**ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ**

|  |
| --- |
| **Техник-специалист по обеспечению и** информационной безопасности на железнодорожном транспорте |
| (наименование профессионального стандарта) |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Акционерное общество «Узбекистон темир йуллари»**  Адрес: улица Тараса Шевченко, 7  ИНН: 201051951; МФО: 00875; тел: 71 238-80-28; факс: 71 233-69-24 | | | |  | |  | |
|  | |
|  | | Регистрационный номер МЗиТО | |
| Реквизиты утверждающей организации | | | |  | |  | |
| **Раздел I. Общие сведения** | | | | | | | | |
| Обеспечение безопасности информации в автоматизированных системах | | | | |  | | I03.024 | |
| (наименование вида профессиональной деятельности) | | | | |  | | Код по дескриптору | |
|  | | | | |  | |  | |
| Основная цель вида профессиональной деятельности: | | | | | | | | |
| Обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно технологическими ресурсами, подлежащими защите | | | | | | | | |
|  |  |  |  | | | | | |
| Группа занятий по НСКЗ: | | | | | | | | |
| 3114 | Младшие специалисты и вспомогательный персонал в физических и инженерных науках |  |  | | | | | |
| (код НСКЗ) | (наименование группы) | (код НСКЗ) | (наименование группы) | | | | | |
|  |  |  |  | | | | | |
| Виды экономической деятельности: | | | | | | | | |
| 62.09.0 | Другие виды деятельности в области информационных технологий и компьютерных систем | | | | | | | |
|  |  | | | | | | | |
| (код ОКЭД) | (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** |
| А | Обслуживание систем защиты информации в автоматизированных системах | 5 | Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем | А/01.4 | 4 |
| Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем | А/02.4 | 4 |
| Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем | А/03.4 | 4 |
| В | Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации | 6 | Диагностика систем защиты информации автоматизированных систем | В/01.5 | 5 |
| Администрирование систем защиты информации автоматизированных систем | В/02.5 | 5 |
| Управление защитой информации в автоматизированных системах | В/03.5 | 5 |
| С | Внедрение систем защиты информации автоматизированных систем | 6 | Установка и настройка средств защиты информации в автоматизированных системах | С/01.5 | 5 |
| Разработка организационно-распорядительных документов по защите информации в автоматизированных системах | С/02.5 | 5 |
| Анализ уязвимостей внедряемой системы защиты информации | С/03.5 | 5 |
| D | Разработка систем защиты информации автоматизированных систем | 7 | Тестирование систем защиты информации автоматизированных систем | D/01.6 | 6 |
| Разработка проектных решений по защите информации в автоматизированных системах | D/02.6 | 6 |
| Разработка эксплуатационной документации на системы защиты информации автоматизированных систем | D/03.6 | 6 |

**III. Характеристика обобщенных трудовых функций**

**3.1. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обслуживание систем защиты информации в автоматизированных системах | Код | А | Уровень квалификации | 4 |

|  |  |
| --- | --- |
| Возможные наименование должностей, профессий | Техник по защите информации I категории  Техник по защите информации II категории Техник по защите информации |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Профессиональный колледж или академический лицей на базе 11-летнего непрерывного цикла общего среднего образования. |
| 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 | Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в установленном законодательством Республики Узбекистан порядке |
| Другие характеристики | Рекомендуется дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |

**3.1.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем | Код | А/01.4 | Уровень квалификации | 4 |

|  |  |
| --- | --- |
| Трудовые действия | Проверка работоспособности системы защиты информации автоматизированной системы |
| Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации |
| Контроль стабильности характеристик системы защиты информации автоматизированной системы |
| Необходимые умения | Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией |
| Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации |
| Производить монтаж и диагностику компьютерных сетей |
| Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи |
| Необходимые знания | Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях |
| Базовая конфигурация системы защиты информации автоматизированной системы |
| Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах |
| Типовые средства, методы и протоколы идентификации, аутентификации и авторизации |
| Нормативные правовые акты в области защиты информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

|  |
| --- |
|  |

**3.1.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем | Код | А/02.4 | Уровень квалификации | 4 |

|  |  |
| --- | --- |
| Трудовые действия | Ведение документов учета, обработки, хранения и передачи |
| Информирование персонала об угрозах безопасности информации |
| Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации |
| Ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем |
| Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем |
| Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем |
| Необходимые умения | Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации |
| Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации |
| Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации |
| Необходимые знания | Нормативные правовые акты в области защиты информации |
| Основные методические и руководящие документы уполномоченных органов исполнительной власти по защите информации |
| Эксплуатационная и проектная документация на автоматизированную систему |
| Основные методы организации и проведения технического обслуживания технических средств информатизации |
| Организационные меры по защите информации |
| Другие характеристики | - |

