Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Южно-Российский институт управления

ЮРИУ РАНХиГС
ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00877FD556E316C61412D78C397507BB4D
Владелец: Рудой Василий Владимирович
Действителен: с 11.09.2026 до 05.12.2027

«УТВЕРЖДАЮ»
Директор ЮРИУ РАНХиГС
В.В. Рудой
«26» февраля 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации

Обеспечение безопасности персональных данных в информационных системах персональных данных

(наименование программы)

г. Ростов-на-Дону, 2026

Разработчик

Директор центра дополнительного образования Южно-Российского института управления – филиала РАНХиГС, к.п.н., доцент _____ И.Н. Шлеверда

Руководитель программы

Директор центра дополнительного образования Южно-Российского института управления – филиала РАНХиГС, к.п.н., доцент _____ И.Н. Шлеверда

Руководитель структурного подразделения

Заместитель директора Южно-Российского института управления – филиала РАНХиГС _____ А.В. Баранов

Программа повышения квалификации рассмотрена на заседании ученого совета ЮРИУ РАНХиГС и рекомендована к реализации, протокол № 53 от «26» февраля 2026 г.

СОДЕРЖАНИЕ

		Стр.
1.	ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ……	4
	1.1. Цель *и задачи (при необходимости)* реализации программы……	4
	1.2. Нормативные правовые акты…….....	4
	1.3. Планируемые результаты обучения……..	6
	1.4. Категория слушателей…	12
	1.5. Формы и технологии обучения……..	12
	1.6. Период обучения, срок освоения и режим занятий….....	12
	1.7. Документ о квалификации…….	12
2.	СОДЕРЖАНИЕ ПРОГРАММЫ…….	13
	2.1. Календарный учебный график……	13
	2.2. Учебный план……	14
	2.3. Содержание программы по модулям (или) разделам, (или) дисциплинам и (или) темам ……	20
3.	ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ…	21
	3.1.Материально-техническое и программное обеспечение реализации программы…….	21
	3.2. Учебно-методическое и информационное обеспечение программы	22
4.	ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ……	33
5.	ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ……	37

Приложение № 1. Аннотация
Приложение № 2 Сведения о преподавательском составе и ведущих специалистах (кадровая справка)

ВНЕШНЯЯ РЕЦЕНЗИЯ

на дополнительную профессиональную программу повышения квалификации

«Обеспечение безопасности персональных данных в информационных системах персональных данных»

Категория слушателей программы. Программа предназначена для лиц, замещающих государственные должности, для государственных гражданских служащих (федеральных или субъектов Российской Федерации), муниципальных служащих или лиц, замещающих муниципальные должности, сотрудников организаций, учреждений и предприятий различных форм собственности. К освоению программы допускаются лица, имеющие или получающие среднее профессиональное образование или высшее образование.

Актуальность программы.

Совокупность организационных мер и средств защиты информации, включающих средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в информационной системе информационные технологии является системой защиты персональных данных.

Существующая в современном мире концепция защиты информационных прав человека нашла свое отражение в национальном законодательстве об охране персональных данных. Разработаны многочисленные стандарты и нормы, обеспечивающие их надлежащую защиту, но каждая организация, системно работающая с большими массивами информации, обязана создать собственную информационную систему защиты, что позволит избежать утечек информации. В связи с этим актуальным является повышение квалификации граждан, в должностные обязанности которых входит обеспечение безопасности персональных данных. Программа разработана на основании требований действующего законодательства Российской Федерации и нормативных документов, регламентирующих вопросы защиты персональных данных, с учетом развития информационных технологий.

Цель программы. Целью реализации программы является совершенствование имеющихся компетенций, необходимых для профессиональной деятельности в области обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, с учетом соответствующего профессионального стандарта, повышение профессионального уровня в рамках имеющейся квалификации.

Основное направление подготовки. Приказ Минтруда России от 14.09.2022 N 533н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (Зарегистрировано в Минюсте России 14.10.2022 N 70515). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

Приказ Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

Особенности программы. Формы обучения – очная; очная с применением дистанционных образовательных технологий и электронного обучения; заочная с применением электронного обучения.

Срок реализации программы.

24 академических часа. Занятия проводятся в течение 3 рабочих дней по расписанию: 3 рабочих дня в неделю, до 8 академических часов в день. По окончании курса проводится итоговая аттестация.

40 академических часов. Занятия проводятся в течение 5 рабочих дней по расписанию: 5 рабочих дня в неделю, до 8 академических часов в день. По окончании курса проводится итоговая аттестация.

Заключение.

Программа соответствует требованиям, предъявляемым к дополнительным профессиональным программам повышения квалификации и рекомендуется к реализации.

Механизм реализации программы выражен в формах, методах и средствах обучения, учете особенностей учащихся. Включенные в структуру программ темы раскрывают сущность актуальных на сегодняшний день проблем. Кроме того, структура каждой программы в целом логична и последовательна, а включенные в нее темы раскрывают сущность актуальных на сегодняшний день задач и проблем в изучаемой сфере.

Содержание представленной программы и ее оценочных средств итоговой аттестации отражает оценку достижений запланированных результатов обучения и уровня сформированности у слушателей компетенций, заявленных в образовательной программе. Контроль и оценка результатов освоения программ включают в себя показатели оценки результатов, формы и методы контроля и оценки освоенных профессиональных компетенций. Все это в совокупности позволяет сделать вывод о высококачественном содержании образовательной программе и ее практической значимости.

Рецензент

Начальник отдела организационной работы и делопроизводства Министерства общего и профессионального образования Ростовской области — А. И. Михайличенко

ВНУТРЕННЯЯ РЕЦЕНЗИЯ

на дополнительную профессиональную программу повышения квалификации

«Обеспечение безопасности персональных данных в информационных системах персональных данных»

Категория слушателей программы. Программа предназначена для лиц, замещающих государственные должности, для государственных гражданских служащих (федеральных или субъектов Российской Федерации), муниципальных служащих или лиц, замещающих муниципальные должности, сотрудников организаций, учреждений и предприятий различных форм собственности. К освоению программы допускаются лица, имеющие или получающие среднее профессиональное образование или высшее образование.

Актуальность программы.

Обеспечение безопасности персональных данных в информационных системах остается важной и актуальной задачей, требующей постоянного внимания и усовершенствования подходов в связи с быстро меняющимися условиями и угрозами.

Актуальность программы обеспечения безопасности персональных данных в информационных системах обусловлена несколькими ключевыми факторами: увеличение киберугроз, законодательные требования, повышение рисков для конфиденциальности, управление доверияими пользователей, рост объема персональных данных, технологические изменения и инновации, необходимость соответствия стандартам, сохранение конфиденциальности, бизнес-процессы и управление информацией.

Особенность программы состоит в том, что она дает возможность самостоятельно применять полученные в процессе обучения знания, умения и навыки, использовать наиболее целесообразные приемы, методы и средства управления в любой сфере деятельности (в государственных органах, государственных корпорациях и фондах, бюджетных учреждениях, а также коммерческих компаниях, часто взаимодействующих с государством).

Цель программы. Целью реализации программы является совершенствование имеющихся компетенций, необходимых для профессиональной деятельности в области обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, с учетом соответствующего профессионального стандарта, повышение профессионального уровня в рамках имеющейся квалификации.

Основное направление подготовки.

Приказ Минтруда России от 14.09.2022 N 533н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (Зарегистрировано в Минюсте России 14.10.2022 N 70515). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

Приказ Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

Особенности программы.

Формы обучения – очная; очная с применением дистанционных образовательных технологий и электронного обучения; заочная с применением электронного обучения.

Срок реализации программы.

24 академических часа. Занятия проводятся в течение 3 рабочих дней по расписанию: 3 рабочих дня в неделю, до 8 академических часов в день. По окончании курса проводится итоговая аттестация.

40 академических часов. Занятия проводятся в течение 5 рабочих дней по расписанию: 5 рабочих дня в неделю, до 8 академических часов в день. По окончании курса проводится итоговая аттестация.

Заключение.

Программа соответствует требованиям, предъявляемым к дополнительным профессиональным программам повышения квалификации и рекомендуется к реализации.

В целом, рецензируемая программа дополнительного профессионального образования (повышение квалификации) отвечает основным требованиям профессионального стандарта, а также позволяет обучающимся развить необходимые компетенции, повысить квалификацию и быть готовым осуществлять свою профессиональную деятельность на высоком уровне.

Рецензент

Доцент кафедры информационных технологий Южно-Российского института управления – филиала РАНХиГС, к. физ.- мат. н. Н.Д. Никоненко

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель и задачи реализации программы

Цель: совершенствование имеющихся компетенций, необходимых для профессиональной деятельности в области обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, с учетом соответствующего профессионального стандарта, повышение профессионального уровня в рамках имеющейся квалификации.

Задачи реализации программы:

- изучить требования, предъявляемые к обеспечению персональных данных при их обработке в информационных системах персональных данных.
- сформировать набор знаний, умений и навыков, необходимых в последующей профессиональной деятельности.

1.2. Нормативные правовые акты

Дополнительная профессиональная программа повышения квалификации разработана на основе следующих нормативных документов:

Федеральный закон от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации" (с изм. и доп. от 25 апреля 2026 г. № 107-ФЗ, изменения вступают в силу с 25 апреля 2026 г.)

Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» (с изм. и доп. от 28 декабря 2025 г. № 505-ФЗ, вступ. в силу с 1 января 2026 г.).

Постановление Правительства РФ от 12.05.2012 г. № 473 «Об утверждении устава федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (с изм. и доп. от 30 июля 2025 г.).

Приказ Минобрнауки России от 24.03.2025 N 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам" (Зарегистрировано в Минюсте России 22.04.2025 N 81928, действует до 1 сентября 2031г.).

