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

**СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ**

УТВЕРЖДЕНА
Решением УС СЗИУ РАНХиГС
от «17» февраля 2026 г. протокол № 5

# ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
**повышения квалификации**

# ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Санкт-Петербург, 2026

Разработчик - факультет дополнительного профессионального образования.

Руководитель структурного подразделения:
кандидат политических наук, декан ФДПО — Н.В. Горбатова
(ученая степень и (или) ученое звание, должность, структурное подразделение) (подпись) (И.О. Фамилия)

Программа повышения квалификации рассмотрена на заседании ученого совета СЗИУ и рекомендована к реализации, протокол № 1 от «27» января 2026 г.

# СОДЕРЖАНИЕ

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

## 1.1. Цель и задачи реализации программы

Дополнительная профессиональная программа повышения квалификации «Защита персональных данных в информационных системах» направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности. Программа рассчитана на специалистов, ответственных за обработку и защиту персональных данных; руководителей подразделений и предприятий, сотрудников административно-хозяйственных блоков; а также слушателей, желающих более детально понять требования регуляторов в области защиты персональных данных в информационных системах.

Задачи:

- изучить требования для обеспечения безопасности персональных данных в информационных системах;
- научиться использовать инструменты защиты для обеспечения безопасности данных в информационных системах.

## 1.2. Нормативная правовая база

Программа разработана на факультете дополнительного профессионального образования. на основании ряда законов и нормативных правовых актов в области дополнительного профессионального образования, в т.ч:

Федеральный закон от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации»;

Постановление Правительства РФ от 12.05.2012 N 473 (ред. от 30.07.2025) «Об утверждении устава федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»;

Постановление Правительства РФ от 07.03.2025 N 291 "Об утверждении Положения о реализации мероприятий по организации профессионального обучения и дополнительного профессионального образования отдельных категорий граждан";

Приказ Минпросвещения России от 26.08.2020 N 438 "Об утверждении Порядка организации и осуществления образовательной деятельности по основным программам профессионального обучения" (Зарегистрировано в Минюсте России 11.09.2020 N 59784);

Приказ Минобрнауки России от 17.11.2020 N 1427 "Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность" (Зарегистрировано в Минюсте России 18.02.2021 N 62548);

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);

Приказ Минобрнауки России от 24 марта 2025 года № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (Зарегистрировано в Минюсте России 22 апреля 2025 года, рег. № 81928);

Приказ РАНХиГС от 02 декабря 2025 года № 02-0 2669/001 «Об утверждении порядка разработки и утверждения в Академии дополнительных профессиональных программ – программ повышения квалификации, программ профессиональной переподготовки»

## 1.3. Планируемые результаты обучения

Планируемые результаты обучения включены в таблицу (таблица 1)

| Виды деятельности | Профессиональные компетенции' или трудовые функции ОПК и УК[1] | Знания | Умения | Практический опыт |
|---|---|---|---|---|
| ВД 1. Организационно-управленческая деятельность | ПСК – 1[1] – Управление защитой информации в автоматизированных системах | Основных методов управления защитой информации | Определять подлежащие защите информационные ресурсы автоматизированных систем | Составления комплекса правил, процедур, практических приемов, принципов, методов, средств обеспечения защиты информации в автоматизированной системе |
| | ПСК – 2[1] – Анализ уязвимостей внедряемой системы защиты информации | Основных методов и средств криптографической защиты информации | Классифицировать и оценивать угрозы безопасности информации автоматизированной системы | Проведения экспертизы состояния защищённости информации автоматизированных систем |

### 1.4. Категория слушателей

Программа профессионального обучения разработана в рамках федерального проекта "Активные меры содействия занятости" национального проекта "Кадры".

[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)

К освоению дополнительных профессиональных программ допускаются:

1) лица, имеющие среднее профессиональное и (или) высшее образование;

2) лица, получающие среднее профессиональное и (или) высшее образование.

### 1.5. Формы обучения и сроки освоения

Форма обучения: очная.

Срок освоения (в час.) - 72 акад.ч, в т.ч.:

контактная работа – 40 акад.ч.;

самостоятельная работа – 30 акад.ч.

итоговая аттестация – 2 акад. час.

### 1.6. Период обучения и режим занятий

Продолжительность обучения – 9 дней.

