Федеральное государственное бюджетное образовательное учреждение высшего образования

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

Институт «Высшая школа государственного управления»
Центр «Цифровая школа госуправления»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
04017FBC00BBB26C814C7A22DD0C330C2E
Владелец: Кондратенко Олег Игоревич
Действителен: с 10.04.2025 до 10.04.2026

«УТВЕРЖДАЮ»
Директор Института ВШГУ РАНХиГС
О.И. Кондратенко
«05» марта 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации

ИНОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(наименование программы)

Москва, 2026

Разработчик:

И.М. Лапшин,
директор программы центра «Цифровая школа госуправления»
Института ВШГУ РАНХиГС

Руководители программы:

Ф.Р. Гадзаов,
директор центра «Цифровая школа
госуправления» Института ВШГУ РАНХиГС,
кандидат экономических наук

И.М. Лапшин,
директор программы центра «Цифровая школа госуправления»
Института ВШГУ РАНХиГС

Дополнительная профессиональная программа повышения квалификации рассмотрена на заседании ученого совета Института ВШГУ, рекомендована к утверждению и реализации, протокол № 08 от «05» марта 2026 года.

СОДЕРЖАНИЕ

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

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель и задачи реализации программы

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность» разработана в рамках государственного задания федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» на 2026 год и на плановый период 2027 и 2028 годов и направлена на повышение профессионального уровня в рамках имеющейся квалификации в области информационной безопасности.

Цель реализации программы: повышение уровня сознательности и квалификации специалистов в области информационной безопасности с целью эффективной защиты информации и информационных технологий, а также минимизация рисков, связанных с недостаточной информационной безопасностью.

Задачи реализации программы:

– знать организационно-правовые основы технической защиты информации в Российской Федерации;

– знать основы организации технической защиты информации на предприятии, а также каналы утечки информации;

– изучить основные направления обеспечения защиты информации

1.2. Нормативные правовые акты

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

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Приказ Минобрнауки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».
3. Приказ Минобрнауки России от 19 октября 2020 г. № 1316 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».
4. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
5. Приказ Минобрнауки России от 12.09.2013 № 1061 (ред. от 13.12.2021) «Об утверждении перечней специальностей и направлений подготовки высшего образования».
6. Приказ РАНХиГС от 19.04.2019 № 02-461 «Об утверждении локальных нормативных актов РАНХиГС по дополнительному профессиональному образованию» (п.3 Порядок реализации дополнительных профессиональных программ в РАНХиГС).
7. Приказ РАНХиГС от 02.12.2025 № 02-02669/001 «Об утверждении порядка разработки и утверждения в Академии дополнительных профессиональных программ – программ повышения квалификации, программ профессиональной переподготовки».

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

9. Приказ Минтруда России от 14.09.2022 № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» (зарегистрировано в Минюсте России 14.10.2022 № 70543).

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

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

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

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

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

15. Нормативные документы, определяющие требования к выпускнику программы:

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

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

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

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

1.3. Планируемые результаты обучения

Таблица 1.3.1

Перечень компетенций, планируемых к освоению (результаты обучения)

Виды деятельности	**Общепрофессиональные/ профессиональные компетенции ОПК, ПК или трудовые функции (ПСК и СК)** ***(формируются и (или) совершенствуются)***	**Практический опыт**	**Знания**	**Умения**
1	2	3	4	5
ВД 1. Обеспечение информационной безопасности	ОПК-8.[2] Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Владеть навыками использования информационных технологий при решении прикладных задач анализа данных, навыками анализа решений, оценки ресурсов, необходимых для реализации решений	Знать: информационные технологии для решения прикладных задач анализа данных	Уметь: выполнять постановки прикладных задач анализа данных и решать их с помощью современных программных инструментальных средств.
ВД 2. Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	ПСК-1. [3] Управление защитой информации в автоматизированных системах	Владеть: составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; нормативные правовые акты в области защиты информации	Уметь: оценивать информационные риски в автоматизированных системах применять технические средства контроля эффективности мер защиты информации; определять подлежащие защите информационные ресурсы автоматизированных систем; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; применять технические средства контроля эффективности мер защиты информации

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

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

1.4. Категория слушателей

К освоению программы допускаются федеральные государственные гражданские служащие, замещающие должности государственной гражданской службы всех категорий и групп должностей.

