ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГАЗПРОМ»

ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «УЧЕБНЫЙ ЦЕНТР ПУБЛИЧНОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ГАЗПРОМ»

УТВЕРЖДАЮ
Директор
ЧОУ ДПО «Учебный центр
ПАО «Газпром»

А.П. Козаченко
«10» 01 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Средства криптографической защиты информации в инфокоммуникационных сетях»
(очное обучение)

СНО 08.10.01.010.56

СОГЛАСОВАНО
Начальник Управления
ПАО «Газпром»

О.И. Шаповалов
«29» 12 2023 г.

СОГЛАСОВАНО
Заместитель
начальника Департамента
ПАО «Газпром»

С.В. Будовый
«29» 12 2023 г.

Программа рассмотрена и одобрена на заседании педагогического совета ЧОУ ДПО «Учебный центр ПАО «Газпром». Протокол от 30 ноября 2023 г. № 3

Хволово – 2023 г.

РУКОВОДИТЕЛЬ И СОСТАВИТЕЛИ ПРОГРАММЫ

Дополнительная профессиональная программа повышения квалификации «Средства криптографической защиты информации в инфокоммуникационных сетях» (далее – Программа) разработана авторским коллективом ЧОУ ДПО «Учебный центр ПАО «Газпром» (далее – Учебный центр).

Вид деятельности	Должность	Ученая степень, ученое звание	Инициалы, фамилия
Руководитель	Заместитель директора по учебной работе	кандидат технических наук, доцент	А.В. Коновалов
Разработчики (составители) программы	Начальник Отдела 101	-	А.А. Петренко
	Главный специалист Отдела 101	-	М.М. Конышев
	Старший методист Отдела 414	кандидат технических наук	В.И. Булах

Распространение Программы осуществляется в соответствии с действующим законодательством и с соблюдением требований, установленных ПАО «Газпром».

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Программа разработана в соответствии с требованиями:

Указа Президента Российской Федерации от 06 марта 1997 г. № 188 «Перечень сведений конфиденциального характера»;

Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 05 декабря 2016 г. № 646;

Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (приказ ФАПСИ от 13 июня 2001 г. № 152);

Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (приказ ФСБ России от 9 февраля 2005 г. № 66);

Положений «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (СТР-К, приняты в ОАО «Газпром», его дочерних обществах и организациях к руководству и исполнению приказом ОАО «Газпром» от 03 июля 2003 г. № 66);

Инструкции по организации работы со средствами криптографической защиты информации в ОАО «Газпром» (приказ ОАО «Газпром» от 30 апреля 2009 г. № 122, в редакции приказа от 28 декабря 2011 г. № 398);

Методических рекомендаций по обеспечению информационной безопасности в ОАО «Газпром», его дочерних обществах и организациях (утверждено в ОАО «Газпром» от 11 апреля 2005 г. № 07-247).

Программа предназначена для подготовки работников дочерних обществ и организаций ПАО «Газпром» (далее ДОО ПАО «Газпром»), использующих в электронном документообороте криптографические средства защиты информации (далее слушатели).

Срок обучения: 24 академических часа.

Категория слушателей: работники ДОО ПАО «Газпром», осуществляющие электронный документооборот с использованием средств криптографической защиты информации и имеющие высшее или среднее специальное образование.

Программа реализуется в очной форме.

1.1. Цель и задачи реализации программы

Целью реализации Программы является повышение уровня теоретических знаний и практических навыков слушателей в области самостоятельной настройки и эксплуатации программных средств шифрования информации, используемых в ДОО ПАО «Газпром» при защищенном информационном обмене, а также изучение порядка и особенностей применения средств криптографической защиты информации в соответствии с действующими нормативными документами.

