

**Об утверждении профессионального стандарта "Деятельность в области кибербезопасности"**

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30 июня 2025 года № 329/НҚ

      В соответствии с пунктом 5 статьи 5 Закона Республики Казахстан "О профессиональных квалификациях", ПРИКАЗЫВАЮ:

      1. Утвердить прилагаемый профессиональный стандарт "Деятельность в области кибербезопасности".

      2. Комитету информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

      1) в течение пяти календарных дней после подписания настоящего приказа направление его на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения "Институт законодательства и правовой информации Республики Казахстан" Министерства юстиции Республики Казахстан для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

      2) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан после его официального опубликования.

      3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

      4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

|  |  |
| --- | --- |
| *Министр цифрового развития,*  *инноваций и аэрокосмической промышленности*  *Республики Казахстан* | *Ж. Мадиев* |

      "СОГЛАСОВАН"

Министерство труда и

Социальной защиты населения

Республики Казахстан

|  |  |
| --- | --- |
|  | Утвержден приказом |

**Профессиональный стандарт: "Деятельность в области кибербезопасности"**

**Глава 1. Общие положения**

      1. Область применения профессионального стандарта: Профессиональный стандарт "Деятельность в области кибербезопасности" разработан в соответствии со статьей 5 Закона Республики Казахстан "О профессиональных квалификациях" и может применяться при формировании требований к соискателю для приема на работу, формировании образовательных программ, в том числе обучения персонала на предприятиях, признания профессиональной квалификации работников и выпускников организаций образования, а также для решения широкого круга задач в области управления персоналом в организациях и на предприятиях.

      2. В настоящем профессиональном стандарте применяются следующие термины и определения:

      1) Отраслевые рамки квалификаций (ОРК) – составная часть (подсистема) национальной системы квалификаций, рамочная структура дифференцированных уровней квалификации, признаваемых в отрасли

      2) Вид трудовой деятельности – часть профессиональной группы, совокупность профессий, сформированная целостным набором трудовых функций и необходимых для их выполнения компетенций

      3) Трудовая функция (функция) – набор взаимосвязанных действий, направленных на решение одной или нескольких задач процесса труда

      4) Профессиональная задача (задача) – нормативное представление о действиях, связанных с реализацией трудовой функции и достижением необходимого результата в определенной профессиональной группе или подгруппе

      5) Профессия – род занятий, осуществляемый физическим лицом и требующий определенной квалификации для его выполнения

      6) Должность – функциональное место в системе организационно-административной иерархии организации, служебное положение работника

      7) Занятие – набор работ, осуществляемых на рабочем месте, приносящих заработок или доход, характеризующихся высокой степенью совпадения выполняемых основных задач и обязанностей

      8) Знания – информация, нормы, используемые в индивидуальной и профессиональной деятельности

      9) Умение – способность физически и (или) умственно выполнять отдельные единичные действия в рамках профессиональной задачи;

      10) Компетенция – способность применять навыки, позволяющие выполнять одну или несколько профессиональных задач, составляющих трудовую функцию;

      11) Квалификация – официальное признание ценности в виде диплома, сертификата, подтверждающее наличие у лица компетенций, соответствующих требованиям к выполнению трудовых функций в рамках конкретного вида профессиональной деятельности (требований профессионального стандарта или требований, сложившихся в результате практики), сформированных в процессе образования, обучения или трудовой деятельности (обучения на рабочем месте, дающее право на осуществление трудовой деятельности

      3. В настоящем профессиональном стандарте применяются следующие сокращения:

      1) IPsec – Internet Protocol Security

      2) NGFW – Next-Generation Firewall

      3) DLP – Data Loss Prevention

      4) IDS – Intrusion Detection System

      5) ИКТ – Информационно-коммуникационные технологии

      6) ИТ – Информационные технологии;

      7) ИС – Информационные системы

      8) ПО – Программное обеспечение

      9) ОРК – Отраслевая рамка квалификации;

      10) ПС – Профессиональный стандарт

      11) ЕСКД – Единая система конструкторской документации

      12) ЕСТД – Единая система технологической документации

      13) ЕСПД – Единая система программной документации

      14) ЕТКС – Единый тарифно-квалификационный справочник работ и профессий рабочих

      15) ОКЭД – Общий классификатор видов экономической деятельности

      16) ПАС – Программно-аппаратные средства

      17) БД – Базы данных

      18) МСКО – Международная стандартная классификация образования

      19) НПА – нормативные правовые акты

      20) НТД – нормативно техническая документация

      21) ТЗИ – техническая защита информации

      22) ПЭМИН – побочные электромагнитные излучения и наводки

      23) ТКУИ – технические каналы утечки информации

      24) ИБ – информационная безопасность

      25) СУБД – Система управления базами данных

      26) ОС – Операционная система

      27) Стек – Это совокупность технологий, инструментов и компонентов, которые используются вместе для создания программного обеспечения или управления IT-инфраструктурой

      28) СВТ – средства вычислительной техники

**Глава 2. Паспорт профессионального стандарта**

      4. Название профессионального стандарта: Деятельность в области кибербезопасности

      5. Код профессионального стандарта: J056

      6. Указание секции, раздела, группы, класса и подкласса согласно ОКЭД:

      J Информация и связь

      62 Компьютерное программирование, консультационные и другие сопутствующие услуги

      62.0 Компьютерное программирование, консультационные и другие сопутствующие услуги

      62.09 Другие виды деятельности в области информационных технологий и информационных систем

      62.09.9 Другие виды деятельности в области информационных технологий и информационных систем, не включенные в другие группировки