Требования к поступающим: высшее образование (бакалавриат, специалитет, магистратура), среднее профессиональное образование по программам подготовки специалистов среднего звена.

1.5. Формы и технологии обучения

Форма обучения – очная (с применением дистанционных образовательных технологий (ДОТ)).

1.6. Период обучения, срок освоения и режим занятий

Период обучения составляет: 1 месяц 1 неделя 6 дней.

Общая трудоемкость программы составляет 72 академических часа контактной работы со слушателем с применением дистанционных образовательных технологий (ДОТ).

Режим занятий: до 4 академических часов в день.

Предельная максимальная численность лекционной/практической группы – 95 слушателей.

1.7. Документ о квалификации

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

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Календарный учебный график

Таблица 2.1.1

Календарный учебный график

Период обучения – 1 месяц 1 неделя 6 дней					
1 неделя	2 неделя	3 неделя	4 неделя	5 неделя	6 дней
УЗ ДОТ	УЗ ДОТ	УЗ ДОТ	УЗ ДОТ	УЗ ДОТ	УЗ ДОТ / ИА ДОТ

Календарные учебные графики заполнены с помощью условных обозначений:

УЗ ДОТ – учебные занятия с применением дистанционных образовательных технологий;

ИА ДОТ – итоговая аттестация с применением дистанционных образовательных технологий.

2.2. Учебный план

Таблица 2.2.1

Учебный план
по дополнительной профессиональной программе повышения квалификации
«Информационная безопасность»

№п/п	Наименование раздела, модуля, дисциплины, темы, практики, стажировки	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий), час.					Самостоятельная работа (в т.ч. электронное обучение (ЭО), час	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские/лаборатор ные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции/ в интерактивной форме	Практические (семинарские/лаборатор ные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
1.	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1.	**Введение. Базовые принципы и методы обеспечения информационной безопасности**	**2**							**2**	**2**								**ОПК-8 ПСК-1**
2.	**Организационно-правовые основы технической защиты информации в Российской Федерации**	**16**							**16**	**12**	**4**							**ОПК-8 ПСК-1**
2.1	Организационные и правовые основы применения технических средств защиты информации	8							8	6	2							ОПК-8 ПСК-1
2.2	Основные понятия, термины и объекты защиты, классификация видов защищаемой информации	8							8	6	2							ОПК-8 ПСК-1
3.	**Основы организации технической защиты**	**18**							**18**	**8**	**10**							**ОПК-8 ПСК-1**

	информации на предприятии. Каналы утечки информации																	
3.1	Построение системы управления информационной безопасностью (СУИБ) в организации: политика, процессы и роли	8							8	4	4							ОПК-8 ПСК-1
3.2	Анализ и оценка рисков. Моделирование и категорирование угроз и уязвимостей	10							10	4	6							ОПК-8 ПСК-1
4.	**Основные направления обеспечения защиты информации**	**30**							**30**	**12**	**18**							**ОПК-8 ПСК-1**
4.1	Обеспечение защиты информации при управлении доступом	8							8	4	4							ОПК-8 ПСК-1
4.2	Разработка технического задания (частного технического задания) на систему защиты информационной системы)	6							6	2	4							ОПК-8 ПСК-1
4.3	Обеспечение защиты вычислительных сетей. Контроль целостности и защищенности информационной инфраструктуры. Защита от вредоносного кода	6							6	2	4							ОПК-8 ПСК-1
4.4	Предотвращение утечек информации. Порядок осуществления контроля за соблюдением требований к размещению технических средств информационных систем государственными органами	6							6	2	4							ОПК-8 ПСК-1
4.5	Управление инцидентами информационной безопасности	4							4	2	2							ОПК-8 ПСК-1
5.	**Мониторинг информационной безопасности**	**4**							**4**	**2**	**2**							**ОПК-8 ПСК-1**

	Итого:	**70**							**70**	**36**	**34**							
	Итоговая аттестация (тестирование)	**2**															**З/2**	
	Всего:	**72**							**70**	**36**	**34**						**2**	

