ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ГАЗПРОМ ДОБЫЧА НАДЫМ»

УТВЕРЖДАЮ

Главный инженер – первый заместитель
генерального директора
ООО «Газпром добыча Надым»

_____ В.Н. Полозов
«_____»_____ 2024 г.

Направление: ОБЩЕОТРАСЛЕВОЕ

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА - программа повышения квалификации руководителей и специалистов по курсу «Обеспечение информационной безопасности объектов критической информационной инфраструктуры»

Образовательная организация: Учебно-производственный центр
при администрации ООО «Газпром добыча Надым»

Код документа: СНО 08.08.01.441.12

г. Надым 2024

От 03.04.2024
№ УПД-28

АННОТАЦИЯ

Дополнительная профессиональная программа предназначена для повышения квалификации руководителей и специалистов по курсу «Обеспечение информационной безопасности объектов критической информационной инфраструктуры». Целью данного обучения является обеспечение необходимого уровня квалификации в области информационной безопасности специалистов ООО «Газпром добыча Надым».

В программе теоретического обучения рассматриваются вопросы требований законодательства в сфере критической информационной инфраструктуры, защиты информации в автоматизированных системах в процессе их эксплуатации.

В программе практики отрабатываются навыки выявления ошибок на этапах категорирования объектов критической информационной инфраструктуры, использование программных комплексов для управления системой резервного копирования на предприятии.

Программа предназначена для работников, занимающихся разработкой учебно-методических материалов для обучения персонала ООО «Газпром добыча Надым», для руководителей и специалистов Учебно-производственного центра ООО «Газпром добыча Надым», занимающихся организацией и обучением персонала, а также для специалистов, осуществляющих данное обучение.

Сведения о документе:

1 РАЗРАБОТАН	Учебно-производственным центром при администрации ООО «Газпром добыча Надым»
2 ВНЕСЕН	Учебно-производственным центром при администрации ООО «Газпром добыча Надым»
3 УТВЕРЖДЕН	Главным инженером – первым заместителем генерального директора ООО «Газпром добыча Надым» (В.Н. Полозов)
4 СОГЛАСОВАН	Заместителем генерального директора по корпоративной защите ООО «Газпром добыча Надым» (Ю.В. Скорик) Начальником службы корпоративной защиты ООО «Газпром добыча Надым» (А.В. Тарасенко)
5 СРОК ДЕЙСТВИЯ	5 лет

Распространение настоящих учебно-методических материалов осуществляется в соответствии с действующим законодательством и с соблюдением правил, установленных ПАО «Газпром».

Список исполнителей:

Рецензенты:

Начальник отдела информационной безопасности Службы корпоративной защиты ООО «Газпром добыча Надым»	С.Э. Измайлов
Заведующий Пангодинским отделением по обучению персонала Учебно-производственного центра при администрации ООО «Газпром добыча Надым»	С.Э. Лушников

Методическое обеспечение разработки и составления программы повышения квалификации рабочих:

Ведущий инженер по подготовке кадров Учебно-производственного центра при администрации ООО «Газпром добыча Надым»	Ж.А. Караматова
Методист Пангодинского отделения по обучению персонала Учебно-производственного центра при администрации ООО «Газпром добыча Надым»	Ю.В. Хрулёва
Инженер по подготовке кадров Учебно-производственного центра при администрации ООО «Газпром добыча Надым»	А.Р. Яруллина

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Область применения

Настоящая дополнительная профессиональная программа предназначена для повышения квалификации руководителей и специалистов по курсу «Обеспечение информационной безопасности объектов критической информационной инфраструктуры», осуществляющих обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите и включает в себя:

– общие положения;

– термины и определения;

– обозначения и сокращения;

– характеристику профессиональной деятельности в области повышаемой квалификации;

– планируемые результаты обучения;

– условия реализации программы повышения квалификации руководителей и специалистов;

– учебно-тематический план;

– календарный учебный график;

– содержание программы повышения квалификации;

– оценочные материалы для контроля освоения программы повышения квалификации;

– методические материалы.

Дополнительная профессиональная программа повышения квалификации предназначена для использования:

– руководителями и специалистами служб по управлению персоналом ООО «Газпром добыча Надым»;

– руководителями и специалистами, занимающимися организацией обучения и обучением персонала в ООО «Газпром добыча Надым».

1.2 Цель реализации программы обучения

Программа повышения квалификации имеет своей целью освоение новых компетенций и (или) совершенствование имеющихся, необходимых для профессиональной деятельности специалистов, осуществляющих эксплуатацию и обеспечивающих функционирование автоматизированных систем объектов критической информационной инфраструктуры Общества, с учетом требований профессионального стандарта, представленного в таблице № 1.

Таблица №1 - Профессиональный стандарт «Специалист по защите информации в автоматизированных системах»

Код профессионального стандарта	Наименование профессионального стандарта
06.033	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 525н

1.3 Нормативная правовая основа разработки

Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 25.12.2023) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2024)

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к дознанию систем Безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению независимости значимых объектов критической информационной инфраструктуры Российской Федерации»

Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утвержденное приказом ПАО «Газпром» от 01.12.2023 № 454

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

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры и компенсирующие мероприятия, реализация которых необходима в случае отсутствия или невозможности настройки средств защиты информации, встроенных в общесистемное, прикладное программное обеспечение и (или) программно-аппаратные средства АСУ технологическими процессами и (или) обеспечения их взаимодействия со средствами защиты информации, сформированные во

исполнение норм Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» (утв. Заместителем генерального директора по корпоративной защите 02.08.2023)

1.4 Требования к слушателям

Категория слушателей – руководители и специалисты ООО «Газпром добыча Надым», осуществляющие эксплуатацию и, обеспечивающие информационную безопасность и функционирование автоматизированных систем объектов критической информационной инфраструктуры Общества, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защиты.

Уровень образования слушателей для допуска к обучению:

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

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

1.5 Срок освоения программы повышения квалификации рабочих, форма обучения

Продолжительность обучения - 24 часа.

Форма обучения – очная (с отрывом от работы), очно-заочная.

Возможно применение электронного обучения и дистанционных образовательных технологий.

1.6 Форма аттестации, форма документа, выдаваемого по результатам обучения

Оценка качества освоения программы обучения включает промежуточную аттестацию по каждому разделу программы обучения и итоговую аттестацию. Промежуточная аттестация по разделу 1 проводится с применением перечня вопросов, представленных в п 10.1.1. настоящей программы. Промежуточная аттестация по разделам 2 и 3 проводится в форме тестирования с применением АОС (ЭУМП) по тематике раздела.

Итоговая аттестация проходит в форме экзамена. Экзамен проводится в виде итогового тестирования с применением обучающе-контролирующей системы ОЛИМПОКС.

Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца (Приложение № 2).

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы и (или) отчисленным, выдается справка об обучении или о периоде обучения установленного образца (в соответствии с

Положением о СНФПО персонала ПАО «Газпром», его дочерних обществ и организаций, утв. приказом ПАО «Газпром» от 01.12.2023 № 454).

2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В программе повышения квалификации руководителей и специалистов используются следующие термины и их определения:

Автоматизированная обучающая система - интерактивная обучающая система, предназначенная для приобретения и контроля знаний обучающегося, разработанная с использованием современных средств компьютерного дизайна (графики, видеофрагментов, анимационных фрагментов, текстовых ссылок и других мультимедийных технологий) в соответствии с утвержденной учебной программой для конкретной специальности (профессии) или группы специальностей (профессий).

[Унификация учебно-методических материалов и их оформление, СНО 05.01.09.024.01, п. 4.1.3]

Дополнительное профессиональное образование - образование, направленное на удовлетворение образовательных и профессиональных потребностей, профессиональное развитие работника, обеспечение соответствия его квалификации меняющимся условиям профессиональной деятельности и социальной среды, осуществляемое посредством реализации дополнительных профессиональных программ.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Итоговая аттестация - форма оценки степени и уровня освоения обучающимися образовательной программы.

[Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», ст. 59, п. 1]

Квалификация работника - уровень знаний, умений, профессиональных навыков и опыта работы.

[Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», ст. 2, п. 5]

Компетенция - совокупность профессиональных знаний, личностно-деловых и управленческих характеристик работника, необходимых для эффективного решения поставленных задач

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Нормативы оснащенности учебных кабинетов, учебных мастерских - документ, включающий в себя перечень оборудования, плакатов, видеофильмов, АОС, тренажеров и других технических средств обучения, необходимых для обучения персонала.

Образование - единый целенаправленный процесс воспитания и обучения, являющийся общественно значимым благом и осуществляемый в интересах человека, семьи, общества и государства, а также совокупность

приобретаемых знаний, умений, навыков, ценностных установок, опыта деятельности и компетенций определенных объема и сложности в целях интеллектуального, духовно-нравственного, творческого, физического и/или профессионального развития человека, удовлетворения его образовательных потребностей и интересов.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Образовательная организация - некоммерческая организация, осуществляющая на основании лицензии образовательную деятельность в качестве основного вида деятельности в соответствии с целями, ради достижения которых такая организация создана.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Образовательная программа - комплекс основных характеристик образования (объем, содержание, планируемые результаты) и организационно-педагогических условий, который представлен в виде учебного плана, календарного учебного графика, рабочих программ учебных предметов, курсов, дисциплин (модулей), иных компонентов, оценочных и методических материалов.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Обучающиеся - физические лица, осваивающее образовательную программу. В зависимости от уровня осваиваемой образовательной программы, формы обучения, режима пребывания в образовательной организации к обучающимся относятся учащиеся, студенты, аспиранты, слушатели. [Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Обучение - целенаправленный процесс организации деятельности обучающихся по овладению знаниями, умениями, навыками и компетенциями, приобретению опыта деятельности, развитию способностей, приобретению опыта применения знаний в профессиональной деятельности и формированию у обучающихся мотивации получения образования в течение всей жизни. [Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Организация, осуществляющая образовательную деятельность - образовательная организация, а также организации, осуществляющие обучение [Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Организация, осуществляющая обучение - юридическое лицо, осуществляющее на основании лицензии наряду с основной деятельностью образовательную деятельность в качестве дополнительного вида деятельности.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Педагогическая деятельность - деятельность, осуществляемая для достижения результатов, предусмотренных образовательной программой или рядом образовательных программ.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Педагогический работник - физическое лицо, которые состоит в трудовых отношениях с организацией, осуществляющей образовательную деятельность, и выполняют обязанности по обучению, воспитанию обучающихся и (или) организации образовательной деятельности. Педагогические работники в организациях СНФПО: штатные преподаватели, методисты и мастера производственного обучения, а также внештатные преподаватели и инструкторы производственного обучения.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Профиль компетенций - структурированный перечень компетенций для определенной должности с указанием требуемого для эффективного выполнения задач уровня их развития.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Учебно-методические материалы (УММ) – нормативная и учебно-методическая документация для организации и осуществления образовательной деятельности.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454, п. 2]

Учебный план – документ, который определяет перечень, трудоемкость, последовательность и распределение по периодам обучения учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности и, если иное не установлено нормативными правовыми актами, формы промежуточной аттестации обучающихся.