      7. Краткое описание профессионального стандарта: Обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности

      8. Перечень карточек профессий:

      2) Специалист-криминалист по цифровым технологиям - 6 уровень ОРК

      3) Специалист по вопросам безопасности (ИКТ) - 7 уровень ОРК

      7) Специалист по безопасности сервисов - 6 уровень ОРК

      8) Аудитор по информационной безопасности - 6 уровень ОРК

      9) Шифровальщик данных - 6 уровень ОРК

      10) Аудитор по информационной безопасности - 7 уровень ОРК

      11) Специалист по информационной безопасности - 7 уровень ОРК

      12) Специалист по информационной безопасности - 6 уровень ОРК

      13) Инженер по защите информации - 6 уровень ОРК

      14) Инженер по защите информации - 7 уровень ОРК

      15) Специалист по безопасности сервисов - 7 уровень ОРК

      16) Шифровальщик данных - 7 уровень ОРК

      17) Специалист-криминалист по цифровым технологиям - 7 уровень ОРК

      18) Администратор по информационной безопасности - 7 уровень ОРК

      19) Специалист по защите информации - 7 уровень ОРК

      20) Специалист по вопросам безопасности (ИКТ) - 6 уровень ОРК

      21) Специалист по защите информации - 6 уровень ОРК

**Глава 3. Карточки профессий**

|  |  |  |  |
| --- | --- | --- | --- |
| 10. Карточка профессии "Специалист-криминалист по цифровым технологиям": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-008 | | |
| Наименование профессии: | Специалист-криминалист по цифровым технологиям | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Расследование компьютерных преступлений  2. Криминалистическая экспертиза цифровых устройств и оборудования | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Расследование компьютерных преступлений |  |  | |
| Навык 1:  Первичное реагирование на компьютерные преступления | Умения:  1. Определять источники и причины возникновения инцидентов;  2. Оценивать последствия выявленных инцидентов;  3. Идентифицировать проникновения в корпоративную сеть;  4. Устранять все установленные способы доступа злоумышленников в сеть организации;  5. Анализировать структуру механизма возникновения и обстоятельства события;  6. Определять причину и условия изменения программного обеспечения;  7. Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;  8. Выявлять несоответствия имеющейся информации ее расположению в системе. | |
| Знания:  1. Основные виды компьютерных преступлений;  2. Способы доступа злоумышленников в сеть организации;  3. Основные угрозы безопасности информации и модели нарушителя в ИС организации;  4. Принципы построения и функционирования систем и сетей передачи информации;  5. национальный стандарт в сфере обеспечения информационной безопасности;  6. Технические каналы "утечки" информации;  7. Нормативные правовые акты в области защиты информации;  8. Эталонная модель взаимодействия открытых систем;  9. Основные методы организации и проведения технического обслуживания технических средств информатизации;  10. Организационные меры по защите информации;  11. Регламент учета выявленных инцидентов;  12. Форматы хранения информации в анализируемой компьютерной системе;  13. Основные форматы файлов, используемые в компьютерных системах;  14. Порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов;  15. Уголовное законодательство Республики Казахстан;  16. Законодательство в области административных правонарушениях Республики Казахстан. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Планирование мер по предотвращению взломов и несанкционированного доступа | Умения:  1. Разрабатывать меры по предотвращению и своевременному обнаружению взломов;  2. Производить поиск уликовой информации на компьютерах;  3. Выявлять методы и средства контр криминалистики: полно дисковое шифрование, удаленное хранение информации;  4. Осуществлять сбор доказательной базы и ее оформление/хранение;  5. Моделировать реальную атаку на организацию с принятием мер по минимизации ущерба. | |
| Знания:  1. Принципы построения и функционирования систем и сетей передачи информации;  2. Эталонную модель взаимодействия открытых систем;  3. Национальный стандарт в сфере информационной безопасности;  4. Основные угрозы безопасности информации и модели нарушителя в ИС организации;  5. Методы и средства контр криминалистики;  6. Принципы построения средств защиты информации от "утечки" по техническим каналам;  7. Нормативные правовые акты в области защиты информации;  8. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС;  9. Методы сокрытия уликовых данных от обнаружения;  10. Документирование информации по расследованию. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Криминалистическая экспертиза цифровых устройств и оборудования |  |  | |
| Навык 1:  Криминалистическая экспертиза компьютеров | Умения:  1. Расследовать инциденты информационной безопасности;  2. Фиксировать время инцидента;  3. Проводить первичную диагностику компьютерного устройства;  4. Работать с аппаратными блокираторами записи и дубликаторами носителей информации;  5. Работать с дистрибутивами для криминалистического анализа;  6. Производить снятие образа (идентичной копии) жесткого диска (НМЖД) и других носителей информации, включая снятие образа с раздела или отдельного сектора жесткого диска;  7. Производить обработку сформированных образов дисков;  8. Осуществлять сбор данных с жестких дисков;  9. Осуществлять анализ файлов, найденных на жестких дисках;  10. Производить извлечение данных из файлов;  11. Производить исследование дампов оперативной памяти;  12. Производить поиск артефактов на жестком диске и периферии;  13. Работать с системными логами и журналами операционных систем и прикладных программ;  14. Восстанавливать удаленные данные;  15. Осуществлять сбор доказательной базы и ее оформление/хранение;  16. Проводить исследования на наличие ПЭМИН в средствах СВТ. | |
