Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Андрей Драгомирович Хлутков
Должность: директор
Дата подписания: 18.12.2025 12:05:04
Уникальный программный ключ:
880f7c07c583b07b775f6604a630281b13ca9fd2

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

УТВЕРЖДЕНА
ученым советом СЗИУ РАНХиГС
Протокол от «28» августа 2025 г. № 1

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

повышения квалификации

«Информационная безопасность. Защита персональных данных»

Санкт-Петербург, 2025

Разработчик:

Факультет дополнительного профессионального образования СЗИУ РАНХиГС

Руководитель структурного подразделения
Кандидат политических наук, декан ФДПО
(ученая степень и (или) ученое звание, должность, структурное подразделение)

(подпись)

Н.В. Горбатова
(И.О. Фамилия)

Дополнительная профессиональная программа рассмотрена и одобрена на заседании совета ФДПО «18» июня 2025г., протокол №2.

СОДЕРЖАНИЕ

1. Общая характеристика программы

1.1. Цель и задачи реализации программы

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность. Защита персональных данных» направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации лиц, замещающих муниципальные должности и должности муниципальной службы в органах местного самоуправления муниципальных образований Ленинградской области.

Задачи:

- Изучить требования для обеспечения безопасности данных;
- Научиться использовать инструменты для обеспечения безопасности данных.

1.2. Нормативная правовая база

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность. Защита персональных данных» разработана на факультете дополнительного профессионального образования. На основании ряда законов и нормативных правовых актов в области дополнительного профессионального образования, в т.ч:

1. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 28.02.2025) "Об образовании в Российской Федерации" (с изм. и доп., вступ. в силу с 01.03.2025);

2. Постановление Правительства РФ от 12.05.2012 N 473 (ред. от 04.03.2025) "Об утверждении устава федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации";

3. 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";

4. 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);

5. Приказ Минобрнауки России от 13.08.2020 N 1016 (последняя редакция) "Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 38.03.04 Государственное и муниципальное управление" (Зарегистрировано в Минюсте России 27.08.2020 N 59497);

6. 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);

7. Приказ Минпросвещения России от 14.07.2023 N 534 (ред. от 05.11.2024) "Об утверждении Перечня профессий рабочих, должностей служащих, по которым осуществляется профессиональное обучение" (Зарегистрировано в Минюсте России 14.08.2023 N 74776);

8. Проект перечня востребованных на рынке труда профессий, должностей, специальностей для организации в 2025 году профессионального обучения и дополнительного профессионального образования отдельных категорий граждан в рамках федерального проекта «Активные меры содействия занятости» национального проекта «Кадры»;

9. Приказ РАНХиГС от 19.04.2019 № 02-461 «Об утверждении локальных нормативных актов РАНХиГС по дополнительному профессиональному образованию»;

10. Приказ РАНХиГС от 13.08.2021 № 02-835 «Об утверждении положения о порядке разработки и утверждения в РАНХиГС дополнительных профессиональных программ – программ профессиональной переподготовки, программ повышения квалификации»;

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

[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)

	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".

Условиями участия отдельных категорий граждан в мероприятиях по обучению является отнесение их к одной из категорий, предусмотренных Постановлением 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".

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.) - 40 акад.ч, в т.ч.:

контактная работа – 38 акад.ч.;

итоговая аттестация – 2 акад. час.

1.6. Период обучения и режим занятий

Продолжительность обучения – 5 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 (5 дней)				
1 день	**2 день**	**3 день**	**4 день**	**5 день**
УЗ	УЗ	УЗ	УЗ	УЗ/ИА

УЗ – учебные занятия;

ИА – итоговая аттестация

2.2. Учебный план

Таблица 3. Учебный план

	Наименование дисциплины (модуля), практики, стажировки	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа, час	Текущий контроль успеваемости	Промежуточная аттестация	Итоговая аттестация (Вид,час)	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции в интерактивной форме	Лабораторные занятия (практикумы)/в интерактивной форме	Практические занятия/ в интерактивной форме	Контактная самостоятельная работа, час			Лекции / в интерактивной форме	Лабораторные занятия (практикумы)/в интерактивной форме	Практические (семинарские) занятия/ в интерактивной форме	Контактная, самостоятельная работа, час					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1.	Основы информационной безопасности	4	4	4														ПСК – 1
2.	Техническая защита информации	26	26	4		22												ПСК – 1
3.	Защита информации с использованием шифровальных (криптографических) средств	8	8	4		4												ПСК – 2
	Итого	38	38	12		26												
	Итоговая аттестация	2															Э(Т) 2	
	Всего	40	38	12		26											2	

2.3. Содержание программ по разделам и темам

Таблица 4. Содержание программы

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

3. Организационно-педагогическое обеспечение

3.1. Кадровое обеспечение

Таблица 4. Сведения о профессорско-преподавательском составе.

Ф.И.О. Преподавателя/ ведущего специалиста	Специальность, присвоения квалификация по диплому	Дополнительн /ая/ые квалификаци/я/и	Место работы, должность, основное/ дополнительное место работы	Ученая степень, ученое (почетное) звание	Стаж работы в области профессиональной деятельности/ по дополнительной квалификации	Стаж научно-педагогической работы		Наименование преподаваемой дисциплины/темы (модуля), практики/стажировок и (при наличии) по данной программе
						Всего	В том числе по преподаваемой дисциплине (модулю)	
1	2	3	4	5	6	7	8	9
Наумов Владимир Николаевич	ВВМУРЭ им. А.С. Попова, специальность «Автоматика, телемеханика и вычислительная техника», квалификация «Инженер электронной техники		Профессор кафедры бизнес-информатики СЗИУ	Доктор военных наук, профессор	47	38	7	Тема 1. Основы информационной безопасности
Шабалин Андрей Андреевич	ФГБОУ ВО «Санкт-Петербургский горный университет». Нефтегазовое дело. Квалификация бакалавр. Нефтегазовое дело. Квалификация магистр.		ООО "ЭнДжиАр Софтлаб". должность -- аналитик ИБ. Договор ГПХ.	-	5	5	5	Тема 1. Основы информационной безопасности Тема 2. Техническая защита информации Тема 3. Защита информации с использованием шифровальных (криптографических) средств

3.2. 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.

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

3.3. 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.

4. 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".

4.1 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

4.2 Интернет-ресурсы

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

5. Оценка качества освоения программы

Контроль знаний может осуществляться перед началом (по требованию заказчика), во время обучения и, в обязательном порядке, 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%

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.