

**ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГАЗПРОМ»**

**ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«ОТРАСЛЕВОЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ УЧЕБНО-ТРЕНАЖЕРНЫЙ ЦЕНТР ГАЗПРОМА»**

---

УТВЕРЖДАЮ

Директор  
ЧУ ДПО «Газпром ОНУТЦ»

\_\_\_\_\_ А.С. Кандалов

« \_\_\_\_\_ » \_\_\_\_\_ 2022 г.

<b>ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ</b>	
Сертификат:	01580078002BAF7CAB43E5E6E025AA45E9
Владелец:	КАНДАЛОВ АЛЕКСЕЙ СЕРГЕЕВИЧ, ЧУ ДПО ГАЗПРОМ ОНУТЦ, ДИРЕКТОР
Действителен: с 11.10.2022 по 11.01.2024	

Направление: ОБЩЕОТРАСЛЕВОЕ

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА  
повышения квалификации специалистов  
по курсу «Информационная безопасность при реализации обучения  
с использованием дистанционных образовательных технологий»**

Образовательная организация: ЧУ ДПО «Газпром ОНУТЦ»

Код документа: СНО 05.04.01.037.01

Код курса: 03 1015 261 Э

**Калининград 2022**

## АННОТАЦИЯ

---

Настоящая дополнительная профессиональная программа предназначена для повышения квалификации специалистов по курсу «Информационная безопасность при реализации обучения с использованием дистанционных образовательных технологий». Данная программа предназначена для повышения квалификации штатных и внештатных преподавателей и мастеров производственного обучения образовательных подразделений дочерних обществ ПАО «Газпром» и образовательных организаций ПАО «Газпром».

В программе теоретического обучения рассматриваются основные положения информационной безопасности и защиты информации, основные законодательные акты, касающиеся вопросов информационной безопасности. Вводится понятие информации с точки зрения предмета защиты информации, определяются основные категории, которым должна удовлетворять информация. Вводится понятие атаки на информацию, рассматриваются основные виды атак, их последствия и способы их предотвращения.

### Сведения о документе:

1 РАЗРАБОТАН	ЧУ ДПО «Газпром ОНУТЦ»
2 ВНЕСЕН	ЧУ ДПО «Газпром ОНУТЦ»
3 УТВЕРЖДЕН	Директором ЧУ ДПО «Газпром ОНУТЦ» А.С. Кандаловым 04.02.2022
4 СОГЛАСОВАН	
5 СРОК ДЕЙСТВИЯ	5 лет
6 ВВЕДЕН ВПЕРВЫЕ	

© ПАО «Газпром», 2022

© Разработка и оформление  
ЧУ ДПО «Газпром ОНУТЦ», 2022

Распространение настоящего документа осуществляется в соответствии с действующим законодательством и с соблюдением правил, установленных ПАО «Газпром».

**Список исполнителей:**

Разработчик:

Специалист 1-й категории

учебного отдела ЧУ ДПО «Газпром ОНУТЦ»

Ю.В. Долженкова

Ответственный за методическое обеспечение разработки и составления настоящей учебно-программной документации:

Специалист 1-й категории

учебного отдела ЧУ ДПО «Газпром ОНУТЦ»

Ю.В. Долженкова

Нормоконтролер:

Инженер 1-й категории группы нормоконтроля

производственно-технического отдела

ЧУ ДПО «Газпром ОНУТЦ»

Е.И. Горбачева

Рецензент:

Ведущий инженер лаборатории геоэкологии АО

ИО РАН

А.В. Мышерин

## СОДЕРЖАНИЕ

1 Общие положения .....	6
1.1 Область применения.....	6
1.2 Цель реализации дополнительной профессиональной программы.....	6
1.3 Нормативно-правовые основания разработки.....	6
1.4 Требования к слушателям .....	7
1.5 Срок освоения программы повышения квалификации, форма обучения ...	7
1.6 Форма аттестации, форма документа, выдаваемого по результатам обучения.....	7
2 Термины и определения .....	8
3 Обозначения и сокращения.....	10
4 Характеристика профессиональной деятельности в области повышаемой квалификации .....	11
5 Планируемые результаты обучения .....	12
5.1 Планируемые результаты освоения программы повышения квалификации .....	12
6 Организационно-педагогические условия реализации программы повышения квалификации.....	14
6.1 Требования к квалификации педагогических работников, обеспечивающих реализацию образовательного процесса в рамках программы повышения квалификации по курсу.....	14
6.2 Материально-технические условия реализации программы повышения квалификации по курсу .....	14
6.3 Требования к информационным и учебно-методическим условиям .....	15
7 Учебный план .....	16
8 Календарный учебный график.....	19
9 Структура и содержание программы повышения квалификации по курсу.....	20
9.1 Учебно-тематический план.....	20
9.2 Содержание программы повышения квалификации по курсу.....	25
10 Оценочные материалы для контроля освоения программы повышения квалификации по курсу .....	28
10.1 Общая характеристика контроля и оценивания качества освоения программы повышения квалификации по курсу.....	28
10.2 Комплект контрольно-оценочных средств .....	29

11 Методические материалы.....	45
11.1 Методические рекомендации по организации и проведению учебного процесса .....	45
11.2 Учебно-методическое обеспечение .....	45

## **1 ОБЩИЕ ПОЛОЖЕНИЯ**

### **1.1 Область применения**

Настоящая дополнительная профессиональная программа предназначена для повышения квалификации специалистов по курсу «Информационная безопасность при реализации обучения с использованием дистанционных образовательных технологий» в целях формирования и развития компетенций, необходимых для профессиональной деятельности в области курса.