| Знания:  1. Файловые системы;  2. Операционные системы;  3. Основные принципы информационной безопасности и методы работы средств защиты;  4. Инструментарий компьютерной криминалистики;  5. Устройство жестких дисков и других накопителей;  6. Архитектуру и пользовательские интерфейсы операционных систем;  7. Архитектура, устройство и функционирование вычислительных систем;  8. Инструментарий для работы с файловой системой, включая восстановление данных;  9. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации;  10. Методы перехвата информации по ТКУИ;  11. Методику исследования средств СВТ на наличие ПЭМИН;  12. Методику проведения исследований средств СВТ на наличие незадекларированных технических возможностей. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Криминалистическая экспертиза сетевых устройств | Умения:  1. Производить анализ сетевого стека и браузеров;  2. Производить анализ email-сообщений и устанавливать принадлежность адреса электронной почты;  3. Работать с инструментарием для создания дампа сетевого трафика;  4. Осуществлять перехват и исследование сетевого трафика;  5. Осуществлять исследование логов web-серверов;  6. Устанавливать принадлежность и расположение IP-адреса;  7. Устанавливать принадлежность доменного имени. | |
| Знания:  1. Принципы построения и функционирования систем и сетей передачи информации;  2. Эталонную модель взаимодействия открытых систем;  3. Методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях;  4. Основные принципы проведения сетевой криминалистики;  6. Источники данных для проведения сетевой криминалистики и их исследование;  7. Особенности инструментария для создания дампа сетевого трафика. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Криминалистическая экспертиза мобильных устройств | Умения:  1. Осуществлять идентификацию устройства мобильной связи;  2. Осуществлять клонирование всех данных с цифрового устройства, периферийного оборудования и накопителей информации;  3. Осуществлять получение информации с мобильных телефонов;  4. Осуществлять получение информации с SIM-карты;  5. Осуществлять получение информации с встроенной и внешней карты памяти;  6. Осуществлять контроль почтовых отправлений, телеграфных и иных сообщений;  8. Работать с программными и аппаратными инструментальными средствами для доступа к данным мобильного телефона. | |
| Знания:  1. Принципы и устройства мобильной связи;  2. Программно-аппаратный инструментарий для доступа к данным мобильного телефона;  3. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации;  4. Мобильные операционные системы;  5. Файловые системы мобильных устройств. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Стрессоустойчивость  Умение работать в команде  Аналитическое мышление  Критическое мышление | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | - | |
| 11. Карточка профессии "Специалист по вопросам безопасности (ИКТ)": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-005 | | |
| Наименование профессии: | Специалист по вопросам безопасности (ИКТ) | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик: | -  - | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Противодействие вредоносному влиянию программно-технического воздействия на подсистемы, устройства, элементы и каналы инфокоммуникационных систем | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Оценивание уровня безопасности компьютерных систем и сетей  2. Разработка системы безопасности компьютерных систем и сетей | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Оценивание уровня безопасности компьютерных систем и сетей |  |  | |
| Навык 1:  Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации | Умения:  1.Определять параметры функционирования программно-аппаратных средств защиты информации;  2.Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации;  3.Оценивать эффективность защиты информации;  4.Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации;  5.Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия. | |
| Знания:  1.Принципы построения компьютерных систем и сетей;  2.Методы и методики оценки безопасности программно-аппаратных средств защиты информации;  3.Принципы построения программно-аппаратных средств защиты информации;  4.Принципы построения подсистем защиты информации в компьютерных системах;  5.Методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации;  6.Методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации;  7.Методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей;  8.Способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности;  9.Национальные, стандарты в сфере обеспечения информационной безопасности;  10.Нормативные правовые акты в сфере обеспечения ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Формирование политик безопасности компьютерных систем и сетей | Умения:  1.Анализировать компьютерную систему для определения необходимого уровня защищенности;  2.Разрабатывать профили защиты компьютерных систем;  3.Формулировать задания по безопасности компьютерных систем;  4.Выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации. | |
| Знания:  1.Принципы построения компьютерных систем и сетей;  2.Модели безопасности компьютерных систем;  3.Виды политик безопасности компьютерных систем и сетей;  4.Принципы построения средств криптографической защиты информации;  5.Национальные стандарты в сфере обеспечения ИБ;  6.Возможности используемых и планируемых к использованию средств защиты информации;  7.Нормативные правовые акты в сфере обеспечения ИБ.  . | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Проведение анализа безопасности компьютерных систем | Умения:  1.Анализировать компьютерную систему для определения уровня защищенности;  2.Прогнозировать возможные пути развития действий нарушителя информационной безопасности;  3.Производить анализ политики безопасности на предмет адекватности;  4.Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;  5.Составлять и оформлять аналитический отчет по результатам проведенного анализа;  6.Разрабатывать предложения по устранению выявленных уязвимостей. | |
| Знания:  1.Принципы построения компьютерных систем и сетей;  2.Уязвимости компьютерных систем и сетей;  3.Криптографические методы защиты информации;  4.Принципы построения систем управления базами данных;  5.Средства анализа конфигураций;  6.Национальные стандарты в сфере обеспечения ИБ;  7.Нормативные правовые акты в сфере обеспечения ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 4:  Проведение анализа безопасности компьютерных систем | Умения:  1. Анализировать компьютерную систему для определения уровня защищенности и доверия;  2. Прогнозировать возможные пути развития действий нарушителя информационной безопасности;  3. Производить анализ политики безопасности на предмет адекватности;  4. Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;  5. Составлять и оформлять аналитический отчет по результатам проведенного анализа;  6. Разрабатывать предложения по устранению выявленных уязвимостей;  7. Осуществлять мероприятия в рамках ТЗИ;  8. Проводить исследования на наличие ПЭМИН в средствах СВТ. | |
