Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Институт «Высшая школа государственного управления»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 458F8CD8698157343F17480C0CF8B0A9
Владелец: Кондратенко Олег Игоревич
Действителен: с 19.03.2026 до 12.06.2027

«УТВЕРЖДАЮ»
Директор Института ВШГУ РАНХиГС
О.И. Кондратенко
«08» октября 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации

Защита персональных данных

(наименование программы)

Москва - 2026

Разработчик:

Д.Л. Тодоров,
заместитель директора научно-образовательного центра
обмена лучшими практиками государственного управления
и формирования инвестиционного климата в субъектах РФ
Дирекции регионального развития Института ВШГУ РАНХиГС

Руководитель программы:

Е.Н. Подшивалов,
заместитель директора
Института ВШГУ РАНХиГС

Дополнительная профессиональная программа повышения квалификации рассмотрена на заседании ученого совета Института ВШГУ, рекомендована к реализации, протокол № 41 от «08» октября 2026 года.

Содержание

1. Общая характеристика программы....4
1.1. Цель и задачи реализации программы....4
1.2. Нормативные правовые акты....4
1.3. Планируемые результаты обучения....6
1.4. Категория слушателей....9
1.5. Формы и технологии обучения....9
1.6. Период обучения, срок освоения и режим занятий....9
1.7. Документ о квалификации....10
2. Содержание программы....10
2.1. Календарный учебный график....10
2.2. Учебный план....11
2.3. Содержание программы....14
3. Организационные условия реализации программы....18
3.1. Материально-техническое и программное обеспечение реализации программы....18
3.2. Учебно-методическое и информационное обеспечение программы....18
4. Оценка качества освоения программы....25
4.1. Формы и объем промежуточной аттестации....25
4.2. Формы и объем итоговой аттестации....28
5. Индикаторы сформированных компетенций....32

Приложение № 1. Сведения о профессорско-преподавательском составе и ведущих специалистах (кадровая справка) [1].

[1] Кадровая справка не входит в состав программы и формируется отдельно.

1. Общая характеристика программы

Дополнительная профессиональная программа повышения квалификации *«Защита персональных данных»* разработана в соответствии с распоряжением Правительства Российской Федерации от 21 апреля 2023 г. № 1019-р и поручением Президента Российской Федерации (Пр-2180 от 16.11.2022) в целях создания условий для кадрового обеспечения достижения национальных целей развития Российской Федерации и реализации мероприятий программы социально-экономического развития Донецкой Народной Республики, Луганской Народной Республики, Запорожской и Херсонской областей.

Реализация программы повышения квалификации осуществляется Российской академией народного хозяйства и государственной службы при Президенте Российской Федерации совместно с Финансовым университетом при Правительстве Российской Федерации в сетевой форме и направлена на повышение профессионального уровня слушателей в рамках имеющейся квалификации.

1.1. Цель и задачи реализации программы

Цель реализации программы: совершенствование профессиональных компетенций и (или) получение новой компетенции, необходимой для профессиональной деятельности в сфере обеспечения правомерной обработки и комплексной защиты персональных данных в условиях цифровизации государственного и организационного управления, с учетом требований законодательства Российской Федерации, применения современных информационных технологий и реализации правовых, организационных и технических мер по предотвращению нарушений и обеспечению информационной безопасности.

Задачи программы:

– обеспечение системного изучения нормативного правового регулирования в области персональных данных;

– формирование профессиональных компетенций в области правомерной обработки персональных данных;

– развитие навыков разработки и внедрения организационно-распорядительной документации, регулирующей обработку и защиту персональных данных (политики, положения, регламенты);

– освоение современных методов и средств технической защиты персональных данных;

– формирование компетенций в области анализа рисков и управления инцидентами информационной безопасности;

– развитие практических навыков применения требований законодательства и стандартов при организации процессов обработки персональных данных, подготовке необходимой документации, взаимодействии с субъектами персональных данных и контролирующими органами, а также при проведении внутренних проверок и аудитов.

1.2. Нормативные правовые акты

Дополнительная профессиональная программа повышения квалификации разработана на основании следующих нормативно-правовых документов:

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный закон от 21 декабря 2021 № 414-ФЗ «Об общих принципах организации публичной власти в субъектах Российской Федерации».
3. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

4. Приказ Минобрнауки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

5. Приказ Министерства образования науки Российской Федерации от 12.09.2013 № 1061 «Об утверждении перечней специальностей и направлений подготовки высшего образования».

6. Приказ РАНХиГС от 20.04.2026 № 02-00742/001 «Об утверждении порядка реализации дополнительных профессиональных программам в Академии».

7. Приказ РАНХиГС от 02 декабря 2025 года № 02-02669/001 «Об утверждении порядка разработки и утверждения в Академии дополнительных профессиональных программ - программ повышения квалификации, программ профессиональной переподготовки».

8. Приказ от 13 января 2026 года № 02-00009/001 «Об утверждении Положения об итоговой аттестации слушателей дополнительных профессиональных программ в Академии».

9. Приказ Министерства труда и социальной защиты РФ от 14 сентября 2022 г. № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»».

10. Федеральный государственный образовательный стандарт высшего образования – бакалавриат по направлению подготовки 38.03.04 Государственное и муниципальное управление, утвержденный приказом Министерства науки и высшего образования Российской Федерации от 13 августа 2020 г. № 1016.

11. Постановление Правительства РФ от 11.10.2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

12. Приказ РАНХиГС от 22.09.2017 № 01-6230 «Об утверждении Положения о применении в Академии электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

13. Методические рекомендации-разъяснения по разработке дополнительных профессиональных программ на основе профессиональных стандартов (утв. Минобрнауки России 22.04.2015 № ВК-1032/06).

14. Методические рекомендации по использованию электронного обучения, дистанционных образовательных технологий при реализации дополнительных профессиональных образовательных программ Министерства образования и науки Российской Федерации от 10.04.2014 № 06-381.

15. Нормативные документы, определяющие требования к выпускнику программы:

– «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ.

– ОК 010-2014 (МСКЗ-08). Общероссийский классификатор занятий» (принят и введен в действие приказом Росстандарта от 12.12.2014 № 2020-ст).

– «ЕКС - Единый классификационный справочник должностей руководителей, специалистов и других служащих, установленный постановлением Правительства РФ от 31.10.2002 № 787.