Приказ Минобрнауки России от 12.09.2013 N 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования" (с изм. и доп. от 13.12.2021).

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

Приказ РАНХиГС "Об утверждении порядка разработки и утверждения в Академии дополнительных профессиональных программ - программ повышения квалификации, программ профессиональной переподготовки" от 02 декабря 2025 года N 02-02669/001.

Приказ от 19 апреля 2019 года N 02-461 "Об утверждении локальных нормативных актов РАНХиГС по дополнительному профессиональному образованию"

Приказ РАНХиГС "Об утверждении Правил приема на обучение по дополнительным профессиональным программам в Академию" от 13 января 2026 года N 02-00010/001.

Приказ РАНХиГС "Об утверждении Положения об итоговой аттестации слушателей дополнительных профессиональных программ в Академии" от 13 января 2026 года N 02-00009/001.

Приказ РАНХиГС Об утверждении порядка реализации дополнительных профессиональных программам в Академии от 20 апреля 2026 года N 02-00742/001.

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

Методические рекомендации Министерства образования и науки Российской Федерации от 22.01.2015г. № ДЛ-1/05вн «Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов».

Постановление Правительства РФ от 11.10.2023 N 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Устав ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, утверждённый постановлением Правительства РФ от 12 мая 2012 г. № 473.

Приказ РАНХиГС «Об утверждении образовательного стандарта Академии по направлению подготовки 38.03.04 Государственное и муниципальное управление» от 15.04.2024 года №7397.

Приказ Минтруда России от 14.09.2022 N 533н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (Зарегистрировано в Минюсте России 14.10.2022 N 70515). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

Приказ Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

ОКВЭД 2 - Общероссийский классификатор видов экономической деятельности ОК 029-2014 (КДЕС Ред. 2). Утвержден Приказом Росстандарта от 31.01.2014 № 14-ст с введением в действие с 1 февраля 2014 года и отменой с 1 января 2015 года предыдущих редакций ОКВЭД.

Единый квалификационный справочник должностей руководителей, специалистов и других служащих, Раздел I, Общеотраслевые квалификационные характеристики должностей работников, занятых на предприятиях, в учреждениях и организациях, утвержденный Постановлением Минтруда РФ от 21.08.1998 № 37 (ред. от 27.03.2018).

Справочник квалификационных требований к специальностям, направлениям подготовки (к укрупненным группам специальностей и направлений подготовки), к профессиональному уровню, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих (утв. Министерством труда и социальной защиты Российской Федерации) (по состоянию на 14 августа 2025 г.). https://base.garant.ru/71710924/

1.3.Планируемые результаты обучения

Перечень профессиональных компетенций в рамках имеющейся квалификации и профессиональных компетенций, планируемых к освоению (результаты обучения)

Таблица 1

Виды деятельности	*ПСК (профессионально-специализированная компетенция) (формируются и (или) совершенствуются)*	*Практический опыт*	*Знания*	*Умения*
ВД. 1 Обслуживание систем защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости (трудовая функция код А/01.5, (А/02.5), А/03.5, уровень квалификации 5)	ПСК – 1. Проведение технического обслуживания систем защиты информации автоматизированных систем (А/01.5)[1]	Проверка работоспособности системы защиты информации автоматизированной системы; Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации; Контроль стабильности характеристик системы защиты информации автоматизированной системы	Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; Базовая конфигурация системы защиты информации автоматизированной системы; Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах; Типовые средства, методы и протоколы идентификации, аутентификации и авторизации; Нормативные правовые акты в области защиты информации; Организационные меры по защите информации	Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией; Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации; Производить монтаж и диагностику компьютерных сетей; Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи.

[1] Приказ Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543), А/01.5, уровень квалификации 5

	ПСК – 2. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем (A/02.5)[2]	Ведение документов учета, обработки, хранения и передачи информации ограниченного доступа; Информирование персонала об угрозах безопасности информации; Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации; Ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем; Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем; Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем; Подготовка сведений об отсутствии необходимости присвоения категорий значимости объекту критической информационной инфраструктуры, на котором	Нормативные правовые акты в области защиты информации; Основные методические и руководящие документы федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации; Эксплуатационная и проектная документация на автоматизированную систему; Основные методы организации и проведения технического обслуживания технических средств информатизации; Организационные меры по защите информации	Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации

[2] Приказ Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543) , A/02.5, уровень квалификации 5

		используется автоматизированная система, и направление в письменном виде этих сведений в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме		
	ПСК – 3. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем (A/03.5)[3]	Включение в организационно-распорядительные документы по защите информации процедур уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации; Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания); Физическое уничтожение машинных носителей информации, обрабатываемой автоматизированной	Процедуры архивирования информации, обрабатываемой автоматизированной системой; Назначение и принципы работы основных узлов современных технических средств информатизации; Организация технического обслуживания и ремонта компонентов автоматизированной системы; Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации; Нормативные правовые акты в области защиты информации;	Использовать программные средства для архивирования информации; Использовать программные и программно-аппаратные средства для уничтожения (стирания) информации и носителей информации; Использовать типовые криптографические средства защиты информации, в том числе электронную подпись

[3] Приказ Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543) , A/01.5, уровень квалификации 5

		системой; Архивирование информации, обрабатываемой автоматизированной системой	Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации.	
ВД 2. Техническое обслуживание средств защиты информации в компьютерных системах и сетях (трудовая функция код А/02.5, А/03.5, уровень квалификации 5)	ПСК- 4. Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях (А/02.5)[4]	Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях Установка программно-аппаратных средств защиты информации в компьютерных сетях Установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации Настройка программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам Устранение неисправностей программно-аппаратных средств защиты информации в компьютерных сетях согласно технической документации Инструктирование пользователей по порядку безопасной работы в компьютерных сетях Оформление	Топология и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях Состав и основные характеристики оборудования, применяемого при построении компьютерных сетей Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях Типичные сетевые атаки и способы защиты от них Сущность и содержание понятия информационной безопасности, характеристики ее составляющих Основные источники угроз информационной безопасности и меры по их предотвращению Программно-аппаратные средства и методы защиты информации	Применять программно-аппаратные средства защиты информации в компьютерных сетях Устанавливать межсетевые экраны в компьютерных сетях Конфигурировать межсетевые экраны в соответствии с заданными правилами Работать в компьютерных сетях с соблюдением действующих требований по защите информации Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях Формулировать предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях

[4] Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 533н), А/02.5, уровень квалификации 5

		эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях	Порядок обеспечения безопасности информации при эксплуатации компьютерных сетей Формы и методы инструктажа пользователей по порядку работы в компьютерных сетях Нормативные правовые акты в области защиты информации Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Организационные меры по защите информации	
	ПСК-5. Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения (A/03.5)[5]	Установка программного обеспечения Настройка программного обеспечения с соблюдением требований по защите информации Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам Инструктирование пользователей о соблюдении	Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота Общие принципы функционирования вредоносного программного обеспечения Принципы функционирования средств антивирусной защиты	Устанавливать программное обеспечение в соответствии с технической документацией Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота

[5] Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 533н), A/03.5, уровень квалификации 5

		требований по защите информации при работе с программным обеспечением Проверка функционирования встроенных средств защиты информации программного обеспечения Обнаружение признаков наличия вредоносного программного обеспечения	Источники угроз информационной безопасности и меры по их предотвращению Общие принципы функционирования средств защиты информации программного обеспечения, в том числе средств криптографической защиты информации Порядок эксплуатации средств антивирусной защиты Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Организационные меры по защите информации	Работать с программным обеспечением с соблюдением действующих требований по защите информации Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации

1.4. Категория слушателей

Программа предназначена для лиц, замещающих государственные должности, для государственных гражданских служащих (федеральных или субъектов Российской Федерации), муниципальных служащих или лиц, замещающих муниципальные должности, сотрудников организаций, учреждений и предприятий различных форм собственности.

К освоению программы допускаются лица, имеющие или получающие среднее профессиональное образование или высшее образование.

1.5. Формы и технологии обучения

Форма обучения – очная; очная с применением дистанционных образовательных технологий и электронного обучения; заочная с применением электронного обучения.

1.6. Период обучения, срок освоения и режим занятий

Форма обучения – очная. 40 академических часов: 38 часов контактной работы, 2 часа итоговой аттестации.

Форма обучения – очная с применением дистанционных образовательных технологий и электронного обучения. Срок освоения - 40 академических часов: 24 часа контактной работы (ДОТ), 14 часов самостоятельной работы с применением электронного обучения (ЭО), 2 часа итоговой аттестации (ЭО)

Форма обучения – заочная с применением электронного обучения. Срок освоения - 40 академических часов: 38 часов самостоятельной работы с применением электронного обучения (ЭО), 2 часа итоговой аттестации (ЭО).

40 академических часа: 5 дней, 5 дней в неделю, до 8 академических часа в день.

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.

При освоении дополнительной профессиональной программы параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение о повышении квалификации выдаются одновременно с получением соответствующего документа об образовании и о квалификации.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1.Календарный учебный график

ОЧНАЯ ФОРМА

Таблица 2

Период обучения (5 дней)				
1 день	**2 день**	**3 день**	**4 день**	**5 день**
УЗ	УЗ	УЗ	УЗ	УЗ ИА

ОЧНАЯ ФОРМА С ПРИМЕНЕНИЕМ ДОТ и ЭО

Таблица 3

Период обучения (5 дней)				
1 день	**2 день**	**3 день**	**4 день**	**5 день**
УЗ ДОТ СР ЭО	УЗ ДОТ СР ЭО	УЗ ДОТ СР ЭО	УЗ ДОТ СР ЭО	УЗ ДОТ СР ЭО ИА ЭО

ЗАОЧНАЯ ФОРМА С ПРИМЕНЕНИЕМ ЭО

Таблица 4

Период обучения (5 дней)				
1 день	**2 день**	**3 день**	**4 день**	**5 день**
СР ЭО	СР ЭО	СР ЭО	СР ЭО	СР ЭО ИА ЭО

Условные обозначения:

УЗ – учебные занятия;

УЗ ДОТ – учебные занятия с применением дистанционных образовательных технологий;

СР ЭО – самостоятельная работа с применением электронного обучения.

