Утвержден

приказом Министерства труда

и социальной защиты

Российской Федерации

от \_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_\_

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

**Специалист по обеспечению безопасности значимых объектов критической информационной структуры**

|  |  |
| --- | --- |
|  |  |
|  | Регистрационный номер |

Содержание

[I. Общие сведения 1](#_Toc57538769)

[II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности) 3](#_Toc57538772)

[III. Характеристика обобщенных трудовых функций 5](#_Toc57538773)

[3.1. Обобщенная трудовая функция «Планирование и разработка мероприятий по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса» 6](#_Toc57538774)

[3.2. Обобщенная трудовая функция «Обеспечение функционирования системы безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса»…………………………………………………………………………………………..…………..16](#_Toc57538775)

[3.3. Обобщенная трудовая функция «Контроль состояния безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса»…………………..27](#_Toc57538775)

[3.4. Обобщенная трудовая функция «Совершенствование системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса»……………………………………………………………34](#_Toc57538780)

[IV. Сведения об организациях - разработчиках 42](#_Toc57538781)

I. Общие сведения

|  |  |  |
| --- | --- | --- |
| Эксплуатация и контроль состояния защищенности системы безопасности значимых объектов критической информационной инфраструктуры на объектах топливно-энергетического комплекса |  |  |
| (наименование вида профессиональной деятельности) |  | Код |

Основная цель вида профессиональной деятельности:

|  |
| --- |
| Обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры, входящих в состав объектов топливно-энергетического комплекса Российской Федерации, при проведении в отношении них компьютерных атак. |

Группа занятий:

|  |  |  |  |
| --- | --- | --- | --- |
| 1330 | Руководители в сфере информационно-телекоммуникационных технологий | 2522 | Системные администраторы |
| 2523 | Специалисты по компьютерным сетям | 2529 | Специалисты по базам данных и сетям, не входящие в другие группы |
| (код ОКЗ[[1]](#endnote-1) | (наименование) | (код ОКЗ) | (наименование) |

Отнесение к видам экономической деятельности:

|  |  |
| --- | --- |
| 62.02.1 | Деятельность по планированию, проектированию компьютерных систем |
| 62.02.2 | Деятельность по обследованию и экспертизе компьютерных систем |
| 62.02.3 | Деятельность по обучению пользователей |
| 62.02.4 | Деятельность по подготовке компьютерных систем к эксплуатации |
| 62.02.9 | Деятельность консультативная в области компьютерных технологий прочая |
| 62.09 | Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая |
| 71.20.9 | Деятельность по техническому контролю, испытаниям и анализу прочая |
| (код ОКВЭД[[2]](#endnote-2)) | (наименование вида экономической деятельности) |

**II. Описание трудовых функций, входящих в профессиональный стандарт   
(функциональная карта вида профессиональной деятельности)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Обобщенные трудовые функции | | | Трудовые функции | | |
| Код | наименование | уровень квалификации | Наименование | код | уровень (подуровень) квалификации |
| A | Планирование и разработка мероприятий по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса | 6 | Обоснование требований к системе безопасности значимых объектов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса | А/01.6 | 6 |
| Планирование мероприятий по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса | А/02.6 | 6 |
| Разработка организационно-распорядительных документов по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса | А/03.6 | 6 |
| B | Обеспечение функционирования системы безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | 6 | Обеспечение реализации организационных мер и эксплуатации средств защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса. | B/01.6 | 6 |
| Осуществление в установленном порядке реагирования на компьютерные инциденты в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса. | B/02.6 | 6 |
| Обеспечение координации деятельности работников подразделений, эксплуатирующих значимые объекты критической информационной инфраструктуры, представителей организаций, привлекаемых для защиты значимых объектов критической информационной инфраструктуры. | B/03.6 | 6 |
| C | Контроль состояния безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | 6 | Проведение оценки соответствия системы безопасности значимых объектов критической информационной инфраструктуры требованиям по безопасности. | C/01.6 | 6 |
| Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса. | C/02.6 | 6 |
| Документирование результатов реализации мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры. | C/03.6 | 6 |
| D | Совершенствование системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | 7 | Выявление угроз безопасности информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | D/01.7 | 7 |
| Анализ функционирования системы безопасности и состояния безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры, наличия в них уязвимостей. | D/02.7 | 7 |
| Разработка предложений по развитию системы безопасности и реализация мер по совершенствованию безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса. | D/03.7 | 7 |