– «Справочник квалификационных требований к специальностям, направлениям подготовки, знаниям и умениям, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих» (утв. Минтрудом России) https://www.consultant.ru/document/cons_doc_LAW_219036

1.3. Планируемые результаты обучения

Таблица 1.3.1

Перечень компетенций, планируемых к освоению (результаты обучения)

Виды деятельности	**Общепрофессиональные, профессионально-специализированные компетенции или трудовые функции (ОПК, ПСК, ПЛК)** ***(формируются и (или) совершенствуются)***	**Практический опыт**	**Знания**	**Умения**
ВД 1. Обеспечение информационной безопасности	ОПК-8[2]. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	*Владеть навыками:* – использования современных информационных систем и цифровых платформ для обработки и защиты персональных данных; – работы с государственными информационными системами и цифровыми сервисами в бюджетной и управленческой деятельности; – применения инструментов проектного управления (в том числе цифровых) при реализации проектов в сфере информационной безопасности; – анализа и оптимизации процессов с использованием принципов бережливого управления; – проведения оценки соответствия деятельности организации требованиям законодательства о персональных данных; – выявления и анализа угроз безопасности персональных данных; – моделирования процессов обеспечения информационной безопасности и построения систем защиты персональных данных; – разработки и внедрения организационно-распорядительной документации по защите персональных данных; – реализации комплекса правовых, организационных и технических мер по защите персональных данных;	*Знать:* – принципы функционирования современных информационных систем, используемых в государственном управлении и организациях, включая системы обработки персональных данных; – основы цифровизации бюджетной системы РФ и особенности использования информационных технологий в бюджетном процессе; – подходы к организации проектной деятельности в органах государственной власти с применением цифровых инструментов управления проектами; – принципы бережливого управления и возможности их реализации с использованием информационных технологий; – требования законодательства Российской Федерации в области защиты персональных данных, включая нормативно-правовые акты и подзаконное регулирование; – правовые основы обработки персональных данных в информационных системах персональных данных (ИСПДн); – классификацию и содержание угроз безопасности персональных данных в ИСПДн;	*Уметь:* – применять современные информационные технологии при решении профессиональных задач в сфере государственного управления и защиты персональных данных; – использовать цифровые инструменты для анализа бюджетных процессов и управления финансовой информацией; – применять методы проектного управления при реализации задач по защите персональных данных; – внедрять инструменты бережливого управления для оптимизации процессов обработки и защиты персональных данных; – интерпретировать и применять нормы законодательства в области защиты персональных данных в практической деятельности; – идентифицировать угрозы безопасности персональных данных и оценивать риски при их обработке в ИСПДн; – разрабатывать модели угроз и определять требования к системе защиты персональных данных; – организовывать процессы обработки персональных данных в соответствии с установленными требованиями;

[2] ФГОС ВО - бакалавриат по направлению подготовки 38.03.04 Государственное и муниципальное управление, утвержденный приказом Минобрнауки России от 13.08.2020 № 1016.

		– организации внутреннего контроля и аудита в области защиты персональных данных; – распределения ответственности и координации деятельности работников, участвующих в обработке персональных данных.	– полномочия и функции государственных регуляторов в сфере защиты персональных данных и их нормативно-методические документы; – принципы построения систем защиты персональных данных и архитектуру информационной безопасности; – методы моделирования угроз и процессов обеспечения информационной безопасности; – состав и содержание организационных, правовых и технических мер защиты персональных данных; – требования к организации работы с персональными данными, включая распределение ответственности и назначение ответственных лиц.	– разрабатывать локальные нормативные акты организации по защите персональных данных; – определять и реализовывать необходимые организационные и технические меры защиты персональных данных; – взаимодействовать с государственными органами и регуляторами по вопросам защиты персональных данных.
ВД 2. Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	ПСК-1[3]. Администрирование систем защиты информации автоматизированных систем	*Владеть навыками:* – выполнения установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы; – управления полномочиями доступа пользователей автоматизированной системы; – информирования пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации	*Знать:* – принципы формирования политики информационной безопасности в автоматизированных системах; – программно-аппаратные средства защиты информации автоматизированных систем; – основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; – методы контроля эффективности защиты информации от утечки по техническим каналам; – критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; – принципы организации и структура систем защиты программного обеспечения автоматизированных систем; – основные меры по защите информации в автоматизированных системах.	*Уметь:* - формировать политику безопасности программных компонентов автоматизированных систем; - устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации; - использовать криптографические методы и средства защиты информации в автоматизированных системах; - анализировать события, связанные с защитой информации в автоматизированных системах.

[3] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н (трудовая функция В/02.6).

	ПСК-2[4]. Управление защитой информации в автоматизированных системах	*Владеть навыками:* – анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность; – составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; – оценки последствий от реализации угроз безопасности информации в автоматизированной системе; – анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации.	*Знать:* – основные методы управления защитой информации; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – методы защиты информации от несанкционированного доступа и утечки по техническим каналам; – нормативные правовые акты в области защиты информации; – национальные, межгосударственные и международные стандарты в области защиты информации; – руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.	*Уметь:* – оценивать информационные риски в автоматизированных системах; – классифицировать и оценивать угрозы безопасности информации; – применять нормативные документы по защите от несанкционированного доступа к информации и противодействию технической разведке; – применять технические средства контроля эффективности мер защиты информации.
Перечень компетенций (профессиональных и личностных качеств)	**Характеристики компетенций (умения)**	**Поведенческие индикаторы**		
Принятие управленческих решений	ПЛК-1[5]. Умение оперативно принимать и реализовывать управленческие решения	– оперативно принимает решения на своем уровне ответственности, соблюдая установленную процедуру принятия решений; – решения принимаются взвешенно с учетом возможных рисков; – выстраивает систему мотивации на основе прозрачных и понятных показателей; – несет ответственность за свои решения и действия		

[4] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н (трудовая функция B/03.6).

[5] Методический инструментарий по установлению квалификационных требований для замещения должностей государственной гражданской службы (версия 4.0) http://rosmintrud.ru/ministry/programms/gossluzhba/16/1

1.4. Категория слушателей

К освоению программы допускаются лица, замещающие должности в органах публичной власти, руководители, сотрудники подведомственных организаций Донецкой и Луганской Народных Республик, Запорожской и Херсонской областей и иные лица.

Требования к поступающим: среднее профессиональное и (или) высшее образование (бакалавриат, магистратура, специалитет).

1.5. Формы и технологии обучения

Форма и технологии обучения – очная (с применением электронного обучения и дистанционных образовательных технологий).