ИА – итоговая аттестация;

ИА ЭО – итоговая аттестация с применением электронного обучения.

2.2.Учебный план

ОЧНАЯ ФОРМА

Таблица 5.

№п/п	Наименование (модуля/раздела/дисциплины/темы), практики (стажировки)	Общая трудоемкость, час.	Контактная работа, час.						Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий), час.						Самостоятельная работа (с применением электронного обучения (ЭО), час	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В форме практической подготовки	В том числе					Всего	В форме практической подготовки	В том числе								
					Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальное и групповое консультирование, межмодульное консультирование				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальное и групповое консультирование, межмодульное консультирование					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1.	Теоретико-методологическая база государственного регулирования в сфере информационной безопасности (ИБ)	**8**	**8**	-	2	6	-	-	-	-	-	-	-	-	-	-	-	-		ПСК-1 ПСК-2 ПСК-3
2.	Федеральное законодательство РФ в области защиты информации, стандарты информационной безопасности	**6**	**6**	-	2	4	-	-	-	-	-	-	-	-	-	-	-	-		ПСК-1 ПСК-2 ПСК-3
3.	ФСТЭК России. Руководящие документы	**8**	**8**	-	2	6	-	-	-	-	-	-	-	-	-	-	-	-		ПСК-3 ПСК-4 ПСК-5
4.	Компьютерная безопасность. Технологии защиты данных	**8**	**8**	-	2	6	-	-	-	-	-	-	-	-	-	-	-	-		ПСК-1 ПСК-2

																				ПСК-3 ПСК-4 ПСК-5
5.	Виды и классификация сетевых атак	**8**	**8**	-	2	6	-	-	-	-	-	-	-	-	-	-	-	-		ПСК-1 ПСК-2 ПСК-3 ПСК-4 ПСК-5
	Итого	**38**	**38**	**-**	**10**	**28**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**		
	Итоговая аттестация	**2**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2/ 3 (Т)**	
	ВСЕГО:	**40**	**38**	**-**	**10**	**28**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2**	

ОЧНАЯ ФОРМА С ПРИМЕНЕНИЕМ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ И ЭЛЕКТРОННОГО ОБУЧЕНИЯ

Таблица 6.

№п/п	Наименование (модуля/раздела/дисциплины/темы), практики (стажировки)	Общая трудоемкость, час.	Контактная работа, час.						Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий), час.						Самостоятельная работа (с применением электронного обучения (ЭО), час	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В форме практической подготовки	В том числе					Всего	В форме практической подготовки	В том числе								
					Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальное и групповое консультирование, межмодульное консультирование				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальное и групповое консультирование, межмодульное консультирование					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1.	Теоретико-методологическая база государственного регулирования в сфере информационной безопасности (ИБ)	**8**	-	-	-	-	-	-	-	**8**	-	2	2	-	-	4	-	-		ПСК-1 ПСК-2 ПСК-3
2.	Федеральное законодательство РФ в области защиты информации, стандарты информационной безопасности	**6**	-	-	-	-	-	-	-	**6**	-	2	2	-	-	2	-	-		ПСК-1 ПСК-2 ПСК-3
3.	ФСТЭК России. Руководящие документы	**8**	-	-	-	-	-	-	-	**8**	-	2	2	-	-	4	-	-		ПСК-3 ПСК-4 ПСК-5
4.	Компьютерная безопасность. Технологии защиты данных	**8**	-	-	-	-	-	-	-	**8**	-	2	4	-	-	2	-	-		ПСК-1 ПСК-2 ПСК-3

																				ПСК-4 ПСК-5
5.	Виды и классификация сетевых атак	**8**	-	-	-	-	-	-	-	**8**	-	2	4	-	-	2	-	-		ПСК-1 ПСК-2 ПСК-3 ПСК-4 ПСК-5
	Итого	**38**	-	-	-	-	-	-	-	**38**	-	**10**	**14**	-	-	**14**	-	-		
	Итоговая аттестация	**2**	-	-	-	-	-	-	-	**-**	-	**-**	**-**	-	-	**-**	-	-	**2/ 3 (Д/ЭО)**	
	ВСЕГО:	**40**	-	-	-	-	-	-	-	**38**	-	**10**	**14**	-	-	**14**	-	-	**2**	

ЗАОЧНАЯ ФОРМА С ПРИМЕНЕНИЕМ ЭО

Таблица 7.

№п/п	Наименование (модуля/раздела/дисциплины/темы), практики (стажировки)	Общая трудоемкость, час.	Контактная работа, час.						Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий), час.						Самостоятельная работа (с применением электронного обучения (ЭО), час	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В форме практической подготовки	В том числе					Всего	В форме практической подготовки	В том числе								
					Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальное и групповое консультирование, межмодульное консультирование				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальное и групповое консультирование, межмодульное консультирование					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1.	Теоретико-методологическая база государственного регулирования в сфере информационной безопасности (ИБ)	8	-	-	-	-	-	-	-	-	-	-	-	-	-	8	-	-		ПСК-1 ПСК-2 ПСК-3
2.	Федеральное законодательство РФ в области защиты информации, стандарты информационной безопасности	6	-	-	-	-	-	-	-	-	-	-	-	-	-	6	-	-		ПСК-1 ПСК-2 ПСК-3
3.	ФСТЭК России. Руководящие документы	8	-	-	-	-	-	-	-	-	-	-	-	-	-	8	-	-		ПСК-3 ПСК-4 ПСК-5
4.	Компьютерная безопасность. Технологии защиты данных	8	-	-	-	-	-	-	-	-	-	-	-	-	-	8	-	-		ПСК-1 ПСК-2 ПСК-3 ПСК-4 ПСК-5

5.	Виды и классификация сетевых атак	8	-	-	-	-	-	-	-	-	-	-	-	-	-	8	-	-		ПСК-1 ПСК-2 ПСК-3 ПСК-4 ПСК-5
	Итого	**38**	-	-	-	-	-	-	-	-	-	-	-	-	-	**38**	-	-		
	Итоговая аттестация	**2**	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	-	-	**2/ 3 (Д/ЭО)**	
	ВСЕГО:	**40**	-	-	-	-	-	-	-	-	-	-	-	-	-	**38**	-	-	**2**	

2.3. Содержание программы по темам

Таблица 8

Номер *темы* и её наименование	Содержание темы
Тема 1 Теоретико-методологическая база государственного регулирования в сфере информационной безопасности (ИБ)	Информация и формы ее существования. Содержание и структура понятия «обеспечение информационной безопасности». Система информационной безопасности. Объекты защиты в концепциях информационной безопасности. Категории и носители информации. Средства защиты информации. Государственное регулирование в сфере информационной безопасности: цели, задачи, методы.
Тема 2. Федеральное законодательство РФ в области защиты информации, стандарты информационной безопасности	Нормативная база в сфере цифровых технологий. Федеральное законодательство РФ в области защиты информации. Зарубежный опыт. Организационно-правовые основы технической защиты конфиденциальной информации и обеспечения безопасности персональных данных
Тема 3. ФСТЭК России. Руководящие документы	Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"). Приказ ФСТЭК России от 11.04.2025 N 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 N 82619). НПА и Методические документы ФСТЭК. "Методический документ "Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах" (утв. ФСТЭК России 12.04.2026)
Тема 4. Компьютерная безопасность. Технологии защиты данных	Рекомендации и основные мероприятия по организации и техническому обеспечению безопасности персональных данных. Специализированные системы защиты персональных данных. Выявление угроз и уязвимостей безопасности персональных данных. Основы построения комплексной системы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных
Тема 5. Виды и классификация сетевых атак	Сетевые атаки: виды и классификации. Технологии обнаружения атак и алгоритмы действий по их устранению. Методы защиты. Способы борьбы.

3. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1.Материально-техническое и программное обеспечение реализации программы

ЮРИУ – филиал РАНХиГС располагает необходимой материально-технической базой, обеспечивающей проведение программы повышения квалификации, предусмотренной учебным планом и соответствующей действующим санитарным и противопожарным правилам и нормам. Реализуемая программа повышения квалификации обеспечена всеми необходимыми материально-техническими ресурсами.

Для проведения лекций и практических занятий при освоении программы *в очной форме* без использования дистанционных технологий и/или электронного обучения требуются аудитории, оснащенные проекторами, оборудованные микрофонами, столами, стульями, маркерными/меловыми досками. Также программа создается на информационно-образовательном портале https://uriu.gosedu.ru, где размещаются учебное расписание программы, презентации экспертов (при необходимости).

Реализация программы по очной форме обучения с применением ЭО и ДОТ и заочной форме с применением ЭО.

Для очной формы с применением ЭО и ДОТ, заочной формы с применением ЭО обучение и итоговая аттестация проходят в формате онлайн на информационно-образовательном портале https://uriu.gosedu.ru.

Для реализации программы *по очной форме обучения с применением ЭО и ДОТ* необходимо следующее материально-техническое обеспечение:

автоматизированное рабочее место преподавателя (АРМ), оборудованная персональным компьютером или ноутбуком с доступом в интернет;

рабочее место слушателя, оборудованное персональным компьютером (ноутбуком/планшетом/ смартфоном) с доступом в интернет;

доступ к образовательному порталу https://uriu.gosedu.ru., позволяющий проводить обучение в дистанционном формате онлайн. Может быть использована одна из платформ для проведения вебинаров: МТС Линк.