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | A | Уровень квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Инженер по защите информации на объектах КИИ  Специалист по защите информации на объектах КИИ I категории  Специалист по защите информации на объектах КИИ II категории  Специалист по защите информации на объектах КИИ  Инженер-программист по технической защите информации на объектах КИИ I категории  Инженер-программист по технической защите информации на объектах КИИ II категории  Инженер-программист по технической защите информации на объектах КИИ  Инженер-программист на объектах КИИ I категории  Инженер-программист на объектах КИИ II категории  Инженер-программист на объектах КИИ III категории  Инженер-программист на объектах КИИ |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование - бакалавриат |
| Требования к опыту практической работы | Для должностей с категорией - опыт работы в должности с более низкой (предшествующей) категорией не менее одного года |
| Особые условия допуска к работе | Наличие допуска к государственной тайне[[3]](#endnote-3) (при необходимости) |
| Другие характеристики | - |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2522 | Системные администраторы |
| ЕКС[[4]](#endnote-4) | - | Инженер-программист (программист) |
| - | Инженер-программист по технической защите информации |
| ОКПДТР[[5]](#endnote-5) | 22824 | Инженер-программист |
| 26579 | Специалист по защите информации |
| 22567 | Инженер по защите информации |
| ОКСО[[6]](#endnote-6) | 2.10.03.01 | Информационная безопасность |

3.1.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обоснование требований к системе безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | A/01.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | | X | Заимствовано из оригинала |  |  | |
|  |  | |  |  | Код оригинала | Регистрационный номер профессионального стандарта | |
| Трудовые действия | | | Анализ информационной инфраструктуры значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | | | | |
| Анализ защищенности информационной инфраструктуры значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | | | | |
| Анализ требований к назначению, структуре и конфигурации создаваемой значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса с целью выявления угроз безопасности информации | | | | |
| Разработка модели угроз безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | | | | |
| Присвоение объекту критической информационной инфраструктуры одной из категорий значимости или обоснование отсутствия необходимости | | | | |
| Формирование требований по защите информации на значимых объектах критической информационной инфраструктуры, включая использование математического аппарата для решения прикладных задач | | | | |
| Выбор и обоснование критериев эффективности функционирования защищенных значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса | | | | |
| Формирование разделов технических заданий на создание систем безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | | | | |
| Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | | | | |
| Необходимые умения | | | Применять нормативные правовые акты, определяющие требования к обеспечению информационной безопасности объекта критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также Министерством энергетики Российской Федерации в части сопровождения жизненного цикла объекта критической информационной инфраструктуры. | | | | |
| Определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса, подлежащие защите. | | | | |
| Классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса | | | | |
| Разрабатывать модели угроз безопасности информации и нарушителей в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | | | | |
| Необходимые знания | | | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры | | | | |
| Нормативные правовые акты в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. | | | | |
| Основные методические и руководящие документы по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры | | | | |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) | | | | |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса | | | | |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса | | | | |
| Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование предприятий (объектов) топливно-энергетического комплекса. | | | | |
| Другие характеристики | | | - | | | | |

3.1.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Планирование мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | A/02.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Определение комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Формирование разделов технических заданий на создание систем безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности |
| Определение правил и процедур управления системой защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Оформление заявки на разработку системы защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Определение правил и процедур защиты информации при выводе значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса из эксплуатации |
| Необходимые умения | Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации |
| Выбирать меры защиты информации, подлежащие реализации в системе защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса. |
| Выбирать программно-аппаратные средства защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности информации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса. |
| Определять комплекс мер для обеспечения безопасности информационной в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Формировать перечень мероприятий по предотвращению угроз безопасности информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, |
| Основные методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса. |
| Основные методы организации и проведения технического обслуживания средств защиты информации |
| Другие характеристики | - |