Программа реализуется в сетевой форме (см. табл. 1.5.1).

Таблица 1.5.1

Распределение частей образовательной программы в соответствии с учебным планом в сетевой форме

№ п/п	Наименование модуля/ видов оценки качества освоения программы	Наименование организации	Реализация уч. часов базовой организацией	Реализация уч. часов организацией-участником
1.	Модуль 1. Основы публичного управления в Российской Федерации	ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»	22	-
2.	Модуль 2. Требования законодательства в области обеспечения безопасности персональных данных	Финансовый университет при Правительстве Российской Федерации	-	52
3.	Модуль 3. Управление защитой персональных данных при их обработке в информационных системах персональных данных	Финансовый университет при Правительстве Российской Федерации	-	38
4.	Модуль 4. Практическая реализация механизмов защиты персональных данных в организации	Финансовый университет при Правительстве Российской Федерации	-	28
5.	Промежуточная аттестация по модулям 2-4	Финансовый университет при Правительстве Российской Федерации	-	2
6.	Итоговая аттестация	ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»	2	-
		ИТОГО:	**24**	**120**

1.6. Период обучения, срок освоения и режим занятий

Период обучения по программе составляет: 2 месяца 1 неделя 2 дня (таблица 2.1.1).

Общая трудоемкость программы - 144 академических часа, из которых 86 академических часов контактной работы со слушателем с применением ДОТ, в том числе 2 академических часа промежуточной аттестации (тестирование) с применением ДОТ и 2 академических часа итоговой аттестации (тестирование) с применением ДОТ; 58 академических часов – самостоятельная работа с применением электронного обучения.

Режим занятий: до 8 академических часов в день.

Предельная максимальная численность лекционной группы – 250 слушателей, практической (семинарской) группы – 120-150 слушаталей.

1.7. Документ о квалификации

Удостоверение о повышении квалификации федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации».

2. Содержание программы

2.1. Календарный учебный график

Таблица 2.1.1

Календарный учебный график

Период обучения – 2 месяца 1 неделя 2 дня	
1-2 месяца	1 неделя 2 дня
УЗ ДОТ, СР ЭО	УЗ ДОТ, СР ЭО, ПА ДОТ, ИА ДОТ

Календарный учебный график заполнен с помощью условных обозначений:

УЗ ДОТ – учебные занятия с применением дистанционных образовательных технологий.

СР ЭО – самостоятельная работа с применением электронного обучения.

ПА ДОТ – промежуточная аттестация с применением дистанционных образовательных технологий.

ИА ДОТ – итоговая аттестация с применением дистанционных образовательных технологий.

2.2. Учебный план

Таблица 2.2.1

Учебный план
по дополнительной профессиональной программе повышения квалификации
«Защита персональных данных»

№ п/п	Наименование модуля/темы	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий), час.					Самостоятельная работа (в т.ч. электронное обучение), час[6]	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.) ДОТ	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские/лабораторные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские/лабораторные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1.	**Модуль 1. Основы публичного управления в Российской Федерации**	**22**												**22**				**ОПК-8 ПЛК-1**
1.1.	Бюджетная система и бюджетный процесс Российской Федерации	8												8				ОПК-8 ПЛК-1
1.2.	Организация проектной деятельности в органах государственной власти	8												8				ОПК-8 ПЛК-1
1.3.	Основы бережливого управления	6												6				ОПК-8 ПЛК-1
2.	**Модуль 2. Требования законодательства в области обеспечения безопасности персональных данных**	**52**							**34**	**14**	**20**			**18**				**ОПК-8 ПСК-1 ПСК-2**
2.1.	Правовое регулирование защиты персональных данных при их обработке в информационных системах	16							10	4	6			6				ОПК-8 ПСК-1 ПСК-2

[6] Самостоятельная работа предполагает изучение слушателями материалов, расположенных на платформе new.portal.gosedu

	персональных данных																	
2.2.	Угрозы безопасности персональным данным в информационных системах обработки персональных данных	18							12	6	6			6				ОПК-8 ПСК-1 ПСК-2
2.3.	Государственные регуляторы и их нормативно-правовая документация в области защиты персональных данных	18							12	4	8			6				ОПК-8 ПСК-1 ПСК-2
3.	**Модуль 3. Управление защитой персональных данных при их обработке в информационных системах персональных данных**	**38**							**28**	**12**	**16**			**10**				**ОПК-8 ПСК-1 ПСК-2**
3.1.	Защита персональных данных при их обработке в информационных системах персональных данных	10							8	4	4			2				ОПК-8 ПСК-1 ПСК-2
3.2.	Моделирование систем и процессов обеспечения информационной безопасности	14							10	4	6			4				ОПК-8 ПСК-1 ПСК-2
3.3.	Организация работ и назначение ответственных лиц за обработку персональных данных	14							10	4	6			4				ОПК-8 ПСК-1 ПСК-2
4.	**Модуль 4. Практическая реализация механизмов защиты персональных данных в организации**	**28**							**20**	**8**	**12**			**8**				**ОПК-8 ПСК-1 ПСК-2**
4.1.	Меры, необходимые и достаточные для выполнения обязанностей, при обработке персональных данных в организации	14							10	4	6			4				ОПК-8 ПСК-1 ПСК-2
4.2.	Принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке	14							10	4	6			4				ОПК-8 ПСК-1 ПСК-2

5.	**Промежуточная аттестация по модулю 2-4**	**2**														**2/З(Д)[7]**		
	Итого:	**142**							**82**	**34**	**48**			**58**		**2**		
	Итоговая аттестация:	**2**	**тестирование**														**2/З(Д)[8]**	**ОПК-8 ПСК-1 ПСК-2 ПЛК-1**
	Всего:	**144**							**82**	**34**	**48**			**58**		**2**	**2**	

[7] Промежуточная аттестация осуществляется в форме тестирования с применением дистанционных образовательных технологий и реализуется сетевым партнером.
[8] Итоговая аттестация осуществляется в форме тестирования с применением дистанционных образовательных технологий.