При применении электронного обучения *по заочной форме с применением ЭО*, обучающийся самостоятельно изучает материал в порядке, определенном педагогическим работником в целях освоения обучающимися учебных предметов, курсов и дисциплин (модулей), предусмотренных образовательной программой.

Во время обучения слушатели имеют удаленный 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.

Лицензионное программное обеспечение:

1. ОС Windows 10 и стандартные инструменты комплекта операционной системы (калькулятор, paint и т.п.)
2. Microsoft Office
3. Яндекс браузер.

3.2.Учебно-методическое и информационное обеспечение программы

Примерный материал к темам для практических заданий для очного формата и для самостоятельной работы (заочного формата)

Тема. Теоретико-методологическая база государственного регулирования в сфере информационной безопасности (ИБ)

Вопросы для самопроверки:

1. Раскройте содержание понятия «информационная безопасность» в нормативноправовой базе РФ. Чем трактовка ИБ в Доктрине ИБ отличается от определений в отдельных отраслевых актах?
2. Перечислите ключевые интересы личности, общества и государства в информационной сфере согласно Доктрине информационной безопасности РФ. Приведите по одному примеру угрозы для каждого интереса.
3. Что понимается под «государственным регулированием в сфере ИБ»? Назовите 3–4 основных метода такого регулирования (правовое, техническое, организационное и т. п.) и кратко раскройте каждый.
4. В чём разница между понятиями «защита информации», «информационная безопасность» и «кибербезопасность» с точки зрения российского законодательства и доктринальных документов?
5. Назовите не менее пяти базовых нормативных документов, формирующих теоретикометодологическую основу ИБ в РФ, и укажите роль каждого из них (например, Конституция — основа прав и свобод; Доктрина ИБ — стратегические цели и угрозы и т. д.).
6. Сопоставьте уровни регулирования ИБ: международный, федеральный, ведомственный, уровень организации. Приведите по одному документу для каждого уровня и объясните, как они «стыкуются» между собой.
7. Как принципы правового регулирования в сфере информации и ИБ (законность, баланс интересов, приоритет защиты критических объектов и т. п.) реализуются в конкретных положениях ФЗ «Об информации, информационных технологиях и о защите информации» и ФЗ «О безопасности»?
8. Проанализируйте, как категории информации (общедоступная, ограниченного доступа, государственная тайна, персональные данные) определяют разные режимы защиты и разные инструменты государственного контроля.
9. Объясните, каким образом рискориентированный подход применяется в государственном регулировании ИБ (на примере категорирования объектов КИИ, оценки угроз, планирования мер защиты).
10. В чём состоит разграничение полномочий между основными регуляторами в сфере ИБ (ФСТЭК, ФСБ, Минцифры, Роскомнадзор)? Приведите по одной типичной задаче для каждого органа.

Задание 1. Матрица угроз и мер регулирования

Цель: связать типовые угрозы с инструментами государственного регулирования и полномочиями регуляторов.

Задание:

1. Выберите 5 типовых угроз ИБ (например, утечка персональных данных, атака на ГИС, компрометация учётных записей, DDoSатака, внедрение вредоносного ПО).
2. Заполните таблицу: угроза — возможные последствия — нормативные акты, регулирующие эту сферу — регуляторы, отвечающие за контроль — меры государственного регулирования (лицензирование, категорирование, сертификация, проверки, требования к СЗИ и т. п.).

3. Сделайте вывод: каких инструментов регулирования, на ваш взгляд, недостаточно для эффективного противодействия этим угрозам.

Тема. Федеральное законодательство РФ в области защиты информации, стандарты информационной безопасности

Вопросы для самопроверки:

1. Перечислите не менее пяти федеральных законов, которые формируют правовую основу защиты информации в РФ. Кратко укажите предмет регулирования каждого (1–2 предложения).
2. Раскройте содержание понятий «информация», «защита информации», «оператор персональных данных», «персональные данные» в терминах российского законодательства (со ссылкой на соответствующие акты).
3. Какие категории информации выделяются в российском праве (общедоступная, ограниченного доступа, государственная тайна, персональные данные и др.)? Как от категории зависит правовой режим защиты?
4. В чём разница между «конфиденциальностью», «целостностью» и «доступностью» информации с точки зрения целей защиты и как эти цели отражаются в нормативных документах?
5. Назовите основные полномочия регуляторов (ФСТЭК, ФСБ, Роскомнадзор) в части защиты информации и укажите по одному ключевому акту, который закрепляет эти полномочия.
6. Сопоставьте требования Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) "О персональных данных" и Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 26.06.2026) "Об информации, информационных технологиях и о защите информации" по таким аспектам, как обязанности оператора, допустимые меры защиты, основания для обработки. Где нормы пересекаются, а где различаются?
7. Как соотносятся обязательные требования (законы, приказы регуляторов) и добровольные стандарты (ГОСТ, ISO) в системе защиты информации? Приведите 2–3 примера, когда применение стандарта фактически становится обязательным (например, через отсылку в приказе).
8. Проанализируйте, как принцип «адекватности мер защиты» (соразмерности угрозам и ценности информации) реализуется в приказах ФСТЭК по защите персональных данных и ГИС. Приведите примеры конкретных мер, которые зависят от уровня защищённости/класса системы.
9. Объясните, в каких случаях для защиты информации требуется лицензирование деятельности, сертификация средств защиты, аттестация объекта информатизации. Укажите нормативные акты, устанавливающие эти требования.
10. Как регулируется трансграничная передача персональных данных по действующему законодательству? Какие действия обязан предпринять оператор и какие риски возникают при нарушении требований?

Задание 1. Карта нормативных требований для типовой ИСПДн

Цель: научиться определять применимые требования и выстраивать их иерархию. Задание:

1. Представьте, что вы отвечаете за защиту персональных данных в муниципальном учреждении (обработка данных сотрудников и заявителей, хранение в локальной сети, передача по электронной почте).
2. Составьте перечень обязательных нормативных актов и документов (федеральные законы, приказы ФСТЭК, методические документы), которые определяют требования к такой системе.

3. Для каждого документа укажите, какие именно требования из него применимы (например, категорирование, модель угроз, меры защиты, контроль).

4. Выделите, какие меры являются обязательными, а какие рекомендательными (на основе стандартов).

Тема. ФСТЭК России. Руководящие документы

Вопросы для самопроверки:

1. Как в руководящих и методических документах ФСТЭК реализуется принцип «адекватности мер защиты»? Приведите 3 примера, где набор мер зависит от уровня/класса системы либо от результатов оценки угроз.

2. Объясните, как соотносятся между собой модель угроз, техническое задание и проектная документация с точки зрения требований ФСТЭК. Какие документы ФСТЭК задают состав и содержание этих материалов?

3. В каких случаях требуется аттестация объекта информатизации и какие документы ФСТЭК регламентируют этот процесс? Перечислите основные этапы и результаты работ по аттестации.

4. Проанализируйте, как в документах ФСТЭК учитывается жизненный цикл информационной системы (создание, эксплуатация, вывод из эксплуатации). Приведите по 1–2 требованиям для каждого этапа.

Задание 3. Перевод требований в задачи для исполнителей

Цель: превратить нормативные формулировки в практические задачи. Задание:

1. Возьмите 5–7 мер защиты из Приказа ФСТЭК России от 11.04.2025 N 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 N 82619) или Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных") (например, «идентификация и аутентификация», «регистрация событий безопасности», «управление обновлениями»).

2. Переформулируйте каждую меру в виде конкретной задачи для ИТспециалиста или администратора ИБ (что сделать, к какому сроку, какой результат подтвердить, какими документами/отчётами).

3. Для каждой задачи укажите, как проверить выполнение (чеклист, отчёт SIEM, журнал изменений и т. п.).

Тема. Компьютерная безопасность. Технологии защиты данных.

Вопросы для самопроверки:

1. Раскройте содержание понятий «компьютерная безопасность», «защита данных», «конфиденциальность, целостность, доступность (триада CIA)». Как эти категории соотносятся с практическими мерами защиты?

2. Перечислите основные типы угроз компьютерной безопасности (вредоносное ПО, фишинг, DDoS, утечки по вине персонала и т. п.) и сопоставьте их с уровнями модели OSI либо с этапами кибератаки (KILL CHAIN).

3. Назовите 3–4 ключевых принципа проектирования безопасных систем (принцип минимальных привилегий, эшелонированная защита, отказоустойчивость и др.) и приведите по одному примеру реализации каждого принципа в корпоративной среде.

4. Что такое «вектор атаки» и «поверхность атаки»? Приведите 2–3 примера расширения поверхности атаки в современных организациях (облака, мобильные устройства, IoT) и способы её сокращения.

5. Объясните разницу между идентификацией, аутентификацией и авторизацией. Приведите примеры технологий для каждого этапа (пароли, токены, биометрия, RBAC, ABAC).

Задание 1. Карта технологий защиты для типовой инфраструктуры

Цель: научиться подбирать технологии под архитектуру и риски. Задание:

1. Представьте типовую инфраструктуру госоргана: рабочие места, серверы, вебпортал, ГИС, обмен данными через СМЭВ, удалённый доступ.

2. Составьте таблицу: компонент инфраструктуры — ключевые угрозы — целевые свойства ИБ (CIA) — набор технологий/мер защиты (например, антивирус, NGFW, шифрование дисков, MFA).

3. Для каждой меры укажите, на какой уровень защиты она работает (периметр, хост, приложение, данные) и какое требование регуляторов поддерживает (ФСТЭК, Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) "О персональных данных" и т. п.).

4. Сделайте вывод (5–7 предложений) о балансе между защитой и удобством пользователей.

Задание 2. Анализ сценария атаки и выбор мер

Цель: развить навыки моделирования угроз и выбора контрмер. Задание:

1. Сценарий: злоумышленник рассылает фишинговые письма с вредоносным вложением; один сотрудник открывает файл, запускается шифровальщик, который распространяется по сети.