[Положение о Системе непрерывного фирменного профессионального образования персонала ПАО «Газпром», его дочерних обществ и организаций, утверждено Приказом ПАО «Газпром» от 01.12.2023 № 454 п. 2]

3 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В программе повышения квалификации используются следующие сокращения:

АОС – автоматизированная обучающая система;
АСУ – автоматизированная система управления;
ВД – вид деятельности;
ИОС – интерактивные обучающие системы;
КИИ – критическая информационная инфраструктура;
КИПиА – контрольно-измерительное оборудование и автоматика;
ЛДК – личностно-деловая компетенция;
ОРД – организационно-распределительные документы;
ОКИИ – объекты критической информационной инфраструктуры;
ПК – профессиональная компетенция;
ПИР – проектно-изыскательные работы;
ПС – профессиональный стандарт;
ПО – программное обеспечение;
ПТУ – программно-технические устройства;
РД – рабочая документация;
ТО – техническое обслуживание;
УК – управленческая компетенция;
ЭУМП – электронно-учебное методическое пособие.

4 ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ПОВЫШАЕМОЙ КВАЛИФИКАЦИИ

Область профессиональной деятельности специалистов, освоивших программу повышения квалификации по данному курсу – эксплуатация и обеспечение функционирования автоматизированных систем объектов КИИ, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

Объектами профессиональной деятельности специалистов, освоивших программу повышения квалификации являются объекты критической информационной инфраструктуры на предприятии.

Специалисты, освоившие программу повышения квалификации по данному курсу, готовятся к следующим видам деятельности:

– обеспечение защиты информации в автоматизированных системах объектов КИИ в процессе их эксплуатации;

– участие во внедрении систем защиты информации автоматизированных систем;

– реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта;

– проведение мероприятий по категорированию объектов критической информационной инфраструктуры.

5 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

5.1 Требования к результатам освоения программы повышения квалификации в соответствии с требованиями профессиональных стандартов

Определение результатов освоения программы повышения квалификации в части обобщенных трудовых функций и трудовых функций применяемых профессиональных стандартов представлено в таблице № 2.

Таблица № 2 – Определение результатов освоения программы повышения квалификации в соответствии с требованиями профессиональных стандартов

Код профессионального стандарта*	Код ОТФ, ТФ	Наименование ОТФ, ТФ в соответствии с ПС	Уровень (подуровень) квалификации в соответствии с ПС	Код и наименование соответствующих видов деятельности (профессиональный модулей) в программе	Требуемые профессиональные компетенции
06.033	B	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	6	ВД1 (ПМ1) Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	
	B/01.6	Диагностика систем защиты информации автоматизированных систем			ПК 1.1 Диагностировать системы защиты информации автоматизированный систем
	B/02.6	Администрир ование систем защиты информации автоматизированных систем			ПК 1.2 Администрировать системы защиты информации автоматизированный систем
	B/05.6	Мониторинг защищенности информации в автоматизированных системах			ПК 1.3 Проводить мониторинг защищенности информации в автоматизированных системах
	B/06.6	Аудит защищенности информации в автоматизированных системах			ПК 1.4 Проводить аудит защищенности информации в автоматизированных системах

	С	Внедрение систем защиты информации автоматизированных систем	7		
	С/01.6	Установка и настройка средств защиты информации в автоматизированных системах		ВД 2 (ПМ 2) Внедрение систем защиты информации автоматизированных систем	ПК 2.1 Устанавливать и настраивать средства защиты информации в автоматизированных системах
	С/03.6	Анализ уязвимостей внедряемой системы защиты информации			ПК 2.2 Проводить анализ уязвимостей внедряемой системы защиты информации

5.2 Планируемые результаты освоения программы повышения квалификации

В результате обучения по программе повышения квалификации руководителей и специалистов обучающийся должен освоить / развить управленческие (УК) и личностно-деловые компетенции (ЛДК), представленные в таблице № 3.

Таблица № 3 – Перечень управленческих и личностно-деловых компетенций

Код	Наименование общих компетенций
УК 1	Умение обеспечить результат
ЛДК1	Системное мышление
ЛДК2	Понимание специфики организации

В результате обучения по программе повышения квалификации слушатель должен совершенствовать профессиональные компетенции, представленные в таблице № 4.

Таблица № 4 – Перечень профессиональных компетенций по видам деятельности, формируемых и/или развиваемых при повышении квалификации руководителей и специалистов по курсу

Код	Наименование видов деятельности (профессиональный модулей) и формируемые профессиональных компетенций	Код профессионального стандарта	Код ОТФ и ТФ в профессиональном стандарте	Наименование дисциплины
ВД1 (ПМ1)	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	06.033		

ПК 1.1	Диагностировать системы защиты информации автоматизированных систем		B/01.6	ПМ 1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации
ПК 1.2	Администрировать системы защиты информации автоматизированных систем		B/02.6	ПМ 1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации
ПК 1.3	Проводить мониторинг защищенности информации в автоматизированных системах		B/05.6	ПМ 1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации
ПК 1.4	Проводить аудит защищенности информации в автоматизированных системах		B/04.6	ПМ 1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации
ВД2 (ПМ 2)	Внедрение систем защиты информации автоматизированных систем			
ПК 2.1	Устанавливать и настраивать средства защиты информации в автоматизированных системах	06.033	C/01.6	ПМ 2 Внедрение систем защиты информации автоматизированных систем
ПК 2.2	Проводить анализ уязвимостей внедряемой системы защиты информации		C/03.6	ПМ 2 Внедрение систем защиты информации автоматизированных систем
* Модульно-компетентностный подход предусматривает, что освоение каждого из видов деятельности осуществляется в рамках профессионального модуля с одноименным виду деятельности названием. ** Указываются формируемые / развиваемые компетенции в соответствии с профессиональным стандартом (трудовые функции или действия), и/или в соответствии с ФГОС, и/или в соответствии с квалификационными требованиями, указанными в квалификационных справочниках по соответствующим должностям, профессиям и специальностям. *** В соответствии с кодами профессионального стандарта.				

С целью овладения видом деятельности «Обеспечение информационной безопасности объектов критической информационной инфраструктуры» и соответствующими профессиональными компетенциями обучающийся в результате освоения программы повышения квалификации по курсу должен:

получить практический опыт:

– участия в приемочных испытаниях значимого объекта и его подсистемы безопасности;

– проведения мероприятий по обеспечению безопасности значимых объектов пр выводе их из эксплуатации;

– управления (администрирования) подсистемой безопасности значимого объекта;

– управления конфигурацией подсистемы безопасности значимого объекта;

– участия в приемочных испытаниях значимого объекта и его подсистемы безопасности;

– участия в мероприятиях по обеспеченирю безопасностизначимых объектов при выводе их из эксплуатации;

– управления (администрирования) подсистемой безопасности значимого объекта (в части установки и настройки агентов средств защиты информации, устанавливаемых на средства вычислительной техники значимого объекта, средств защиты информации, встроенных в общесистемное, прикладное (специальное) программное обеспечение и (или) программно-аппаратные средства автоматизированных систем управления технологическими процессами значимого объекта);

– управления конфигурацией значимого объекта и его подсистемой безопасности;

– участия в приемочных испытаниях значимого объекта и его подсистемы безопасности.

уметь:

- осуществлять эксплуатацию значимых объектов критической информационной инфраструктуры;

– реагировать на компьютерные инциденты в ходе эксплуатации значимого объекта;

– осуществлять действия в нештатных ситуациях в ходе эксплуатации значимого объекта;

– осуществлять эксплуатацию значимых объектов критической информационной инфраструктуры в соответствии с правилами безопасности, установленными организационной-распорядительными документами по безопасности значимых объектов;

– обеспечить функционирование значимых объектов критической инфомационной инфраструктуры в соответствии с правилами безопасности, установленными организационной-распорядительными документами по безопасности значимых объектов;

- обеспечить функционирование подсистем безопасности значимых объектов критической инфомационной инфраструктуры в соответствии с правилами безопасности, установленными организационной-распорядительными документами по безопасности значимых объектов;

– проводить мероприятия по категорированию объектов критической информационной инфраструктуры.

знать:

– мероприятия по категорированию объектов критической

информационной инфраструктуры;

– планирование мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

– проведение внутреннего контроля организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых органиационных и технических мер;

– проведения анализа функционирования системы безопасности в рамках совершенствования безопасности значимых объектов;

– проведение мероприятий по категорированию объектов критической информационной инфраструктуры.

6 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

6.1 Требования к квалификации педагогических работников, обеспечивающих реализацию образовательного процесса при реализации программы повышения квалификации по курсу

Требования к образованию педагогических работников, освоению педагогическими работниками, обеспечивающими обучение, 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).

Для проведения занятий по программе повышения квалификации рабочих по курсу целевого назначения привлекаются руководители и специалисты ООО «Газпром добыча Надым», имеющие соответствующую профессиональную подготовку и обладающие теоретическими знаниями и практическим опытом, необходимыми для качественного проведения учебных занятий.

6.2 Материально-технические условия реализации программы повышения квалификации по курсу

Реализация программы повышения квалификации руководителей и специалистов предполагает наличие учебных аудиторий, компьютерных классов, учебных лабораторий и учебно-производственных мастерских, учебных полигонов для изучения теоретических основ (и практических основ выполнения) выполнения работ по обслуживанию электроустановок во взрывоопасных зонах.

Реализация программы повышения квалификации предполагает наличие учебного класса, соответствующего следующим параметрам:

– площадь не менее 2 м^2 на одного слушателя (для компьютерного класса на менее 4,5 м^2);

– оснащение системами отопления и/или кондиционирования воздуха, обеспечивающими поддержание комфортной температуры;

– достаточное освещение и вентиляция для максимального уменьшения утомляемости слушателей в процессе обучения.