### **1.2 Цель реализации дополнительной профессиональной программы**

Программа повышения квалификации имеет своей целью совершенствование и получение новых компетенций, необходимых для выполнения вида профессиональной деятельности: организация обучения.

### **1.3 Нормативно-правовые основания разработки**

Нормативно-правовую основу разработки настоящей программы повышения квалификации составляют следующие нормативные документы:

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с последующими изменениями и дополнениями)

Приказ Министерства образования и науки Российской Федерации от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (с последующими изменениями и дополнениями)

Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», утвержденное Приказом ПАО «Газпром» от 29.01.2016 № 42 (с изменениями, утвержденными Приказом ПАО «Газпром» от 14.12.2016 № 810)

Требования к разработке и оформлению учебно-методических материалов для профессионального обучения и дополнительного профессионального образования персонала дочерних обществ и организаций ПАО «Газпром», утвержденные Департаментом 715 ПАО «Газпром» (Е.Б. Касьян) от 05.08.2019 № 07/15-3005

В случае изменения нормативно-правовой базы, служащей основанием для разработки настоящей дополнительной профессиональной программы, актуализация программы производится в рабочем порядке и повторного согласования и утверждения не требует.

#### **1.4 Требования к слушателям**

Категория слушателей – штатные и внештатные преподаватели; мастера производственного обучения образовательных подразделений дочерних обществ ПАО «Газпром» и образовательных организаций ПАО «Газпром».

Уровень образования слушателей для допуска к обучению – не ниже среднего профессионального образования.

#### **1.5 Срок освоения программы повышения квалификации, форма обучения**

Продолжительность обучения – 40 часов.

Форма обучения – заочная (без отрыва от работы).

#### **1.6 Форма аттестации, форма документа, выдаваемого по результатам обучения**

Формы промежуточного контроля по разделам указаны в учебном плане программы повышения квалификации.

Итоговая аттестация проводится в форме зачета, позволяющего оценить уровень подготовки слушателей и готовность к решению профессиональных задач.

Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Слушателям, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы и/или отчисленным из ЧУ ДПО «Газпром ОНУТЦ», выдается справка об обучении или о периоде обучения.

## 2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В программе повышения квалификации применяются следующие термины и их определения:

**1 безопасность информации:** Состояние информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования и блокирования.

**2 вебинар** (от англ. webinar): Разновидность онлайн-встречи (веб-конференция, онлайн-семинар) или обучающего занятия, при котором связь между участниками поддерживается через Интернет, а также участники видят ведущего, а он их нет.

**3 вирус (компьютерный, программный):** Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

**4 вредоносная программа:** Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**5 информационная система:** Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**6 оператор информационной системы:** Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

**7 предоставление информации:** Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

**8 распространение информации:** Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

**9 фишинг** (от англ. fishing): Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.



**10 электронная подпись:** Средство защиты информации, аналог бумажной подписи, который позволяет удостовериться в авторстве документа (я – автор) в факте того, что автор оставил свою подпись (я подписываю), и также убедиться в том, что документ не был изменен третьим лицом, т. е. сведения верны.

### **3 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

В программе повышения квалификации используются следующие обозначения и сокращения:

ЛДК – лично-деловая компетенция;

ПК – профессиональная компетенция;

СНФПО – Система непрерывного фирменного профессионального образования персонала ПАО «Газпром»;

ДОТ – дистанционные образовательные технологии.

#### **4 ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ПОВЫШАЕМОЙ КВАЛИФИКАЦИИ**

Область профессиональной деятельности специалистов, освоивших программу повышения квалификации по данному курсу: 01 Образование и наука.

Специалисты, освоившие программу повышения квалификации по данному курсу, готовятся к следующему виду деятельности: организация обучения.

## 5 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

### 5.1 Планируемые результаты освоения программы повышения квалификации

В результате обучения по программе повышения квалификации слушатель должен освоить и развить общепрофессиональные (ОПК), личностно-деловые (ЛДК) компетенции, представленные в таблице 1.

Таблица 1 – Перечень ОПК и ЛДК, развиваемых при повышении квалификации по курсу «Информационная безопасность при реализации обучения с использованием дистанционных образовательных технологий»

Код	Наименование компетенции
ОПК 1	Соблюдать и контролировать соблюдение правил охраны труда, промышленной безопасности при выполнении работ
ЛДК 1	Профессиональное развитие
Примечание – Перечень ОПК и ЛДК указывается в соответствии с Каталогом управленческих и личностно-деловых компетенций для применения в дочерних обществах и организациях ОАО «Газпром», утвержденным Департаментом ОАО «Газпром» (Е.Б. Касьян) 15.04.2013.	

В результате обучения по программе повышения квалификации слушатель должен развить следующие профессиональные компетенции, представленные в таблице 2.

Таблица 2 – Перечень профессиональных компетенций, развиваемых при повышении квалификации

Код	Наименование компетенции
ПК 1	Использование информационно-коммуникационных технологий в профессиональной деятельности
ПК 2	Обеспечение информационной безопасности при подготовке и реализации образовательного процесса с применением электронного обучения и дистанционных образовательных технологий

С целью овладения видом деятельности «Организация обучения» и соответствующими профессиональными компетенциями слушатель в результате освоения программы повышения квалификации по курсу должен:

**знать:**

– сущность и понятие информационной безопасности, характеристику ее составляющих;

- место информационной безопасности в системе национальной безопасности страны;
- классификацию информации по видам тайны и степеням конфиденциальности;
- источники угроз информационной безопасности и меры по их предотвращению;
- современные средства и способы обеспечения информационной безопасности.