2. Перечислите этапы атаки в терминах KILL CHAIN (разведка, доставка, исполнение, закрепление, действия по цели и т. д.).

3. Для каждого этапа предложите 1–2 меры защиты и 1 меру обнаружения/реагирования.

4. Оцените, какие из мер обязательны по требованиям ФСТЭК/ Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) "О персональных данных", а какие являются лучшими практиками (ISO 27001, NIST).

Задание 3. Проектирование политики паролей и MFA

Цель: освоить баланс между безопасностью и удобством. Задание:

1. Разработайте проект политики паролей для учреждения (длина, сложность, срок жизни, запрещённые шаблоны, хранение).

2. Предложите схему внедрения MFA для разных групп пользователей (обычные сотрудники, администраторы, удалённые пользователи).

3. Укажите, какие технологии можно использовать (OTP, PUSH, смарткарты, FIDO2) и как обеспечить отказоустойчивость (резервные коды, офлайндоступ).

4. Соотнесите требования с нормативными документами и методическими рекомендациями (в т. ч. ФСТЭК).

Тема. Виды и классификация сетевых атак

Вопросы для самопроверки:

1. Дайте определение сетевой атаки. Назовите три основные цели сетевых атак (нарушение доступности, целостности, конфиденциальности) и приведите по одному примеру атаки под каждую цель.
2. Чем отличаются пассивные атаки от активных? Приведите по 2 примера каждого типа и объясните, почему их относят к соответствующей категории.
3. Раскройте смысл терминов «поверхность атаки», «вектор атаки», «уязвимость». Покажите на примере DDoS или MITM, как эти понятия связаны между собой.
4. Объясните, что такое DoS и DDoS. В чём принципиальное отличие между ними, и почему DDoS сложнее нейтрализовать?
5. Что понимается под классификацией атак по уровням модели OSI? Назовите по одной характерной атаке для уровней L3, L4 и L7 и кратко опишите механизм каждой.
6. Сопоставьте IPспуфинг и ARPспуфинг: в чём разница по уровню модели OSI, целям и типичным последствиям? Какие меры защиты эффективны против каждого из них?
7. Проанализируйте, как SQLинъекция и XSS различаются по вектору, цели и месту исполнения кода. К каким уровням модели OSI их уместно относить и почему?
8. Объясните, как классификация атак по условию начала (по запросу, по событию, безусловные) помогает в проектировании систем обнаружения и предотвращения вторжений (IDS/IPS). Приведите по одному примеру для каждого типа.
9. Как соотносятся атаки «нулевого дня» и эксплуатация известных уязвимостей с точки зрения подготовки злоумышленника, времени обнаружения и мер защиты? Какие процессы в организации помогают снижать риски в обоих случаях?
10. Сравните SYNфлуд (L4) и HTTPфлуд (L7) как разновидности атак на отказ в обслуживании. Почему средства защиты для них должны различаться?

Задание 1. Классификация и сопоставление атак

Цель: научиться различать типы атак и соотносить их с механизмами и защитой. Задание:

1. Составьте таблицу из 10 атак (например, DDoS, MITM, SQLинъекция, XSS, ARPспуфинг, MACфлуд, DNSспуфинг, фишинг, брутфорс, replayатака).
2. Для каждой укажите: тип по характеру воздействия (пассивная/активная), уровень OSI, основную цель (доступность/целостность/конфиденциальность), возможный ущерб, 2–3 меры защиты (технические и организационные).
3. Сделайте вывод (5–7 предложений) о том, какие типы атак наиболее критичны для госучреждений и почему.

Задание 2. Разбор кейса по уровням OSI

Цель: развить навык локализации атак в сетевой архитектуре. Задание:

1. Дана ситуация: злоумышленник подменяет ответы DNSсервера, чтобы перенаправить пользователей на фишинговый сайт.
2. Определите уровень OSI, на котором реализуется атака, и объясните механизм.
3. Опишите, как эта атака затрагивает триаду CIA (конфиденциальность, целостность, доступность).
4. Предложите 3–4 технические меры защиты (например, DNSSEC, мониторинг аномалий, сегментация, журналирование) и 1–2 организационные (обучение пользователей, регламент проверки ссылок).
5. Укажите, какие нормативные документы (ФСТЭК, приказы, методические рекомендации) поддерживают внедрение этих мер.

Рекомендуемые литературные источники нормативно-правовые документы для обеспечения программы:

Нормативно-правовые документы:

1. Конституция Российской Федерации
2. Гражданский кодекс Российской Федерации.
3. Уголовный кодекс Российской Федерации.
4. Трудовой Кодекс Российской Федерации.
5. Федеральный закон от 12.06.2024 N 135-ФЗ «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации».
6. Федеральный закон от 08.08.2024 N 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных».
7. Федеральный закон от 03.10.2014 N 279-ФЗ "О ратификации Договора о Евразийском экономическом союзе".
8. Федеральный закон от 17.07.2009 N 172-ФЗ (ред. от 30.09.2024) «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов».
9. Федеральный закон от 06.10.2003 N 131-ФЗ (ред. от 20.03.2025) «Об общих принципах организации местного самоуправления в Российской Федерации».
10. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 01.04.2025) «Об оперативно-розыскной деятельности».
11. Федеральный закон от 26.07.2017 N 187-ФЗ (ред. от 07.04.2025) "О безопасности критической информационной инфраструктуры Российской Федерации".
12. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) «О персональных данных».
13. Федеральный закон от 01.04.2025 N 41-ФЗ (ред. от 31.07.2025) «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».
14. Федеральный закон от 03.12.2012 N 230-ФЗ (ред. от 28.12.2025) "О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам".
15. Федеральный закон от 26.05.2021 N 141-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях".
16. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 31.07.2025) «Об электронной подписи».
17. Федеральный закон от 27.05.2003 N 58-ФЗ (ред. от 29.09.2025) «О системе государственной службы Российской Федерации».
18. Федеральный закон от 25.12.2008 N 273-ФЗ (ред. от 28.12.2025) «О противодействии коррупции».
19. Федеральный закон от 02.03.2007 N 25-ФЗ (ред. от 28.12.2025) «О муниципальной службе в Российской Федерации».

20. Федеральный закон от 27.07.2010 N 210-ФЗ (ред. от 29.12.2025) «Об организации предоставления государственных и муниципальных услуг».

21. Федеральный закон от 27.07.2004 N 79-ФЗ (ред. от 08.03.2026) «О государственной гражданской службе Российской Федерации».

22. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 26.06.2026) «Об информации, информационных технологиях и о защите информации».

23. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 04.07.2026) (с изм. и доп., вступ. в силу с 07.07.2026).

24. Указ Президента РФ от 13.06.2024 N 500 «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

25. Указ Президента Российской Федерации от 18 мая 2009 г. № 559 (ред. от 31.12.2025) «О представлении гражданами, претендующими на замещение должностей федеральной государственной службы, и федеральными государственными служащими сведений о доходах, об имуществе и обязательствах имущественного характера».

26. Указ Президента Российской Федерации от 21 июля 2010 г. № 925 (ред. от 31.12.2025) «О мерах по реализации отдельных положений Федерального закона «О противодействии коррупции».

27. Постановление Правительства РФ от 08.09.2010 N 697 (ред. от 23.04.2026) «О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия»).

28. Указ Президента РФ 7 мая 2012 года № 601 «Об основных направлениях совершенствования системы государственного управления».

29. Указ Президента РФ от 07.05.2012 N 601 «Об основных направлениях совершенствования системы государственного управления».

30. Указ Президента РФ от 21 мая 2012 г. № 636 «О структуре федеральных органов исполнительной власти».

31. Указ Президента Российской Федерации от 08 июля 2013 г. № 613 (ред. от 31.12.2025) «Вопросы противодействия коррупции».

32. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

33. Указ Президента РФ от 12.08.2002 N 885 (ред. от 25.08.2021) «Об утверждении общих принципов служебного поведения государственных служащих».

34. Указ Президента РФ от 19.05.2008 N 815 (ред. от 25.01.2024) «О мерах по противодействию коррупции».

35. Указ Президента РФ от 01.07.2010 N 821 (ред. от 09.07.2025) «О комиссиях по соблюдению требований к служебному поведению федеральных государственных служащих и урегулированию конфликта интересов» (вместе с «Положением о комиссиях по соблюдению требований к служебному поведению федеральных государственных служащих и урегулированию конфликта интересов»).

36. Указ Президента РФ от 02.04.2013 N 309 (ред. от 31.12.2025) «О мерах по реализации отдельных положений Федерального закона «О противодействии коррупции» (вместе с «Положением о порядке направления запросов в Федеральную службу по финансовому мониторингу при осуществлении проверок в целях противодействия коррупции»).

37. Постановление Правительства РФ от 08.06.2011 N 451 (ред. от 16.04.2026) «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и

муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» (вместе с «Положением об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»).

38. Постановление Правительства РФ от 25.01.2013 N 33 (ред. от 03.04.2026) «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» (вместе с «Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг»).

39. Постановление Правительства РФ от 09.02.2012 N 111 (ред. от 20.11.2018) «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» (вместе с «Правилами использования усиленной квалифицированной электронной подписи органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой", "Требованиями к обеспечению совместимости средств электронной подписи при организации электронного взаимодействия органов исполнительной власти и органов местного самоуправления между собой»).

40. Постановление Правительства РФ от 25.08.2012 N 852 (ред. от 20.07.2021) «Об утверждении Правил использования усиленной квалифицированной электронной подписи при обращении за получением государственных и муниципальных услуг и о внесении изменения в Правила разработки и утверждения административных регламентов предоставления государственных услуг».

41. Постановление Правительства РФ от 25.06.2012 N 634 (ред. от 13.03.2023) «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг» (вместе с "Правилами определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг»).