Оборудование учебного класса и рабочих мест класса:

– рабочее место преподавателя, включающее в себя: рабочий стол, стул, кресло, персональный компьютер;

– посадочные места по количеству слушателей;
– проектор, экран для проектора;
– доска для письма с фломастерами или флипчарт.

Оборудование компьютерного класса и рабочих мест компьютерного класса:

– автоматизированные рабочие места, включающие в себя: рабочий стол, кресло, персональный компьютер (по количеству посадочных мест);
– проектор, экран для проектора;
– доска для письма с фломастерами или флипчарт.

6.3 Требования к информационным и учебно-методическим условиям

Реализация программы повышения квалификации руководителей и специалистов по курсу обеспечивается комплектом учебно-методической литературы и учебно-информационных и дидактических материалов для проведения теоретического обучения и практики и включает в себя комплект нормативно правовой документации, учебники и учебные пособия, справочники, раздаточный материал, перечни вопросов для промежуточной аттестации по разделам, перечень тестовых дидактических материалов для проведения итоговой аттестации.

Каждый слушатель должен быть обеспечен современными учебными, учебно-методическими материалами, печатными и/или электронными информационными ресурсами, электронными образовательными ресурсами.

В процессе освоения программы слушателям предоставляется доступ к различным учебно-методическим материалам, в том числе ИОС для проведения лабораторно-практических работ.

Перечень информационного и учебно-методического обеспечения обучения представлен в разделе «Методические материалы» (подраздел «Учебно-методическое обеспечение») данной программы повышения квалификации специалистов по курсу.

7 УЧЕБНЫЙ ПЛАН

УЧЕБНЫЙ ПЛАН

повышения квалификации руководителей и специалистов
по курсу «Обеспечение информационной безопасности объектов критической информационной инфраструктуры»

Наименование дисциплин, профессиональных модулей, практик и др.	Объем обучения, час									Объем времени на проведение аттестации (промежуточной, итоговой), час			
	Всего	Обязательные аудиторные учебные			Дистанционные занятия			Самостоятельная работа*					
		Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы	Всего	из них		
			лекции	практические занятия (деловые игры, тренинги)		вебинары	практические занятия				зачет**	экзамен	Защита реферата/ выполнение итоговой прак-
1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	18	18	8	10	–	–	–	–	–	–	–	–	–
2 Охрана труда и промышленная безопасность	2	2	–	–	–	–	–	2	2	–	зачет	–	–
3 Основы экологии и экологическая безопасность	2	2	–	–	–	–	–	2	2	–	зачет	–	–
Итоговая аттестация (экзамен) ***	2	–	–	–	–	–	–	–	–	2	–	–	–
Всего	**24**	**22**	8	10	–	–	–	4	4	**2**	–	2	–

* Осуществляется с использованием АОС и УЭМП, разрабатываемых в ЧУ ДПО «Газпром ОНУТЦ». Перечень рекомендуемых наглядных пособий и ИОС приведен в Разделе 11.2.2 учебно–программной документации;
** Промежуточная аттестация проводится в форме устного опроса за счет часов, отведенных на изучение дисциплины. Перечень вопросов для устного опроса представлен в Разделе 10.1.1 учебно–программной документации;
*** Итоговая аттестация проводится в форме экзамена, включающего итоговое тестирование в обучающе-контролирующей системе ОЛИМПОКС

8 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный график по программе повышения квалификации руководителей и специалистов по курсу «Обеспечение информационной безопасности объектов критической информационной инфраструктуры» составляется перед началом обучения, определяется утвержденным расписанием учебных занятий и заменяется для каждой группы обучающихся по данной программе.

Форма календарного учебного графика приведена в Приложении № 1 к данной программе повышения квалификации.

9 СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

9.1 Структура и содержание учебной спецдисциплины «Обеспечение информационной безопасности объектов критической информационной инфраструктуры»

9.1.1 Учебно-тематический план

Наименование разделов, тем	Объем времени, отведенный на освоение разделов, тем, час								Коды формируемых компетенций	Формы контроля	Уровень усвоения	
	Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия			Самостоятельная работа				
		Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы		лекции	практические занятия
			лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия					
1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	**18**	**18**	**8**	**10**	–	–	–	–	–	ОК1-2	опрос*		
1.1 Общие требования законодательства в сфере критической информационной инфраструктуры	1	1	1	–	–	–	–	–	–	ОК1-6, ПК1	–	2	–
1.2 Порядок взаимодействия при обнаружении компьютерных инцидентов, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак	2	2	2	–	–	–	–	–	–	ОК1-6, ПК1	–	2	–

Наименование разделов, тем	Объем времени, отведенный на освоение разделов, тем, час									Коды формируемых компетенций	Формы контроля	Уровень усвоения	
	Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия			Самостоятельная работа					
		Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы			лекции	практические занятия
			лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия						
1.3 Порядок категорирования объектов критической информационной инфраструктуры	3	3	1	2	–	–	–	–	–	ОК1-6, ПК1	–	2	3
1.4 Необходимые организационные меры по обеспечению безопасности объектов критической информационной инфраструктуры	3	3	1	2	–	–	–	–	–	ОК1-6, ПК1	–	2	3
1.5 Необходимые технические меры по обеспечению безопасности объектов критической информационной инфраструктуры	3	3	1	2	–	–	–	–	–	ОК1-6, ПК1	–	2	3
1.6 Внутренний контроль Общества в области обеспечения безопасности объектов критической информационной инфраструктуры	3	3	1	2	–	–	–	–	–	ОК1-6, ПК1	–	2	3
1.7 Реализация комплексных целевых программ по обеспечению безопасности значимых объектов критической информационной инфраструктуры	3	3	1	2	–	–	–	–	–	ОК1-6, ПК1	–	2	3
Итого	**18**	**18**	**8**	**10**	–	–	–	–	–	–	Зачет	–	–

* Промежуточная аттестация проводится в форме устного опроса за счет часов, отведенных на изучение дисциплины. Перечень вопросов для устного опроса представлен в Разделе 10.1.1 учебно–программной документации

П р и м е ч а н и е – Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т. п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

9.1.2 Содержание учебной спецдисциплины «Обеспечение информационной безопасности объектов критической информационной инфраструктуры»

1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации

Тема 1.1 Общие требования законодательства в сфере критической информационной инфраструктуры

Цели и задачи реализации ФЗ от 26.07.2017 года № 187 «О безопасности критической информационной инфраструктуры Российской Федерации»;

Правила категорирования объектов КИИ РФ;

Требования к созданию сил обеспечения безопасности объектов КИИ;

Функции участников системы безопасности значимых объектов КИИ;

Планирование и реализация мероприятий по обеспечению безопасности объектов КИИ;

Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ;

Государственный контроль в области обеспечения безопасности объектов КИИ.

Тема 1.2 Порядок взаимодействия при обнаружении компьютерных инцидентов, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак

Политика управления инцидентами информационной безопасности и компьютерными инцидентами в ООО «Газпром добыча Надым», Положение о группе реагирования на инциденты информационной безопасности ООО «Газпром добыча Надым», Классификатор инцидентов информационной безопасности, компьютерных инцидентов (Приказ Общества от 20.06.2022 ОД-1656);

Регламент реагирования на компьютерные инциденты значимых объектов критической информационной инфраструктуры ООО «Газпром добыча Надым» (приказ Общества от 20.12.2023 № ОД-2818);

План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (приказом Общества от 13.10.2023 № ОД-2174).

Тема 1.3 Порядок категорирования объектов критической информационной инфраструктуры

Определение постоянно действующей комиссии по категорированию объектов КИИ Общества;

Определение перечня объектов КИИ Общества, подлежащих категорированию;

Определение угроз безопасности информации, их возможных последствий и категорий нарушителей в отношении объекта КИИ;

Определение состава программных и программно-аппаратных средств, входящих в состав объекта КИИ.

Практические занятия

Просмотр видеофильма «Создание системы обеспечения безопасности объектов КИИ (АСУ ТП). Типовые ошибки на этапах категорирования, проектирования и внедрения». Обсуждение проблемных вопросов по теме. Рассмотрение нормативной правовой базы.

Тема 1.4 Необходимые организационные меры по обеспечению безопасности объектов критической информационной инфраструктуры

Установление контролируемой зоны;

Физический доступ;

Определение компенсирующих мероприятий;

Разработка организационно-распорядительных документов:

– описание настроек параметров безопасности прикладного и общесистемного ПО;

– описание настроек параметров безопасности антивирусных средств

– защиты;

– описание настроек средств межсетевого экранирования;

– структурная и логическая схема объекта КИИ;

– правила взаимодействия средств межсетевого экранирования;

– паспорта активного сетевого оборудования;

– матрица доступа прикладного и общесистемного ПО;

– график резервного копирования информационных активов АСУ ТП;

– акты выполненных работ по ТО;

– журнал регистрации результатов проверки СНИ и мобильных ПТУ;

– перечень ОРД для ознакомления сил обеспечения безопасности объектов КИИ и сторонних организаций, привлекаемых к работам на объекте КИИ.

Практические занятия

Просмотр видеофильма «Использование программного комплекса Acronis Backup Advanced для управления системой резервного копирования на предприятии».

Обсуждение проблемных вопросов по теме. Рассмотрение нормативной правовой базы.

Тема 1.5 Необходимые технические меры по обеспечению безопасности объектов критической информационной инфраструктуры

Функционирование объектов КИИ в отдельных сегментах сетей технологических объектов. Антивирусная защита. Идентификация и аутентификация. Управление доступом:

Защита машинных носителей;

Аудит безопасности;

Обеспечение целостности;

Обеспечение доступности;

Защита технических средств и систем;

Защиты информационной (автоматизированной) системы и её компонентов.

Практические занятия

Просмотр видеофильма «Применение Efros Config Inspector для защиты АСУ ТП (187 ФЗ)». Обсуждение проблемных вопросов по теме. Рассмотрение нормативной правовой базы.

Тема 1.6 Внутренний контроль Общества в области обеспечения безопасности объектов критической информационной инфраструктуры

Проведение внутреннего контроля организации работ по обеспечению безопасности объектов КИИ и эффективности принимаемых организационных и технических мер. План проведения проверки соблюдения требований безопасности на объектах КИИ Общества. Результаты проведения внутреннего контроля работ по обеспечению безопасности объектов КИИ. Типовые нарушения, выявленные на объектах КИИ Общества.