## **6 ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ**

### **6.1 Требования к квалификации педагогических работников, обеспечивающих реализацию образовательного процесса в рамках программы повышения квалификации по курсу**

Требования к образованию педагогических работников, освоению ими дополнительных профессиональных программ, к опыту работы педагогических работников в области профессиональной деятельности, соответствующей направленности программы обучения, должны соответствовать Требованиям к квалификации педагогических работников организаций, осуществляющих образовательную деятельность, и образовательных организаций ПАО «Газпром» (приложения № 1 и 2 к письму «О требованиях к педагогическим работникам ПАО «Газпром» от 24.03.2017 № 07/15/05-221).

### **6.2 Материально-технические условия реализации программы повышения квалификации по курсу**

Реализация программы повышения квалификации предполагает наличие доступа педагогических работников и слушателей к информационно-телекоммуникационной сети Интернет (далее – сеть Интернет):

- с использованием установленных программно-технических средств для слушателей и преподавателей на скорости не ниже 512 Кбит/с;
- в труднодоступных районах, подключаемых к сети Интернет с использованием спутниковых каналов связи, скорость прямого канала должна быть не ниже 512 Кбит/с, обратного – не ниже 128 Кбит/с.

Также должен быть обеспечен порт доступа в сеть Интернет со скоростью не ниже 10 Мбит/с и возможностью установления не менее 20 одновременных сессий по 512 Кбит/с.

Рабочие места педагогического работника и слушателей должны быть оборудованы персональным компьютером и компьютерной периферией (веб-камерой, микрофоном, аудиоколонками и/или наушниками).

Технические средства обучения:

- компьютер, подключенный к сети Интернет;

– мультипортальная система дистанционного обучения «СНФПО Онлайн».

### **6.3 Требования к информационным и учебно-методическим условиям**

Реализация программы повышения квалификации специалистов по курсу должна предусматривать обеспечение комплектом учебно-информационных и дидактических материалов для проведения теоретического обучения.

В процессе освоения программы повышения квалификации по курсу слушатели должны быть обеспечены доступом к учебным материалам посредством выдачи раздаточных материалов, предоставления им доступа к нормативной правовой документации как в печатном, так и в электронно-цифровом виде.

В процессе освоения программы повышения квалификации для получения доступа к материалам, а также различным базам данных с документацией слушателям должна быть обеспечена возможность работы на компьютере и использования сети Интернет для самостоятельного поиска необходимой информации. Для этого компьютерные классы должны быть подключены к сети Интернет.

Реализация программы повышения квалификации в части применения электронного обучения обеспечивается посредством предоставления слушателям доступа к мультипортальной системе дистанционного обучения «СНФПО Онлайн».

Перечень информационного и учебно-методического обеспечения обучения представлен в разделе «Методические материалы» (подраздел «Учебно-методическое обеспечение») данной дополнительной профессиональной программы.

## 7 УЧЕБНЫЙ ПЛАН

### УЧЕБНЫЙ ПЛАН

повышения квалификации специалистов

по курсу «Информационная безопасность при реализации обучения  
с использованием дистанционных образовательных технологий»

Наименование разделов	Объем обучения, час									Объем времени на проведение аттестации (промежуточной, итоговой), час			
	Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия		Самостоятельная работа		в т. ч. консультаций при выполнении самостоятельной работы	Всего	из них		
		Всего	из них		Всего	из них		зачет			экзамен	защита реферата / выполнение итоговой практической работы	
			лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия						
1 Вводное занятие	1	–	–	–	1	1	–	–	–	–	–	–	–
2 Понятие информационной безопасности, основные принципы и определения	4	–	–	–	3	3	–	1	–	–	–	–	–





Наименование разделов	Объем обучения, час									Объем времени на проведение аттестации (промежуточной, итоговой), час				
	Всего	Обязательные аудитор-ные учебные занятия			Дистанционные занятия			Самостоятельная работа			Всего	из них		
		Всего	из них		Всего	из них		Всего	в т. ч. кон-сультаций при выпол-нении само-стоятельной работы	Всего		из них		
			лек-ции	практи-ческие занятия (дело-вые игры, тре-нинги)		лек-ции	практиче-ские занятия					за-чет	экза-мен	защита реферата / выполне-ние итого-вой прак-тической работы
Итоговая аттестация	2	–	–	–	–	–	–	–	–	2	2	–	–	
<b>Итого</b>	<b>40</b>	–	–	–	<b>34</b>	<b>34</b>	–	<b>4</b>	–	<b>2</b>	<b>2</b>	–	–	

## **8 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК**

Календарный учебный график по программе повышения квалификации специалистов по курсу «Информационная безопасность при реализации обучения с использованием дистанционных образовательных технологий» определяется Графиком реализации программ дополнительного профессионального образования ЧУ ДПО «Газпром ОНУТЦ» и графиком электронного обучения.