| Знания:  1. Принципы построения компьютерных систем и сетей;  2. Уязвимости компьютерных систем и сетей;  3. Криптографические методы защиты информации;  4. Принципы построения систем управления базами данных;  5. Средства анализа конфигураций;  6. Национальные стандарты в области защиты информации;  7. Нормативные правовые акты в сфере обеспечения ИБ;  10. Методы перехвата информации по ТКУИ;  11. Методика исследования средств СВТ на наличие ПЭМИН;  12. Методика проведения исследований средств СВТ на наличие незадекларированных технических возможностей. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Разработка системы безопасности компьютерных систем и сетей |  |  | |
| Навык 1:  Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей | Умения:  1.Формировать модели угроз и модели нарушителя безопасности компьютерных систем;  2.Выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы;  3.Разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;  4.Применять национальные стандарты в области защиты информации для оценки защищенности компьютерной системы;  5.Осуществлять принятие решений о необходимости использования программно-аппаратных средств защиты информации. | |
| Знания:  1.Порядок организации работ по защите информации;  2.Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях;  3.Методы анализа безопасности компьютерных систем;  4.Виды атак и механизмы их реализации в компьютерных системах;  5.Методы выявления каналов утечки информации;  6.Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных;  7.Принципы построения средств защиты информации компьютерных систем;  8.Формальные модели управления доступом;  9.Криптографические алгоритмы и особенности их программной реализации;  10.Нормативные правовые акты в сфере обеспечения ИБ;  12.Национальные стандарты в сфере обеспечения ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей | Умения:  1.Проводить исследования для нахождения наиболее целесообразных практических решений по обеспечению защиты информации;  2.Разрабатывать архитектуру и интерфейсы средств защиты информации,  3. Проводить процедуры восстановления работоспособности средств и систем защиты после сбоев. | |
| Знания:  1.Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях;  2.Виды атак и механизмы их реализации в компьютерных системах;  3.Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных;  4.Принципы построения систем защиты информации компьютерных систем, в том числе антивирусного программного обеспечения;  5.Методы анализа безопасности компьютерных систем;  6.Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации;  7.Формальные модели управления доступом;  8.Принципы и методы проектирования программно-аппаратного обеспечения;  9.Методологии и технологии разработки программного обеспечения;  10.Принципы и методы управления проектами в области информационной безопасности;  11.Криптографические алгоритмы и особенности их программной реализации;  12.Нормативные правовые акты в сфере обеспечения ИБ;  13.Национальные стандарты в сфере обеспечения ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Аналитическое мышление  Критический анализ  Системное мышление  Умение решать нестандартные задачи  Внимательность к деталям | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | Специалист по вопросам безопасности (ИКТ) | |
| 15. Карточка профессии "Специалист по безопасности сервисов": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-004 | | |
| Наименование профессии: | Специалист по безопасности сервисов | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Производить поиск и обнаруживать уязвимые места системы для несанкционированного доступа | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Взаимодействие с разработчиками и менеджерами сервисов для устранения обнаруженных уязвимостей  2. Выступление консультантом и заказчиком новой функциональности, связанной с информационной безопасностью | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Взаимодействие с разработчиками и менеджерами сервисов для устранения обнаруженных уязвимостей |  |  | |
| Навык 1:  Сбор и анализ информации об обнаруженных уязвимостях сервисов | Умения:  1. Применять инструменты и методы сбора информации об уязвимостях;  2. Анализировать полученные данные об уязвимостях;  3. Классифицировать и приоритизировать уязвимости по степени критичности;  4. Выявлять потенциальные угрозы и риски, связанные с обнаруженными уязвимостями. | |
| Знания:  1. Методологии анализа уязвимостей;  2. Источники информации об уязвимостях (базы данных уязвимостей, отчеты безопасности);  3. Основные виды атак и их последствия;  4. Основные принципы и методы тестирования безопасности;  5. Современные подходы к анализу угроз и рисков. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Постановка и прием задачи по устранению обнаруженных уязвимостей сервисов | Умения:  1. Формулировать задачи для разработчиков по устранению уязвимостей;  2. Разрабатывать рекомендации по исправлению уязвимостей;  3. Контролировать процесс исправления уязвимостей и оценивать его результат;  4. Взаимодействовать с командами разработки и управления сервисами по вопросам безопасности;  5. Проверять корректность внедренных исправлений. | |
| Знания:  1. Методы предотвращения сетевых атак;  2. Методы анализа защищенности внешнего периметра корпоративной сети;  3. Методы анализа защищенности внутренней ИТ-инфраструктуры объекта аудита;  4. Методы и порядок проведения тестирования ПО;  5. Языки программирования (Python, Bash, PowerShell, JS, SQL). | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Выступление консультантом и заказчиком новой функциональности, связанной с информационной безопасностью |  |  | |
| Навык 1:  Подготовка и размещение публикаций и сообщений о сервисах в средствах массовой информации и других открытых доступных источниках | Умения:  1. Разрабатывать аналитические и экспертные материалы по вопросам информационной безопасности;  2. Адаптировать сложные технические сведения для различных целевых аудиторий, включая топ-менеджмент и технических специалистов;  3. Формировать стратегию информационного продвижения в сфере безопасности;  4. Организовывать публикации в специализированных изданиях и на профессиональных платформах;  5. Контролировать соответствие публикаций требованиям конфиденциальности и нормативным требованиям. | |