Практические занятия

Просмотр видеоролика «Поговорим о КИИ». Обсуждение проблемных вопросов по теме. Рассмотрение нормативной правовой базы.

Тема 1.7 Реализация комплексных целевых программ по обеспечению безопасности значимых объектов критической информационной инфраструктуры

Сроки проведения проектно-изыскательских работ (ПИР), разработки рабочей документации (РД) и капитального строительства (КС).

Основные технические решения по дооснащению систем безопасности средствами защиты информации. Типовая структурная схема комплекса технических средств.

Практические занятия

Просмотр видеоролика «Обзор нововведений ПК Efros ACS. Презентация многофункционального комплекса по защите сетевой инфраструктуры Efros Defence Operations». Обсуждение проблемных вопросов по теме. Рассмотрение нормативной правовой базы.

9.2 Структура и содержание учебной дисциплины «Охрана труда и промышленная безопасность»

9.2.1 Учебно-тематический план

Наименование разделов, тем		Объем времени, отведенный на освоение разделов, тем, час									Коды формируемых компетенций	Формы контроля**	Уровень усвоения	
		Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия			Самостоятельная работа*					
			Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы			лекции	практические занятия
				лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия						
1	Законодательство в области охраны труда и промышленной безопасности	1	1	–	–	–	–	–	1	1	ОК1-2		–	3
2	Организация охраны труда и промышленной безопасности в ООО «Газпром добыча Надым»	1	1	–	–	–	–	–	1	1			–	3
	Промежуточная аттестация	–	–	–	–	–	–	–	–	–		зачет		
	Итого	**2**	2	–	–	–	–	–	2	2	–	–	–	–

* Осуществляется с использованием компьютерных обучающих систем, разрабатываемых в ЧУ ДПО «Газпром ОНУТЦ». Перечень рекомендуемых наглядных пособий и ИОС приведен в разделе 11.2.2 учебно–программной документации.

** Промежуточная аттестация по разделу в форме зачета (тестирование в ЭУМП) проводится за счет часов, отведенных на изучение данного раздела.

П р и м е ч а н и е – Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т. п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

9.2.2 Содержание программы учебной дисциплины «Охрана труда и промышленная безопасность»

Тема 1 Законодательство в области охраны труда и промышленной безопасности

Основные понятия и задачи охраны труда и промышленной безопасности.

Изменения в законодательстве в области охраны труда и промышленной безопасности. Управление безопасностью труда. Обязанности организации, эксплуатирующей опасный производственный объект. Обязанности работников опасного производственного объекта. Требования промышленной безопасности по готовности к действиям по локализации и ликвидации последствий аварии на опасном производственном объекте. Производственный контроль за соблюдением требований промышленной безопасности. Обязательное страхование гражданской ответственности за причинение вреда в результате аварии или инцидента на опасном производственном объекте.

Ответственность за нарушение законодательства в области охраны труда и промышленной безопасности.

Самостоятельная работа

Анализ нарушений законодательства в области охраны труда и промышленной безопасности на конкретных примерах. Практическое изучение новых и анализ основных изменений в действующих нормативных и технических документах по охране труда и промышленной безопасности в ПАО «Газпром».

Работа на персональном компьютере с применением ЭУМП «Основы управления охраной труда в организации».

Тема 2 Организация охраны труда и промышленной безопасности в ООО «Газпром добыча Надым»

Самостоятельная работа

Работа на персональном компьютере с применением ЭУМП «Основы управления охраной труда в организации».

9.3 Структура и содержание учебной дисциплины «Охрана окружающей среды и экологическая безопасность»

9.3.1 Учебно-тематический план

Наименование разделов, тем		Объем времени, отведенный на освоение разделов, тем, час									Коды формируемых компетенций	Формы контроля**	Уровень усвоения	
		Всего	Обязательные аудиторные учебные занятия			Дистанционные занятия			Самостоятельная работа*					
			Всего	из них		Всего	из них		Всего	в т. ч. консультаций при выполнении самостоятельной работы				
				лекции	практические занятия (деловые игры, тренинги)		лекции	практические занятия					лекции	практические занятия
1	Охрана окружающей среды. Основные понятия. Законодательство в области экологической безопасности	1	1	–	–	–	–	–	1	1	ОК1-2		–	3
2	Экологический менеджмент ПАО «Газпром»	1	1	–	–	–	–	–	1	1			–	3
	Промежуточная аттестация	–	–	–	–	–	–	–	–	–		зачет		
	Итого	**2**	2	–	–	–	–	–	2	2	–	–	–	–

* Осуществляется с использованием компьютерных обучающих систем, разрабатываемых в ЧУ ДПО «Газпром ОНУТЦ». Перечень рекомендуемых наглядных пособий и ИОС приведен в разделе 11.2.2 учебно–программной документации.

** Промежуточная аттестация по разделу в форме зачета (тестирование в ЭУМП) проводится за счет часов, отведенных на изучение данного раздела.

П р и м е ч а н и е – Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т. п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

9.3.2 Содержание программы учебной дисциплины «Охрана окружающей среды и экологическая безопасность»

Тема 1 Охрана окружающей среды. Основные понятия.

Законодательство в области экологической безопасности. Понятия и категории экологии. Роль экологии в охране природной среды и рациональном природопользовании. Окружающая среда как система, ее составные части и степень устойчивости. Основные экологические проблемы на объектах нефтегазового комплекса. Использование природных ресурсов. Негативное воздействие на окружающую среду. Загрязнение окружающей среды. Обзор современных подходов к решению экологических проблем в ПАО «Газпром». Меры снижения антропогенной нагрузки на окружающую среду при осуществлении производственной деятельности.

Российское законодательство в области экологической безопасности и охраны окружающей среды. Основы государственной экологической политики Российской Федерации. Международные обязательства Российской Федерации в области охраны окружающей среды.

Самостоятельная работа

Работа на персональном компьютере с АОС «Основы природоохранной деятельности».

Тема 2 Экологический менеджмент ПАО «Газпром»

Основы экологического менеджмента. Экологический менеджмент как часть общей системы корпоративного управления. Экологическая политика ПАО «Газпром». Система экологического менеджмента ПАО «Газпром». Порядок функционирования системы экологического менеджмента ПАО «Газпром». Координационный комитет ПАО «Газпром» по вопросам охраны окружающей среды и энергоэффективности. Экологическая политика и соответствующие обязательства ПАО «Газпром», дочернего общества. Планирование в системе экологического менеджмента. Управление рисками, экологическими аспектами. Экологические цели и планы по их реализации.

Самостоятельная работа

Работа на персональном компьютере с АОС «Основы природоохранной деятельности».

10 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

10.1 Комплект контрольно-оценочных средств

Оценка качества освоения программ повышения квалификации специалистов включает промежуточную аттестацию в форме устного опроса с применением перечня вопросов, представленных в разделе 10.1.1. и итоговую аттестацию в форме экзамена (итогового тестирования) с применением обучающе-контролирующей системы ОЛИМПОКС.

Результатом освоения программы является готовность слушателя к выполнению видов деятельности - «Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации», «Внедрение систем защиты информации автоматизированных систем».

10.1.1 Перечень вопросов для промежуточной аттестации по разделу 1

1. Назовите федеральный закон, лежащий в основе обеспечения безопасности КИИ РФ (187-ФЗ)
2. Какие 2 федеральных органа определены указами Президента уполномоченными в области обеспечения безопасности КИИ РФ? (ФСТЭК России и ФСБ России)
3. В каких сферах функционируют объекты КИИ РФ? А в ООО «Газпром добыча Надым»? (ТЭК, Энергетика, транспорт, телекоммуникации и связь, здравоохранение, банковская сфера и т.д.; в ГДН – ТЭК)
4. Какой главный подход предусмотрен законодательством при обеспечении безопасности КИИ? (Каким образом и по какому принципу дифференцируют объекты КИИ) (Категорирование по уровням значимости, 3 уровня)
5. Какие документы, касающиеся объектов КИИ, обязан сформировать субъект КИИ для направления в адрес ФСТЭК России? Установлены ли сроки? (Перечень ОКИИ, подлежащих категорированию, сведения об ОКИИ, установлены 10, 20 рабочих дней).
6. Какие функциональные типы подразделений предусмотрены, при формировании сил обеспечения безопасности значимых объектов КИИ, согласно Приказу ФСТЭК России № 235 "Об утверждении Требований к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования? (Подразделение по безопасности, эксплуатирующие, обеспечивающие функционирование)
7. Какие виды ответственности предусмотрены законодательством за нарушения требований 187-ФЗ и принятых в соответствии с ним нормативных правовых актов по обеспечению безопасности КИИ РФ? (Административная, уголовная)
8. Какая организация обеспечивает координацию деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий

компьютерных атак и реагирования на компьютерные инциденты (КИ)? (Национальной координационный центр по компьютерным инцидентам (НКЦКИ))

9. Какие группы организованы в ПАО «Газпром» и его ДОО для обработки инцидентов ИБ в течение их жизненного цикла? (ГРИИБ – в ДОО, КГРИИБ в СКЗ ПАО «Газпром»)

10. Какие инциденты ИБ являются компьютерными инцидентами (КИ)? (приведшие к нарушению функционирования объекта КИИ)

11. Обеспечение каких трех свойств информации образуют «фундамент» информационной безопасности? (доступность, целостности, конфиденциальность)

12. Сколько классов выделяется компьютерных инцидентов (КИ)? (3 класса)

13. Какой документ оформляется группой реагирования на инциденты информационной безопасности (ГРИИБ) субъекта КИИ в рамках реагирования на компьютерный инцидент (КИ) и передается через КГРИИБ в НКЦКИ? (карточка учета КИ, состоящая из 2 частей)

14. Как дифференцируются уровни опасности проведения целевых компьютерных атак на информационную инфраструктуру РФ? (3 уровня: Желтый, оранжевый, красный)

15. Какой «орган» создается в организации-субъекте КИИ для проведения категорирования, в соответствии с правилами категорирования объектов КИИ (постановление Правительства РФ от 8 февраля 2018 г. № 127? (постоянно действующая комиссия по категорированию)

16. Перечислите основные этапы категорирования:

1) Определение процессов, в рамках видов деятельности Общества,

2) Выявление среди них критических процессов – процессов, нарушение и (или) прекращение которых может привести к негативным последствиям, выраженным в показателях критериев значимости,

3) определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов.