## 9 СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПО КУРСУ

### 9.1 Учебно-тематический план

Наименование разделов, тем	Объем времени, отведенный на освоение разделов, тем, час									Коды формируемых компетенций	Форма контроля	Уровень освоения	
	Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия		Самостоятельная работа		лекции			практические занятия	
		Всего	из них		Всего	из них		Всего					в т. ч. консультаций при выполнении самостоятельной работы
			лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия						
1 Вводное занятие	1	–	–	–	1	1	–	–	–	–	–	–	–
2 Понятие информационной безопасности, основные принципы и определения	4	–	–	–	3	3	–	1	–	ЛДК 1 ПК 1 ПК 2	–	2	–
2.1 Понятие информации, виды информации	1	–	–	–	1	1	–	–	–				

Наименование разделов, тем	Объем времени, отведенный на освоение разделов, тем, час									Коды формируемых компетенций	Форма контроля	Уровень освоения	
	Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия			Самостоятельная работа				лекции	практические занятия
		Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы				
			лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия						
2.2 Основные термины в области информационной безопасности	3	–	–	–	2	2	–	1	–				
3 Информационная безопасность при разработке и использовании в учебном процессе учебно-методических материалов	10	–	–	–	9	9	–	1	–	ЛДК 1 ПК 1 ПК 2	–	2	–
3.1 Авторское право	5	–	–	–	4	4	–	1	–				

Наименование разделов, тем	Объем времени, отведенный на освоение разделов, тем, час									Коды формируемых компетенций	Форма контроля	Уровень освоения	
	Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия			Самостоятельная работа				лекции	практические занятия
		Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы				
			лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия						
3.2 Информация ограниченного доступа, не являющаяся сведениями, составляющими государственную тайну	5	–	–	–	5	5	–	–	–	–	–	2	–
4 Требования информационной безопасности при реализации обучения с использованием ДОТ	16	–	–	–	14	14	–	2	–	ЛДК 1 ПК 1 ПК 2	–	2	–
4.1 Работа с персональными данными	6	–	–	–	5	5	–	1	–		–	–	–

Наименование разделов, тем	Объем времени, отведенный на освоение разделов, тем, час										Коды формируемых компетенций	Форма контроля	Уровень освоения	
	Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия			Самостоятельная работа		лекции			практические занятия	
		Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы					
			лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия							
4.2 Основные составляющие информационной безопасности	10	–	–	–	9	9	–	1	–					
5 Общие вопросы информационной безопасности	2	–	–	–	2	2	–	–	–	ЛДК 1 ПК 1 ПК 2	–	2	–	
6 Охрана труда и промышленная безопасность <sup>1)</sup>	4	–	–	–	4	4	–	–	–	ОПК 1 ЛДК 1	–	1	–	
7 Основы экологии и экологическая безопасность	2	–	–	–	2	2	–	–	–	ЛДК 1	–	1	–	
Итоговая аттестация	2	–	–	–	–	–	–	–	–	–	Зачет	–	–	
<b>Итого</b>	<b>40</b>	–	–	–	<b>34</b>	<b>34</b>	–	<b>4</b>	–	–	<b>2</b>	–	<b>40</b>	

Наименование разделов, тем	Объем времени, отведенный на освоение разделов, тем, час						Коды формируемых компетенций	Форма контроля	Уровень освоения		
	Всего	Обязательные аудиторные учебные занятия		Дистанционные занятия		Самостоятельная работа			лекции	практические занятия	
		Всего	из них		Всего	из них					
			лекции	практические занятия (деловые игры, тренинги)		лекции					практические занятия
<p>Примечание – Для характеристики уровня освоения учебного материала используются следующие обозначения:</p> <p>1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т. п.);</p> <p>2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);</p> <p>3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).</p>											



## **9.2 Содержание программы повышения квалификации по курсу**

### **Раздел 1 Вводное занятие**

Ознакомление слушателей с графиком электронного обучения.

Ознакомление слушателей с документами ЧУ ДПО «Газпром ОНУТЦ»: Уставом; Лицензией на осуществление образовательной деятельности; Правилами поведения слушателей; локальными нормативными актами, регламентирующими организацию и осуществление образовательной деятельности, права и обязанности слушателей.

Ознакомление слушателей с памяткой для участников образовательного процесса при онлайн-обучении.

Проведение инструктажа по корпоративной этике при организации электронного обучения и использовании дистанционных образовательных технологий.

Проведение инструктажа по информационной безопасности для преподавателей и обучающихся.

Информирование слушателей о необходимости прохождения входного анкетирования и заполнения необходимых документов для начала обучения: согласие на обработку персональных данных; заявление о присоединении к договору на оказание образовательных услуг.

### **Раздел 2 Понятие информационной безопасности, основные принципы и определения**

#### **Тема 2.1 Понятие информации, виды информации**

Понятие информации. Основные качества информации с точки зрения информационной безопасности.

#### **Тема 2.2 Основные термины в области информационной безопасности**

Основные термины в области информационной безопасности. Причины утечек информации, распределение утечек информации.

### **Раздел 3 Информационная безопасность при разработке и использовании в учебном процессе учебно-методических материалов**

#### **Тема 3.1 Авторское право**

Общие положения об авторском праве. Права автора онлайн-курса, способы отчуждения прав на онлайн-курс.

#### **Тема 3.2 Информация ограниченного доступа, не являющаяся сведениями, составляющими государственную тайну**

Виды информации по категориям доступа. Федеральные законы «О коммерческой тайне» и «Об информации, информационных технологиях и о защите информации».