Режим занятий - 5 дней в неделю, не более 8 акад.ч. в день.

### 1.7. Документ о квалификации

Вид документа, выдаваемый при успешном освоении программы - удостоверение о повышении квалификации РАНХиГС.

## 2. Содержание программы

### 2.1. Календарный учебный график

Таблица 2. Календарный учебный график

| | **Период обучения - (9 дней)** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| УЗ | УЗ/СР | УЗ/СР | УЗ/СР | УЗ/СР | УЗ/СР | УЗ/СР | УЗ/СР | УЗ/СР/ИА |

УЗ – учебные занятия;

СР – самостоятельная работа;

ИА – итоговая аттестация

## 2.2. Учебный план

Таблица 3.1 Учебный план (очная форма)

| №п/п[1] | Наименование темы | Общая трудоемкость, час. | Контактная работа, час. | | | | | Самостоятельная работа, час [8] | Контактная работа (с применением дистанционных образовательных технологий), час.[6] | | | | | Самостоятельная работа (в т.ч. электронное обучение (ЭО), час[7] | Текущий контроль успеваемости [8] | Промежуточная аттестация (форма/час)[9] | Итоговая аттестация (вид /час.)[10] | Код компетенции[11] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Всего | В том числе | | | | | Всего[4] | В том числе | | | | | | | | |
| | | | | Лекции / в интерактивной форме | Практические (семинарские/лабораторные) занятия /в интерактивной форме[6] | Контактная самостоятельная работа, час[7] | Индивидуальные и групповые консультации | | | Лекции/ в интерактивной форме[5] | Практические (семинарские/лабораторные) занятия /в интерактивной форме[5] | Контактная самостоятельная работа. час7 | Индивидуальные и групповые консультации | | | | | |
| 1. | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 1. | Основы информационной безопасности | 16 | 4 | 4 | | – | – | 12 | | | | | | | | | | ПСК-1 |
| 2. | Техническая защита информации | 38 | 28 | 4 | 24 | – | – | 10 | | | | | | | | | | ПСК-1 |
| 3. | Защита информации с использованием шифровальных (криптографических) средств | 16 | 8 | 4 | 4 | – | – | 8 | | | | | | | | | | ПСК-2 |
| | Итого: | 70 | 40 | 12 | 28 | _ | _ | 30 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Итоговая аттестация | 2 | | | | _ | _ | | | | | | | | | | 2 | |
| | Всего: | 72 | 40 | 12 | 28 | _ | _ | 30 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 |

Таблица 3.2 Учебный план (очная, с применением ДОТ)

| №п/п[1] | Наименование темы | Общая трудоемкость, час. | Контактная работа, час. | | | | | Самостоятельная работа, час [8] | Контактная работа (с применением дистанционных образовательных технологий), час.[6] | | | | | Самостоятельная работа (в т.ч. электронное обучение (ЭО), час[7] | Текущий контроль успеваемости [8] | Промежуточная аттестация (форма/час)[9] | Итоговая аттестация (вид /час.)[10] | Код компетенции[11] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Всего | В том числе | | | | | Всего[4] | В том числе | | | | | | | | |
| | | | | Лекции / в интерактивной форме | Практические (семинарские/лабораторные) занятия /в интерактивной форме[6] | Контактная самостоятельная работа, час[7] | Индивидуальные и групповые консультации | | | Лекции/ в интерактивной форме[5] | Практические (семинарские/лабораторные) занятия /в интерактивной форме[5] | Контактная самостоятельная работа, час7 | Индивидуальные и групповые консультации | | | | | |
| 1. | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 1. | Основы информационной безопасности | 16 | _ | _ | _ | _ | _ | 12 | 4 | 4 | _ | _ | _ | _ | _ | _ | _ | ПСК-1 |
| 2. | Техническая защита информации | 38 | _ | _ | _ | _ | _ | 10 | 28 | 4 | 24 | _ | _ | _ | _ | _ | _ | ПСК-1 |
| 3. | Защита информации с использованием шифровальных (криптографических) средств | 16 | _ | _ | _ | _ | _ | 8 | 8 | 4 | 4 | _ | _ | _ | _ | _ | _ | ПСК-2 |
| | Итого: | 70 | _ | _ | _ | _ | _ | 30 | 40 | 12 | 28 | _ | _ | _ | _ | _ | 0 | 0 |
| | Итоговая аттестация | 2 | _ | _ | _ | _ | _ | | | | | _ | _ | _ | _ | _ | 2 | |
| | Всего: | 72 | _ | _ | _ | _ | _ | 30 | 40 | 12 | 28 | _ | _ | _ | _ | _ | 2 | 0 |

## 2.3. Содержание программ по темам

Приводится содержание программы. Содержание теоретического и практического материала раскрывается в логической последовательности изучения модулей/разделов/дисциплин/тем учебного плана. Содержание программы раскрывается с учетом современного развития образования и науки, техники, культуры, а также перспектив их развития (Таблица 4).