4) формирование перечня ОКИИ, подлежащих категорированию

17. Какие программно-аппаратные средства включаются в состав объекта КИИ? (АРМ, серверы, коммутаторы, ПЛК, межсетевые экраны)

18. Какой процесс, обязательный в рамках категорирования объекта КИИ, определяет, существует ли возможность возникновения компьютерного инцидента на объекте КИИ? (анализ угроз безопасности информации)

19. Каким образом приказом ФСТЭК от 25 декабря 2017 г. № 239 организовано представление состава мер обеспечения безопасности для объектов КИИ? (Меры разбиты на группы (17 шт.) по направлениям защиты, и соотнесены с 3 категориями значимости объектов КИИ)

20. Как обеспечивается выполнение мер, которые невозможно полностью реализовать с помощью имеющихся СЗИ? (Разрабатываются и принимаются компенсирующие меры)

21. Перечислите основные группы мер:

1) Идентификация и аутентификация (ИАФ)

2) Управление доступом (УПД)

3) Защита технических средств и систем (ЗТС)

4) Аудит безопасности (АУД)

5) Антивирусная защита (АВЗ)

22. Допускается ли невыполнение на объекте КИИ каких-либо мер, предусмотренных «Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденными Приказом ФСТЭК от 25 декабря 2017 г. № 239? (Да, по результатам адаптации по каждому ОКИИ, например, при несоответствии категории значимости, отсутствии защищаемого компонента (не имеет смысла) или в связи с невозможностью реализации (в частности без значительных затрат)).

23. Какой главный принцип организации вычислительной сети лежит в основе обеспечения функционирования объекта КИИ? (Функционирование объекта КИИ должно быть обеспечено в отдельных сегментах сетей технологических объектов дочерних обществ путём физического выделения сегмента сети, использования специальных шин (интерфейсов взаимодействия) или применения средств межсетевого экранирования).

24. Какие нарушители (внутренние, внешние) а также векторы атак характерны для объектов КИИ Общества – АСУ ТП? (Только внутренние: работники Общества и подрядных организаций; подключение съемных носителей и мобильных устройств к техническим средствам АСУ ТП, в том числе как следствие – вирусное заражение).

25. Какими средствами обеспечивается защита от вирусного заражения? (применение антивирусного ПО, блокирование подключения съемных носителей, реализация организационно-технических мероприятий).

26. Какими основными способами достигается безопасность на АРМ и серверах АСУ ТП? (Безопасная настройка BIOS: пароль, ограничение загрузки, отключение неиспользуемых портов; Операционной системы: управление пользователями и паролями, настройка политик регистрации событий, отключение или удаление компонентов неиспользуемого ПО, настройка ограничения подключения устройств; Специального ПО (SCADA): управление пользователями и паролями, настройка политик регистрации событий)

27. Проведение какого мероприятия, согласно пунктам 35 и 36 Приказа ФСТЭК России «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования» от 21.12.2017 № 235, должно осуществляться в рамках контроля состояния безопасности значимых объектов КИИ, и с какой периодичностью? (Внутренний контроль организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер, не реже, чем раз в 3 года)

28. Какие основные 3 направления подлежат проверке в ходе Внутреннего контроля? (ОРД по безопасности КИИ, Архитектуру сети объекта КИИ, настройки программно-аппаратных средств)

29. Какие типовые недостатки чаще всего выявляются в ходе Внутреннего контроля?

30. Какие документы оформляются и утверждаются по результатам Внутреннего контролся? (Акт Внутреннего контроля. План устранения недостатков, выявленных в ходе проведения внутреннего контроля…)

31. Какие уровни иерархии создаются в рамках создаваемой системы безопасности? (технологические объекты, филиалы и администрация Общества)

32. Какие системы включены в состав подсистем безопасности КИИ Общества?

33. Какие обязанности возложены на ДО в рамках подготовки к строительству и введению в эксплуатацию СБ и ПсБКИИ?

10.1.2 Перечень тестовых дидактических материалов для итогового тестирвания

Вопрос № 1 Какой закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак?

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

Ответы:

1 ФЗ-187
2 ФЗ-98
3 ФЗ-152
4 ФЗ-184

Вопрос № 2 Когда вступил в действие ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации»?

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

Ответы:

1 2016
2 2019
3 2017
4 2018

Вопрос № 3 Ключевые полномочия ФСТЭК России в области обеспечения безопасности КИИ?

1) Требования по обеспечению безопасности;
2) Требования к созданию систем безопасности;
3) Оценка безопасности;
4) Требования к средствам ГосСОПКА

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

Ответы:

1 1 и 3;
2 3 и 4;
3 1 и 2;

4 1 и 4

Вопрос № 4 Ключевые полномочия ФСБ России в области обеспечения безопасности КИИ?

1) реестр значимых объектов КИИ;
2) госконтроль обеспечения безопасности;
3) перечень информации, представляемой в ГосСОПКА;
4) Национальный координационный центр по компьютерным инцидентам;

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

Ответы:

1 2 и 3;
2 3 и 4;
3 1 и 2;
4 1 и 4

Вопрос № 5 Ключевые полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ возложены на:

1) ФСБ России;
2) ФСТЭК России;
3) МВД России;
4) ФССП России;

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

Ответы:

1 1 и 3;
2 3 и 4;
3 2;
4 1 и 2.

Вопрос № 6 В соответствии с ФЗ-187 под субъектами КИИ понимают:

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

Ответы:

1 Уполномоченные федеральные органы исполнительной власти;
2 Информационные системы, информационно-телекоммуникационные сети, а также автоматизированные системы управления субъектов критической информационной инфраструктуры, функционирующие в 13 сферах;
3 Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели.

Вопрос № 7 Что представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, и проверку сведений о результатах ее присвоения?

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

Ответы:
1 Классификация;
2 Категорирование;
3 Перечисление.

Вопрос № 8 Каким Постановлением Правительства РФ утверждены Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений?

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

Ответы:
1 № 127;
2 № 162;
3 № 743;
4 № 808.

Вопрос № 9 Сколько критериев значимости объектов КИИ существует для присвоения категории?

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

Ответы:
1 3 (духовная, социальная, экологическая);
2 5 (социальная, политическая, экономическая, экологическая, значимость для обеспечения обороны страны, безопасности государства и правопорядка);
3 6 (социальная, экологическая, духовная, политическая, экономическая, значимость для обеспечения обороны страны, безопасности государства и правопорядка);
4 4 (социальная, политическая, экономическая, экологическая).

Вопрос № 10 Какая категория значимости объектов КИИ является самой высокой?

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

Ответы:
1 Первая;
2 Вторая;
3 Третья;
4 Без категории.

Вопрос № 11 1Какие критерии являются самыми значимыми в нашем обществе?

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

Ответы:
1 Экологическая, политическая;
2 Социальная, экономическая;

3 Социальная, экологическая;
4 Для обеспечения обороны страны, безопасности государства и правопорядка, политическая.

Вопрос № 12 К какому критерию значимости относится прекращение или нарушение функционирования объектов транспортной инфраструктуры?

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

Ответы:
1 Социальная значимость;
2 Политическая значимость;
3 Экономическая значимость;
4 Значимость для обороны страны, безопасности государства и правопорядка.

Вопрос № 13 К какому критерию значимости относится вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия?

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

Ответы:
1 Социальная значимость;
2 Политическая значимость;
3 Экологическая значимость;
4 Значимость для обороны страны, безопасности государства и правопорядка.

Вопрос № 14 В какой срок после утверждения направляется Перечень объектов КИИ, подлежащих категорированию, в печатном и электронном виде в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ?

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

Ответы:
1 10 рабочих дней;
2 14 дней;
3 1 месяц;
4 3 месяца.

Вопрос № 15 В какой срок, после утверждения Акта категорирования субъект КИИ должен направить в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости

присвоения ему одной из таких категорий?

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

Ответы:

1 10 рабочих дней;
2 14 дней;
3 1 месяц;
4 3 месяца.

Вопрос № 16 В какой срок, в случае изменений сведений об объекте КИИ, субъект КИИ должен направить в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, новые сведения в печатном и электронном виде?

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

Ответы:

1 10 дней;
2 20 рабочих дней;
3 1 месяц;
4 3 месяца.

Вопрос № 17 Кто пересматривает установленные категории значимости?

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

Ответы:

1 ФСБ России;
2 ФСТЭК России;
3 субъект КИИ;
4 объект КИИ.

Вопрос № 18 Пересмотр установленных категорий значимости осуществляется:

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

Ответы:

1 Не реже 1 раза в 1 год;
2 Не реже 2 раз в 1 год;
3 Не реже 1 раза в 3 года;
4 Не реже 1 раза в 5 лет.

Вопрос № 19 В каком приказе ФСТЭК России прописаны требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования»:

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

Ответы:

1 № 227;
2 № 229;
3 № 235;
4 № 236.

Вопрос № 20 Какие подразделения входят в состав сил по обеспечению безопасности объектов КИИ?

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

Ответы:

1 Подразделения, ответственные за обеспечение безопасности значимых объектов КИИ; подразделения, эксплуатирующие значимые объекты КИИ; подразделения, обеспечивающие функционирование значимых объектов КИИ;
2 Подразделения, эксплуатирующие значимые объекты КИИ; подразделения, обеспечивающие функционирование значимых объектов КИИ;
3 Подразделения, обеспечивающие функционирование значимых объектов КИИ;
4 Подразделения, ответственные за обеспечение безопасности значимых объектов КИИ.

Вопрос № 21 В функции руководителя субъекта КИИ входит:
1) создание системы безопасности, организация и контроль ее функционирования;
2) проведение анализа угроз безопасности информации;
3) определение состава и структуры системы безопасности;
4) обеспечение реализации требований по обеспечению безопасности значимых объектов КИИ;
5) создание или определение структурного подразделения, ответственного за обеспечение безопасности значимых объектов КИИ;
6) осуществление реагирования на компьютерные инциденты;

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

Ответы:

1 1, 2 и 5;
2 1, 3 и 5;
3 2, 3 и 4;
4 3, 4 и 5.