1.2. Планируемые результаты освоения программы

По завершению курса слушатели должны:

знать:

основные принципы работы защищенных телекоммуникационных систем и использования в них механизмов защиты информации;

нормативные документы и инструкции, регламентирующие работу со средствами криптографической защиты информации в ПАО «Газпром»;

назначение и разницу применения закрытого и открытого ключей;

основные виды электронной подписи, их особенности и место хранения сертификатов;

основные характеристики и функциональные возможности программных средств шифрования КриптоПро CSP, программного комплекса (далее – ПК) «Litoria Desktop» и им подобным;

уметь:

самостоятельно настраивать и эксплуатировать программные средства шифрования КриптоПро CSP, ПК «Litoria Desktop» и им подобные;

самостоятельно устанавливать и обновлять сертификаты корневого удостоверяющего центра и промежуточных удостоверяющих центров;

самостоятельно устанавливать и обновлять личный сертификат и сертификаты контрагентов.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

№ п/п	Наименование темы	Трудоемкость, час.	Аудиторные занятия				Аттестация *промежуточная / итоговая*
			Всего, час.	Из них			Форма аттестации (зачет и др.)
				Лекция	Семинар	Практические занятие	
1	**Вводная часть.** Постановка задач. Введение.	1	1	1			
2	**Тема 1.** Криптографические методы защиты информации	3	3	3			
3	**Тема 2.** Основы организации инфраструктуры открытых ключей	4	4	4			
4	**Тема 3**. Сертификаты открытых ключей и их правовое обеспечение	2	2	2			
5	**Тема 4.** Использование электронной подписи и шифрования данных стандартными средствами и с помощью ПК «Litoria Desktop»	10	10			10	
6	**Итоговая аттестация (зачет)**	4	4			2	2 Зачет (Т)
	ИТОГО:	**24**	**24**	**10**	**0**	**12**	**2**

Примечание:

«Т» – прием промежуточной или итоговой аттестации, осуществляемый по традиционной образовательной технологии.

2.2. Календарный учебный график

Период обучения (дни, недели)[1)]	Наименование темы (раздела, дисциплины, модуля)
1	**Вводная часть.** Постановка задач. Введение
1	**Тема 1.** Криптографические методы защиты информации
1	**Тема 2.** Основы организации инфраструктуры открытых ключей
2	**Тема 3.** Сертификаты открытых ключей и их правовое обеспечение
2, 3	**Тема 4.** Использование электронной подписи и шифрования данных стандартными средствами и с помощью ПК «Litoria Desktop»
3	**Итоговая аттестация (зачет)**

[1)]Даты обучения будут определены в расписании занятий при наборе группы на обучение

2.3. Рабочая программа

Тема 1. Криптографические методы защиты информации

История криптографической защиты информации.

Открытый и закрытый ключи.

Хеш-функция.

Электронная подпись (далее – ЭП) и её применение в системе защиты информации и системе электронного документооборота.

Тема 2. Основы организации инфраструктуры открытых ключей

Терминология инфраструктуры открытых ключей (далее – ИОК).

Сервисы ИОК.

Основные компоненты ИОК. Удостоверяющий центр (далее – УЦ). Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты.

Виды архитектур ИОК.

Физическая структура ИОК.

Тема 3. Сертификаты открытых ключей и их правовое обеспечение

Формат сертификата ключа проверки электронной подписи (открытого ключа).

Особенности сертификатов открытых ключей. Сертификаты конечных субъектов. Сертификаты удостоверяющих центров.

Способы проверки статуса сертификата.

Правовое обеспечение деятельности удостоверяющих центров. Нормативная база, регламентирующая деятельность удостоверяющих центров.

Тема 4. Использование ЭП и шифрования данных стандартными средствами и с помощью ПК «Litoria Desktop»

Тема 4.1. Получение и установка сертификатов корневого и промежуточного УЦ.

Проверка статуса сертификата.

Подключение к серверам по протоколу HTTPS.

Односторонняя (сервер) и двухсторонняя (клиент-сервер) аутентификация с использованием сертификатов.