### **Раздел 4 Требования информационной безопасности при реализации обучения с использованием ДОТ**

#### **Тема 4.1 Работа с персональными данными**

Обработка, хранение, передача, предоставление и уничтожение персональных данных.

#### **Тема 4.2 Основные составляющие информационной безопасности**

Безопасные пароли. Безопасная работа в сети Интернет. Мобильные угрозы. Криптография в мессенджерах. Защита от фишинговых атак. Безопасность ПО для видеоконференций. Безопасное хранение данных. Безопасность рабочих мест. Требования к антивирусной защите.

### **Раздел 5 Общие вопросы информационной безопасности**

Электронно-цифровая подпись. Формирование ЭЦП и использование для защиты электронных документов от подделки. Удостоверяющие центры. Их основные задачи. Система удостоверяющих центров в России и за рубежом. Уничтожение данных вследствие стихийного бедствия, пожара или наводнения. Уничтожение, кража, раскрытие или модификация данных вследствие взлома

или проникновения в помещение. Уничтожение, модификация, раскрытие данных или нарушение работы системы вследствие успешно проведенной атаки. Возможные варианты действий при различных атаках.

## **Раздел 6 Охрана труда и промышленная безопасность**

Основные понятия. Управление охраной труда. Обязанности работодателя по обеспечению безопасных условий и охраны труда. Права и обязанности работника. Опасные и вредные производственные факторы. Основы предупреждения производственного травматизма. Порядок расследования и учета несчастных случаев на производстве. Оказание первой помощи пострадавшим на производстве.

Основные понятия в области промышленной безопасности. Опасные производственные объекты. Требования промышленной безопасности. Правовое регулирование в области промышленной безопасности. Требования промышленной безопасности к эксплуатации опасного производственного объекта. Требования к организации производственного контроля за соблюдением требований промышленной безопасности. Федеральный государственный надзор в области промышленной безопасности. Ответственность за нарушение законодательства в области промышленной безопасности.

## **Раздел 7 Основы экологии и экологическая безопасность**

Техногенные загрязнения окружающей среды и основные методы ее защиты. Показатели качества окружающей среды. Источники загрязнения атмосферы. Рассеивание выбросов в атмосфере. Оценка воздействия на окружающую среду. Порядок проведения оценки воздействия на окружающую среду. Понятие экологического риска. Снижение негативного воздействия энергетических предприятий на окружающую среду.

## **10 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПО КУРСУ**

### **10.1 Общая характеристика контроля и оценивания качества освоения программы повышения квалификации по курсу**

Данные оценочные материалы предназначены для проведения итоговой аттестации слушателей в форме тестирования.

Тестирование проводится в рамках определенного времени. Затраты времени для тестирования определяются исходя из примерных затрат времени на выполнение одного задания (например, 1–2 минуты) и количества предложенных заданий.

В основу подсчета результатов тестирования положена система рейтинговой оценки. Путем деления количества полученных правильных ответов на количество выданных заданий и последующим умножением на 100 определяется процент правильных ответов. Для оценки степени усвоения пройденного учебного материала может использоваться шкала, приведенная в таблице 3.

Таблица 3 – Шкала для оценки степени усвоения пройденного учебного материала

Процент правильных ответов	Оценка
90–100 %	5 (отлично)
80–89 %	4 (хорошо)
60–79 %	3 (удовлетворительно)
менее 60 %	2 (неудовлетворительно)

## 10.2 Комплект контрольно-оценочных средств

### Перечень тестовых дидактических материалов

**Вопрос № 1**    Информация – это...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1      Совокупность содержащихся в базах данных сведений.
- 2      Совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях.
- 3      Сведения (сообщения, данные), воспроизводимые различными системами.
- 4      Сведения (сообщения, данные) независимо от формы их представления.

**Вопрос № 2**    Информационная система – это...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1      Совокупность информации, информационных технологий и технических средств.
- 2      Совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему.
- 3      Совокупность информационных технологий и технических средств.
- 4      Совокупность информации, технических средств и персонала, обслуживающего информационную систему.
- 5      Совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему.

**Вопрос № 3**    Владелец информации – это...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1      Лицо, самостоятельно создавшее информацию.
- 2      Лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации.

- 3 Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
- 4 Лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

**Вопрос № 4** Какой антивирус нужно использовать на рабочем месте?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Самый распространенный.
- 2 Бесплатный.
- 3 Утвержденный в организации.
- 4 Самый надежный.

**Вопрос № 5** В каком месте безопаснее хранить документы?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 На системном диске компьютера.
- 2 На любом логическом диске компьютера, кроме системного.
- 3 На съемном жестком диске.

**Вопрос № 6** Что из перечисленного не является объектом авторского права?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Произведение искусства.
- 2 Научная статья.
- 3 Технология производства.
- 4 Литературное произведение.

**Вопрос № 7** Кто является автором произведения?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Лицо, указанное в качестве автора на оригинале или экземпляре произведения, считается его автором, если не доказано иное.
- 2 Лицо, указанное в качестве автора на оригинале или экземпляре произведения.
- 3 Лицо, зарегистрировавшее произведение.
- 4 Лицо, указанное в Едином государственном реестре объектов авторского права.

**Вопрос № 8** Информация по категории доступа классифицируется как...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Конфиденциальная.
- 2 Общедоступная.
- 3 Особо конфиденциальная.
- 4 Ограниченного доступа.
- 5 Широкого доступа.