2.3. Содержание программы

Таблица 2.3.1

Содержание программы

Номер модуля/темы и их наименование	Содержание модуля/темы
Модуль 1. Основы публичного управления в Российской Федерации	
Тема 1.1. Бюджетная система и бюджетный процесс Российской Федерации	Принципы построения бюджетной системы Российской Федерации, а также порядок организации и реализации бюджетного процесса на всех уровнях государственной власти, с развитием практических навыков применения бюджетного законодательства в профессиональной деятельности
Тема 1.2. Организация проектной деятельности в органах государственной власти	Сущность и особенности организации проектной деятельности в органах государственной власти, включая нормативно-правовые основы, цели и принципы внедрения проектного управления в государственном секторе. Этапы жизненного цикла проекта, распределение ролей и ответственности участников, а также методы планирования, мониторинга и оценки эффективности реализации проектов. Инструменты управления рисками, использования цифровых решений и практика внедрения проектного подхода в системе государственного управления.
Тема 1.3. Основы бережливого управления	Сущность и принципы бережливого управления, направленного на повышение эффективности деятельности за счёт выявления и устранения потерь, оптимизации процессов и ориентации на ценность для потребителя. Основные инструменты и методы бережливого подхода, включая картирование процессов, стандартизацию, непрерывное улучшение и вовлечение персонала. Возможности применения бережливого управления в практике организаций, в том числе в государственном секторе.
Модуль 2. Требования законодательства в области обеспечения безопасности персональных данных	
Тема 2.1. Правовое регулирование защиты персональных данных при их обработке в информационных системах персональных данных	Актуальность проблемы обеспечения безопасности персональных данных при их обработке в информационных системах. ГОСТ 50922-2006 «Защита информации. Основные термины и определения». Эволюция понятия «информационная безопасность» в Российской Федерации. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Классификация персональных данных исходя из правового режима. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Разъяснения Роскомнадзора от 02.09.2013 «Отнесение фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим ПДн и особенности их обработки». Оператор персональных данных. Обеспечение безопасности персональных данных при их обработке. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Постановление Правительства

	РФ от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Приказ ФСТЭК России от 18.02.2013 г. № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Информационная система персональных данных. Алгоритм формирования ИСПДн.
Тема 2.2. Угрозы безопасности персональным данным в информационных системах обработки персональных данных	Сущность угроз безопасности и основы подходов к оценке рисков. Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию. Угрозами информационному обеспечению государственной политики Российской Федерации. Угрозами развитию отечественной индустрии информации. Угрозами развитию отечественной индустрии информации. Угрозами безопасности информационных и телекоммуникационных средств и систем. Источники угроз информационной безопасности. Классификация нарушителей безопасности информационных систем персональных данных. Основные элементы инсайдерских правонарушений. Компоненты и модели реализации внутренней угрозы. Угрозы утечки персональных данных по техническим каналам утечки информации. Угрозы НСД, основанные на использовании уязвимостей ПО. Угрозы НСД, основанные на использовании уязвимостей протоколов сетевого взаимодействия. Угрозы НСД, основанные на использовании уязвимостей средства защиты информации (СЗИ). Угрозы НСД, основанные на использовании уязвимостей, обусловленных применением вредоносных программ, наличием в ИС закладочных устройств и/или программных закладок. Угрозы НСД, возникающие в результате сбоев и аварийных ситуаций в ИС.
Тема 2.3. Государственные регуляторы и их нормативно-правовая документация в области защиты персональных данных	Государственные органы исполнительной власти, осуществляющие надзор за соблюдением требований законодательства в области обработки персональных данных. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Полномочия данной Службы приведены в указе Президента РФ от 16.08.2004 №1085 «Вопросы Федеральной службы по техническому и экспортному контролю». Минобороны России, СВР России, ФСБ России, ФСО России и Главное управление специальных программ Президента Российской Федерации (ГУСП). Нормативно-правовая документация государственных органов исполнительной власти, осуществляющих надзор за соблюдением требований законодательства в области обработки персональных данных. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Постановление Правительства РФ от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами". Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях

	обработки персональных данных, осуществляемой без использования средств автоматизации». Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка).
Модуль 3. Управление защитой персональных данных при их обработке в информационных системах персональных данных	
Тема 3.1. Защита персональных данных при их обработке в информационных системах персональных данных	Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Разработка частной модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных организации. Определение уровня защищённости персональных данных. Состав и содержание мер по обеспечению безопасности персональных данных. Создание системы защиты персональных данных; сертифицированные средства защиты персональных данных в информационных системах защиты персональных данных; аттестация информационных систем персональных данных. Особенности использования средств криптографической защиты информации в рамках построения системы защиты персональных данных в организации. Особенности обработки персональных данных с использованием средств автоматизации и без использования средств автоматизации. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне информационных систем персональных данных. Разработка организационно-распорядительной документации, необходимой для организации обработки персональных данных
Тема 3.2. Моделирование систем и процессов обеспечения информационной безопасности	Виды моделей систем и процессов защиты информации. Классификация моделей. Методы оценки защищенности информации. Аналитический подход. Теоретический подход. Аналитико-эмпирический подход. Аналитическое моделирование систем и процессов обеспечения информационной безопасности. Модель противоправных действий по незаконному воздействию на защищаемую информацию. Модель процесса борьбы с противоправными действиями, направленными на защищаемую информацию. Применение методов компьютерного имитационного моделирования для обеспечения комплексной безопасности объекта информатизации. Цели компьютерного учения. Явные признаки вредоносной деятельности. Скрытыми признаками активности вредоносного ПО. Ликвидация последствий вредоносной активности на отдельном компьютере. Математическое моделирование уровня информационной безопасности объекта. Определение единого динамического коэффициента возникновения угрозы. Построение спектра угроз. Определение пределов значимости угроз. Построение гистограммы уязвимости. Определение предела значимости уязвимости. Определение риска. Определение коэффициента уязвимости объекта информатизации.
Тема 3.3. Организация работ и назначение ответственных лиц за обработку персональных данных	Основные направления управленческой (организационной) работы в сфере информационной безопасности на уровне отдельного предприятия. Общая структура политики информационной безопасности предприятия как основного организующего документа в этой области. Требования нормативных правовых документов. Разработка и анализ политик информационной безопасности. Назначение ответственного за организацию обработки ПДн и комиссии. Обязанности ответственного за организацию обработки ПДн. Содержание приказа о назначении ответственного за организацию обработки ПДн. Минимальный перечень мероприятий.
Модуль 4. Практическая реализация механизмов защиты персональных данных в организации	

Тема 4.1. Меры, необходимые и достаточные для выполнения обязанностей, при обработке персональных данных в организации	Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом. Меры по обеспечению безопасности персональных данных при их обработке. Постановление Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке», Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
Тема 4.2. Принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке	Основные направления защиты информации. Виды защиты информации. Правовые меры защиты. Физическая защита. Криптографические методы защиты информации. Техническая защита информации. Основные принципы, направления и методы технической защиты информации. Классификация направлений и методов инженерно-технической защиты информации. Методы нейтрализации угроз несанкционированных и непреднамеренных воздействий на носители информации, средства и системы информатизации. Организация научных исследований и разработок в области технической защиты информации. Приобретение статуса оператора персональных данных. Процедуры взаимодействия с внешней средой организации. Общественный контроль. Общественная аккредитация.