| Знания:  1. Стандартов распространенных форматов текстовых и табличных данных;  2. Методов создания рекламных текстов;  3. Законодательства РК в области интеллектуальной собственности;  4. Правил использования информационных материалов в Интернет. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Проведение демонстрации возможностей продукта | Умения:  1. Разрабатывать сценарии демонстрации продукта с учетом потребностей бизнеса и специфики отрасли;  2. Адаптировать демонстрационные материалы под различные категории заказчиков и партнеров;  3. Аргументированно представлять конкурентные преимущества продукта;  4. Управлять процессом презентации, вовлекать аудиторию и эффективно реагировать на вопросы;  5. Анализировать эффективность демонстрации и разрабатывать предложения по совершенствованию продукта. | |
| Знания:  1. Устройства и возможности продукта;  2. Управления программами;  3. Показатели эффективности;  4. Современные подходы к разработке и интеграции безопасных IT-решений;  5. Национальные стандарты в сфере обеспечения информационной безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Гибкость мышления  Умение работать в команде  Дисциплинированность  Инициативность  Организованность  Внимательность  Исполнительность  Ориентация на результат  Высокая обучаемость | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2015 "Информационная технология. Методы и средства обеспечения безопасности Системы менеджмента информационной безопасностью" СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | Специалист по безопасности сервисов | |
| 16. Карточка профессии "Аудитор по информационной безопасности": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-002 | | |
| Наименование профессии: | Аудитор по информационной безопасности | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Проводить аудиторскую проверку по определению уровней безопасности | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Оценка и анализ рисков информационной безопасности  2. Обеспечение задач аудиторского задания  3. Выполнение задач аудиторского задания | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Оценка и анализ рисков информационной безопасности |  |  | |
| Навык 1:  Применение методов анализа рисков для идентификации и оценки угроз | Умения:  1. Использование методик анализа рисков для идентификации и оценки угроз.  2. Разработка комплексных стратегий по минимизации рисков и устранению уязвимостей в информационных системах.  3. Оценка воздействия потенциальных угроз на организацию, разработка планов по снижению рисков. | |
| Знания:  1. Методы анализа рисков, включая как качественные, так и количественные методы.  2. Принципы управления рисками и их минимизации.  3. Инструменты и технологии для проведения анализа рисков и оценки уязвимостей.  4. Современные методологии анализа рисков, включая использование Big Data для предсказания угроз. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Разработка и внедрение политики безопасности на основе оценки рисков и потребностей. | Умения:  1. Разработка политики безопасности, стандартов и процедур защиты информации для организации.  2. Внедрение стандартизированных процессов безопасности, их адаптация под нужды организации.  3. Формирование и поддержка культуры безопасности в организации через регулярное обновление политик. | |
| Знания:  1. Принципы и подходы к разработке политики информационной безопасности.  2. Национальный стандарт в области разработки и внедрения политики безопасности  3. Технологии защиты информации на уровне корпоративной инфраструктуры. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Обеспечение задач аудиторского задания |  |  | |
| Навык 1:  Методическое обеспечение аудита ИБ | Умения:  1. Участвовать в разработке (актуализации) методических и организационно-распорядительных документов, регламентирующих аудиторскую деятельность;  2. Проводить презентации методических и организационно-распорядительных документов;  3. Проводить ознакомление сотрудников с регламентирующей документацией. | |
| Знания:  1. Порядок разработки, оформления и утверждения методических и организационно-распорядительных документов;  2. Национальные стандарты в сфере обеспечения информационной безопасности;  3. Эффективных методов ознакомления персонала с методическими документами обеспечения аудита ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Организационное обеспечение аудита ИБ | Умения:  1. Участвовать в организации взаимодействия с представителями проверяемой организации (подразделения) по вопросам аудита ИБ;  2. Осуществлять сбор руководящих документов (приказы, распоряжения, инструкции) по вопросам хранения, порядка доступа и передачи информации;  3. Проводить аудит ИБ. | |
| Знания:  1. Этапы и формы деловой коммуникации;  2. Принципы и правила общения в деловой среде;  3. Порядков проведения аудита ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Консультирование по вопросам безопасности на всех уровнях организации. | Умения:  1. Обучение сотрудников методам защиты данных и созданию безопасной рабочей среды.  2. Консультирование по вопросам соблюдения политики безопасности, рекомендаций по безопасному использованию информационных технологий.  3. Проведение регулярных консультаций для руководства о текущих угрозах и методах их предотвращения. | |
| Знания:  1. Принципы защиты данных, методы контроля за соблюдением стандартов безопасности.  2. Психология и требования безопасности для сотрудников.  3. Процессы и процедуры для построения и поддержания политики безопасности в организации. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 3:  Выполнение задач аудиторского задания |  |  | |
| Навык 1:  Подготовка отчета и представление результатов внешним и внутренним аудиторам. | Умения:  1. Создание отчетов с выводами и рекомендациями по улучшению системы защиты данных,  2. Обсуждение и представление результатов аудита с внутренними и (или) внешними аудиторами;  3. Проведение визуализациии данных для улучшения восприятия отчета и принятия решений. | |