Вопрос № 22 В функции структурного подразделения по безопасности входит:
1) разработка предложений по совершенствованию организационно-распорядительных документов по безопасности значимых объектов КИИ;
2) определение состава и структуры системы безопасности;
3) создание системы безопасности, организация и контроль ее функционирования;
4) проведение анализа угроз безопасности информации;
5) создание или определение структурного подразделения, ответственного за обеспечение безопасности значимых объектов КИИ;
6) осуществлять реагирование на компьютерные инциденты;

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

Ответы:

1 1, 2 и 5;
2 1, 3 и 5;
3 1, 4 и 6;

4 3, 4 и 5.

Вопрос № 23 В функции структурного подразделения, эксплуатирующего значимый объект КИИ входит:

1) эксплуатация значимых объектов критической информационной инфраструктуры в соответствии с правилами безопасности, установленными организационно-распорядительными документами по безопасности значимых объектов (инструкциями, руководствами);
2) определение состава и структуры системы безопасности;
3) создание системы безопасности, организация и контроль ее функционирования;
4) осуществление действий в нештатных ситуациях в ходе эксплуатации значимого объекта;
5) создание или определение структурного подразделения, ответственного за обеспечение безопасности значимых объектов КИИ;
6) осуществлять реагирование на компьютерные инциденты;

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

Ответы:
1 1, 2, 4;
2 1, 4, 6;
3 2,5, 6;
4 4, 5, 6.

Вопрос № 24 В функции структурного подразделения, обеспечивающего функционирование входит:

1) эксплуатация значимых объектов критической информационной инфраструктуры в соответствии с правилами безопасности, установленными организационно-распорядительными документами по безопасности значимых объектов (инструкциями, руководствами);
2) определение состава и структуры системы безопасности;
3) создание системы безопасности, организация и контроль ее функционирования;
4) осуществление действий в нештатных ситуациях в ходе эксплуатации значимого объекта;
5) создание или определение структурного подразделения, ответственного за обеспечение безопасности значимых объектов КИИ;
6) осуществлять реагирование на компьютерные инциденты;

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

Ответы:
1 1, 2, 4;
2 1, 2, 5;
3 1, 2, 6;
4 2, 4, 6.

Вопрос № 25 В каком нормативном документе Общества прописаны функции участников системы безопасности значимых объектов КИИ?

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

Ответы:
1 Приказ от 22.01.2024 № ОД-163;
2 Приказ от 13.10.2023 № ОД-2174;
3 Приказ от 24.08.2023 № ОД-1848;
4 Приказ от 03.03.2023 № ОД-535.

Вопрос № 26 Основанием для проведения плановых проверок федеральным органом исполнительной власти, уполномоченных в области обеспечения безопасности КИИ РФ, на соблюдение субъектом КИИ требований по обеспечению безопасности объектов КИИ служат:
1) истечение 3 лет с занесения сведений в реестр значимых объектов КИИ;
2) истечение срока предписания об устранении выявленного нарушения требований по обеспечению безопасности объектов КИИ;
3) истечение 3 лет проведения последней плановой проверки в отношении значимого объекта КИИ;
4) возникновение компьютерного инцидента, повлекшего негативные последствия, на объекте КИИ;
5) требование прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов;

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

Ответы:
1 1 и 2;
2 4 и 5;
3 2 и 4;
4 1 и 3.

Вопрос № 27 Основанием для внеплановых проверок федеральным органом исполнительной власти, уполномоченных в области обеспечения безопасности КИИ РФ, на соблюдение субъектом КИИ требований по обеспечению безопасности объектов КИИ служат:
1) истечение 3 лет с занесения сведений в реестр значимых объектов КИИ;
2) истечение срока предписания об устранении выявленного нарушения требований по обеспечению безопасности объектов КИИ;
3) истечение 3 лет проведения последней плановой проверки в отношении значимого объекта КИИ;
4) возникновение компьютерного инцидента, повлекшего негативные последствия, на объекте КИИ;
5) требование прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов.

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

Ответы:
1 1, 2 и 5;
2 1, 4 и 5;
3 2, 4 и 5;
4 1, 2 и 3.

Вопрос № 28 В каком приказе ФСТЭК России прописаны функции участников системы безопасности значимых объектов КИИ?

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

Ответы:

1 № 239;
2 № 235;
3 № 229;
4 № 227.

Вопрос № 29 В статье 13.12.1 ч.1 КоАП РФ за нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния влечет за собой административный штраф:

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

Ответы:

1 На должностных лиц в размере от 10 тысяч до 50 тысяч руб.; на юридических лиц - от 100 тысяч до 500 тысяч руб.;
2 На должностных лиц в размере от 10 тысяч до 50 тысяч руб.; на юридических лиц - от 50 тысяч до 100 тысяч руб.;
3 На должностных лиц в размере от 20 тысяч до 50 тысяч руб.; на юридических лиц - от 100 тысяч до 500 тысяч руб.;
4 На должностных лиц в размере от 50 тысяч до 100 тысяч руб.; на юридических лиц - от 100 тысяч до 200 тысяч руб.

Вопрос № 30 В статье 13.12.1 ч.3 за нарушение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты влечет за собой административный штраф:

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

Ответы:

1 На должностных лиц в размере от 10 тысяч до 50 тысяч руб.; на юридических лиц - от 100 тысяч до 500 тысяч руб.;

2 На должностных лиц в размере от 10 тысяч до 50 тысяч руб.; на юридических лиц - от 50 тысяч до 100 тысяч руб.;
3 На должностных лиц в размере от 20 тысяч до 50 тысяч руб.; на юридических лиц - от 100 тысяч до 500 тысяч руб.;
4 На должностных лиц в размере от 50 тысяч до 100 тысяч руб.; на юридических лиц - от 100 тысяч до 200 тысяч руб.

Вопрос № 31 В статье 274.1 ч.1 УК РФ за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации» влечет за собой:

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

Ответы:
1 Принудительные работы на срок до 5 лет с ограничением свободы на срок до 2 лет или без такового; либо лишение свободы на срок от 2 до 5 лет со штрафом в размере от 500 тысяч до 1 миллиона руб. или в размере заработной платы или иного дохода, осужденного за период от 1 года до 3 лет;
2 Принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового; либо лишение свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового;
3 Лишение свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового;
4 Лишение свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

Вопрос № 32 Национальный координационный центр по компьютерным инцидентам (НКЦКИ) обеспечивает координацию деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. На скольких уровнях реализуется координация действий в ПАО «Газпром» и его дочерних обществах и организациях?

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

Ответы:
1 3 (Службы корпоративной защиты ПАО «Газпром», администрации, филиалов дочерних обществ);

2 4 (Службы корпоративной защиты ПАО «Газпром», администрации, филиалов и технологических объектов дочерних обществ);
3 2 (Службы корпоративной защиты ПАО «Газпром» и технологических объектов дочерних обществ);
4 1(Службы корпоративной защиты ПАО «Газпром»).

Вопрос № 33 На каком уровне выполняется проведение тренировки по отработке реагирования на компьютерные инциденты?
Укажите **правильный** ответ (или ответы).

Ответы:
1 Администрации, филиалов и технологических объектов дочерних обществ;
2 Уровне филиалов и технологических объектов дочерних обществ;
3 Администрации;
4 Службы корпоративной защиты ПАО «Газпром».

Вопрос № 34 На каком уровне выполняется Информирование руководства Общества об обнаруженных компьютерных инцидентах?
Укажите **правильный** ответ (или ответы).

Ответы:
1 Администрации, филиалов и технологических объектов дочерних обществ;
2 Уровне филиалов и технологических объектов дочерних обществ;
3 Администрации;
4 Службы корпоративной защиты ПАО «Газпром».

Вопрос № 35 На каком уровне выполняется Обнаружение инцидентов ИБ, имеющих признаки компьютерных инцидентов?
Укажите **правильный** ответ (или ответы).

Ответы:
1 Администрации, филиалов и технологических объектов дочерних обществ;
2 Уровне филиалов и технологических объектов дочерних обществ;
3 Администрации;
4 Службы корпоративной защиты ПАО «Газпром».

Вопрос № 36 На каком уровне выполняется взаимодействие с ФСБ России?
Укажите **правильный** ответ (или ответы).

Ответы:
1 Администрации, филиалов и технологических объектов дочерних обществ;
2 Уровне филиалов и технологических объектов дочерних обществ;
3 Администрации;
4 Службы корпоративной защиты ПАО «Газпром».

Вопрос № 37 Каким нормативным документом Общества утвержден План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак?
Укажите **правильный** ответ (или ответы).

Ответы:
1 Приказ от 20.12.2022 № 2983;
2 Приказ от 02.06.2023 № 1024;
3 Приказ от 13.10.2024 № ОД-2174;
4 Приказ от 26.09.2023 № 2060

Вопрос № 38 Какой термин относится к определению «целенаправленное воздействие программно-аппаратных средств на объекты КИИ, сети электросвязи объекта КИИ, в целях нарушения и (или) прекращения их функционирования, и (или) создания угрозы безопасности обрабатываемой информации объекта КИИ»

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

Ответы:
1 Компьютерный инцидент;
2 Компьютерная атака;
3 Инцидент информационной безопасности

Вопрос № 39 Что понимают под информационной безопасностью?

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

Ответы:
1 Конфиденциальность;
2 Доступность;
3 Целостность;
4 Состояние защищенности.

Вопрос № 40 К какому классу относятся компьютерные инциденты, связанные с несанкционированным доступом к информационным ресурсам Объекта КИИ?

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

Ответы:
1 Класс 1;
2 Класс 2;
3 Класс 3.

Вопрос № 41 К какому классу относятся компьютерные инциденты, связанные с блокированием доступности элементов Объекта КИИ?

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

Ответы:
1 Класс 1;
2 Класс 2;
3 Класс 3.

Вопрос № 42 К какому классу относятся компьютерные инциденты, связанные с непреднамеренным нарушением штатного режима функционирования Объекта КИИ в целом или его отдельных

элементов?

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

Ответы:

1 Класс 1;
2 Класс 2;
3 Класс 3.

Вопрос № 43 В соответствие с каким приказом ФСБ разрабатывается план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак?

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

Ответы:

1 № 282;
2 № 366;
3 № 281;
4 № 196.

Вопрос № 44 Сколько карточек оформляется на компьютерные инциденты?

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

Ответы:

1 1;
2 2;
3 3;
4 4.

Вопрос № 45 К какому уровню опасности относится мероприятие по внеплановой проверке соблюдения ограничений на использование на объектах КИИ личных средств вычислительной техники (ноутбуков, планшетов, смартфонов), модемов и иных съемных носителей информации и правил безопасного использования таких средств?

