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

«Электронные документы и электронные подписи»

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 «Электронные документы и электронные подписи» разработана для качественного изменения у слушателей имеющихся профессиональных навыков, необходимых для профессиональной деятельности в области использования средств электронной подписи в защищенном электронном документообороте, и направлена на получение компетенций, необходимых для соответствия требованиям Федерального закона от 06.04.2011 N 63-ФЗ (ред. от 21.04.2025) "Об электронной подписи".

Задачи:

- изучить требования для обеспечения безопасности данных;
- научиться использовать инструменты для обеспечения безопасности данных.

1.2. Нормативная правовая база

Дополнительная профессиональная программа повышения квалификации «Электронные документы и электронные подписи» 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 09.12.2016 N 1547 (ред. от 03.07.2024) "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование" (Зарегистрировано в Минюсте России 26.12.2016 N 44936);

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. Перечень 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»;

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

9. 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 (ПК) или трудовые функции (ПСК)	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[2] – 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]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), код трудовой функции B/03.6

[2] Там же, код трудовой функции B/09.6

	ПК-5[3] Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием	Архитектуру подсистемы безопасности значимого объекта	Проектировать подсистемы безопасности информационной системы в соответствии с техническим заданием	Разработать средства защиты информации с учётом категории значимости значимого объекта
	ПК-11.6[4] Защищать информацию в базе данных с использованием технологии защиты информации	Криптозащиту и основы шифрования	Шифровать и дешифровывать документы	Обеспечение защиты информации

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 – 32 акад.ч.;

самостоятельная работа – 6 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.

[3] Приказ Минобрнауки России от 09.12.2016 N 1547 (ред. от 03.07.2024) "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование" (Зарегистрировано в Минюсте России 26.12.2016 N 44936)

[4] Там же

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	СР/ИА

УЗ – учебные занятия;

СР – самостоятельная работа;

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.	Электронный документ	1	1	1														ПК-5.3
2.	Простая электронная подпись (ПЭП)	3	3	1		2												ПК-5.3 ПСК – 1
3.	Усиленная электронная подпись (УЭП)	4	4	2		2												ПСК – 1
4.	Криптозащита документов. Шифрование и расшифровка	12	8	2		6		4										ПСК – 1 ПСК – 2 ПК-11.6
5.	Неквалифицированная электронная подпись (НЭП)	4	4	1		3												ПСК – 1
6.	Квалифицированная электронная подпись (КЭП)	4	4	1		3												ПСК – 1
7.	Юридическая сила электронных документов.	2	2	2														ПСК-2
8.	Установка личного сертификата электронной подписи	8	6			6		2										ПСК – 2
	Итого	38	32	10		22		6										
	Итоговая аттестация	2															Э(Т) 2	
	Всего	40	32	10		22		6									2	

1. Содержание программ по разделам и темам

Таблица 4. Содержание программы

Номер темы и наименование.	Содержание темы
Электронный документ	Понятие документа? Подлинник и копия документа. Основные виды документов. Документы в электронном виде. Электронный образ документа. Электронный документ. Подлинник и оригинал документа
Простая электронная подпись (ПЭП)	Что такое электронная подпись? Виды электронных подписей. Простая электронная подпись (ПЭП). Ключ ПЭП. Что является и не является ПЭП? Электронные документы и простая электронная подпись в онлайн-системе электронного документооборота с физическими лицами.
Усиленная электронная подпись (УЭП)	Возможности УЭП. Неотрекаемость. Ключи шифрования. Сертификат электронной подписи. Подписание документа. Передача подписанного документа получателю. Проверка усиленной электронной подписи. Программы-криптопровайдеры для подписания документа и проверке электронной подписи. Проверка действительности электронной подписи на Едином портале государственных услуг (ЕПГУ). Состав реальной электронной подписи
Криптозащита документов. Шифрование и расшифровка	Постановка задачи. Главный вопрос криптозащиты документов. Шифрование документа. Передача зашифрованного документа получателю. Расшифровка документа. Достигнутый результат. Программы-криптопровайдеры для шифрования и расшифровки документов.
Неквалифицированная электронная подпись (НЭП)	Определение. Что требуется для создания НЭП? Область применения НЭП. Портал ФНС. Сервис «Госключ». Стандарт PGP. Практическое занятие по созданию сертификата НЭП, подписания документа и проверке подписи с использованием GPG.
Квалифицированная электронная подпись (КЭП)	Определение. Квалифицированный сертификат. Удостоверяющие центры. Отличия КЭП от НЭП. Формы КЭП. Отсоединенная электронная подпись. Присоединенная электронная подпись
Юридическая сила электронных документов.	Эквивалентность документов на бумажном носителе и электронных документов. Определение эквивалентности. Юридическая сила и признание электронных документов. Соглашение об электронном документообороте. Признание электронных документов, подписанных ПЭП. Признание электронных документов, подписанных НЭП. Признание электронных документов, подписанных КЭП. Практические аспекты применения электронной подписи Электронная подпись в информационных системах, онлайн-сервисах. Электронная подпись в системах электронного документооборота. Электронная подпись для электронных торговых площадок. Электронная подпись для документов-результатов предоставления государственных услуг на ЕПГУ. Применение электронной подписи в реальных жизненных ситуациях
Программа-криптопровайдер. Установка личного сертификата электронной подписи	Практическое занятие по работе со средствами электронной подписи. Программа-криптопровайдер. Установка личного сертификата электронной подписи. Подписание документа. Проверка электронной подписи. Шифрование и расшифровка документа.