3.1.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка организационно-распорядительных документов по обеспечению безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | A/03.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Анализ технической документации информационной инфраструктуры значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Подготовка (разработка) документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации |
| Подготовка (разработка) документов, определяющих правила и процедуры управления конфигурацией системой безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры |
| Подготовка (разработка) документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в автоматизированной системе |
| Подготовка (разработка) документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации |
| Проведение (разработка) проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации |
| Необходимые умения | Определять меры (для защиты информации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса. |
| Применять нормативные документы по противодействию технической разведке |
| Планировать политику безопасности программных компонентов значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Разрабатывать политики безопасности информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
|  | Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации |
| Основные методические и руководящие документы по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем защиты информации |
| Основные угрозы безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Другие характеристики | - |

**3.2. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обеспечение функционирования системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | B | Уровень квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Инженер по защите информации на объектах КИИ  Специалист по защите информации на объектах КИИ I категории  Специалист по защите информации на объектах КИИ II категории  Специалист по защите информации на объектах КИИ  Инженер-программист по технической защите информации на объектах КИИ I категории  Инженер-программист по технической защите информации на объектах КИИ II категории  Инженер-программист по технической защите информации на объектах КИИ  Инженер-программист на объектах КИИ I категории  Инженер-программист на объектах КИИ II категории  Инженер-программист на объектах КИИ III категории  Инженер-программист на объектах КИИ |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование - бакалавриат |
| Требования к опыту практической работы | Для должностей без категорий - опыт работы не требуется  Для должностей с категорией - опыт работы в должности с более низкой (предшествующей) категорией не менее одного года |
| Особые условия допуска к работе | Наличие допуска к государственной тайне (при необходимости) |
| Другие характеристики | - |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2523 | Специалисты по компьютерным сетям |
| ЕКС | - | Инженер-программист (программист) |
| - | Инженер-программист по технической защите информации |
| ОКПДТР | 22824 | Инженер-программист |
| 26579 | Специалист по защите информации |
| 22567 | Инженер по защите информации |
| ОКСО | 2.10.03.01 | Информационная безопасность |

3.2.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обеспечение реализации организационных мер и эксплуатации средств защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса. | Код | B/01.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Установка обновлений программного обеспечения значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Управление полномочиями пользователей значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Обнаружение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Устранение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Устранение инцидентов, возникших в процессе эксплуатации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Уничтожение информации, обрабатываемой значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры |
| Уничтожение машинных носителей информации, обрабатываемой на значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры |
| Архивирование информации, обрабатываемой на значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры |
| Резервирование программного обеспечения, технических средств, каналов передачи данных значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса управления на случай возникновения нештатных ситуаций |
| Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций |
| Осуществление автономной наладки технических и программных средств системы защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Ведение протоколов и журналов учета при изменении конфигурации систем безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Необходимые умения | Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации |
| Создавать, удалять и изменять учетные записи пользователей значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Конфигурировать параметры средств защиты информации и системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса |
| Администрировать программные средства системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Определять параметры настройки программного обеспечения системы защиты информации значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса. |
| Реализовывать правила разграничения доступа персонала к объектам доступа |
| Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты |
| Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Использовать криптографические методы и средства защиты информации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Регистрировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Анализировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Использовать программные средства для архивирования информации |
| Использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации |
| Применять типовые программные средства резервирования и восстановления информации в значимых объектах критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Применять средства обеспечения отказоустойчивости значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Определять источники и причины возникновения инцидентов |
| Оценивать последствия выявленных инцидентов |
| Обнаруживать нарушения правил разграничения доступа |
| Устранять нарушения правил разграничения доступа |
| Использовать криптографические методы и средства защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Организовывать ремонтное обслуживание компонентов значимых объектов критической информационной инфраструктуры |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Программно-аппаратные средства защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Организационные меры по защите информации |
| Критерии оценки защищенности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Технические средства контроля эффективности мер защиты информации |
| Регламент информирования персонала значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса о выявленных инцидентах |
| Регламент учета выявленных инцидентов |
| Регламент устранения инцидентов |
| Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Процедуры по архивированию информации, обрабатываемой на значимых объектах критической информационной инфраструктуры |
| Регламент значимых объектов критической информационной инфраструктуры по уничтожению информации и машинных носителей информации |
| Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Другие характеристики | - |