Тема 4.2. Основы использования инфраструктуры открытых ключей на базе стандартных средств Windows или альтернативных операционных систем

Настройка почтового клиента (Outlook) на работу с сертификатами.

Подписание и отправка сообщений с ЭП.

Передача и прием зашифрованных сообщений.

Установка и настройка ПК «Litoria Desktop».

Тема 4.3. Формирование электронной подписи и шифрование данных сторонними программными средствами. Основы организации защищенного документооборота

Шифрование данных и формирование электронной подписи средствами ПК «Litoria Desktop».

Особенности использования ПК «Litoria Desktop» для шифрования данных и формирования электронной подписи.

Организация обмена конфиденциальной информацией с использованием электронной подписи, проверка подписи и её заверение.

3. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

3.1. Формы аттестации

3.1.1. Для проверки качества освоения учебного материала промежуточная аттестация не предусмотрена.

3.1.2. Итоговая аттестация проводится в форме зачета.

Зачет включает в себя проверку (в пределах Программы) теоретических знаний методом компьютерного тестирования слушателей и выполнение ими на автоматизированном рабочем месте (далее – АРМ) практического задания с использованием изученных программных средств.

Прием зачетов проводится комиссией, установленной решением Учебного центра на календарный год.

Слушателям, успешно прошедшим итоговую аттестацию, выдается документ о квалификации – удостоверение о повышении квалификации установленного образца.

Слушателям, не прошедшим итоговую аттестацию или показавшим неудовлетворительные результаты, а также слушателям, освоившим часть Программы, выдается справка об обучении или о периоде обучения по образцу, устанавливаемому Положением об образовательной деятельности Учебного центра.

3.2. Оценочные материалы, обеспечивающие реализацию программы

В компьютерном тесте предложено 14 вопросов, как правило, предлагается по четыре варианта ответа на каждый контрольный вопрос, при этом правильный ответ может быть один или несколько в зависимости от типа вопроса. Вместе с этим слушателю предлагается выполнить одно из практических заданий.

Оценки выставляются по следующим критериям:

Оценка	Количество правильных ответов/ выполнение практического задания	Количество неправильных ответов
«зачет»	7 – 14 (50% и более), практическое задание выполнено в полном объеме	0 - 6
«незачет»	0 - 6 (менее 50%) или практическое задание не выполнено (при любом количестве правильных ответов)	7 - 14

3.3. Методические рекомендации

3.3.1. Перечень вопросов для подготовки к теоретической части зачета

1. Объясните значение терминов «инфраструктура» и «инфраструктура открытых ключей».
2. Объясните сущность понятия «аутентификация», раскройте её место в инфраструктуре открытых ключей.
3. Что обозначает понятие «дайджест» (хэша) сообщения, раскройте его место в инфраструктуре открытых ключей.
4. Дайте понятие «электронная подпись», какие основные функции обеспечиваются с её помощью?
5. Объясните двойственность использования ключевой пары (открытого и закрытого ключа). С какой целью используются ключи отправителя и получателя?
6. Расскажите о предназначении сертификата ключа проверки ЭП, как гарантируется его подлинность?
7. Назовите основные компоненты инфраструктуры открытых ключей (ИОК), приведите примеры обеспечиваемых ими сервисов.
8. Какую структуру имеет Сеть удостоверяющих центров Группы Газпром. Чем, на Ваш взгляд, это обусловлено?
9. Приведите пример цепочки физических (реальных) объектов, использующих компоненты и сервисы ИОК.
10. Дайте краткое определение сертификата ключа проверки ЭП и объясните его предназначение.
11. Назовите виды электронной подписи и опишите их особенности.
12. Назовите способы проверки статуса сертификата открытого ключа. Какие из названных способов используются в рамках Сети удостоверяющих центров Группы Газпром?
13. Назовите основные особенности регламентов корневого и промежуточных удостоверяющих центров.
14. Порядок установки, активации (регистрации) и возможности меню «Настройки» программного комплекса «Litoria Desktop».