3. Организационные условия реализации программы

3.1. Материально-техническое и программное обеспечение реализации программы

РАНХиГС располагает необходимой материально-технической базой, обеспечивающей проведение программы повышения квалификации и итоговой аттестации, предусмотренной учебным планом программы и соответствующей действующим санитарным и противопожарным правилам и нормам. Реализуемая программа повышения квалификации обеспечена всеми необходимыми материально-техническими ресурсами. Занятия по программе проводятся в помещениях, оснащенных для проведения лекционных занятий и тренингов. При проведении лекционных и практических занятий, итоговой аттестации используется мультимедийное оборудование.

Для обеспечения обучения слушателей по программе имеется следующая материально-техническая база:

- лекционные аудитории, оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном и имеющие выход в сеть Интернет;
- помещения для проведения практических занятий, оборудованными учебной мебелью;
- библиотека, имеющую рабочие места для слушателей, оснащенные компьютерами с доступом к базам данных и сети Интернет;
- компьютерные классы.

Во время обучения слушатели имеют доступ к библиотечному фонду с необходимым количеством учебной, методической литературы и другой печатной продукции, для самостоятельной работы, а также к автоматизированным системам хранения и поиска информации, национальным и международным информационным ресурсам.

Программное обеспечение: лицензионные системные программы операционные системы, обеспечивающие взаимодействие всех других программ с оборудованием и взаимодействие пользователя персонального компьютера с программами; универсальные офисные прикладные программы и средства ИКТ, например: программа подготовки презентаций; использование Интернет, электронной почты; использование автоматизированных поисковых систем Интернет.

Слушатели получают методическую поддержку в процессе обучения и по завершении обучения, в т.ч. имеют возможность получать консультации по электронной почте у преподавателей, принимающих участие в обучении.

Реализация программы в дистанционном режиме осуществляется через Систему дистанционного обучения (СДО) WebTutor. Слушателям предоставляется авторизованный доступ на информационно-образовательный портал ВШГУ через ввод логина и пароля. Логин и пароль присваивается администратором системы дистанционного обучения. Вебинары проводятся в режиме видеоконференции на платформе МТС Линк.

Дистанционное обучение включает в себя изучение материалов, прохождение электронных курсов, онлайн тестирование на информационно-образовательных порталах Института ВШГУ и Финансового университета при Правительстве Российской Федерации.

3.2. Учебно-методическое и информационное обеспечение программы

Самостоятельная работа

Слушатели самостоятельно изучают электронные курсы, расположенные на платформе Института ВШГУ new.portal.gosedu.ru:

1. Основы публичного управления Российской Федерации, в том числе:

1) Бюджетная система и бюджетный процесс Российской Федерации.
2) Организация проектной деятельности в органах государственной власти.
3) Основы бережливого управления.

Также слушатели самостоятельно осваивают вебинары, опубликованные на образовательной платформе сетевого партнера http://www.fa.ru/Pages/Home.aspx

Примерный перечень вопросов для самостоятельной работы.

1. Понятие, сущность и классификация персональных данных в деятельности организации
2. Правовые основы обработки и защиты персональных данных в Российской Федерации
3. Принципы обработки персональных данных и условия их законного использования
4. Права субъектов персональных данных и обязанности оператора
5. Организация системы защиты персональных данных в деятельности организации
6. Разработка и внедрение политики обработки персональных данных
7. Документальное обеспечение процессов обработки персональных данных
8. Порядок получения и оформления согласия на обработку персональных данных
9. Обеспечение конфиденциальности и разграничение доступа к персональным данным
10. Информационные системы персональных данных: классификация, угрозы и модели нарушителя
11. Организационные и технические меры защиты персональных данных
12. Особенности обработки персональных данных в цифровой среде и сети Интернет
13. Аудит и оценка соответствия деятельности организации требованиям законодательства о персональных данных
14. Контроль и надзор в сфере защиты персональных данных. Ответственность за нарушения
15. Современные тенденции и перспективы развития системы защиты персональных данных

Нормативные правовые документы:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) http://www.consultant.ru/document/cons_doc_LAW_28399.
2. Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 г. № 646 https://base.garant.ru/71556224/
3. Федеральный закон РФ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 09.02.2009 г. № 8-ФЗ https://base.garant.ru/194874.
4. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» 27.07.2006 г. № 149-ФЗ https://base.garant.ru/12148555.
5. Федеральный закон РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ https://base.garant.ru/12148567.
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
8.

9. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

10. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

11. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

12. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (зарегистрировано в Минюсте России 16.06.2025 № 82619).

13. Приказ Роскомнадзора «Об утверждении требований и методов по обезличиванию персональных данных» от 05.09.2013 № 996 https://normativ.kontur.ru/document?moduleId=1&documentId=218622.

14. Постановление Правительства РФ «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512 https://base.garant.ru/193541.

15. Постановление Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г. № 687 https://base.garant.ru/193875.

16. Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 21.03.2012 г. № 211 https://base.garant.ru/70152982.

17. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119 https://base.garant.ru/70252506.

18. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

19. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

20. Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171.

Документы национальной системы стандартизации Российской Федерации в области защиты информации

21. ГОСТ 30373-95/ГОСТ Р 50414-92 Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний.

22. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

23. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества.

24. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

25. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

26. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной

безопасности в организации. Основные термины и определения.

27. ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.

28. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

29. ГОСТ Р 58189-2018. Защита информации. Требования к органам по аттестации объектов информатизации.

30. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

31. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

32. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

33. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

34. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

35. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности.

36. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

37. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

38. Рекомендации по стандартизации Р 50.1.050-2004. Защита информации. Система обеспечения качества техники защиты информации. Общие положения.

39. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации.

40. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения.

Нормативные распорядительные документы ФСТЭК России

41. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

42. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

43. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

44. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка).

ФСТЭК России, 2008 г.

45. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008

46. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.

47. Приказ ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

48. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

49. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

50. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

51. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (зарегистрировано в Минюсте России 16.06.2025 № 82619).

52. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

53. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

54. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

55. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

56. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

57. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

58. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Одобрены решением коллегии Гостехкомиссии России от 2 марта 2001 г. № 7.2.

59. Типовое положение об испытательной лаборатории. Утверждено Гостехкомиссией России, 25 ноября 1994 г.

60. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 9 февраля 2016 г. № 9.

61. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты). Утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28.

62. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

63. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.

64. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

65. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

Основная и дополнительная литература

1. Аверченков В. И. Защита персональных данных в организации: монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин - 4-е изд. - Москва: ФЛИНТА, 2021. - 124 с. - ISBN 978-5-9765-1273-3. - URL: https://znanium.com/catalog/product/1843194.
2. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш - 2-е изд. -М.: ИЦ РИОР: НИЦ ИНФРА- М, 2014. - 216 с. https://znanium.ru/catalog/document?id=52118.
3. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. – 4-е изд., перераб. и доп. – Москва: ДМК Пресс, 2025. – 436 с. – ISBN 978-5-93700-219-9 - https://znanium.ru/catalog/document?id=418731&ysclid=mo9sp6nxr5601076844.
4. Бычков А. И. Проблемы защиты персональных данных / А. И. Бычков. – Москва: Infotropic Media, 2020. – 116 с. – ISBN 978-5-9998-0352-8. — URL: https://e.lanbook.com/book/234317.
5. Внуков, А. А. Защита информации: учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584050.
6. Войниканис Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом: учебник для вузов / Е. А. Войниканис; под редакцией М. А. Федотова. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 50 с. — (Высшее образование). — ISBN 978-5-534-19364-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589232.
7. Галатенко В.А. Стандарты информационной безопасности. - М.: Интернет-университет информационных технологий, 2025 г. - 264 с. - https://znanium.ru/catalog/document?id=448431&ysclid=mo9ssay51g777310597.

8. Гродзенский Я. С. Информационная безопасность: учебное пособие / Я. С. Гродзенский. – Москва: РГ-Пресс, 2025. – 144 с. – (Высшее образование). – ISBN 978-5-9988-1755-7.
9. Дубинин, Е.А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2022. - 192 с. - https://znanium.ru/catalog/document?id=400262&ysclid=mo9ssyajnr857969572.
10. Дупан (Гутникова) А.С., Жулин, А.Б., Жарова А.К. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет. М.: Издательский дом ВШЭ, 2026. - 344 с. - https://znanium.ru/catalog/document?id=359198&ysclid=mo9stu75fg24089389.
11. Жарова А. К. Информационное право. Правовое регулирование создания и использования информационной инфраструктуры: учебник для вузов / А. К. Жарова. — Москва: Издательство Юрайт, 2026. — 300 с. — (Высшее образование). — ISBN 978-5-534-19904-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588704.
12. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2026. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584673.
13. Козьминых С. И. Организационное и правовое обеспечение информационной безопасности: учебное пособие. – М.: – Финансовый университет при Правительстве Российской Федерации, кафедра «Информационная безопасность», 2020. 497с. - https://znanium.ru/catalog/document?id=375641&ysclid=mo9suim9z1832266191
14. Копылов В.А. О структуре и составе информационного законодательства И Государство, и право. 2024. № 10. – 232 с.
15. Минаев В.А., Фисун А.П. Правовое обеспечение информационной безопасности, Москва, 2018 г. 368 с.
16. Организационное и правовое обеспечение информационной безопасности: учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584372.
17. Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2024. — 392 с. - https://znanium.ru/catalog/document?id=325489&ysclid=mo9swgtkvt866364823.
18. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В. И. Петренко, И. В. Мандрица – 5-е изд., стер. – Санкт-Петербург: Лань, 2024. – 108 с. – ISBN 978-5-507-47575-9. – URL: https://e.lanbook.com/book/392402.
19. Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. – 5-е изд., стер. – Санкт-Петербург: Лань, 2025. – 336 с. – ISBN 978-5-8114-8945-2.
20. Рассолов И. М. Информационное право: учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 427 с. — (Высшее образование). — ISBN 978-5-534-18043-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/582668.

Интернет-ресурсы и справочные системы

- www.council.gov.ru – Совет Федерации Федерального Собрания Российской Федерации
- www.duma.gov.ru – Государственная Дума Российской Федерации
- http://pravo.gov.ru/ - Официальный интернет-портал правовой информации Российской Федерации
- https://publication.pravo.gov.ru/. - Официальное опубликование правовых актов
- http://nlr.ru/ - Российская национальная библиотека
- https://rusneb.ru/ -Национальная электронная библиотека
- https://www.rsl.ru/ - Российская государственная библиотека
- https://www.rambler.ru/ - Поисковая система
- https://yandex.ru/ - Поисковая система
- http://www.consultant.ru/ - Консультант плюс
- https://www.garant.ru/ - Гарант
- https://znanium.com - электронно-библиотечная система Znanium
- https://www.bib1io-online.ru – электронно-библиотечная система издательства «ЮРАЙТ»
- http://elibrary.ru - научная электронная библиотека eLibraiy.ru

4. Оценка качества освоения программы

4.1. Формы и объем промежуточной аттестации

Промежуточная аттестация (зачет) осуществляется в форме тестирования с применением дистанционных образовательных технологий и реализуется сетевым партнером.

Примерный перечень вопросов для проведения промежуточной аттестации

Инструкция для слушателя: выберите один или несколько правильных вариантов ответов.