3.2.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Осуществление в установленном порядке реагирования на компьютерные инциденты в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса. | Код | B/02.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Обнаружение инцидентов в процессе эксплуатации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Идентификация инцидентов в процессе эксплуатации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Устранение инцидентов, возникших в процессе эксплуатации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Восстановление после сбоев и отказов программного обеспечения значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Необходимые умения | Определять источники и причины возникновения инцидентов |
| Оценивать последствия выявленных инцидентов |
| Обнаруживать нарушения правил разграничения доступа |
| Устранять нарушения правил разграничения доступа |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры.  Нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Организационные меры по защите информации |
| Критерии оценки защищенности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Технические средства контроля эффективности мер защиты информации |
| Регламент информирования персонала значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса о выявленных инцидентах |
| Регламент учета выявленных инцидентов |
| Регламент устранения инцидентов |
| Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Другие характеристики | - |

3.2.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обеспечение координации деятельности работников подразделений, эксплуатирующих значимых объектов критической информационной инфраструктуры, представителей организаций, привлекаемых для защиты значимых объектов критической информационной инфраструктуры | Код | B/03.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | | X | Заимствовано из оригинала |  |  |
|  |  | |  |  | Код оригинала | Регистрационный номер профессионального стандарта |
| Трудовые действия | | Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | | | | |
| Информирование персонала об угрозах безопасности информации | | | | |
| Информирование пользователей о правилах эксплуатации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса с учетом требований по защите информации | | | | |
| Информирование персонала о правилах эксплуатации системы защиты значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса и отдельных средств защиты информации | | | | |
| Проведение занятий с персоналом по работе с системой защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса, включая проведение практических занятий с персоналом на макетах или в тестовой зоне | | | | |
| Необходимые умения | | Консультировать персонал значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса в отношении комплекса мер (правил, процедур, практических приёмов, руководящих принципов, методов, средств) для обеспечения защиты информации. | | | | |
| Осуществлять планирование и организацию работы персонала значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса с учетом требований по защите информации | | | | |
| Необходимые знания | | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры.  Нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. | | | | |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры | | | | |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) | | | | |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса | | | | |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса | | | | |
| Другие характеристики | | - | | | | |

**3.3. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Контроль состояния безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | C | Уровень квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Инженер по защите информации на объектах КИИ  Специалист по защите информации на объектах КИИ I категории  Специалист по защите информации на объектах КИИ II категории  Специалист по защите информации на объектах КИИ  Инженер-программист по технической защите информации на объектах КИИ I категории  Инженер-программист по технической защите информации на объектах КИИ II категории  Инженер-программист по технической защите информации на объектах КИИ  Инженер-программист на объектах КИИ I категории  Инженер-программист на объектах КИИ II категории  Инженер-программист на объектах КИИ III категории  Инженер-программист на объектах КИИ |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование - бакалавриат |
| Требования к опыту практической работы | Не менее одного года в области защиты информации или не менее двух лет в области информационных технологий для должностей без категорий  Для должностей с категорией - опыт работы в должности с более низкой (предшествующей) категорией не менее одного года |
| Особые условия допуска к работе | Наличие допуска к государственной тайне (при необходимости) |
| Другие характеристики | Рекомендуется дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2529 | Специалисты по базам данных и сетям, не входящие в другие группы |
| ЕКС | - | Инженер-программист (программист) |
| - | Инженер-программист по технической защите информации |
| ОКПДТР | 22567 | Инженер по защите информации |
| 26579 | Специалист по защите информации |
| ОКСО | 2.10.03.01 | Информационная безопасность |

3.3.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение оценки соответствия системы безопасности значимых объектов критической информационной инфраструктуры И требованиям по безопасности. | Код | C/01.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Проведение проверки готовности персонала к эксплуатации системы защиты информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Экспертиза состояния защищенности информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Оценка защищенности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса с помощью типовых программных средств |
| Определение правил и процедур мониторинга обеспечения уровня защищенности информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Необходимые умения | Определять состояние параметров защищенности значимых объектов критической информационной инфраструктуры |
| Определять адекватность компенсационных мер |
| Определять защищенность значимых объектов критической информационной инфраструктуры в соответствии с требованиями по безопасности |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Другие характеристики | - |