Таблица 4. Содержание программы

| **Номер *модуля/раздела /дисциплины/темы* и его наименование** | **Содержание *темы*** |
|---|---|
| Тема 1. Основы информационной безопасности | Правовое, нормативное и методическое регулирование деятельности в области защиты информации<br>Защита персональных данных |
| Тема 2. Техническая защита информации | Основы организации и ведения работ по обеспечению безопасности персональных данных<br>Угрозы уязвимости автоматизированных информационных систем<br>Технические каналы утечки информации<br>Оценка уровня защищённости информационных систем<br>Методы и средства технической защиты информации от несанкционированного доступа |
| Тема 3. Защита информации с использованием шифровальных (криптографических) средств | Криптографические методы защиты информации<br>Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств |

# 3. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

## 3.1. Материально-техническое и программное обеспечение реализации программы

Программа обеспечена оборудованными аудиториями, оснащёнными мультимедийным/видеопроекционным оборудованием, позволяющим работать с текстом, изображениями, воспроизводить демонстрационные материалы, в ходе проведения лекционных и практических занятий, текущего контроля успеваемости и итоговой аттестации.

Программа обеспечена условиями для функционирования электронной информационно-образовательной среды, включающей в себя лицензионные программные продукты Microsoft Office (Excel, Word, Outlook. Power Point и др). обеспечивающие освоение слушателями образовательной программы в полном объеме.

На лекционных занятиях рассматриваются ключевые и наиболее сложные вопросы дисциплины. Лекция сопровождается презентациями, что позволяет самостоятельно работать над повторением и закреплением материала.

Подготовка к практической работе предусматривает изучение теоретического материала. Перед выполнением практической работы необходимо внимательно ознакомиться с описанием практического задания, уяснить, в чем состоят её цель и заданные результаты. Выполнение каждой работы сопровождается оформлением в виде слайдов презентации.

Для активизации работы слушателей во время контактной работы с преподавателем часть занятий проводятся в интерактивной форме.

*Пример практического занятия*

Таблица 1.1. Определение необходимого уровня защищенности ИСПДн

| Тип актуальных угроз | Категория обрабатываемых данных | Персональные данные сотрудников оператора | | Персональные данные субъектов, не являющихся сотрудниками оператора | |
|---|---|---|---|---|---|
| | | < 100 000 | ≥ 100 000 | < 100 000 | ≥ 100 000 |
| 1 | ИСПДн-С | УЗ 1 | УЗ 1 | УЗ 1 | УЗ 1 |
| | ИСПДн-Б | УЗ 1 | УЗ 1 | УЗ 1 | УЗ 1 |
| | ИСПДн-И | УЗ 1 | УЗ 1 | УЗ 1 | УЗ 1 |
| | ИСПДн-О | УЗ 2 | УЗ 2 | УЗ 2 | УЗ 2 |
| 2 | ИСПДн-С | УЗ 2 | УЗ 2 | УЗ 2 | УЗ 1 |
| | ИСПДн-Б | УЗ 2 | УЗ 2 | УЗ 2 | УЗ 2 |
| | ИСПДн-И | УЗ 3 | УЗ 3 | УЗ 3 | УЗ 2 |
| | ИСПДн-О | УЗ 3 | УЗ 3 | УЗ 3 | УЗ 2 |
| 3 | ИСПДн-С | УЗ 3 | УЗ 3 | УЗ 3 | УЗ 2 |
| | ИСПДн-Б | УЗ 3 | УЗ 3 | УЗ 3 | УЗ 3 |
| | ИСПДн-И | УЗ 4 | УЗ 4 | УЗ 4 | УЗ 3 |
| | ИСПДн-О | УЗ 4 | УЗ 4 | УЗ 4 | УЗ 4 |

## 3.2. Учебно-методическое и информационное обеспечение программы

В образовательной деятельности предусмотрены следующие виды учебных занятий и учебных работ: лекции, практические занятия, включающие в т.ч. разбор кейсов, консультации, обеспечивающие высокое качество учебного процесса.