**Вопрос № 9** Какую информацию из перечисленной можно отнести к коммерческой тайне?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 О нарушениях законодательства Российской Федерации.
- 2 О технологии изготовления пищевых продуктов.
- 3 О наличии свободных рабочих мест.
- 4 О системе оплаты труда.

**Вопрос № 10** Действие закона «О персональных данных» не распространяется на персональные данные, которые обрабатываются...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Банковскими организациями.
- 2 Физическими лицами для личных и семейных нужд (если при этом не нарушаются права субъектов персональных данных).
- 3 Сотрудниками Почты России.
- 4 Организациями хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

**Вопрос № 11** Обезличивание персональных данных – это...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Стирание Ф. И. О. субъекта.
- 2 Уничтожение данных о субъекте.
- 3 Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- 4 Статистическая обработка данных.

**Вопрос № 12** Какая из служб имеет право доступа непосредственно к персональным данным в ходе проверки?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Роскомнадзор.
- 2 ФСТЭК.
- 3 ФСБ России.
- 4 Никакая из перечисленных.



**Вопрос № 13** Какими кодексами предусмотрена ответственность за нарушение требований к обработке персональных данных?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 КоАП РФ.
- 2 УК РФ.
- 3 ТК РФ.
- 4 Всеми перечисленными.

**Вопрос № 14** Можно ли открывать прикрепленные файлы в письмах, пришедших из неизвестных источников?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Нет.
- 2 Да, после проверки антивирусом.
- 3 Да.

**Вопрос № 15** Можно ли использовать на рабочем месте незарегистрированный носитель информации?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Да.
- 2 Да, только для записи.
- 3 Нет.
- 4 Да, только после проверки антивирусом.

**Вопрос № 16** Минимальная длина пароля в случае смены ежемесячно равна...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 6 символам.
- 2 8 символам.

3 10 символам.

4 12 символам.

**Вопрос № 17** Можно ли использовать одинаковые пароли для различных ресурсов?

Укажите **правильный** ответ (или ответы).

**Ответы:**

1 Да, только для корпоративных.

2 Да, только для однотипных.

3 Нет.

4 Везде можно, чтобы не забыть пароль.

**Вопрос № 18** Куда стоит записать пароль от корпоративной учетной записи?

Укажите **правильный** ответ (или ответы).

**Ответы:**

1 Его нельзя записывать, нужно запомнить.

2 В блокнот, который носите с собой.

3 На бумажный носитель, хранимый на рабочем месте.

4 В телефон.

**Вопрос № 19** Можно ли воспользоваться чужими учетными данными, если нужного сотрудника нет на месте?

Укажите **правильный** ответ (или ответы).

**Ответы:**

1 Да, если он на больничном.

2 Да, если он в отпуске.

3 Да, если разрешил руководитель.

4 Нет.

**Вопрос № 20** Вам необходимо открыть файл, находящийся на съемном носителе, принесенном слушателем, что нужно сделать в первую очередь?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Проверить файл антивирусом.
- 2 Проверить весь съемный диск антивирусом.
- 3 Закрыть все открытые программы.
- 4 Ничего.

**Вопрос № 21** При первом входе в систему с новой учетной записью следует...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Сообщить руководителю.
- 2 Сообщить системному администратору.
- 3 Сменить пароль.
- 4 Сменить имя пользователя.

**Вопрос № 22** Что нужно сделать в первую очередь при подключении к компьютеру нового съемного носителя?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Перезагрузить компьютер.
- 2 Проверить весь съемный носитель антивирусом.
- 3 Закрыть все открытые программы.
- 4 Ничего.

**Вопрос № 23** Состояние информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, подделки, копирования и блокирования – это...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Безопасность информации.
- 2 Информационная безопасность РФ.
- 3 Предоставление информации.
- 4 Распространение информации.

**Вопрос № 24** Информационная безопасность – механизм защиты, обеспечивающий...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Конфиденциальность информации.
- 2 Целостность информации.
- 3 Доступность информации.
- 4 Избыточность информации.

**Вопрос № 25** Доступ к информации – это...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Возможность получения информации и ее использования.
- 2 Возможность получения информации.
- 3 Возможность использования информации.
- 4 Возможность получения информации и ее создания.

**Вопрос № 26** Какие права принадлежат автору курса?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Исключительное право на произведение.
- 2 Право автора на имя.
- 3 Право на неприкосновенность произведения.
- 4 Право на обнародование произведения.

**Вопрос № 27** Если в создании курса участвовали два лица и более, то...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Автором считается тот, кто заявлен в сопроводительной документации к курсу.
- 2 Автором курса считается тот, кто внес больший вклад в его разработку.
- 3 Автором курса являются все лица, участвовавшие в его создании.
- 4 Все они являются его соавторами с соответствующим режимом его совместного использования.

**Вопрос № 28** Каким образом допускается использовать материалы, размещенные в общедоступных источниках, которые с большой вероятностью являются интеллектуальной собственностью третьих лиц, а также объектами авторского права?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Допускается произвольное использование.
- 2 Допускается использование таких материалов от своего имени.
- 3 Допускается использование посредством цитирования в объеме, оправданном целью цитирования.
- 4 Допускается использование в качестве иллюстраций и примеров в объемах, оправданных поставленной целью.