3.3.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | C/02.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Проведение предварительных испытаний системы защиты информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Анализ недостатков в функционировании системы защиты информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Проведение приемочных испытаний системы безопасности значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Ведение протоколов и журналов учета при осуществлении мониторинга систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Ведение протоколов и журналов учета при осуществлении аудита систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний |
| Необходимые умения | Применять технические средства контроля эффективности мер защиты информации. |
| Осуществлять контроль обеспечения уровня защищенности в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Другие характеристики | - |

**3.3.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Документирование результатов реализации мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры | Код | C/03.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Документирование программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации |
| Обоснование и контроль результатов управленческих решений в области безопасности информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Ведение документов учета, обработки, хранения и передачи информации ограниченного доступа |
| Необходимые умения | Документировать действия по устранению неисправностей в работе системы защиты информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса. |
| Документировать процедуры и результаты контроля функционирования системы защиты информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Другие характеристики | - |

**3.4. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Совершенствование системы безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | D | Уровень квалификации | 7 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Главный специалист по защите информации  Ведущий инженер-разработчик систем защиты информации  Ведущий специалист по защите информации  Руководитель проектов в области разработки систем защиты информации |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование - специалитет, или магистратура в области информационной безопасности  и  Дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности  или  Высшее образование - аспирантура (адъюнктура)  и  Дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |
| Требования к опыту практической работы | Не менее пяти лет в области защиты информации, в том числе на руководящих должностях не менее трех лет, для имеющих высшее образование - специалитет или магистратура в области информационной безопасности  или  Не менее трех лет в области защиты информации, в том числе на руководящих должностях не менее двух лет, для имеющих высшее образование - аспирантура (адъюнктура) |
| Особые условия допуска к работе | Наличие допуска к государственной тайне (при необходимости) |
| Другие характеристики | - |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 1330 | Руководители в сфере информационно-телекоммуникационных технологий |
| ЕКС | - | Инженер-программист (программист) |
| -  - | Инженер-программист по технической защите информации |
| ОКПДТР | 20911 | Главный специалист по защите информации |
| ОКСО | 2.10.05.01 | Компьютерная безопасность |
| 2.10.05.02 | Информационная безопасность телекоммуникационных систем |
| 2.10.05.03 | Информационной безопасности автоматизированных систем |
| 2.10.05.04 | Информационно-аналитические системы безопасности |
| 2.10.05.05 | Безопасность информационных технологий в правоохранительной сфере |
| 2.10.05.06 | Криптография |
| 2.10.05.07 | Противодействие техническим разведкам |
| 2.10.04.01 | Информационная безопасность |
| ОКСВНК[[7]](#endnote-7) | 05 13 19 | Методы и системы защиты информации, информационная безопасность |

3.4.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Выявление угроз безопасности информации значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | D/01.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Анализ изменения угроз безопасности информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса, возникающих в ходе их эксплуатации. |
| Выявление основных угроз безопасности информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Обоснование критериев эффективности функционирования защищенных значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Принятие мер защиты информации при выявлении новых угроз безопасности информации |
| Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем безопасности |
| Разработка аналитических и компьютерных моделей значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Исследование аналитических и компьютерных моделей значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Необходимые умения | Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации |
| Классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса |
| Анализировать основные узлы и устройства современных значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Применять действующую нормативную базу в области обеспечения безопасности информации |
| Контролировать безотказное функционирование технических средств защиты информации |
| Восстанавливать (заменять) отказавшие технические средства защиты информации |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Принципы построения и функционирования систем и сетей передачи информации |
| Эталонная модель взаимодействия открытых систем |
| Основные угрозы безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Основные меры по защите информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Особенности защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса управления технологическими процессами |
| Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Технические средства контроля эффективности мер защиты информации |
| Другие характеристики | - |