Темы занятий, даты и время проведения, а также преподаватели, задействованные в их проведении, указываются в программе (брошюра).

Обязательным условием проведения занятий выступает выделение 70% учебного времени на проведение практических занятий с использованием интерактивных образовательных технологий (практикумы и др.). Предусмотрена организация консультационной помощи слушателям.

**Рекомендуемые для использования при освоении дисциплины (модуля) и при итоговой аттестации нормативные правовые документы**

1.«Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020);
2.Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.11.2024) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2025);
3.Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 28.12.2024) "Об электронной подписи".

**Основная литература**

1.Белов А. С. Модернизация системы информационной безопасности Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2023. - № 4. - С. 76-80.
2.Васильев В. И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова // Вопросы кибербезопасности. - 2024. - № 2. - С. 27-38.
3.Мансуров Г. З. Право цифровой безопасности : учебник / Г. З. Мансуров. – Москва : Директ-Медиа, 2023. – 148 с

**Интернет-ресурсы**

1.Правительство России. [Электронный ресурс]. - Режим доступа http://government.ru/
2.Совет Безопасности Российской Федерации http://www.scrf.gov.ru/

## 4. Оценка качества освоения программы

Контроль знаний осуществляется по результатам освоения программы повышения квалификации.

Итоговая аттестация выпускников - экзамен в форме тестирования. Материалы итоговой аттестации формируют задействованные в программе лекторы. Результаты итоговой аттестации должны свидетельствовать о заявленных в программе умениях и навыках.

Общее число тестовых заданий – 15.

*Примерные вопросы итоговой аттестации:*

**1. Что такое информационная безопасность?**

А) Защита информации от несанкционированного доступа, использования, изменения или уничтожения

Б) Обеспечение конфиденциальности, целостности и доступности информации

В) Все вышеперечисленное

**2. Является ли адрес электронной почты - персональными данными?**

А) Да

Б) Нет

В) В сочетании с местом работы

Г) Если в наименовании адреса указано ФИО, например ad.ivanov@yandex.ru

**3. Какую роль играет физическая безопасность в обеспечении информационной безопасности?**

А) Физическая безопасность не имеет отношения к информационной безопасности

Б) Физическая защита информационных ресурсов, предотвращение физического доступа к данным

В) Ограничение доступа к помещениям, где хранятся носители информации

**4. Для чего используется хэширование?**

А) Для обеспечения целостности данных

Б) Для аутентификации пользователей

В) Для предотвращения атак типа “отказ в обслуживании”

**5. Что представляет собой стандарт ISO/IEC 27799?**

А) Стандарт по защите персональных данных о здоровье

Б) Новая версия BS 17799

В) Определения для новой серии ISO 27000

При проведении тестирования (зачета или экзамена в форме тестирования) результаты определяются в процентах правильно выполненных задач, которые переводятся в оценки по прилагаемой в таблице 6 шкале.

Таблица 6. Шкала перевода результатов тестирования в оценки

| **Оценка** | **Критерий (%)** |
|---|---|
| 2 – неудовлетворительно | от 0% до 65% |
| 3 – удовлетворительно | от 65% (включительно) до 75% |
| 4 – хорошо | от 75% (включительно) до 85% |
| 5 – отлично | от 85% (включительно) до 100% |

## 5.ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ (при необходимости)

В результате освоения программы у слушателя сформированы компетенции ПСК-1, ПСК-2. (Таблица 7).

Таблица 7. Характеристика результатов освоения программы

| Компетенция (код, содержание) | Индикаторы |
|---|---|
| ПСК – $1^1$ – Управление защитой информации в автоматизированных системах | - способен обеспечивать защиту информации в автоматизированных системах, используя основные приемы, методы, средства по защите информации |
| ПСК – $2^1$ – Анализ уязвимостей внедряемой системы защиты информации | - способен защитить информацию от несанкционированного доступа и утечки по техническим каналам и проводить экспертизу состояния защищённости информации автоматизированных систем |

По результатам оказания услуг слушателям, успешно освоившим программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.