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.

Примеры практического занятия

- определение необходимого уровня защищенности

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

- создание и установка личного сертификата электронной подписи.

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.

2. **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. Федерального закона от 06.04.2011 N 63-ФЗ (ред. от 21.04.2025) "Об электронной подписи";

3. Федеральный закон от 21.04.2025 №94-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи».

4.1 Основная литература

4. 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.

5. 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.

6. 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/
3. Пройти тест (для самостоятельной работы): URL: https://nalog-nalog.ru/tests/ecp-i-mchd-test-s-otvetami/

7. 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

6.В чём отличие симметричного и асимметричного шифрования?

А**)** Симметричное использует два ключа, асимметричное — один

Б) Симметричное использует один общий ключ, асимметричное — пару "открытый/закрытый"

В) Симметричное быстрее, но менее безопасно

Г) Асимметричное невозможно использовать для ЭП

7. Какой закон регулирует применение электронной подписи в РФ?

А) 152-ФЗ

Б) 187-ФЗ

В) 63-ФЗ

Г) 1119-ПП

8. Конфиденциальность информации – это:

А) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Б) Возможность получения информации и ее использования

В) Обязательство на рассказывать места хранения баз данных

Г) Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

9. Доступ к информации – это:

А) Проведение мероприятий по контролю за обладание информацией

Б) Возможность получения информации и ее использования

В) Наличие сведений о том, где находится информация и как ее можно получить

Г) Логин и пароль, использующийся при прохождении идентификации пользователя

10. Юридическая сила документа – это:

А) Наличие в тексте документа ссылок на нормативные правовые акты

Б) Общеобязательность для всех субъектов права

В) Свойство официального документа вызывать правовые последствия

Г) Надлежащее оформление и структурирование документа

11. Электронная подпись позволяет:

А) Реализовать совместную работу сотрудников с электронным документом, его регистрацию и доставку конечному получателю

Б) Идентифицировать владельца подписи и установить отсутствие изменений в электронном документе после его подписания

В) Исправить правописание в электронном документе и оформить его в соответствии с требованиями ГОСТ

12. Почему важно использовать уникальные пароли для каждого аккаунта?

А) Упрощает доступ к данным

Б) Увеличивает возможность забыть пароли

В) Уменьшает риск компрометации всех учетных записей при утечке одного пароля

13. Выберите признак, соответствующий квалифицированной подписи:

А) Требует только пароль

Б) Создаётся через OpenSSL

В) Не имеет юридической силы

Г) Выдаётся аккредитованным УЦ и создаётся с использованием сертифицированного СКЗИ

14. Что такое угроза информационной безопасности?

А) Реализованная атака

Б) Уязвимость системы

В) Ошибка пользователя

Г) Потенциальное событие, способное нанести ущерб

15. Для чего используется список отозванных сертификатов (CRL)?

А) Чтобы хранить корневые сертификаты

Б) Чтобы проверять срок действия ЭП

В) Чтобы определить недействительные сертификаты

Г) Чтобы ускорить проверку подписи

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 – Управление защитой информации в автоматизированных системах	- способен обеспечивать защиту информации в автоматизированных системах, используя основные приемы, методы, средства по защите информации
ПСК – 2 – 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
ПК-5 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием	- способен разработать средства защиты информации с учётом категории значимости значимого объекта
ПК-11.6 Защищать информацию в базе данных с использованием технологии защиты информации	- способен обеспечить защиту информации в базе данных

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