42. Постановление Правительства РФ от 28.11.2011 N 976 (ред. от 25.09.2018) «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

43. Постановление Правительства РФ от 10.10.2020 N 1646 (ред. от 17.12.2025) «О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий, финансовое обеспечение которых осуществляется (планируется осуществлять) за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов» (вместе с «Положением о формировании и ведении реестра ИТ-расходов на создание, развитие, ввод в эксплуатацию, эксплуатацию и вывод из эксплуатации ИТ-активов, финансовое обеспечение которых осуществляется (планируется осуществлять) за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов", "Положением о ведомственных программах цифровой трансформации»).

44. Распоряжение Правительства РФ от 25.12.2013 № 2516-р (ред. от 13.10.2017) «Об утверждении Концепции развития механизмов предоставления государственных и муниципальных услуг в электронном виде».

45. Распоряжение Правительства РФ от 09.06.2014 № 991-р (ред. от 25.05.2017) «Об утверждении плана мероприятий («дорожной карты») по реализации Концепции

развития механизмов предоставления государственных и муниципальных услуг в электронном виде, утв. распоряжением Правительства РФ от 25.12.2013 № 2516-р».

46. Распоряжение Правительства РФ от 28.12.2016 № 2867-р «Об утверждении формы представления сведений о адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети "Интернет", на которых государственным гражданским служащим или муниципальным служащим, гражданином Российской Федерации, претендующим на замещение должности государственной гражданской службы Российской Федерации или муниципальной службы, размещались общедоступная информация, а также данные, позволяющие его идентифицировать».

47. Распоряжение Правительства РФ от 17.12.2009 № 1993-р (ред. от 28.12.2011) «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых в электронном виде».

48. Приказ Минкомсвязи России от 23.06.2015 N 210 (ред. от 22.02.2017) «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия» (Зарегистрировано в Минюсте России 25.08.2015 N 38668).

49. Приказ Минцифры России от 13.11.2020 N 584 (ред. от 02.11.2023) «Об утверждении Требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей» (Зарегистрировано в Минюсте России 02.12.2020 N 61213) (с изм. и доп., вступ. в силу с 01.09.2024).

50. Приказ Минцифры России от 08.11.2021 N 1138 «Об утверждении Порядка формирования и ведения реестров, выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации» (Зарегистрировано в Минюсте России 30.11.2021 N 66117).

51. Приказ ФСБ России от 27.12.2011 N 796 (ред. от 13.04.2022) «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» (Зарегистрировано в Минюсте России 09.02.2012 N 23191).

52. Приказ ФСБ России от 27.12.2011 N 795 (ред. от 02.02.2024) «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» (Зарегистрировано в Минюсте России 27.01.2012 N 23041).

53. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375).

54. Приказ ФСТЭК России от 11.04.2025 N 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 N 82619).

55. Письмо Минтруда России от 14.02.2017 N 18-3/10/П-866 «О Методических рекомендациях по заполнению формы представления сведений об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети "Интернет", на которых государственным гражданским служащим или муниципальным служащим, гражданином Российской Федерации, претендующим на замещение должности государственной гражданской службы Российской Федерации или муниципальной службы, размещались общедоступная информация, а также данные, позволяющие его идентифицировать».

56. Письмо Минцифры России от 12.05.2025 N П25-44929 «О применении отдельных положений Федерального закона от 28.02.2025 N 23-ФЗ».

57. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7).

58. «Типовой кодекс этики и служебного поведения государственных служащих Российской Федерации и муниципальных служащих» (одобрен решением президиума Совета при Президенте РФ по противодействию коррупции от 23 декабря 2010 г. (протокол N 21)).

Основная литература

1. Петренко В. И., Мандрица И. В. Защита персональных данных в информационных системах. Практикум: учебное пособие для СПО/ Петренко В. И., Мандрица И. В. – 4е изд., стер. – Санкт-петербург: Лань, 2026. – 108 с.

2. Максуров А.А. Обеспечение информационной безопасности в сети Интернет: монография / Издательство: НИЦ ИНФРА-М, 2025 – 226 с.

3. Антропцева, И. О. Цифровизация публичного финансового контроля: монография / И. О. Антропцева. - Москва: Статут, 2024. - 182 с. - ISBN 978-5-8354-2028-5. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2193109 (дата обращения: 27.11.2025). – Режим доступа: по подписке.

4. «Правовое регулирование информационных отношений в сфере обработки персональных данных», автор И. Г. Шаблинский, под редакцией М. А. Федотова. 2-е изд., перераб. и доп. — Москва: Издательство «Юрайт», 2024.

5. Повышение эффективности и развитие личностного роста государственных и муниципальных служащих/ А.В. Баранов, Н.В. Бережная, Е.М. Медякова, Н.А. Кислицкая, О.В. Котлярова, Э.В. Малиненко, С.А. Литвинова, З.С. Мартемьянова, А.И. Морозова, А.В. Тагаев. – Ростов-на-Дону: Южно-Российский институт управления - филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (ЮРИУФ РАНХиГС), 2021. – 296 с.

6. Цифровое и проектное управление / А.В. Баранов, Е.М. Медякова, Н.А. Кислицкая, А.Б. Бабанов, О.В. Котлярова, Т.Д. Кривошеева, С.А. Литвинова, Н.Д. Никоненко, А.В. Тагаев, В.Х. Тарацуян. – Ростов-на-Дону: Южно-Российский институт управления - филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (ЮРИУФ РАНХиГС), 2021. – 294 с.

7. Винокуров В.А. Должности Российского государства: понятие и классификация // Журнал российского права, 2020, N 7

8. Зобнин, А.В. Информационно-аналитическая работа в государственном и муниципальном управлении: учебное пособие / А.В. Зобнин. — 3-е изд., испр. — Москва: ИНФРА-М, 2021. — 145 с. - Текст: электронный. - URL: https://znanium.com/catalog/product/987242. – Режим доступа: по подписке.

9. Королев Г.Н. Мелкое взяточничество: теория и практика правоприменения // Российский судья, 2020, N 9

10. Мелёшина Д.А., Никоненко Н.Д. «Умный город» и цифровая трансформация в России: современное состояние и перспективы// информационное развитие России: состояние, тенденции и перспективы, 2020, С.199-203.

11. Мелюхин И. С. Информационно-аналитическая деятельность как она есть. – Режим доступа: URL: http://it-claim.ru/Library/Books/SC/articles

12. Семенов Е. Ю. Совершенствование правовых и организационных аспектов защиты персональных данных в Российской Федерации //Закон и право. – 2022. – №. 1. – С. 94-96.

13. Современные инструменты управления данными Климова Е.Н., Перова М.В., Гайсинский И.Е., Барашко Е.Н. // В книге: Инновационное развитие науки: возможности, проблемы, перспективы. Монография. – М.: Издательство «Перо», 2021.

14. Трихина Н. Н., Кузнецов М. И. Обеспечение безопасности личных данных граждан в цифровой среде //Социальные институты в правовом измерении: теория и практика. – 2022. – С. 189-193.

15. Фаронов А.Е. Основы информационной безопасности при работе на компьютере: учебное пособие / Фаронов А.Е.. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/89453.html.

16. КСБ-СОФТ. Защита персональных данных в 2026 году: требования, риски и новые подходы к построению системы [Электронный ресурс] // КСБ-СОФТ : блог. — 2026. — URL: https://ksb-soft.ru/blog/zashchita-pdn/zashchita-personalnykh-dannykh-v-2026-godu-trebovaniya-riski-i-novye-podkhody-k-postroeniyu-sistemy-/.

17. Пуляев А. Новый приказ ФСТЭК по персональным данным 2026: что изменится для бизнеса [Электронный ресурс] // ADVOLAW : аналитика. — 2026. — URL: https://advolaw.ru/analytics/post/novyj-prikaz-fstek-po-personalnym-dannym-2026.

Дополнительная литература

1. Автоматизация процессов документооборота и делопроизводства. [Электронный ресурс]. – Режим доступа: http://ecm.ict-online.ru.

2. Александр Мираков, директора проектов компании РБК СОФТ. ECM-Journal. Пять главных проблем внедрения СЭД [Электронный ресурс]. – Режим доступа: https://ecm-journal.ru/docs/Pjat-glavnykh-problem-vnedrenija-SEhD.aspx

3. Афанасьева М.П. Роль законодательного регулирования в механизме обеспечения конституционного права на равный доступ к отдельным видам публичной службы // Государственная власть и местное самоуправление, 2020, N 4

4. Канатьев К. Н. и др. Анализ угроз безопасности беспроводной сети и разработка оптимальных методов их предупреждения //Инновации и инвестиции. – 2022. – №. 3. – С. 116-123.

5. Кузнецов В.И., Трунцевский Ю.В., Ломакина Л.А. Увольнение государственных гражданских служащих в связи с утратой доверия: проблемы теории и практики // Журнал российского права, 2020, N 1

Интернет-источники:

1. Официальный сайт Президента Российской Федерации – www.kremlin.ru.

2. Официальный сайт Правительства Российской Федерации – www.government.ru.

3. Официальный сайт «Открытое Правительство» - www.open.gov.ru

4. Официальный сайт Правительства Ростовской области - www.donland.ru.