| Знания:  1. Основы отчетности и метрики эффективности безопасности;  2. Законодательство в сфере информатизации;  3. Подходы к обеспечению соответствия нормативным требованиям и сертификациям. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Проверка и анализ фактического соблюдения требований НПА и НТД в сфере ИКТ и обеспечения ИБ в процессах обеспечения ИБ объекта аудита ИБ | Умения:  1. Собирать и изучать проектную и эксплуатационную документацию на ИС, интервьюировать сотрудников и регистрировать сведения.  2. Оценивать применимость НПА и НТД к объекту аудита ИБ.  3. Оценивать соответствие принятых организационных и программно- технических решений обеспечения ИБ требованиям НПА и НТД.  4. Определять и оценивать вероятные угрозы безопасности в отношении ресурсов объекта аудита и уязвимостей защиты.  5. Анализировать риски, связанные с возможностью осуществления угроз безопасности в отношении ресурсов объекта аудита ИБ.  6. Выявлять узкие места в системе защиты и архитектуре объекта аудита ИБ. | |
| Знания:  1. Законодательство в сфере обеспечения информационной безопасности;  2. Методики, программных средств выявления рисков и угроз ИБ;  3. Методов, процедур и порядка сбора аудиторских свидетельств. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Проверка и анализ текущего состояния защищенности объекта аудита ИБ | Умения:  1. Проверять состояние физической безопасности объекта аудита.  2. Проверять характеристики безопасности объекта аудита, связанные с архитектурой.  3. Проверять характеристики безопасности, связанные с конфигурацией встроенных механизмов ИБ серверного и сетевого оборудования объекта аудита.  4. Проверять конфигурации ПО на наличие эксплуатационных уязвимостей. | |
| Знания:  1. Методы предотвращения сетевых атак.  2. Методы анализа защищенности внешнего периметра корпоративной сети.  3. Методы анализа защищенности внутренней ИТ-инфраструктуры объекта аудита.  4. Методы и порядок проведения тестирования ПО. | |
| Возможность признания навыка: | Не требуется | |
| Навык 4:  Выявление уязвимостей программного обеспечения объекта аудита | Умения:  1. Проводить статический анализ исходного кода ПО  2. Проводить динамический анализ исходного кода  3. Выявлять уязвимости ПО объекта аудита | |
| Знания:  1. Программные средства обнаружения недостатков ПО.  2. Методы статического анализа программного кода.  3. Методы динамического анализа программного кода.  4. Инструментальные средства анализа защищенности и уязвимостей.  5. Языки программирования (Python, Bash, PowerShell, JS, SQL) | |
| Возможность признания навыка: | Не требуется | |
| Навык 5:  Тестирование ПО на работоспособность в различных режимах нагрузки | Умения:  1. Составлять сценарии тестирования ПО по принципу "черного ящика" и "белого ящика".  2. Выполнять сценарии тестирования ПО в тестовой среде и в закрытой среде (sandbox).  3. Анализировать поведение ПО в процессе тестирования.  4. Тестировать ПО на предельные режимы работы.  5. Проверять объект аудита на устойчивость к сетевым атакам (DDoS, flood и другим).  6. Проверять процедуры аутентификации под нагрузкой в условиях сетевой атаки. | |
| Знания:  1. Методы и программные средства анализа защищенности и уязвимостей.  2. Методы и программные средства для проведения нагрузочного тестирования.  3. Методы и программные средства для проведения отладки программ.  4. Языки программирования (Python, Bash, PowerShell, JS, SQL) | |
| Возможность признания навыка: | Не требуется | |
| Навык 6:  Выявление уязвимостей оборудования сети объекта аудита | Умения:  1. Идентифицировать и инвентаризовать ресурсы сети.  2. Идентифицировать и учитывать сервисы и информационные потоки сети.  3. Сканировать уязвимости уровня ОС хостов сети в сегментах сети.  4. Идентифицировать и учитывать настройки безопасности сегментов сети.  5. Создавать и анализировать отчеты о соответствии стандартам ИБ. | |
| Знания:  1. Методы и программные средства анализа защищенности и уязвимости  2. Техники инвентаризации ресурсов сети  3. Принципы формирования отчҰтов ИБ | |
| Возможность признания навыка: | Не требуется | |
| Навык 7:  Документирование процесса и результата выполнения задачи аудиторского задания | Умения:  1. Осуществлять подготовительную работу перед документированием  2. Формировать, вести, хранить рабочую документацию аудиторского задания  3. Готовить итоговый документ, формируемый по результатам аудиторского задания | |
| Знания:  1. Порядок проведения подготовительных мероприятий, предшествующих документированию  2. Принципы формирования и ведения рабочей и отчетной документации  3. Методы систематизации и обобщения результатов аудита | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Гибкость мышления  Умение работать в команде  Дисциплинированность  Инициативность  Организованность  Исполнительность  Ориентация на результат  Внимательность  Высокая обучаемость | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | Аудитор по информационной безопасности | |
| 17. Карточка профессии "Шифровальщик данных": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-009 | | |
| Наименование профессии: | Шифровальщик данных | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: | 4419-9-003 - Кодировщик | | |
| Основная цель деятельности: | Разработка и эксплуатация систем шифрования данных | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Эксплуатация систем шифрования данных  2. Оценивание уровня безопасности систем шифрования данных | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Эксплуатация систем шифрования данных |  |  | |
| Навык 1:  Управление функционированием системам шифрования данных | Умения:  1. Осуществлять организацию бесперебойного функционирования систем шифрования данных;  2. Устанавливать и настраивать параметры сетевых протоколов, реализованных в системах шифрования данных;  3. Разрабатывать предложения по совершенствованию и повышению эффективности принимаемых технических мер и проводимых организационных мероприятий по защите систем шифрования данных;  4. Организовывать работы по выполнению требований режима защиты информации ограниченного доступа к системам шифрования данных;  5. Разрабатывать методические материалы и организационно-распорядительные документы по системам шифрования данных. | |