3.3.2. Перечень практических заданий для подготовки к зачету

1. С использованием оснастки «КриптоПРО CSP» пропишите личный сертификат и связанный с ним контейнер закрытого ключа.
2. Осуществите проверку регистрации личного ключа (с помощью локального хранилища) и прокомментируете результаты.
3. Сформируйте и отправьте от имени пользователя «N» (АРМ N) пользователю «00» подписанное сообщение электронной почты. В ответном сообщении от пользователя «00» (АРМ 00) осуществите проверку ЭП.
4. Сформируйте и отправьте от имени пользователя «N» (АРМ N) пользователю «00» зашифрованное и подписанное сообщение электронной

почты. В ответном сообщении от пользователя «00» (АРМ 00) осуществите расшифровку сообщения и проверку ЭП.

5. Используя ПК «Litoria Desktop» от имени пользователя «N» (АРМ N) для пользователя «00» создайте и подпишите файл. Отправьте его как вложение по электронной почте пользователю «00». В ответном сообщении от пользователя «00» (АРМ 00) осуществите проверку ЭП средствами ПК «Litoria Desktop».

6. Используя ПК «Litoria Desktop» от имени пользователя «N» (АРМ N) для пользователя «00» создайте и зашифруйте файл. Отправьте его как вложение по электронной почте пользователю «00». В ответном сообщении от пользователя «00» (АРМ 00) средствами ПК «Litoria Desktop» расшифруйте файл.

7. Используя ПК «Litoria Desktop» от имени пользователя «N» (АРМ N) для пользователя «00» создайте, подпишите и зашифруйте файл. Отправьте его как вложение по электронной почте пользователю «00». В ответном сообщении от пользователя «00» (АРМ 00) средствами ПК «Litoria Desktop» осуществите расшифровку сообщения и проверку ЭП.

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Количество слушателей в учебной группе не должно превышать число автоматизированных рабочих мест в специализированной аудитории.

4.1. Материально-технические условия

Наименование специализированных учебных помещений	Вид занятий	Наименование оборудования, программного обеспечения
Учебный класс (компьютерный класс)	Лекция, практическое занятие	Мультимедийное оборудование. Компьютер, подключенный к локальной сети. Интернет-браузер, Драйверы usb-ключа ЭП, WinRar, Adobe Reader, Microsoft Office, СКЗИ Крипто-Про CSP, ПК «Litoria Desktop 2», учебные USB-токены

4.2. Учебно-методическое и информационное обеспечение

В учебном процессе используются следующие нормативные документы:

1. Доктрина информационной безопасности Российской Федерации.
2. Федеральный Закон Российской Федерации от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (с последующими изменениями).
3. Федеральный Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с последующими изменениями).

4. Положение о Сети удостоверяющих центров Группы Газпром, утвержденное приказом ПАО «Газпром» от 24 ноября 2021 г. № 503.

5. Регламент Корпоративного удостоверяющего центра ОАО «Газпром», утвержденный приказом ОАО «Газпром» от 16 октября 2012 г. № 279.

6. Регламент удостоверяющего центра Администрации ОАО «Газпром», утвержденный приказом ОАО «Газпром» от 16 октября 2012 г. № 279.

7. Положение об электронном документе и использовании неквалифицированной электронной подписи в корпоративных информационных системах Группы Газпром, утвержденное приказом ПАО «Газпром» от 24 ноября 2021 г. № 503.

8. Инструкция по организации работы со средствами криптографической защиты информации в ОАО «Газпром», утвержденная приказом ОАО «Газпром» от 30 апреля 2009 г. № 122.

4.3. Кадровые условия

Кадровое обеспечение программы осуществляют работники Отдела 101 Учебного центра.

4.4. Условия для функционирования электронной информационно-образовательной среды

Слушателям в ходе очного обучения предоставляется доступ к электронной информационно-образовательной среде с рабочих мест по внутренней сети специализированного класса.