1. Что относится к персональным данным?
а) Только паспортные данные
б) Только ФИО
в) Любая информация, относящаяся к прямо или косвенно определенному физическому лицу
г) Только контактные данные

2. Основной нормативный акт РФ в области персональных данных:
а) Гражданский кодекс РФ
б) Федеральный закон № 152-ФЗ «О персональных данных»
в) Трудовой кодекс РФ
г) Налоговый кодекс РФ

3. Кто является оператором персональных данных?
а) Только государственные органы
б) Только коммерческие организации
в) Любое лицо, организующее и (или) осуществляющее обработку персональных данных
г) Только IT-компании

4. Что понимается под обработкой персональных данных?
а) Только хранение данных
б) Только передача данных

в) Любое действие с персональными данными (сбор, запись, хранение и др.)
г) Только удаление данных

5. Когда требуется согласие субъекта персональных данных?
а) Всегда
б) В случаях, не предусмотренных законом как исключение
в) Никогда
г) Только при передаче данных

6. Что является принципом обработки персональных данных?
а) Максимальное распространение
б) Ограничение обработки достижением конкретных целей
в) Свободный доступ
г) Хранение без срока

7. Кто несет ответственность за организацию обработки ПДн в компании?
а) Любой сотрудник
б) Пользователь системы
в) Оператор персональных данных
г) Клиент

8. Что такое обезличивание персональных данных?
а) Удаление данных
б) Передача третьим лицам
в) Действия, в результате которых невозможно определить принадлежность данных конкретному субъекту
г) Архивирование данных

9. Что относится к специальным категориям персональных данных?
а) Адрес проживания
б) Телефон
в) Данные о здоровье, расовой принадлежности, политических взглядах
г) Электронная почта

10. Что такое информационная система персональных данных (ИСПДн)?
а) Любой компьютер
б) Только сервер
в) Совокупность баз данных и технологий, обеспечивающих обработку ПДн
г) Только облачный сервис

11. Что является целью защиты персональных данных?
а) Увеличение прибыли
б) Предотвращение неправомерного доступа и утечек
в) Ускорение работы сотрудников
г) Хранение данных без ограничений

12. Что такое трансграничная передача персональных данных?
а) Передача внутри организации
б) Передача по локальной сети
в) Передача данных на территорию иностранного государства
г) Передача между отделами

13. Какой документ определяет политику обработки ПДн в организации?
а) Устав
б) Должностная инструкция
в) Политика обработки персональных данных
г) Бухгалтерский отчет

14. Что относится к мерам защиты ПДн?
а) Только антивирус
б) Только пароль
в) Организационные и технические меры в комплексе
г) Только резервное копирование

15. Кто контролирует соблюдение законодательства о ПДн в РФ?
а) МВД
б) ФНС
в) Роскомнадзор
г) Банк России

16. Какой принцип ограничивает сроки хранения ПДн?
а) Принцип доступности
б) Принцип прозрачности
в) Принцип хранения не дольше, чем этого требуют цели обработки
г) Принцип открытости

17. Что обязан сделать оператор при утечке персональных данных?
а) Игнорировать
б) Удалить систему
в) Принять меры по устранению нарушения и уведомить уполномоченные органы (при необходимости)
г) Закрыть компанию

18. Что такое согласие субъекта ПДн?
а) Устное разрешение
б) Свободное, конкретное, информированное и сознательное выражение воли
в) Приказ руководителя
г) Договор между сотрудниками

19. Что относится к организационным мерам защиты?
а) Шифрование
б) Антивирус
в) Регламенты, инструкции, разграничение доступа
г) Серверное оборудование

20. Что является нарушением законодательства о ПДн?
а) Обработка с согласия
б) Хранение по закону
в) Обработка без законных оснований
г) Уничтожение по сроку

Таблица 4.1.1

Критерии оценки слушателей (промежуточная аттестация)

Оценка	Требования к знаниям
зачтено	Выставляется слушателю, если он выполнил итоговый тест с результатом **не менее** 60 %
не зачтено	Выставляется слушателю, если он выполнил итоговый тест с результатом **менее** 60 %

4.2. Формы и объем итоговой аттестации

Итоговая аттестация (зачет) осуществляется в форме тестирования с применением дистанционных образовательных технологий на образовательной платформе Института ВШГУ new.portal.gosedu.ru с онлайн-сопровождением слушателей администраторами программы.

Итоговая аттестация является обязательной для слушателей, завершающих обучение по программе.

В соответствии с Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и приказом от 13.01.2026 № 02-00009/001 Об утверждении Положения об итоговой аттестации слушателей дополнительных профессиональных программ в Академии» к итоговой аттестации допускаются слушатели, не имеющие академической задолженности и в полном объеме выполнившие учебный план

Оценка качества освоения программы проводится в отношении соответствия результатов освоения программы заявленным целям и планируемым результатам обучения.

Слушатели, успешно прошедшие итоговую аттестацию, получают соответствующие документы о повышении квалификации, форму которых образовательная организация устанавливает самостоятельно: удостоверение о повышении квалификации.

Слушатели, не прошедшие итоговую аттестацию или получившие на итоговой аттестации неудовлетворительные результаты, вправе пройти повторно итоговую аттестацию в сроки, определяемые образовательной организацией.

Слушателям, не прошедшим итоговую аттестацию по уважительной причине (по медицинским показаниям или в других исключительных случаях, документально подтвержденных), должна быть предоставлена возможность пройти итоговую аттестацию без отчисления из организации, в соответствии с медицинским заключением или другим документом, предъявленным слушателем, или с восстановлением на дату проведения итоговой аттестации.

Слушателям, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, выдается справка об обучении или о периоде обучения по образцу, самостоятельно установленному образовательной организацией.

Примерный перечень тестовых вопросов для проведения итоговой аттестации
Инструкция для слушателя: выберите один или несколько правильных вариантов ответов.

1. Какова ключевая особенность бюджетной системы Российской Федерации?
а) Полная автономия регионов
б) Отсутствие вертикальной структуры
в) Многоуровневая система с разграничением полномочий между уровнями власти
г) Централизация только на муниципальном уровне

2. Какой этап бюджетного процесса включает утверждение бюджета?

а) Составление проекта бюджета
б) Исполнение бюджета
в) Рассмотрение и утверждение бюджета
г) Контроль исполнения

3. В чем заключается цель проектной деятельности в органах государственной власти?
а) Увеличение документооборота
б) Достижение конкретных результатов в ограниченные сроки с использованием ресурсов
в) Сокращение сотрудников
г) Повышение отчетности

4. Какой принцип лежит в основе бережливого управления?
а) Увеличение затрат
б) Централизация решений
в) Устранение потерь и повышение ценности для потребителя
г) Минимизация контроля

5. Что является объектом правового регулирования в области персональных данных?
а) Только бумажные документы
б) Любые операции с персональными данными, включая автоматизированную обработку
в) Только базы данных
г) Только государственные системы

6. Что понимается под информационной системой персональных данных (ИСПДн)?
а) Только сервер хранения данных
б) Только программное обеспечение
в) Совокупность баз данных и обеспечивающих их обработку информационных технологий и технических средств
г) Только облачное хранилище

7. Какова цель классификации ИСПДн?
а) Упрощение документооборота
б) Определение уровня защищенности и необходимых мер безопасности
в) Ускорение обработки данных
г) Сокращение персонала