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

Ответы:

1 Желтый;
2 Оранжевый;
3 Красный.

Вопрос № 46 К какому уровню опасности относится мероприятие по смене аутентификаторов (паролей) учетных записей пользователей программного обеспечения, установленного на соответствующих узлах сети?

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

Ответы:

1 Желтый;
2 Оранжевый;
3 Красный.

Вопрос № 47 К какому уровню опасности относится мероприятие по организации круглосуточного мониторинга информационной безопасности объектов КИИ?

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

Ответы:

1 Желтый;
2 Оранжевый;
3 Красный.

Вопрос № 48 Какие этапы категорирование объектов КИИ?

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

Ответы:

1 Определение постоянно действующей комиссии, определение критических процессов субъекта КИИ, определение перечня объектов категорирования, категорирование объектов КИИ, отправка актов категорирования в ФСТЭК России;
2 Определение постоянно действующей комиссии, определение перечня объектов категорирования, отправка актов категорирования в ФСТЭК России;
3 Определение критических процессов субъекта КИИ, определение перечня объектов категорирования, категорирование объектов КИИ, отправка актов категорирования в ФСТЭК России;
4 Определение критических процессов субъекта КИИ, категорирование объектов КИИ, отправка актов категорирования в ФСТЭК России.

Вопрос № 49 Кто входит в состав комиссии по категорированию объектов КИИ?

1) руководитель субъекта КИИ или уполномоченное им лицо;

2) работники субъекта КИИ, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности и в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов;

3) работники ФСБ России;

4) работники ФСТЭК России;

5) работники субъекта КИИ, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры;

6) работники подразделения по защите государственной тайны субъекта КИИ (в случае, если объект КИИ обрабатывает информацию, составляющую государственную тайну);

7) работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций;

8) работники сторонних организаций;

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

Ответы:

1 2, 3, 7 и 8;
2 1, 2, 5, 6 и 7;
3 3, 4, 6 и 8;
4 3, 4, 5, 6 и 7.

Вопрос № 50 Каким нормативно правовым актом установлен состав комиссии по категорированию объектов КИИ?

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

Ответы:

1 Постановление Правительства РФ № 127;
2 Постановление Правительства РФ № 162;
3 Постановление Правительства РФ № 808;
4 Постановление Правительства РФ № 743;

Вопрос № 51 Функции комиссии по категорированию?

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

Ответы:

1 Определение объектов КИИ, определение процессов, рассматривает возможные действия
нарушителей в отношении объектов КИИ, оценивает в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ, устанавливает каждому из объектов КИИ одной из категорий значимости либо принимает решение об отсутствии необходимости присвоения им одной из категорий значимости;
2 Определение объектов КИИ, устанавливает каждому из объектов КИИ одной из категорий значимости либо принимает решение об отсутствии необходимости присвоения им одной из категорий значимости;
3 Определение процессов, рассматривает возможные действия нарушителей в отношении объектов КИИ, оценивает в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;
4 Определение процессов, рассматривает возможные действия нарушителей в отношении объектов КИИ, устанавливает каждому из объектов КИИ одной из категорий значимости либо принимает решение об отсутствии необходимости присвоения им одной из категорий значимости.

Вопрос № 52 Какие автоматизированные системы управления технологическим процессом относятся к объектам критической информационной инфраструктуры Общества, в соответствии с методическими рекомендациями по категорированию объектов КИИ в ПАО «Газпром» (документ ПАО)?

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

Ответы:

1 Автоматизированная система управления технологическим процессом установки комплексной подготовки газа, автоматизированная система управления технологическим процессом дожимной компрессорной станции;
2 Автоматизированные системы управления технологическим процессом установки комплексной подготовки газа, автоматизированная система управления технологическим процессом установки предварительной подготовки газа;
3 Автоматизированная система управления технологическим процессом установки подготовки нефти и газа;
4 Автоматизированная система управления технологическим процессом подземного хранилища газа, автоматизированная система управления технологическим процессом дожимной компрессорной станции.

Вопрос № 53 Каким приказом Общества создана постоянно действующая комиссия по категорированию объектов КИИ?

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

Ответы:

1 Приказ от 20.12.2022 № 2983;
2 Приказ от 02.06.2023 № 1024;
3 Приказ от 24.08.2023 № 1848;
4 Приказ от 21.12.2023 № ОД-2836

Вопрос № 54 Какие программно-аппаратные средства не подлежат включению в Акт категорирования объектов КИИ?

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

Ответы:

1 Межсетевые экраны;
2 Модемы, ленточные библиотеки
3 Коммутаторы (в том числе неуправляемые), программируемые логические контроллеры;
4 Автоматизированное рабочее место, сервера, мобильные автоматизированное рабочее место.

Вопрос № 55 К какому типу нарушителей относятся лица, не имеющие права доступа к системе, ее отдельным компонентам и реализующие угрозы безопасности информации(УБИ) из-за границ системы?

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

Ответы:

1 Внешний;
2 Внутренний.

Вопрос № 56 К какому типу нарушителей относятся лица, имеющие право постоянного или разового доступа к системе, ее отдельным компонентам?

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

Ответы:

1 Внешний;
2 Внутренний.

Вопрос № 57 Каким приказом ФСТЭК России был доведен состав мер обеспечения безопасности для объектов КИИ каждой категории?

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

Ответы:

1 Приказом ФСТЭК от 25.12.2017 г. №239;
2 Приказом ФСТЭК от 06.12.2017 г. №227;
3 Приказом ФСТЭК от 21.12.2017 г. №235;
4 Приказом ФСТЭК от 22.12.2017 г. №236.

Вопрос № 58 Укажите, какие из нижеперечисленных компенсирующих мер в физической защите являются верными:

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

Ответы:

1 Антивирусная защита;
2 Аудит безопасности;
3 Защита технических средств и систем;
4 Управление доступом;
5 Идентификация и аутентификация;
6 Все вышеперечисленные

Вопрос № 59 Какие подмеры мер «Аудит безопасности» и «Антивирусная защита» верны? Укажите правильные.

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

Ответы:

1 Защита информации о событиях безопасности;
2 Управление физическим доступом;
3 Защита от внешних воздействий;
4 Обновление базы данных признаков вредоносных компьютерных программ.

Вопрос № 60 Какие подмеры мер «Идентификация и аутентификация» верны? Укажите правильные.

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

Ответы:

1 Реализация антивирусной защиты;
2 Регламентация правил и процедур защиты технических средств и систем;
3 Управление идентификаторами;
4 Управление средствами аутентификации.

Вопрос № 61 Какие подмеры мер «Защита технических средств и систем» верны? Укажите правильные.

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

Ответы:

1 Регламентация правил и процедур защиты технических средств и систем;
2 Управление физическим доступом;
3 Реализация модели управления доступом;
4 Управление действиями пользователей до идентификации и аутентификации.

Вопрос № 62 Какие подмеры мер «Управление доступом» верны? Укажите правильные.

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

Ответы:

1 Назначение минимально необходимых прав и привилегий;
2 Разделение полномочий пользователей;
3 Реализация модели управления доступом;
4 Идентификация и аутентификация устройств.

Вопрос № 63 Каким документом утверждены «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»?

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

Ответы:

1 Приказом ФСТЭК России от 21.12.2017 г. №235;
2 Приказом ФСТЭК России от 06.12.2017 г. №227;
3 Приказом ФСТЭК России от 25.12.2017 г. №239;
4 Приказом ФСТЭК России от 22.12.2017 г. №236.

Вопрос № 64 Приказом ФСТЭК России №239 от 25.12.2017 определено 17 групп мер по обеспечению безопасности для значимого объекта соответствующей категории значимости и требуемыми перечнями мероприятий. Укажите, для какой категории значимости определено наибольшее количество мер.

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

Ответы:

1 2 Категория значимости;
2 3 Категория значимости;
3 1 Категория значимости.

Вопрос № 65 Какие способы сегментирования сети, могут использоваться на значимых объектах критической информационной инфраструктуры? Укажите верный вариант ответа.

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

Ответы:

1 Физическое выделение сегмента сети;
2 Использование специализированных шин;
3 Применение средств межсетевого экранирования;
4 Все вышеперечисленные.

Вопрос № 66 Укажите типовые грубые нарушения, выявляемые на объектах КИИ Общества.

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

Ответы:
1 Некорректная настройка средств межсетевого экранирования;
2 Не осуществляется смена паролей от учетных записей операционной системы на АРМ и серверном оборудовании АСУ ТП;
3 К коммутационному оборудованию АСУ ТП подключены сетевые интерфейсы, не документированные на схемах АСУ ТП;
4 Все вышеперечисленные.

Вопрос № 67 Какие ключевые замечания были выявлены при проверке защиты ОС и общесистемного ПО? Укажите верный.

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

Ответы:
1 Некорректно настроены парольная политика и политика аудита;
2 Не выполняется график резервного копирования конфигурационных файлов средств МЭ и активного сетевого оборудования;
3 Применяется избыточное количество правил к рабочей учетной записи ОС;
4 Не ведется анализ частоты использования правил к рабочей учетной записи ОС.

Вопрос № 68 С какой целью выполняется дооснащение объектов на уровне филиалов и технологических объектов дочерних обществ? Выберите правильные варианты ответов.

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

Ответы:
1 Выявления инцидентов;
2 Контроль защищенности, целостности и непрерывности функционирования систем;
3 Возможности восстановления функционирования систем и обеспечения сетевой безопасности, в том числе при передаче информации об инцидентах с технологических объектов в администрацию дочернего общества;
4 Все вышеперечисленные.

Вопрос № 69 Укажите какую первостепенную задачу эксплуатирующая организация (ООО «Газпром добыча Надым») должна выполнить для проведения работ по вводу в действие ПсБКИИ? Укажите верный.

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

Ответы:

1 Выполнить обновление базы данных признаков вредоносных ПО;
2 Выполнить настройку СЗИ, встроенных в ОС, прикладное ПО и (или) программно-аппаратные средства АСУ ТП;
3 Реализовать модель управления доступом;
4 Разработать перечень правил и процедур защиты технических средств и систем.