| Знания:  1. Архитектура, устройство и функционирование вычислительных систем;  2. Сетевые протоколы и их параметры настройки;  3. Особенности применения программных, программно-аппаратных и технических средств в системах шифрования данных;  4. Методы комплексного обеспечения защиты систем шифрования данных;  5. Показатели эффективности применяемых программных, программно-аппаратных и технических средств в системах шифрования данных;  6. Нормативные правовые акты в области защиты информации ограниченного доступа;  7. Национальные стандарты в сфере обеспечения информационной безопасности;  8. Устройство и функционирование современных систем шифрования данных. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Ведение специального делопроизводства и технических документов в процессе эксплуатации | Умения:  1. Выполнять задачи по получению, хранению, учету, выдаче, приему и утилизации специальных документов, применяемых в процессе эксплуатации систем шифрования данных;  2. Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт систем шифрования данных;  3. Вести эксплуатационную документацию систем шифрования данных. | |
| Знания:  1. Правила ведения специального делопроизводства и технических документов систем обеспечения данных;  2. Нормативные правовые акты в сфере обеспечения информационной безопасности;  3. Организационные меры по защите информации в системах шифрования данных;  4. Законодательство в сфере обеспечения информационной безопасности;  5. Устройство и функционирование современных систем шифрования данных. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Оценивание уровня безопасности систем шифрования данных |  |  | |
| Навык 1:  Проведение контрольных проверок работоспособности и эффективности систем шифрования данных | Умения:  1. Определять параметры функционирования программно-аппаратных средств системы шифрования данных;  2. Разрабатывать методики оценки эффективности программно-аппаратных средств систем шифрования данных;  3. Оценивать эффективность программно-аппаратных средств систем шифрования данных;  4. Анализировать программно-аппаратные средства систем шифрования данных с целью определения уровня обеспечиваемой ими защищенности и доверия. | |
| Знания:  1. Методы и методики оценки эффективности программно-аппаратных средств систем шифрования данных;  2. Принципы построения программно-аппаратных средств систем шифрования данных;  3. Методы и средства оценки корректности и эффективности программных реализаций алгоритмов шифрования информации;  4. Методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Проведение анализа безопасности систем шифрования данных | Умения:  1. Анализировать системы шифрования данных с целью определения уровня защищенности и доверия;  2. Прогнозировать возможные пути развития действий нарушителя ИБ;  3. Производить анализ политики безопасности на предмет адекватности;  4. Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств в системах шифрования данных;  5. Составлять и оформлять аналитический отчет по проведенному анализу;  6. Разрабатывать предложения по устранению выявленных уязвимостей. | |
| Знания:  1. Уязвимости компьютерных систем и сетей;  2. Криптографические методы защиты информации;  3. Средства анализа конфигураций. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Структурное мышление  Усидчивость и внимательность  Аналитический ум  Способность к самообучению  Математические способности | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК 1073-2007 Средства криптографической защиты информации. Общие технические требования | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | Шифровальщик данных | |
| 18. Карточка профессии "Аудитор по информационной безопасности": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-002 | | |
| Наименование профессии: | Аудитор по информационной безопасности | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Планировать и контролировать аудит ИБ | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Планирование аудита ИБ  2. Обеспечение аудита ИБ  3. Контроль аудита ИБ | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Планирование аудита ИБ |  |  | |
| Навык 1:  Планирование работы подразделения аудита ИБ | Умения:  1. Планировать работы подразделения аудита ИБ.  2. Анализировать, выбирать (разрабатывать) методику проведения аудита.  3. Управлять проектами. | |
| Знания:  1. Методологических основ аудиторской деятельности.  2. Методов организации аудиторских проверок.  3. Способов, методов и техники проведения аудита. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Планирование аудиторской проверки | Умения:  1. Определять объемы, масштабы аудита;  2. Определять ресурсы, необходимые для выполнения аудита;  3. Подбирать (назначать) членов аудиторской группы;  4. Распределять аудиторские задания и устанавливать конкретные сроки их выполнения;  5. Готовить и согласовывать план и программу проведения аудита ИБ. | |
| Знания:  1. Законодательство в сфере обеспечения информационной безопасности;  2. Методологии, методики и технологии планирования аудита;  3. Методики управления проектами. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Обеспечение аудита ИБ |  |  | |
| Навык 1:  Стратегическое руководство и управление процессами информационной безопасности | Умения:  1. Формирование стратегии информационной безопасности, соответствующей бизнес-целям и угрозам;  2. Разработка планов по интеграции инновационных технологий в процесс защиты информации;  3. Оценка долгосрочных угроз безопасности и создание сценариев реагирования. | |
| Знания:  1. Основные требования к системе менеджмента по информационной безопасности;  2. Подходы к управлению и снижению рисков кибербезопасности;  3. Принципы управления рисками и их минимизации в контексте информационной безопасности;  4. Законодательство в сфере информатизации. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Организационное обеспечение ИБ | Умения:  1. Организовывать взаимодействие с представителями проверяемой организации (подразделения) по вопросам аудита ИБ;  2. Организовывать обучение и повышение квалификации аудиторов ИБ;  3. Управлять аудиторской деятельностью. | |
| Знания:  1. Этапы и формы деловой коммуникации;  2. Принципы и правила общения в деловой среде;  3. Форм и методы обучения и повышения квалификации персонала на рабочем месте;  4. Этапы процесса обучения и повышения квалификации персонала. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Консультирование и инструктаж работников организации по вопросам аудита ИБ | Умения:  1. Консультировать работников проверяемой организации (подразделения) по вопросам, связанным с аудитом ИБ;  2. Консультировать участников аудиторской группы по нерешенным сложным и спорным вопросам, связанным с выполнением аудиторского задания;  3. Инструктировать аудиторскую группу перед заданием с целью уяснения и понимания ее членами целей и задач. | |