2.3 Содержание программы по темам

Таблица 2.3.1

Содержание программы по темам

Номер темы и ее наименование	Содержание темы
Введение. Базовые принципы и методы обеспечения информационной безопасности	
Тема 1.1. Введение. Базовые принципы и методы обеспечения информационной безопасности	Основные понятия информационной безопасности. Базовые принципы защиты информации
Организационно-правовые основы технической защиты информации в Российской Федерации	
Тема 2.1. Организационные и правовые основы применения технических средств защиты информации	Основополагающие правовые рамки применения технических средств защиты информации на территории Российской Федерации
Тема 2.2. Основные понятия, термины и объекты защиты, классификация видов защищаемой информации	Ключевые определения и понятия, лежащие в основе информационной безопасности, а также классификация видов информации и объекты, подлежащие защите
Основы организации технической защиты информации на предприятии. Каналы утечки информации	
Тема 3.1. Построение системы управления информационной безопасностью (СУИБ) в организации: политика, процессы и роли	Комплексный подход к построению системы управления информационной безопасностью (СУИБ) в организации, включающий разработку политики, формализацию процессов и распределение ролей
Тема 3.2. Анализ и оценка рисков. Моделирование угроз и категорирование уязвимостей	Понятие и значение анализа рисков в системе информационной безопасности, его роль в снижении вероятности и последствий инцидентов. Вычисление уровня риска как функции вероятности реализации угрозы и потенциального ущерба. Моделирование угроз и уязвимостей с помощью систематизации и категорирования для выявления критичных зон и активов
Основные направления обеспечения защиты информации	
Тема 4.1. Обеспечение защиты информации при управлении доступом	Основные принципы, методы и средства контроля и управления доступом к

Номер темы и ее наименование	Содержание темы
	информационным ресурсам и защищаемым объектам.
Тема 4.2. Разработка технического задания (частного технического задания) на систему защиты информационной системы)	Проектирования системы безопасности, включающий подробное описание задач и требований к защищаемой информационной системе
Тема 4.3. Обеспечение защиты вычислительных сетей. Контроль целостности и защищенности информационной инфраструктуры. Защита от вредоносного кода	Комплекс мер и технологий, направленных на защиту данных и ресурсов сети от несанкционированного доступа, атак и повреждений. Основные виды вредоносных программ, такие как вирусы, троянские программы, черви, шпионское и рекламное ПО, и их воздействие на информационные системы. Методы профилактики, включая использование антивирусного и антималварного программного обеспечения, регулярное обновление операционной системы и программ, а также меры по ограничению доступа к подозрительным веб-ресурсам и файлам
Тема 4.4. Предотвращение утечек информации. Порядок осуществления контроля за соблюдением требований к размещению технических средств информационных систем государственными органами	Порядок осуществления контроля за соблюдением требований к размещению технических средств информационных систем государственными органами" изучаются комплексные методы и технологии защиты информации от несанкционированного доступа и утечки как через технические, так и через организационные каналы
Тема 4.5. Управление инцидентами информационной безопасности	Стандарты и лучшие практики международного и российского уровня в области управления инцидентами
Мониторинг информационной безопасности	
Тема 5. Мониторинг информационной безопасности.	Системы мониторинга информационной безопасности (SIEM-системы): назначение, архитектура и основные функции. Сбор и анализ событий безопасности в режиме реального времени. Корреляция событий для выявления инцидентов и аномалий. Инструменты и платформы мониторинга: российские решения (MaxPatrol SIEM, R-

Номер темы и ее наименование	Содержание темы
	Vision SOAR) и их применение в государственных органах. Типы индикаторов компрометации (IoC) и их использование для обнаружения угроз. Построение дашбордов и отчетности по состоянию информационной безопасности. Мониторинг критических активов и информационных систем. Практическое занятие: работа с SIEM-системой, анализ логов, выявление аномалий.

3. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое и программное обеспечение реализации программы

РАНХиГС располагает необходимой материально-технической базой, обеспечивающей реализацию программы повышения квалификации, проведение итоговой аттестации, предусмотренной учебным планом.

Для проведения учебных занятий с применением ДОТ используется сервис «МТС Линк» https://mts-link.ru. Итоговая аттестация проводится в Системе дистанционного обучения центра подготовки руководителей и команд цифровой трансформации Института ВШГУ (СДО) https://new.portal.gosedu.ru.

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

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

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

3.2. Учебно-методическое и информационное обеспечение программы

Подготовка к практическому занятию по дисциплинам программы основывается на изучении учебных материалов, списка литературы и информационных ресурсов.

Федеральные законы Российской Федерации

1. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
2. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 03.07.2016 № 238-ФЗ «О независимой оценке квалификации».
7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Акты Президента Российской Федерации

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
10. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Акты Правительства Российской Федерации

11. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
12. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.
13. Положение о лицензировании деятельности по разработке и

производству средств защиты конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171.

14. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

Документы национальной системы стандартизации Российской Федерации в области защиты информации

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

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

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

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

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

20. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

35. СНиП 23-03-2003. Защита от шума.

Нормативные распорядительные документы ФСТЭК России

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

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

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

39. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.

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

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

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

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

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

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

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

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

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

49. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение

председателя Гостехкомиссии России от 30 марта 1992 г.

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

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

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

53. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

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

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

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

57. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31.

58. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования

к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

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

60. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

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

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

Основная и дополнительная литература:

1. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. – 4-е изд., перераб. и доп. – Москва: ДМК Пресс, 2025. – 456 с. – ISBN 978-5-93700-219-9.

2. Гродзенский, Я. С. Информационная безопасность: учебное пособие / Я. С. Гродзенский. – Москва: РГ-Пресс, 2025. – 144 с. – (Высшее образование). – ISBN 978-5-9988-1755-7.

3. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL https://urait.ru/viewer/informacionnaya-bezopasnost-i-zaschita-informacii-588741#page/1.

4. Нестеров, С. А. Основы информационной безопасности: учебное пособие для вузов / С. А. Нестеров. – 3-е изд., испр. и доп. – Москва: Академия, 2025. – 288 с. – (Высшее образование). – ISBN 978-5-7695-9876-3.

5. Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. – 5-е изд., стер. – Санкт-Петербург: Лань, 2025. – 336 с. – ISBN 978-5-8114-8945-2.

6. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 295 с. – (Высшее образование). – ISBN 978-5-534-18672-7.

7. Щербак, А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. – 3-е изд., перераб. – Москва: Юрайт, 2025. – 276 с. – (Высшее образование). – ISBN 978-5-9916-4587-1.

8. Волков, И. П. Применение неинъективных векторов в ранцевых криптосистемах / И. П. Волков, С. М. Петров // Безопасность информационных

технологий. – 2025. – № 1. – С. 15-28. – DOI: 10.26583/bit.2025.1.08.

9. Захарова, Е. А. Повышение точности выявления аномалий для систем обнаружения вторжения с помощью ансамблевого обучения / Е. А. Захарова, Д. В. Смирнов // Безопасность информационных технологий. – 2025. – № 1. – С. 45-62. – DOI: 10.26583/bit.2025.1.11.

10. Константинов, А. Б. Отечественная навигационно-связная экосистема для защиты критической информационной инфраструктуры / А. Б. Константинов // Безопасность информационных технологий. – 2025. – № 1. – С. 78-94. – DOI: 10.26583/bit.2025.1.10.

11. Михайлов, С. В. Методология построения и защиты API простыми словами / С. В. Михайлов // Information Security. Информационная безопасность. – 2025. – № 1. – С. 12-18.

12. Орлов, К. Н. Защита API от бот-атак и эксплуатации уязвимостей / К. Н. Орлов, Т. Л. Иванова // Information Security. Информационная безопасность. – 2025. – № 1. – С. 34-42.

13. Сидоров, В. Г. Нормы испытаний на стойкость к воздействию отдельных частиц: байесовский подход / В. Г. Сидоров // Безопасность информационных технологий. – 2025. – № 1. – С. 5-14. – DOI: 10.26583/bit.2025.1.01.

14. Федоров, А. И. Формирование безопасного цифрового пространства для несовершеннолетних / А. И. Федоров, М. П. Котова // Вопросы безопасности. – 2025. – № 2. – С. 15-28.

Справочные системы:

1. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.

2. Бюро научно-технической информации «Техника для спецслужб». – http://www.bnti.ru/about.asp.

3. Журнал «Безопасность информационных технологий». Сайт журнала –сайт журнала http://www.pvti.ru/articles 14.htm.

4. Журнал «Защита информации. Инсайд»; Сайт журнала – http://www.inside-zi.ru/

5. Журнал «Information Security / Информационная безопасность». Издатель: компания «Гротек». – http://www.itsec.ru

6. Научная электронная библиотека eLIBRARY.RU – http://elibrary.ru/.

7. Сайт Федеральной службы безопасности России (ФСБ России). - http://www.fsb.ru.

8. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.

9. ЭБС издательства Лань – http://e.lanbook.com/.