**3.1.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем | Код | А/03.4 | Уровень квалификации | 4 |

|  |  |
| --- | --- |
| Трудовые действия | Уничтожение информации, обрабатываемой автоматизированной системой |
| Уничтожение машинных носителей информации, обрабатываемой автоматизированной системой |
| Архивирование информации, обрабатываемой автоматизированной системой |
| Необходимые умения | Использовать программные средства для архивирования информации |
| Использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации |
| Использовать типовые криптографические средства защиты информации, в том числе электронную подпись |
| Необходимые знания | Процедуры по архивированию информации, обрабатываемой автоматизированной системой |
| Назначение и принципы работы основных узлов современных технических средств информатизации |
| Организация ремонтного обслуживания компонентов автоматизированной системы |
| Регламент автоматизированной системы по уничтожению информации и машинных носителей информации |
| Нормативные правовые акты в области защиты информации |
| Основные методические и руководящие документы уполномоченных органов исполнительной власти по защите информации |
| Другие характеристики | - |

**3.2. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации | Код | В | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Возможные наименование должностей, профессий | Специалист по защите информации I категории  Специалист по защите информации II категории  Специалист по защите информации |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Техникум,  Высшее образование – первая ступень (бакалавриат).  Высшее образование, полученное до 2001 года.  Ведомственные программы повышения квалификации.  Практический опыт в сфере профессиональной деятельности |
| 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 | Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в установленном законодательством Республики Узбекистан порядке |
| Другие характеристики |  |

**3.2.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Диагностика систем защиты информации автоматизированных систем | Код | В/01.5 | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Трудовые действия | Обнаружение инцидентов в процессе эксплуатации автоматизированной системы |
| Идентификация инцидентов в процессе эксплуатации автоматизированной системы |
| Оценка защищенности автоматизированных систем с помощью типовых программных средств |
| Устранение инцидентов, возникших в процессе эксплуатации автоматизированной системы |
| Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах |
| Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах |
| Необходимые умения | Определять источники и причины возникновения инцидентов |
| Оценивать последствия выявленных инцидентов |
| Обнаруживать нарушения правил разграничения доступа |
| Устранять нарушения правил разграничения доступа |
| Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах |
| Использовать криптографические методы и средства защиты информации в автоматизированных системах |
| Необходимые знания | Нормативные правовые акты в области защиты информации |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Принципы построения средств защиты информации от «утечки» по техническим каналам |
| Критерии оценки защищенности автоматизированной системы |
| Технические средства контроля эффективности мер защиты информации |
| Регламент информирования персонала автоматизированной системы о выявленных инцидентах |
| Регламент учета выявленных инцидентов |
| Регламент устранения инцидентов |
| Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах |
| Другие характеристики | - |

**3.2.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Администрирование систем защиты информации автоматизированных систем | Код | В/02.5 | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Трудовые действия | Установка обновлений программного обеспечения автоматизированной системы |
| Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы |
| Управление полномочиями пользователей автоматизированной системы |
| Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации |
| Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне |
| Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы |
| Необходимые умения | Создавать, удалять и изменять учетные записи пользователей автоматизированной системы |
| Планировать политику безопасности программных компонентов автоматизированных систем |
| Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации |
| Использовать криптографические методы и средства защиты информации в автоматизированных системах |
| Регистрировать события, связанные с защитой информации в автоматизированных системах |
| Анализировать события, связанные с защитой информации в автоматизированных системах |
| Необходимые знания | Принципы формирования политики информационной безопасности в автоматизированных системах |
| Программно-аппаратные средства защиты информации автоматизированных систем |
| Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| Методы контроля эффективности защиты информации от «утечки» по техническим каналам |
| Критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем |
| Технические средства контроля эффективности мер защиты информации |
| Принципы организации и структура систем защиты программного обеспечения автоматизированных систем |
| Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем |
| Основные меры по защите информации в автоматизированных системах |
| Другие характеристики | - |