8. Что включает модель угроз безопасности персональных данных?
а) Только список вирусов
б) Только технические риски
в) Анализ возможных источников угроз, уязвимостей и потенциальных нарушителей
г) Только внутренние угрозы

9. Какой орган осуществляет контроль и надзор в сфере защиты персональных данных?
а) Минфин
б) МВД
в) Роскомнадзор
г) ФАС

10. Какова роль ФСТЭК России в области защиты персональных данных?
а) Контроль налогов
б) Разработка требований по технической защите информации
в) Регистрация организаций
г) Судебный контроль

11. Что относится к полномочиям ФСБ России в данной сфере?
а) Проверка бухгалтерии
б) Регулирование криптографической защиты информации
в) Лицензирование бизнеса
г) Контроль кадров

12. Что является ключевым элементом системы управления защитой ПДн?
а) Только программное обеспечение
б) Только инструкции
в) Комплекс правовых, организационных и технических мер
г) Только кадровая политика

13. Что включает процесс моделирования системы информационной безопасности?
а) Только разработку ПО
б) Анализ угроз, построение моделей нарушителя и определение мер защиты
в) Только аудит
г) Только отчетность

14. Кто должен быть назначен ответственным за обработку персональных данных?
а) Любой сотрудник
б) Только бухгалтер
в) Специально назначенное должностное лицо
г) Внешний подрядчик

15. В чем заключается задача ответственного за ПДн?
а) Ведение бухгалтерии
б) Организация и контроль соблюдения требований законодательства о ПДн
в) Управление продажами
г) Контроль закупок

16. Какие меры относятся к правовым мерам защиты ПДн?
а) Антивирус
б) Шифрование
в) Разработка локальных нормативных актов и договоров
г) Серверное оборудование

17. Что относится к организационным мерам защиты?
а) Программирование
б) Установка ПО
в) Регламентация доступа и обучение сотрудников
г) Настройка серверов

18. Какие меры относятся к техническим мерам защиты?
а) Приказы
б) Инструкции

в) Средства защиты информации (СЗИ), системы контроля доступа
г) Договоры

19. Что является критерием достаточности мер защиты ПДн?
а) Минимальные затраты
б) Соответствие установленным требованиям и уровню угроз
в) Максимальная автоматизация
г) Скорость обработки

20. В чем заключается принцип минимизации данных?
а) Сбор всех возможных данных
б) Обработка только необходимых для целей данных
в) Хранение данных бессрочно
г) Передача третьим лицам

21. Какова цель проведения аудита защиты персональных данных?
а) Увеличение прибыли
б) Оценка соответствия требованиям законодательства и выявление нарушений
в) Сокращение персонала
г) Оптимизация налогов

22. Что включает система внутреннего контроля защиты ПДн?
а) Только проверки IT
б) Регулярный мониторинг, аудит и корректирующие мероприятия
в) Только отчетность
г) Только обучение

23. Какова роль цифровизации в защите персональных данных?
а) Увеличение рисков
б) Исключение контроля
в) Повышение эффективности обработки и внедрение современных средств защиты
г) Отмена требований

24. Что необходимо учитывать при передаче ПДн третьим лицам?
а) Только скорость передачи
б) Наличие правовых оснований и обеспечение защиты данных
в) Удобство системы
г) Стоимость услуг

25. Какой подход является наиболее эффективным при организации защиты ПДн?
а) Реактивный (после инцидента)
б) Минимальный
в) Комплексный и риск-ориентированный
г) Формальный

Таблица 4.2.1

Критерии оценки слушателей (итоговая аттестация)

Оценка	Требования к знаниям
«зачтено»	**60** и более процентов Выставляется, если слушатель успешно справился со всеми заданиями. Допускаются неточности, недостаточно правильные

	формулировки, нарушения логической последовательности в изложении материала, затруднения при выполнении работ
«не зачтено»	Менее **60** процентов Выставляется слушателю, если работа была проведена с существенными ошибками, неуверенно, с большими затруднениями. Как правило, оценка «незачет» ставится слушателям, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

5. Индикаторы сформированных компетенций

В результате освоения программы у слушателя сформированы следующие компетенции:

Таблица 5.1

Индикаторы сформированных компетенций

Компетенция (код, содержание)	Индикаторы
ОПК-8. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	– знает принципы функционирования современных информационных технологий и информационных систем, используемых при обработке персональных данных, включая информационные системы персональных данных (ИСПДн), а также требования законодательства Российской Федерации в области защиты персональных данных; – способен объяснять принципы работы информационных систем и выбирать подходящие технологические решения для обработки и защиты персональных данных с учетом нормативных требований; использует информационные системы и цифровые инструменты для организации обработки персональных данных и обеспечения их защиты в профессиональной деятельности; – знает состав и содержание правовых, организационных и технических мер по обеспечению безопасности персональных данных, а также полномочия государственных регуляторов в данной сфере; – реализует комплекс мер по защите персональных данных, включая разработку локальных нормативных актов и организацию процессов обработки данных; – способен планировать и организовывать проекты по внедрению и совершенствованию систем защиты персональных данных с использованием современных ИТ-инструментов.
ПСК-1. Администрирование систем защиты информации автоматизированных систем	- настраивает и сопровождает системы защиты персональных данных в информационных

	системах в соответствии с установленными требованиями; - осуществляет контроль функционирования средств защиты информации и выявляет инциденты информационной безопасности; - реализует процедуры администрирования доступа пользователей к персональным данным с учетом политики безопасности; - применяет технические средства защиты информации (СЗИ) в автоматизированных системах обработки персональных данных.
ПСК-2. Управление защитой информации в автоматизированных системах	– организует систему управления защитой персональных данных в организации на основе риск-ориентированного подхода; – разрабатывает и внедряет организационные и технические меры по обеспечению безопасности персональных данных; – проводит оценку угроз и уязвимостей информационных систем персональных данных; – контролирует соблюдение требований законодательства и внутренних регламентов в области защиты информации; – координирует деятельность подразделений при реализации мероприятий по защите персональных данных.
ПЛК-1. Умение оперативно принимать и реализовывать управленческие решения	– принимает обоснованные управленческие решения в области защиты персональных данных на основе анализа рисков и нормативных требований; – оперативно реагирует на инциденты информационной безопасности и организует мероприятия по их устранению; – обосновывает выбор мер защиты персональных данных с учетом эффективности и ресурсных ограничений; – организует взаимодействие сотрудников при реализации политики защиты персональных данных в организации.