3.4.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Анализ функционирования системы безопасности и состояния безопасности значимых объектов критической информационной инфраструктуры, наличия в них уязвимостей | Код | D/02.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Анализ программных, архитектурно-технических и схемотехнических решений компонентов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса с целью выявления потенциальных уязвимостей безопасности информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Анализ воздействия изменений конфигурации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса на ее защищенность |
| Выявление уязвимости информационно-технологических ресурсов значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Составление методик тестирования систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Подбор инструментальных средств тестирования систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Составление протоколов тестирования систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Устранение известных уязвимостей значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса, приводящих к возникновению угроз безопасности информации |
| Необходимые умения | Проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств |
| Анализировать программные, архитектурно-технические и схемотехнические решения компонентов значимых объектах критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса с целью выявления потенциальных уязвимостей безопасности информации в значимых объектах критической информационной инфраструктуры на предприятиях ТЭ |
| Анализировать возможные уязвимости автоматизированных систем |
| Выявлять известные уязвимости автоматизированных систем |
| Устранять выявленные уязвимости значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса, приводящие к возникновению угроз безопасности информации |
| Классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры.  Нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Другие характеристики | - |

3.4.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка предложений по развитию системы безопасности и реализация мер по совершенствованию безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса | Код | D/03.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |
|  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Расчет показателей эффективности защиты информации, обрабатываемой в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Обоснование критериев эффективности функционирования защищенных значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Устранение недостатков в функционировании системы защиты информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Выработка рекомендаций для принятия решения о модернизации системы защиты информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса |
| Разработка предложений по совершенствованию системы управления безопасностью информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Выработка рекомендаций для принятия решения о повторной оценке эффективности системы безопасности (аттестации) значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса или о проведении дополнительных испытаний |
| Необходимые умения | Разрабатывать предложения по совершенствованию системы управления защитой информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса. |
| Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности |
| Исследовать модели значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса |
| Классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса |
| Необходимые знания | Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры.  Нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. |
| Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры |
| Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности) |
| Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса |
| Другие характеристики | - |

**IV. Сведения об организациях – разработчиках профессионального стандарта**

**4.1. Ответственная организация-разработчик**

|  |
| --- |
| Ассоциация защиты информации, город Москва |
| Президент Лось Владимир Павлович |

**4.2. Наименования организаций-разработчиков**

|  |  |
| --- | --- |
| 1 | Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина», город Москва |
| 2 | Федеральное государственное автономное образовательное учреждение дополнительного профессионального образования «Институт повышения квалификации руководящих работников и специалистов топливно-энергетического комплекса», город Москва |
| 3 | Автономная некоммерческая организация дополнительного профессионального образования центр повышения квалификации «АИС», город Москва |
| 4 | ФГБУ «ВНИИ труда» Минтруда России, город Москва |
| 5 | Федеральное учебно-методическое объединение в системе высшего образования по УГСНП «Информационная безопасность», город Москва |
| 6 | Ассоциация предприятий компьютерных и информационных технологий, город Москва |

1. Общероссийский классификатор занятий. [↑](#endnote-ref-1)
2. Общероссийский классификатор видов экономической деятельности. [↑](#endnote-ref-2)
3. Закон Российской Федерации от 21 июля 1993 г. N 5485-1 «О государственной тайне» (Собрание законодательства Российской Федерации, 1996, N 15, ст. 1768; 1997, N 41, ст. ст. 4673, 8220, 8221, 8222, 8223, 8224, 8225, 8226, 8227, 8228, 8229, 8230, 8231, 8232, 8233, 8234, 8235; 2002, N 52, ст. 5288; 2003, N 6, ст. 549, N 27, ст. 2700, N 46, ст. 4449; 2004, N 27, ст. 2711, N 35, ст. 3607; 2007, N 49, ст. 6055, ст. 6079; 2009, N 29, ст. 3617; 2010, N 47, ст. 6033; 2011, N 30, ст. 4590, ст. 4596, N 46, ст. 6407; 2013, N 51, ст. 6697; 2015, N 10, ст. 1393). [↑](#endnote-ref-3)
4. Единый квалификационный справочник должностей руководителей, специалистов и других служащих. [↑](#endnote-ref-4)
5. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов. [↑](#endnote-ref-5)
6. Общероссийский классификатор специальностей по образованию. [↑](#endnote-ref-6)
7. Общероссийский классификатор специальностей высшей научной квалификации. [↑](#endnote-ref-7)