5. Центр аналитических систем. http://inalytics.ru/

6. Аналитический портал. Государство. Бизнес. ИТ – Режим доступа: URL: https://www.tadviser.ru/index.php/(Big_Data)

7. Российский рынок СЭД/ECM. [Электронный ресурс]. – Режим доступа:

https://www.tadviser.ru/index.php
8. Системы BI и Big Data в России. Обзор Tadviser.ru – Режим доступа: URL: https://www.tadviser.ru/index.php/BI
9. ООО «Аналитические технологии». – Режим доступа: URL: https://loginom.ru/?utm_source=basegroup_main_menu
10. OLAP-КУБ (динамическая управленческая отчетность). – Режим доступа: URL: https://bud-tech.ru/olap.html

Информационные базы:

1. Поисковая система нормативных правовых актов «Гарант» [Электронный ресурс]. Режим доступа: www.garant.ru
2. Поисковая система нормативных правовых актов «Консультант+» [Электронный ресурс]. Режим доступа: www.consultant.ru

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

К итоговому аттестационному испытанию допускается лицо, успешно завершившее в полном объеме освоение программы дополнительного профессионального образования.

По итогам обучения проводится итоговая аттестация в виде зачета в форме тестирования с применением тестового комплекса (тестовые задания, отражающие содержание каждой темы образовательной программы).

Итоговое аттестационное испытание проводится в соответствии с календарным учебным графиком, утвержденным в образовательной программе.

Компьютерное тестирование проводится с помощью инструментов, встроенных в системы дистанционного обучения, или с помощью отдельных инструментов. Процесс тестирования автоматизирован, осуществляется автоматическая обработка результатов тестирования и процедура оценивания.

Критерии оценки:

В результате освоения программы у слушателя сформированы следующие компетенции:

Шкала оценивания итогового зачета (в форме тестирования)

Максимальный балл – 100

Проходной балл – 50% правильных ответов

0-49%	не зачтено
50-100%	зачтено

Оценочные средства
по дополнительной профессиональной программе
повышения квалификации

Итоговое тестирование
по дополнительной профессиональной программе повышения квалификации

«Обеспечение безопасности персональных данных в информационных системах персональных данных»

Инструкция: *Выберите один верный ответ из ниже предложенных вариантов*

№	Содержание вопроса
1.	В чем состоит суть компрометации информации? 1) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации 2) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений 3) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений
	Правильный ответ: 3
2.	Под угрозой удаленного администрирования в компьютерной сети понимается: 1) несанкционированное управление удаленным компьютером 2) внедрение агрессивного программного кода в рамках активных объектов Web-страниц 3) перехват или подмена данных на путях транспортировки 4) вмешательство в личную жизнь 5) поставка неприемлемого содержания
	Правильный ответ: 1
3.	Наиболее эффективное средство для защиты от сетевых атак: 1) использование сетевых экранов или «firewall» 2) использование антивирусных программ 3) посещение только «надёжных» Интернет-узлов 4) использование только сертифицированных программ-браузеров при доступе к сети Интернет
	Правильный ответ: 1
4.	Утечка информации – это: 1) несанкционированный процесс переноса информации от источника к злоумышленнику 2) процесс раскрытия секретной информации 3) процесс уничтожения информации 4) непреднамеренная утрата носителя информации
	Правильный ответ: 1
5.	Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются: 1) пароли 2) анкеты 3) коды
	Правильный ответ: 1
6.	Троянская программа, троянец – это: 1) вредоносная программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы; активизация компьютерного вируса может вызывать уничтожение программ и данных 2) вредоносная программа, которая проникает на компьютер, используя сервисы компьютерных сетей; их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя 3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а

№	Содержание вопроса
	также действия по удалению, модификации, сбору и пересылке информации третьим лицам
	Правильный ответ: 2
7.	Межсетевой экран (брандмауэр) - это: 1) вредоносная программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы 2) вредоносная программа, которая проникает в компьютер, используя сервисы компьютерных сетей 3) программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров
	Правильный ответ: 3
8.	Средства охранной сигнализации предназначены для: 1) выявления фактов несанкционированного доступа злоумышленника к информации 2) выявления фактов физического проникновения злоумышленника в защищаемое помещение 3) выявление фактов использования злоумышленником полученной конфиденциальной информации
	Правильный ответ: 1
9.	Комплекс правовых норм, непосредственно направленных на обеспечение безопасности и безвредных условий труда называется: 1) безопасностью труда 2) нормами организации труда 3) охраной труда
	Правильный ответ: 3
10.	Что является правовой формой защиты информации? 1) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации 2) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации 3) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения
	Правильный ответ: 1
11.	Что является организационной формой защиты информации? 1) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации 2) регламентация деятельности по защите информации и взаимоотношений персонала, направленная на защиту информации 3) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения
	Правильный ответ: 2
12.	Что понимается под угрозой безопасности информации в компьютерной системе? 1) потенциально возможная уязвимость информации в компьютерной системе 2) потенциально возможное событие, которое может привести к уничтожению,

№	Содержание вопроса
	утрате целостности, конфиденциальности или доступности информации 3) подготовка взлома компьютерной системы
	Правильный ответ: 2
13.	Что такое аудит безопасности? 1) это инструмент политики безопасности, позволяющий контролировать процесс загрузки системных драйверов 2) это инструмент политики безопасности, позволяющий отслеживать действия пользователей и системные события и регистрировать их в журнале 3) это инструмент политики безопасности, позволяющий наблюдать динамические изменения технического состояния аппаратных компонентов компьютера (температура материнской платы, скорость вращения вентилятора на процессоре и т.д.)
	Правильный ответ: 2
14.	Для обеспечения эффективной защиты информации в базах данных необходимо наличие: 1) средств шифрования файлов и папок 2) встроенных в систему управления базой данных функций защиты 3) встроенных в операционную систему функций защиты
	Правильный ответ: 2
15.	Для организации службы защиты информации на предприятии: 1) достаточно руководствоваться только федеральными законами 2) достаточно руководствоваться федеральными законами и ведомственными нормативными актами 3) необходимо дополнительно разработать собственные руководящие документы
	Правильный ответ: 3
16.	Что понимается под угрозой безопасности информации в компьютерной системе? 1) потенциально возможная уязвимость информации в компьютерной системе 2) потенциально возможное событие, которое может привести к уничтожению, утрате целостности, конфиденциальности или доступности информации 3) подготовка взлома компьютерной системы
	Правильный ответ: 2
17.	Для защиты от случайных угроз компьютерной информации используют: 1) обучение пользователей правилам работы с компьютерной системой, разрешительную систему доступа в помещение 2) межсетевые экраны, идентификацию и аутентификацию пользователей 3) дублирование информации, создание отказоустойчивых компьютерных систем, блокировку ошибочных операций
	Правильный ответ: 3
18.	Какие из перечня угроз относятся к преднамеренным угрозам компьютерной информации? 1) шпионаж и диверсии, несанкционированный доступ к информации, вредоносные программы 2) ошибки при разработке компьютерной системы, ошибки в программном обеспечении, электромагнитные излучения и наводки 3) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала

№	Содержание вопроса
	Правильный ответ: 1
19.	Средства шифрования с асимметричными ключевыми системами применяют: 1) для создания резервных копий конфиденциальной информации 2) для шифрования конфиденциальной информации на компьютере 3) для обмена конфиденциальными сообщениями в компьютерных сетях
	Правильный ответ: 3
20.	Средства защиты объектов файловой системы основаны на: 1) определении прав пользователя на операции с файлами и каталогами 2) задании атрибутов файлов и каталогов, независящих от прав пользователей
	Правильный ответ: 1

5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ

В результате освоения программы у слушателя сформированы компетенции:

Таблица 9.

Компетенция (код, содержание)	Индикаторы
ПСК – 1. Проведение технического обслуживания систем защиты информации автоматизированных систем	Владеть знаниями типовых средств и методов защиты информации в локальных и глобальных вычислительных сетях; базовой конфигурации системы защиты информации автоматизированной системы; применения программных и программно-аппаратных средств защиты информации в автоматизированных системах Использовать знания типовые средств, методов и протоколов идентификации, аутентификации и авторизации; нормативных правовых актов в области защиты информации; Способен организовать меры по защите информации; Демонстрирует умения конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией; обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации; Способен производить монтаж и диагностику компьютерных сетей; В своей практике использует умения применять типовые криптографические средства защиты информации, в том числе средства электронной подписи. Владеет практическими навыками проверки работоспособности системы защиты информации автоматизированной системы; Способен проводить контроль соответствия конфигурации системы защиты информации

	автоматизированной системы ее эксплуатационной документации; контроль стабильности характеристик системы защиты информации автоматизированной системы.
ПСК – 2. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	Владеет знаниями нормативных правовых актов в области защиты информации; эксплуатационной и проектной документации на автоматизированную систему; Использует основные методические и руководящие документы федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации; Знает основные методы организации и проведения технического обслуживания технических средств информатизации; Способен организовать меры по защите информации; Демонстрирует умения оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации; Владеет навыками ведения документов учета, обработки, хранения и передачи информации ограниченного доступа; Способен информировать персонал об угрозах безопасности информации; информировать персонал о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации; Демонстрирует навыки ведения протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем; ведения протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем; ведения протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем; Способен подготовить сведения об отсутствии необходимости присвоения категорий значимости объекту критической информационной инфраструктуры, на котором используется автоматизированная система, и направление в письменном виде этих сведений в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме
ПСК – 3. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем	Владеет знаниями процедуры архивирования информации, обрабатываемой автоматизированной системой; назначения и принципов работы

