфиденциальным ресурсам
- Использование двух биометрических характеристик

45. Где хранится информация об ограничениях на возможности работы локального пользователя операционной системы Windows?
- **В разделе HKEY_CLASSES_ROOT реестра**
- В Active Directory
- В файле windows.ini
- В разделе HKEY_CURRENT_USER реестра
- В файле system.ini

46. В чем недостатки шифров одноалфавитной подстановки?
- В сохранении частотных характеристик открытого текста в шифротексте
- В относительно небольшом числе различных ключей
- В необходимости расширения открытого текста, что снижает стойкость шифра

- **В относительно небольшом числе различных ключей и в сохранении частотных характеристик открытого текста в шифротексте**

47. От какой угрозы не защищает электронная подпись?
- Нарушения целостности
- **Нарушения конфиденциальности**
- Нарушения подлинности (авторства)

48. Какая функция называется однонаправленной?
- Функция, направленная в одну сторону
- Функция асимметричного шифрования
- Функция, для которой не существует обратной
- **Функция, обратная к которой вычисляется гораздо сложнее, чем исходная функция**

49. Для чего используется закрытый ключ в асимметричных криптосистемах?
- Для проверки электронной подписи
- Для шифрования данных и проверки электронной подписи
- **Для расшифрования данных и вычисления электронной подписи**
- Для шифрования данных

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., доцент, 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

«Комплексная защита информации»

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.	Основы информационной безопасности. Техническая защита информации.	Статуев А.А.	К.п.н., доцент	Кафедра экономики, управления и информатики	
2	Комплексная защита объектов информатизации.	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

«Комплексная защита информации»

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.	Основы информационной безопасности.				24	20	12	8	4	
2.	Техническая защита информации.				24	20	12	8	4	
3.	Комплексная защита объектов информатизации.				20	12	8	4	8	
	Итоговая аттестация				4				4	Тестирование
				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)

«Комплексная защита информации»

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	Основы информационной безопасности	Теория информационной безопасности и методология защиты информации. Правовое, нормативное и методическое регулирование деятельности в области защиты информации. Правовые основы организации защиты государственной тайны, задачи органов защиты государственной тайны.

		12 часов
2	Техническая защита информации	Угрозы и уязвимости автоматизированных информационных систем. Классификация технических каналов утечки информации. Виды уязвимостей автоматизированных информационных систем. 12 часов
3	Комплексная защита объектов информатизации	Криптографические методы защиты информации. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств. Информационная безопасность автоматизированных систем. 8 часов
	Лабораторные работы	–
	Практические занятия (семинары)	20 часов Основы информационной безопасности Техническая защита информации Комплексная защита объектов информатизации
	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 « Комплексная защита информации» имеется учебно-методическая литература, электронные ресурсы.

Реализация ДПОП ПК «Комплексная защита информации» 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.	Основы информационной безопасности	Компьютер, проектор
2.	Техническая защита информации	Компьютер, проектор
3.	Комплексная защита объектов информатизации	Компьютер, проектор