Правильные ответы к тестовым дидактическим материалам представлены в таблице № 5

Таблица № - Правильные ответы к перечню тестовых дидактических материалов

№ вопроса	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
№ ответа	1	4	3	2	4	3	2	1	2	1
№ вопроса	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
№ ответа	3	1	3	1	1	2	3	4	3	1
№ вопроса	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
№ ответа	2	3	2	3	1	4	3	2	2	3
№ вопроса	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
№ ответа	1	2	1	3	2	4	3	2	4	1
№ вопроса	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**
№ ответа	2	3	1	2	1	2	3	1	2	1
№ вопроса	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**
№ ответа	1	1	4	2	1	2	1	6	1,4	3,4
№ вопроса	**61**	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**	
№ ответа	1,2	1,2,3	3	3	4	4	1	4	2	

11 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

11.1 Методические рекомендации по организации и проведению учебного процесса

Содержание и объем учебного материала в программе приведены с таким расчетом, чтобы к концу обучения слушатели прочно овладели профессиональными компетенциями, приведенными в данной учебно-программной документации, знаниями, умениями и навыками, необходимыми для выполнения работ по обеспечению безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

Учебным планом и программой предусмотрены самостоятельное обучение, теоретическое обучение (лекции) и практические занятия. Изложение учебного материала реализуется совместно с практической деятельностью слушателей.

При проведении теоретических занятий необходимо использовать различные наглядные пособия, электронные презентации и применять технические средства обучения (проекторы, персональные компьютеры и др.).

Образовательная деятельность по дополнительной профессиональной программе организуется в соответствии с утвержденным расписанием учебных занятий.

Основная цель практических занятий - формирование практических навыков в конфигурировании активного сетевого оборудования.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные производственные условия на производственной площадке при конфигурировании активного сетевого оборудования.

Для проверки усвоения изученного теоретического материала проводится текущий контроль в виде устного опроса или тестирования.

Изменения и дополнения в учебно-тематический план и программу могут быть внесены только после их рассмотрения и утверждения педагогическим советом Учебно-производственного центра ООО «Газпром добыча Надым».

11.2 Учебно-методическое обеспечение

Нормативные документы

1. Конституция Российской Федерации Принята всенародным голосованием 12.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года, внесенными Указами Президента РФ от 09.01.1996 № 20, от 10.02.1996 № 173, от 09.06.2001 № 679, от 25.07.2003 № 841

и Федеральными конституционными законами от 25.03.2004 № 1-ФКЗ, от 14.10.2005 № 6-ФКЗ, от 12.07.2006 № 2-ФКЗ, от 30.12.2006 № 6-ФКЗ, от 30.12.2008 и от 30.12.2008 N 7-ФКЗ);

2. Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов» (с последующими изменениями и дополнениями);

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

4. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с последующими изменениями и дополнениями);

5. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (с последующими изменениями и дополнениями);

6. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (с последующими изменениями и дополнениями);

7. СТО Газпром 18000.2-010-2020 (Единая система управления производственной безопасностью. Обеспечение готовности к аварийным ситуациям в Группе Газпром);

8. СТО Газпром 18000.1-002-2020 (Единая сдстема управления производственной безопасностью. Идентификация опасностей и управления рисками в области производственной безопасности);

9. СТО Газпром 18000.1(001-2020 (Единая сдстема управления производственной безопасностью. Установление целей и разработка программ мероприятий, мониторинг их выполнения);

10. СТО Газпром 18000.3-004-2020 (Единая система управления производственной безопасностью. Организация и проведение аудитов);

11. СТО Газпром 18000.2-005-2021 (Единая система управления производственной безопасностью в ПАО «Газпром». Порядок разработки, учета, внесения изменений, признания утратившими силу и отмены документов);

12. СТО Газпром 18000.2-007-2018 (Порядок применения знаков безопасности и других средств визуальной информации об опасностях на объектах ПАО «Газпром»);

13. СТО Газпром 10000.4-008-2019 (Анализ коренных причин происшествий. Порядок их установления и разработки мероприятий по предупреждению);

14. Постановление Министерства труда и социального развития Российской Федерации от 7 апреля 2004 года N 43 «Об утверждении норм бесплатной выдачи сертифицированных специальной одежды, специальной обуви и других средств индивидуальной защиты работникам филиалов, структурных подразделений, дочерних обществ и организаций открытого акционерного общества «Газпром».

Методическая литература

1 Методические рекомендации для преподавателя теоретического обучения: методические рекомендации: СНО 05.11.09.749.03. - Москва: Филиал «УМУгазпром» НОУ «ОНУТЦ ОАО «Газпром», 2015.

2 Методические рекомендации по организации и проведению конкурса профессионального мастерства на лучшего преподавателя образовательного подразделения дочернего общества ОАО «Газпром»: методические указания: СНО 05.11.07.764.03. - Москва: Филиал «УМУгазпром» НОУ «ОНУТЦ ОАО «Газпром», 2015.

3 Методические рекомендации по применению кейс-технологий: методические рекомендации: СНО 05.11.09.571.03. - Москва: Филиал «УМУгазпром» НОУ «ОНУТЦ ОАО «Газпром», 2015.

4 Методические рекомендации о порядке приема на работу специалистов с высшим и средним профессиональным образованием на рабочие должности и организация их обучения по рабочим профессиям в обществах и организациях ПАО «Газпром»: методические рекомендации: СНО 05.11.09.957.03. - Москва: «УМУгазпром» ЧУ ДПО «Газпром ОНУТЦ», 2016.

5 Методические рекомендации по организации интегрированного урока: методические рекомендации: СНО 05.11.09.985.03. - Москва: «УМУгазпром» ЧУ ДПО «Газпром ОНУТЦ», 2016.

6 Методические рекомендации по проведению самообследования при корпоративной аттестации образовательного подразделения ДО ПАО «Газпром»: методические рекомендации: СНО 05.11.09.987.03. - Москва: «УМУгазпром» ЧУ ДПО «Газпром ОНУТЦ», 2016.

7 Методические рекомендации по подготовке и оформлению портфолио для аккредитации преподавателей: методические рекомендации: СНО 05.11.09.986.03. - Москва: «УМУгазпром» ЧУ ДПО «Газпром ОНУТЦ», 2016.

8 Методические рекомендации по совершенствованию педагогических знаний преподавателей, мастеров (инструкторов) производственного обучения образовательных подразделений дочерних обществ ПАО «Газпром»: методические рекомендации: СНО 05.11.09.708.03. - Москва: «УМУгазпром» ЧУ ДПО «Газпром ОНУТЦ», 2016.

9 Методические рекомендации по организации методической работы в образовательных подразделениях дочерних обществ ПАО «Газпром»: методические рекомендации: СНО 05.11.09.755.03. - Москва: «УМУгазпром» ЧУ ДПО «Газпром ОНУТЦ», 2018.

10 Методические рекомендации по составлению паспорта оснащенности образовательного подразделения дочернего общества ПАО «Газпром»: методические рекомендации: СНО 05.11.09.125.01. - Калининград: ЧУ ДПО «Газпром ОНУТЦ», 2018.

11 Инструктивно-методические материалы по разработке оценочных средств для промежуточной и итоговой аттестации с учетом положений профессиональных стандартов при организации профессионального обучения в образовательных подразделениях дочерних обществ ПАО «Газпром»:

методические указания: СНО 05.11.07.1025.03. - Москва: «УМУгазпром» ЧУ ДПО «Газпром ОНУТЦ», 2019.

12 Методика создания интерактивных плакатов (на примере плаката «Ключевые правила безопасности ПАО «Газпром»): рекомендации: СНО 05.11.09.173.01. - Калининград: ЧУ ДПО «Газпром ОНУТЦ», 2019.

11.2.2 Перечень рекомендуемых наглядных пособий и интерактивных обучающих систем

Видеофильмы

1 Инструктаж по охране труда и пожарной безопасности участников образовательного процесса при очном обучении: учебный видеофильм: СНО 05.11.11/01.160.01. - Калининград: ЧУ ДПО «Газпром ОНУТЦ», 2022.

2 Обеспечение безопасности объектов критической инфраструктуры: актуальные проблемы и пути решения. Владимир Шелепов, Национальная компьютерная корпорация. Конференция, 2024.

3 Создание системы обеспечения безопасности объектов КИИ (АСУ ТП). Типовые ошибки на этапах категорирования, проектирования и внедрения. Алексей Орехов, НТЦ "Вулкан". Конференция ФСТЭК, 2023.

4 Развитие отечественных информационных ресурсов, содержащих сведения об угрозах безопасности информации и уязвимостях программного обеспечения. Александр Суховерхов, ФАУ «ГНИИИ ПТЗИ ФСТЭК России». Конференция ФСТЭК, 2024.

5 Использование программного комплекса Acronis Backup Advanced для управления системой резервного копирования на предприятии. Сергей Денисов, ведущий инженер филиала ООО «ГАЗИНФОРМСЕРВИС» в г. Самара.

Автоматизированные обучающие системы

1 Основы природоохранной деятельности: СНО 08.10.04/03.073.01 – Калининград: ЧУ ДПО «Газпром ОНУТЦ», 2020

Электронные учебно-методические пособия

1 Основы управления охраной труда в организации: СНО 08.06.04/08.088.01 – Калининград: ЧУ ДПО «Газпром ОНУТЦ», 2023.

Приложение № 1

Форма календарного учебного графика

Компоненты программы	Аудиторные занятия / электронное обучение / дистанционные занятия			Практика	Итоговая аттестация
	1 день	2 день	3 день		
1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	8	8	2	10	зачет
2 Охрана труда и промышленная безопасность	-	-	2	2	тестирование
3 Охрана окружающей среды экологическая безопасность	-	-	2	2	тестирование
Итоговая аттестация	-	-	2	-	экзамен
Итого	**8**	**8**	**8**	14	2
Всего	**24**				

Приложение № 2

Образец удостоверения о повышении квалификации

Формат А4

УДОСТОВЕРЕНИЕ
о повышении квалификации

_____
(фамилия

_____
имя, отчество)

с по

прошел(а) обучение в Учебно-производственном центре
ООО «Газпром добыча Надым», г. Надым, ЯНАО
по программе
Повышения квалификации руководителей и специалистов по курсу «Обеспечение информационной безопасности объектов критической информационной инфраструктуры»
(наименование программы)

в объеме _____ часов

Начальник Учебно-производственного центра

_____ _____
(подпись) (ФИО)

М.П.

Выдано

Удостоверение является документом о повышении квалификации

89НДМ **000000**
Регистрационный номер **0000**