**3.2.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Управление защитой информации в автоматизированных системах | Код | В/03.5 | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Трудовые действия | Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность |
| Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе |
| Оценка последствий от реализации угроз безопасности информации в автоматизированной системе |
| Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации |
| Необходимые умения | Оценивать информационные риски в автоматизированных системах |
| Классифицировать и оценивать угрозы безопасности информации |
| Определять подлежащие защите информационные ресурсы автоматизированных систем |
| Применять нормативные документы по противодействию технической разведке |
| Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем |
| Конфигурировать параметры системы защиты информации автоматизированных систем |
| Применять технические средства контроля эффективности мер защиты информации |
| Необходимые знания | Основные методы управления защитой информации |
| Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| Методы защиты информации от «утечки» по техническим каналам |
| Нормативные правовые акты в области защиты информации |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Другие характеристики | - |

**3.3. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций | Код | С | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Возможные наименование должностей, профессий | Инженер по защите информации  Специалист по защите информации I категории  Специалист по защите информации II категории  Специалист по защите информации  Инженер-программист по технической защите информации I категории Инженер-программист по технической защите информации II категории Инженер-программист по технической защите информации Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Техникум,  Высшее образование – первая ступень (бакалавриат).  Высшее образование, полученное до 2001 года.  Ведомственные программы повышения квалификации.  Практический опыт в сфере профессиональной деятельности |
| Требования к опыту практической работы | - |
| Особые условия допуска к работе | Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в установленном законодательством Республики Узбекистан порядке |
| Другие характеристики |  |

**3.3.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Установка и настройка средств защиты информации в автоматизированных системах | Код | С/01.5 | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Трудовые действия | Входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы |
| Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы |
| Проведение приемочных испытаний системы защиты информации автоматизированной системы |
| Внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний |
| Необходимые умения | Администрировать программные средства системы защиты информации автоматизированных систем |
| Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации |
| Применять нормативные документы по противодействию технической разведке |
| Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации |
| Необходимые знания | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| Содержание эксплуатационной документации автоматизированной системы |
| Типовые средства, методы и протоколы идентификации, аутентификации и авторизации |
| Основные меры по защите информации в автоматизированных системах |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Другие характеристики | - |

**3.3.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка организационно­ распорядительных документов по защите информации в автоматизированных системах | Код | С/02.5 | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Трудовые действия | Определение правил и процедур управления системой защиты информации автоматизированной системы |
| Определение правил и процедур выявления инцидентов |
| Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы |
| Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации |
| Определение правил и процедур реагирования на инциденты |
| Необходимые умения | Классифицировать и оценивать угрозы информационной безопасности |
| Применять нормативные документы по противодействию технической разведке |
| Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы |
| Контролировать эффективность принятых мер по защите информации в автоматизированных системах |
| Необходимые знания | Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации |
| Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| Принципы построения средств защиты информации от «утечки» по техническим каналам |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Другие характеристики | - |

**3.3.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Анализ уязвимостей внедряемой системы защиты информации | Код | С/03.5 | Уровень квалификации | 5 |

|  |  |
| --- | --- |
| Трудовые действия | Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем |
| Проведение анализа уязвимости программных и программно­аппаратных средств системы защиты информации автоматизированной системы |
| Проведение экспертизы состояния защищенности информации автоматизированных систем |
| Уточнение модели угроз безопасности информации автоматизированной системы |
| Проведение предварительных испытаний системы защиты информации автоматизированной системы |
| Проведение анализа уязвимостей автоматизированных и информационных систем |
| Необходимые умения | Классифицировать и оценивать угрозы безопасности информации автоматизированной системы |
| Разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы |
| Проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств |
| Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации |
| Необходимые знания | Основные методы и средства криптографической защиты информации |
| Способы защиты информации от «утечки» по техническим каналам |
| Способы контроля эффективности защиты информации от «утечки» по техническим каналам |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Содержание эксплуатационной документации автоматизированной системы |
| Другие характеристики | - |

**3.4. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка систем защиты информации автоматизированных систем | Код | D | Уровень квалификации | 6 |

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

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование, полученное до 2001 года.,  Первая ступень высшего образования (бакалавриат)  Магистратура на основе бакалавриата.  Специальность – завершенная программа высшего образования по направлениям высшего образования не имеющим разделение на ступени.  Послевузовское образование, полученное в высших образовательных и научно-исследовательских учреждениях (базовая докторантура, докторантура, самостоятельное соискательство). |
| Требования к опыту практической работы | - |
| Особые условия допуска к работе | Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в установленном законодательством Республики Узбекистан порядке |
| Другие характеристики | Рекомендуется дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |

**3.4.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Тестирование систем защиты информации автоматизированных систем | Код | D/01.6 | Уровень квалификации | 6 |

|  |  |
| --- | --- |
| Трудовые действия | Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем |
| Выявление уязвимости информационно-технологических ресурсов автоматизированных систем |
| Выявление основных угроз безопасности автоматизированных системах |
| Составление методик тестирования автоматизированных систем |
| Подбор инструментальных средств тестирования систем защиты информации автоматизированных систем |
| Составление протоколов тестирования автоматизированных систем |
| Необходимыеумения | Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации |
| Анализировать основные узлы и устройства современных автоматизированных систем |
| Применять действующую нормативную базу в области обеспечения безопасности информации |
| Контролировать безотказное функционирование технических средств защиты информации |
| Восстанавливать (заменять) отказавшие информации |
| Необходимыезнания | Принципы построения и функционирования систем и сетей передачи информации |
| Эталонная модель взаимодействия открытых систем |
| Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| Основные меры по защите информации в автоматизированных системах |
| Особенности защиты информации в автоматизированных системах управления технологическими процессами |
| Принципы построения средств защиты информации от «утечки» по техническим каналам |
| Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| Технические каналы «утечки» информации |
| Технические средства контроля эффективности мер защиты информации |
| Организация защиты информации от «утечки» по техническим каналам на объектах информатизации |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другиехарактеристики | - |

**3.4.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка проектных решений по защите информации в автоматизированных системах | Код | D/02.6 | Уровень квалификации | 6 |

|  |  |
| --- | --- |
| Трудовые действия | Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах |
| Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем |
| Разработка проектов нормативных документов, работу по защите информации |
| Разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах |
| Необходимые умения | Применять действующую нормативную базу в области обеспечения защиты информации |
| Применять нормативные документы по противодействию технической разведке |
| Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе |
| Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы |
| Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации |
| Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем |
| Классифицировать защищаемую информацию по степеням конфиденциальности |
| Определять типы субъектов доступа и объектами защиты |
| Необходимые знания | Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации |
| Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов |
| Особенности защиты информации в автоматизированных системах управления технологическими процессами |
| Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем |
| Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем |
| Основные характеристики технических средств защиты информации от утечек по техническим каналам |
| Принципы формирования политики информационной безопасности в автоматизированных системах |
| Другие характеристики | - |

**3.4.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка эксплуатационной документации на системы защиты информации автоматизированных систем | Код | D/03.6 | Уровень квалификации | 6 |

|  |  |
| --- | --- |
| Трудовые действия | Анализ технической документации информационной инфраструктуры автоматизированной системы |
| Анализ защищенности автоматизированной системы информационной инфраструктуры |
| Формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач |
| Документирование программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации |
| Анализ структурных и функциональных схем защищенных автоматизированных информационных систем |
| Обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем |
| Использование программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах |
| Необходимыеумения | Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах |
| Разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем |
| Проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов |
| Разрабатывать модели автоматизированных систем и систем защиты информации автоматизированных систем |
| Исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем |
| Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем |
| Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите |
| Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности |
| Исследовать эффективность проектных решений программно­аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности |
| Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации |
| Необходимыезнания | Основные методы управления информационной безопасностью |
| Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов |
| Основные методы управления проектами в области информационной безопасности |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| Основные меры по защите информации в автоматизированных системах |
| Особенности защиты информации в автоматизированных системах управления технологическими процессами |
| Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах |
| Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах |
| Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем |
| Основные средства, способы и принципы построения систем защиты информации автоматизированных систем |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации |
| Другиехарактеристики | - |

**IV. Сведения об организациях-разработчиках**

**профессионального стандарта**

4.1. Ответственная организация – разработчик

|  |
| --- |
| **Акционерное общество «Узбекистон темир йуллари»** |
| (наименование организации)  **Председатель правления Хасилов Х.Н.** |
| (должность и ФИО руководителя) (подпись) |

4.2. Наименования организаций – разработчиков

|  |  |
| --- | --- |
| 1 | Управление персоналом и подготовки кадров |
| 2 | Управление экономического анализа и прогнозирования |
| 3 | Информационно-вычислительный центр |
| 4 | Единый диспетчерский центр |
| 5 | УП «Региональные железнодорожные узлы» |

4.3. Решение Совета по профессиональным квалификациям

|  |
| --- |
| Отраслевой совет АО «Ўзбекистон темир йўллари» |
| (наименование Совета) |

|  |  |
| --- | --- |
| № | Содержание решения |
|  | Разработанный профессиональный стандарт рассмотрен, одобрен и направляется на утверждение. |
|  |  |