	основных узлов современных технических средств информатизации; Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации; Организует техническое обслуживание и ремонт компонентов автоматизированной системы; Использует знания нормативных правовых актов в области защиты информации; Использует основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации; Обладает умениями использования программных средств для архивирования информации; использования программных и программно-аппаратных средств для уничтожения (стирания) информации и носителей информации; использования типовых криптографических средств защиты информации, в том числе электронную подпись; Применяет в своей работе навыки включения в организационно-распорядительные документы по защите информации процедур уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации; уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания); физическое уничтожение машинных носителей информации, обрабатываемой автоматизированной системой; архивирование информации, обрабатываемой автоматизированной системой
ПСК- 4. Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях	Владеет знаниями топологии и протоколов сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях Использует знания состава и основных характеристик оборудования, применяемого при построении компьютерных сетей; типовых методов и протоколов идентификации, аутентификации и авторизации в компьютерных сетях; Знает о типичных сетевых атаках и способах защиты от них; сущности и содержании понятия информационной безопасности, характеристики ее составляющих; основных источниках угроз информационной безопасности и меры по их предотвращению; о программно-аппаратных средствах и методах защиты информации; о порядке обеспечения безопасности информации при эксплуатации компьютерных сетей; Использует формы и методы инструктажа пользователей по порядку работы в компьютерных сетях; нормативные правовые акты в области защиты информации; основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по

	защите информации и обеспечению безопасности критической информационной инфраструктуры; Способен организовать меры по защите информации; Владеет навыками ввода в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях Использует в своей практике установку программно-аппаратных средств защиты информации в компьютерных сетях; установку средств межсетевого экранирования в соответствии с действующими требованиями по защите информации; Демонстрирует навыки настройки программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам; Способен устранять неисправностей программно-аппаратных средств защиты информации в компьютерных сетях согласно технической документации; Демонстрирует навыки инструктирования пользователей по порядку безопасной работы в компьютерных сетях; оформления эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях
ПСК-5. Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения	Знает порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота; Владеет знаниями общих принципов функционирования вредоносного программного обеспечения; принципов функционирования средств антивирусной защиты; источников угроз информационной безопасности и меры по их предотвращению; общих принципов функционирования средств защиты информации программного обеспечения, в том числе средств криптографической защиты информации Использует знания порядка эксплуатации средств антивирусной защиты, порядка обеспечения безопасности информации при эксплуатации программного обеспечения; Владеет и использует знания нормативных правовых актов в области защиты информации, методических документов уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры; Умеет устанавливать программное обеспечение в соответствии с технической документацией; Способен выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота; работать с программным обеспечением с соблюдением действующих требований по защите информации; Демонстрирует умения устанавливать обновления

	программного обеспечения, включая программное обеспечение средств защиты информации; Демонстрирует навыки установки программного обеспечения; Настраивает программное обеспечение с соблюдением требований по защите информации; Способен настраивать средства антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам Демонстрирует навыки инструктирования пользователей о соблюдении требований по защите информации при работе с программным обеспечением; Организует проверку функционирования встроенных средств защиты информации программного обеспечения, Способен обнаруживать признаки наличия вредоносного программного обеспечения.

Приложение 1.

АННОТАЦИЯ

Дополнительная профессиональная программа повышения квалификации

«Обеспечение безопасности персональных данных в информационных системах персональных данных»

Программа разработана на основании требований действующего законодательства Российской Федерации и нормативных документов, регламентирующих вопросы защиты персональных данных, с учетом развития информационных технологий.

1. **Направление подготовки:**

Приказ РАНХиГС «Об утверждении образовательного стандарта Академии по направлению подготовки 38.03.04 Государственное и муниципальное управление» от 15.04.2024 года №7397.

Приказ Минтруда России от 14.09.2022 N 533н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (Зарегистрировано в Минюсте России 14.10.2022 N 70515). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

Приказ Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543). Настоящий профстандарт действует с 01.03.2023 по 01.03.2029.

2. **Категория слушателей:** Программа предназначена для лиц, замещающих государственные должности, для государственных гражданских служащих (федеральных или субъектов Российской Федерации), муниципальных служащих или лиц, замещающих муниципальные должности, сотрудников организаций, учреждений и предприятий различных форм собственности. К освоению программы допускаются лица, имеющие или получающие среднее профессиональное образование или высшее образование.

3. **Форма обучения:** 40 академических часа; очная**,** очная с применением ДОТ и ЭО, заочная с применением ЭО.

4. **Период реализации программы:** 5 дней, 5 дней в неделю, до 8 академических часа в день.

5. **Период актуальности программы:** 26 февраля 2027 г.

6. **Язык, на котором реализуется программа:** русский

7. **Основные модули/разделы/дисциплины/темы программы:**

1. Теоретико-методологическая база государственного регулирования в сфере информационной безопасности (ИБ)
2. Федеральное законодательство РФ в области защиты информации, стандарты информационной безопасности
3. ФСТЭК России. Руководящие документы
4. Компьютерная безопасность. Технологии защиты данных
5. Виды и классификация сетевых атак

8. **Формы текущего контроля и промежуточной аттестации успеваемости слушателя:** не предусмотрено

9. **Основная литература:**

1. Петренко В. И., Мандрица И. В. Защита персональных данных в информационных системах. Практикум: учебное пособие для СПО/ Петренко В. И., Мандрица И. В. – 4е изд., стер. – Санкт-петербург: Лань, 2026. – 108 с.

2. Максуров А.А. Обеспечение информационной безопасности в сети Интернет: монография / Издательство: НИЦ ИНФРА-М, 2025 – 226 с.

3. Антропцева, И. О. Цифровизация публичного финансового контроля: монография / И. О. Антропцева. - Москва: Статут, 2024. - 182 с. - ISBN 978-5-8354-2028-5. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2193109 (дата обращения: 27.11.2025). – Режим доступа: по подписке.

4. «Правовое регулирование информационных отношений в сфере обработки персональных данных», автор И. Г. Шаблинский, под редакцией М. А. Федотова. 2-е изд., перераб. и доп. — Москва: Издательство «Юрайт», 2024.

Приложение 2.

Сведения о преподавательском составе и ведущих специалистах
(кадровая справка)

Ф.И.О. преподавателя/ведущего специалиста	**Квалификация по диплому о высшем или среднем профессиональном образовании**	**Дополнительн/ая/ые квалификаци/я/и**	**Ученая степень, ученое (почетное) звание**	**Стаж работы в области профессиональной деятельности**	**Наименование преподаваемой дисциплины/темы (модуля)/стажировки (при наличии)**
1	2	3	4	5	6
Никоненко Наталья Дмитриевна	Высшее. Бакалавриат, Южный федеральный университет: прикладная математика и информатика. Бакалавр прикладной математики и информатики Высшее. Магистратура, Южный федеральный университет: прикладная математика и информатика. Магистр прикладной математики и информатики Высшее. Аспирантура, Южный федеральный университет: кандидат физико-математических наук. Кандидат физико-математических наук	Повышение квалификации. Управление проектами на основе стандарта ANSI PMI® PMBOK® Guide v.6 & Agile Practice Guide, 08.02.2021 Сертификация. Защита персональных данных на предприятии: Что нужно знать ответственному за ПДн, CorpSoft24/Timepad, 23.06.2022 Сертификация. Как быстро и просто выполнить требований к защите персональных данных с помощью облачных сервисов, CorpSoft24, 10.11.2022	Кандидат физико-математических наук, доцент	15	ФСТЭК России. Руководящие документы Компьютерная безопасность. Технологии защиты данных. Виды и классификация сетевых атак

		Повышение квалификации. Внешнеэкономические стратегии предприятия, РАНХиГС, 08.05.2023 Повышение квалификации. Логистика международных перевозок, РАНХиГС, 08.05.2023 Повышение квалификации. Законодательное регулирование работы с Большими данными (Big Data), АНО ДПО «Образовательный центр ГАРАНТ», 16.06.2023 Профессиональная переподготовка. Внешнеэкономическая деятельность, ООО "Информационно-коммуникативные технологии плюс", 03.11.2023			
Шлеверда Иван Николаевич	ФГБОУ ВПО «Северо-Кавказская академия государственной службы», специальность: «Государственное и	Программа ПК РАНХиГС «Использование СДО в образовательном процессе с применением электронного	к.полит.н	11	Теоретико-методологическая база государственного регулирования в сфере

	муниципальное управление», квалификация: Менеджер	обучения и дистанционных образовательных технологий (ЭО и ДОТ)» (удостоверение 600000353206 от 27.03.2020 г., рег. номер 004377 УПК-РАНХиГС-27) г. Москва Программа ПК ФГАОУ ВО «Южный федеральный университет» «Профилактика распространения в образовательных организациях радикальной и иной деструктивной идеологии» (удостоверение 612409223180 от 28.12.2021 г., рег. номер473-02/537) г. Ростов-на-Дону Программа ПК РАНХиГС «Вопросы профилактики терроризма» (удостоверение 0000002999 от 27.05.2022 г., рег. номер 0056-			информационной безопасности (ИБ) Федеральное законодательство РФ в области защиты информации, стандарты информационной безопасности

		2022-У-ИПиНБ) г. Москва Программа ПК РАНХиГС «Социокультурная среда и психолого-педагогическое сопровождение обучающихся инвалидов в образовательных организациях профессионального образования» (удостоверение 0000001718 от 11.05.2022 г., рег. номер 0389-2022-У-Д001348) г. Москва Удостоверение АНО ДПО «Энергобезопасность» № 58/2022-ОТ-Р-11 от 06.06.2022 г. «Обучение по охране труда и проверка знаний требований охраны труда работников организации»			

		Программа ПК РАНХиГС «Актуальная политическая повестка» (удостоверение 600000620199 от 02.03.2022 г., рег. номер 000047-2022-У-ВШГУ) г. Москва Программа ПК РАНХиГС «Преподаватель в цифровой образовательной среде (электронная информационно-образовательная среда в ВУЗе)» (удостоверение 600000661206 от 16.12.2021 г., рег. номер 01493-2021-У-ЦКУ) г. Москва Программа ПК			

		РАНХиГС «Развитие компетенций в сфере регионального и муниципального управления по направлениям современные ИКТ в ГМУ и институциональные основы МСУ» (удостоверение 600000601553 от 26.05.2021 г., рег. номер 00150-2021-У-ИУРР) г. Москва			