**Вопрос № 29** Лицензия в контексте авторского права – это...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Соглашение, по которому автор предоставляет либо обязуется предоставить другой стороне, лицензиату право использования его произведения в установленных договором пределах.
- 2 Соглашение, по которому автор предоставляет либо обязуется предоставить другой стороне бессрочное право использования его произведения.
- 3 Соглашение, по которому автор предоставляет либо обязуется предоставить другой стороне право использования его произведения посредством цитирования в объеме, оправданном целью цитирования.
- 4 Соглашение, по которому автор предоставляет либо обязуется предоставить другой стороне право использования его произведения.

**Вопрос № 30** Выберите из списка угрозы сетевой безопасности.

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Компьютерный вирус.
- 2 Фишинг.
- 3 Спам.
- 4 Троянская вирусная программа.

**Вопрос № 31** Выберите из списка критерии надежного пароля.

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Наличие строчных и прописных букв.
- 2 Наличие цифр и спецсимволов.
- 3 Наличие зашифрованных дат рождения и номера телефона.
- 4 Наличие Ф. И. О. и производных от них.

**Вопрос № 32** Чаще всего фишинговые сообщения содержат...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Различные угрозы, например, закрытия пользовательских банковских счетов.
- 2 Обещания денежного приза.
- 3 Запросы о добровольных пожертвованиях от лица благотворительных организаций.
- 4 Документы и инструкции.

**Вопрос № 33** На каком диске лучше хранить все рабочие файлы?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 На системном логическом диске, на котором установлена операционная система.
- 2 На втором рабочем диске без установленной операционной системы.
- 3 В облачном сервисе.
- 4 На съемном диске.

**Вопрос № 34** Что необходимо сделать, если необходимо на время покинуть рабочее место?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Оставить компьютер включенным с открытым доступом.
- 2 Заблокировать экран.
- 3 Отключить интернет.
- 4 Отключить компьютер от сети.

**Вопрос № 35** Можно ли отправлять электронные письма от чужого имени?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Нельзя ни при каких обстоятельствах.
- 2 Можно, если об этом попросили.

- 3 Можно в любых обстоятельствах.
- 4 Можно, но только с личной почты.

**Вопрос № 36** Рекомендовано ли иметь один и тот же пароль к различным ресурсам корпоративной информационной системы?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Рекомендуется, чтобы пароли пользователей на доступ к различным ресурсам корпоративной информационной системы не различались.
- 2 Рекомендуется, чтобы пароли пользователей на доступ к различным ресурсам корпоративной информационной системы различались.
- 3 Рекомендуется, чтобы пароли пользователей на доступ к различным ресурсам корпоративной информационной системы не различались, но регулярно обновлялись.
- 4 Рекомендуется, чтобы пароли пользователей на доступ к различным ресурсам корпоративной информационной системы не различались, но обновлялись раз в месяц.

**Вопрос № 37** Максимальный период действия пароля не должен превышать...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 10 дней.
- 2 20 дней.
- 3 1 месяц.
- 4 3 месяца.

**Вопрос № 38** При неоднократном неправильном вводе пароля учетная запись должна...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Блокироваться на определенный промежуток времени.
- 2 Блокироваться на неопределенный промежуток времени.
- 3 Блокироваться до разрешения администратора безопасности.



4 Удаляться из системы.

**Вопрос № 39** Какое из требований не является требованием к безопасности пароля?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Строчные и прописные буквы.
- 2 Наличие букв и цифр.
- 3 Наличие спецсимволов.
- 4 Ввод русских букв в латинской раскладке клавиатуры.

**Вопрос № 40** Какой подход рекомендуется при создании паролей для различных ресурсов?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Рекомендовано создавать одинаковые пароли для всех корпоративных ресурсов.
- 2 Рекомендовано создавать одинаковые пароли для всех однотипных ресурсов.
- 3 Не рекомендовано создавать одинаковые пароли для любых ресурсов.
- 4 Не рекомендовано создавать одинаковые пароли для корпоративных ресурсов.

**Вопрос № 41** Где стоит хранить блокнот с паролем от корпоративной учетной записи?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Пароль нельзя где-либо записывать, его нужно запомнить.
- 2 В личных вещах.
- 3 У руководителя.
- 4 У системного администратора.

**Вопрос № 42** При входе в корпоративные ресурсы под учетной записью коллеги необходимо...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Получить письменное разрешение непосредственного руководителя.
- 2 Получить письменное разрешение системного администратора.
- 3 Его физическое присутствие.
- 4 Вход с чужими учетными данными запрещен.

**Вопрос № 43** Для каких целей можно использовать корпоративный e-mail?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Для регистрации в соцсети.
- 2 Для деловой переписки.
- 3 Для личной переписки.
- 4 Для рассылки рекламных материалов.

**Вопрос № 44** Может ли письмо, отправленное с корпоративного адреса, считаться личной перепиской?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Нет, служебную почту можно использовать только при выполнении служебных обязанностей.
- 2 Нет, если вы подписали согласие на просмотр почты работодателем.
- 3 Да, тайна переписки гарантирована Конституцией РФ.
- 4 Да, неприкосновенность частной жизни гарантирована Конституцией РФ.

**Вопрос № 45** Вам нужно переслать письмо с конфиденциальной информацией. Что для этого необходимо?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Использовать находящиеся в свободном доступе средства защиты.

- 2 Заархивировать информацию с паролем.
- 3 Использовать утвержденные в организации средства шифрования.
- 4 Этого нельзя делать ни при каких условиях.