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Итоговая аттестация проводится в виде зачета. Оценивание производится по результатам тестирования. Итоговая аттестация является обязательной для слушателей, завершающих обучение по программе.

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

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

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

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

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

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

Итоговая аттестация слушателей осуществляется аттестационной комиссией, созданной образовательной организацией в соответствии с локальными нормативными актами организации из числа сотрудников РАНХиГС и других организаций.

Вопросы для подготовки к итоговому тестированию

Что включает понятие информационная безопасность?
а) Защита программного обеспечения
б) Защита информации и систем от несанкционированного доступа
в) Обслуживание компьютерной техники

Основные свойства информации для обеспечения ИБ:
а) Достоверность, хранение
б) Конфиденциальность, доступность, целостность
в) Скорость обработки

Что такое конфиденциальность?
а) Свободный доступ к информации
б) Ограничение доступа только для уполномоченных лиц
в) Хранение данных в облаке

Что из перечисленного не является угрозой ИБ?
а) Вирусы
б) Хакерские атаки
в) Плановое обновление ПО

Основной законодательный акт в области защиты информации:
а) Трудовой кодекс
б) Федеральный закон "Об информации, информационных технологиях и защите информации"
в) Налоговый кодекс

Что такое электронная подпись?
а) Просто скан обычной подписи
б) Средство подтверждения подлинности документа в электронном виде
в) Пароль для входа в почту

Какая мера не относится к технической защите информации?
а) Межсетевой экран
б) Антивирус
в) Обучение сотрудников

Что такое аудит информационной безопасности?
а) Разработка новых программ
б) Проверка соблюдения требований и выявление уязвимостей
в) Создание пользовательских инструкций

Кому следует доверять обработку персональных данных?
а) Всем сотрудникам
б) Сотрудникам с соответствующими правами и ответственностью
в) Посторонним лицам

Что означает управление доступом в ИБ?
а) Контроль доступа к зданиям
б) Определение, кому и какие ресурсы доступны в системе
в) Установка паролей

Какую угрозу представляет вредоносный код?
а) Улучшение работы системы
б) Повреждение или кражу информации
в) Оптимизация сети

Основной признак уязвимости:
а) Надежная защита
б) Слабое место в системе, доступное для атаки
в) Надежный сервер

Что необходимо делать при инциденте безопасности?
а) Игнорировать
б) Немедленно реагировать, анализировать и устранять последствия
в) Восстанавливать данные без анализа

Что относится к организационным мерам ИБ?
а) Разработка политики безопасности
б) Техническая настройка фаервола
в) Установка антивируса

Что такое политика безопасности информации?
а) Общие правила и требования организации по защите информации
б) Инструкция по использованию компьютера
в) Перечень лицензионного ПО

Основное назначение систем обнаружения вторжений (IDS):
а) Работа компьютера
б) Выявление попыток несанкционированного доступа
в) Создание резервных копий

Что из перечисленного является способом предотвращения утечки информации?
а) Разглашение паролей
б) Использование систем DLP
в) Совместное использование учетных записей

Что включает управление рисками в ИБ?
а) Игнорирование возможных угроз
б) Оценку и минимизацию вероятности и последствий угроз
в) Установка новой техники

Кто несет ответственность за информационную безопасность в организации?
а) Только системный администратор
б) Все сотрудники в соответствии с регламентами

в) Пользователи сети

Что означает термин “целостность информации”?
а) Запрет на копирование
б) Сохранение информации без изменений и повреждений
в) Совместное использование данных

Критерии оценки слушателя на итоговой аттестации

Оценка	Требования к знаниям
зачтено	Выставляется слушателю, если он правильно выполнил не менее 70% заданий
не зачтено	Выставляется слушателю, если он правильно выполнил менее 70% заданий

5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ

В результате освоения программы у слушателя сформированы компетенции:

Таблица 5.1

Характеристика результатов освоения программы

Компетенция (код, содержание)	Индикаторы
ОПК-8. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Знает организационно-правовые основы технической защиты информации в Российской Федерации и способен использовать информационные технологии при решении прикладных задач анализа данных, навыками анализа решений, оценки ресурсов, необходимых для реализации решений, обеспечивая информационную безопасность
ПСК-1. Управление защитой информации в автоматизированных системах	Способен обеспечить информационную безопасность в органах власти с целью эффективной защиты информации и информационных технологий, а также минимизация рисков, связанных с недостаточной информационной безопасностью