**Вопрос № 46** Что из перечисленного не является признаком фишинговой ссылки?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Орфографические ошибки в письме.
- 2 Отличие фактического адреса ссылки от адреса, указанного в письме.
- 3 Содержащаяся в письме угроза блокировки банковского счета.
- 4 Письмо отправлено с неизвестного корпоративного адреса.

**Вопрос № 47** Можно ли выкладывать материал учебных курсов на свою страницу в соцсети?

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Да, это личная информация.
- 2 Да, если этот курс сделан полностью вами в рамках личной инициативы и не содержит информацию, являющуюся коммерческой тайной или объектом авторского права третьих лиц.
- 3 Да, если выкладывается неполный курс.
- 4 Нет.

**Вопрос № 48** При утрате носителя с информацией, составляющей коммерческую тайну, необходимо...

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Приобрести новый носитель.
- 2 Написать заявление в полицию.
- 3 Сообщить в службу технической поддержки.
- 4 Сообщить администратору информационной безопасности.

**Вопрос № 49** Если вам понадобилась консультация службы технической поддержки, рекомендуется...

Дополните предложение, выбрав **правильный** ответ (или ответы).

**Ответы:**

- 1 Присутствовать при выполнении действий работника службы технической поддержки.
- 2 Предоставить свои учетные данные работнику службы технической поддержки, чтобы он мог выполнить необходимые действия в ваше отсутствие.
- 3 Оставить компьютер включенным для работника службы технической поддержки, чтобы он мог выполнить необходимые действия в ваше отсутствие.
- 4 Установить средства удаленного администрирования.

**Вопрос № 50** Отметьте основные признаки безопасного рабочего места.

Укажите **правильный** ответ (или ответы).

**Ответы:**

- 1 Отсутствие конфиденциальных документов на рабочем столе.
- 2 Блокировка экрана в ваше отсутствие.
- 3 Отсутствие в помещении посторонних при обработке конфиденциальной информации.
- 4 Наличие охраны при входе в здание.

## **11 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ**

### **11.1 Методические рекомендации по организации и проведению учебного процесса**

Учебным планом и программой предусмотрено теоретическое обучение.

В целях обеспечения современного уровня профессионального образования в СНФПО реализация программ повышения квалификации специалистов должна осуществляться с использованием интерактивных обучающих систем, разрабатываемых в ЧУ ДПО «Газпром ОНУТЦ».

Содержание и последовательность изложения изучаемых тем и распределение учебного материала внутри тем могут изменяться в зависимости от специфики контингента слушателей. В процессе обучения допускается внесение необходимых изменений как в содержание программного материала, так и в распределение учебных часов по отдельным темам, при этом общее количество часов, отведенных на изучение курса, должно соответствовать учебному плану.

### **11.2 Учебно-методическое обеспечение**

#### **11.2.1 Список рекомендуемых нормативных документов, учебной и методической литературы**

В списке рекомендуемых нормативных документов ссылки на законодательные и нормативные документы приведены по состоянию на 04.02.2022. Перед использованием настоящей дополнительной профессиональной программы следует проверить действие ссылочных законодательных и нормативных документов по соответствующим правовым базам данных. Если ссылочный документ заменен (изменен), то следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то материал, в котором дана на него ссылка, применяется в части, не затрагивающей эту ссылку.

#### **Нормативные документы**

1 Российская Федерация. Закон. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ : редакция от 30.12.2021.

2 Российская Федерация. Закон. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ : редакция от 02.07.2021.

3 Российская Федерация. Закон. Гражданский кодекс Российской Федерации (часть четвертая) Федеральный закон от 18.12.2006 № 230-ФЗ : редакция от 11.06.2021.

### **Учебники, учебные и справочные пособия**

1 **Родичев Ю. А.** Информационная безопасность. Национальные стандарты Российской Федерации : учебное пособие / Ю. А. Родичев. – Санкт-Петербург : Питер, 2019. – 304 с.

2 **Родичев Ю. А.** Нормативная база и стандарты в области информационной безопасности : учебное пособие / Ю. А. Родичев. – Санкт-Петербург : Питер, 2021. – 256 с.

3 **Сычев Ю. Н.** Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. – Москва : НИЦ ИНФРА-М, 2019. – 223 с.

### **11.2.2 Перечень рекомендуемых наглядных пособий и интерактивных обучающих систем**

1 Информационная безопасность при реализации обучения с использованием электронного обучения и дистанционных образовательных технологий : электронный учебный курс для дистанционного обучения (SCORM-формат). – Калининград : ЧУ ДПО «Газпром ОНУТЦ», 2021 // Мультипортальная система дистанционного обучения «СНФПО Онлайн» : сайт. – URL: [https://go.sdo.snfpo.ru/course\\_sessions/03-10-15-213-262-kurs-povysheniya-kvalifikatsii-informatsionnaya-bezopasnost-pri-realizatsii-obucheniya-s-ispolzovaniem-elektronного-obucheniya-i-distantсионных-obrazovatelnyh-tehnologiy-03-1015-262-e-05-05/apply](https://go.sdo.snfpo.ru/course_sessions/03-10-15-213-262-kurs-povysheniya-kvalifikatsii-informatsionnaya-bezopasnost-pri-realizatsii-obucheniya-s-ispolzovaniem-elektronного-obucheniya-i-distantсионных-obrazovatelnyh-tehnologiy-03-1015-262-e-05-05/apply) – Режим доступа: для зарегистрир. пользователей.