| Знания:  1. Национальный стандарт по управлению рисками информационной безопасности;  2. Методология оценки рисков (OCTAVE);  3. Описание модели руководства и управления ИТ на предприятии;  4. Технологии и инструменты для проведения оценки рисков и мониторинга угроз. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 3:  Контроль аудита ИБ |  |  | |
| Навык 1:  Контроль аудиторского задания | Умения:  1. Контролировать сроки выполнения процедур аудиторского задания.  2. Контролировать качество выполнения процедур аудиторского задания.  3. Контролировать соблюдение аудиторами организационно- распорядительных документов, регламентирующих аудиторскую деятельность. | |
| Знания:  1. Методы защиты персональных данных в облачных сервисах;  2. Принципы криптографии и стандарты для защиты данных;  3. Современные технологии киберзащиты: машинное обучение, искусственный интеллект, блокчейн. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Контроль профессиональных качеств аудитора | Умения:  1. Контролировать соблюдение аудиторами ИБ правил независимости и принципов этики при выполнении аудиторских заданий.  2. Анализировать и оценивать профессиональные знания и качество аудиторов ИБ  3. Работать с аудиторами ИБ для совершенствования их профессиональных навыков | |
| Знания:  1. Национальные стандарты контроля качества аудита  2. Нормативно-правовые акты аудита по обеспечению ИБ  3. Требования по ведению аудита по ИБ | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Проведение тестов на проникновение для оценки безопасности системы | Умения:  1. Проведение комплексных проверок системы безопасности с целью выявления уязвимостей.  2. Использование методов тестирования на проникновение (penetration testing) для оценки защищенности системы.  3. Применение средств мониторинга для постоянного отслеживания эффективности защиты информации. | |
| Знания:  1. Инструменты и методы тестирования на проникновение (например, Metasploit, Nessus, Burp Suite).  2. Технологии обнаружения и предотвращения атак (IDS, IPS).  3. Принципы проведения аудита безопасности на основе реальных сценариев угроз. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Умения интегрировать знания  Анализировать ситуацию  Умение распознавать изменения в бизнес-среде и определять стратегическое направление развития подразделения и/или предприятия | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2015 "Информационная технология. Методы и средства обеспечения безопасности Системы менеджмента информационной безопасностью" СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | Аудитор по информационной безопасности | |
| 19. Карточка профессии "Специалист по информационной безопасности": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-007 | | |
| Наименование профессии: | Специалист по информационной безопасности | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности при наличии базового (высшего) ИТ образования | | |
| Другие возможные наименования профессии: | 2524-0-003 - Инженер по защите информации  2524-0-004 - Специалист по безопасности сервисов  2524-0-006 - Специалист по защите информации  2524-0-005 - Специалист по вопросам безопасности (ИКТ) | | |
| Основная цель деятельности: | Контролировать процесс управления и обеспечения ИБ организации | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Координирование процессов обеспечения ИБ  2. Анализ и контроль мероприятий по управлению и обеспечению ИБ | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Координирование процессов обеспечения ИБ |  |  | |
| Навык 1:  Постановка задач и контроль их выполнения в сфере обеспечения ИБ | Умения:  1. Координировать деятельность по разработке (актуализации) политики ИБ, ТД процессов управления ИБ и документов, регламентирующих процессы обеспечения ИБ.  2. Публиковать и доводить утвержденную (актуализированной) политику ИБ организации до сведения сотрудников.  3. Участвовать в разработке соглашений о конфиденциальности или неразглашении информации с сотрудниками организации, подрядчиками и третьими сторонами | |
| Знания:  1. Базовые принципы регламентации бизнес-процессов;  2. Законодательства в сфере обеспечения ИБ;  3. Национальные стандарты в сфере обеспечения ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Планирование процессов управления и обеспечения ИБ организации | Умения:  1. Оценивать текущий уровень НТД, регламентирующих процессы обеспечения ИБ;  2. Разрабатывать (актуализировать) ТД, регламентирующие процессы обеспечения ИБ;  3. Разрабатывать профили защиты и задания по безопасности для ИС и компонентов информационно- коммуникационной инфраструктуры. | |
| Знания:  1. Принципы защитных механизмов программных и аппаратных средств организации;  2. Научные исследования в сфере обеспечения ИБ;  3. Принципы и методологию проектирования ИС. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Анализ и контроль мероприятий по управлению и обеспечению ИБ |  |  | |
| Навык 1:  Подготовка планов мероприятий по обеспечению ИБ организации | Умения:  1. Анализировать защищенности бизнес- процессов и активов, связанных с автоматизированной обработкой информации;  2. Выбирать инструментарий и методы обеспечения ИБ;  3. Разрабатывать мероприятия, направленные на реализацию политики ИБ организации;  4. Составлять план по обеспечению непрерывности бизнеса и восстановления после инцидентов ИБ и форс-мажорных ситуаций. | |
| Знания:  1. Основные тенденции развития отечественного и зарубежного рынка инструментариев и средств обеспечения ИБ;  2. Принципы и методы выявления и блокирования каналов утечки информации;  3. НТД и методы классификации, учета и маркировки активов, связанных с обработкой информации;  4. НТД в сфере обеспечения непрерывности бизнес-процессов. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Подготовка технической документации для осуществления закупок оборудования, программных средств и систем (подсистем) | Умения:  1. Разрабатывать технические спецификации, тендерную документацию на закупаемые средства обеспечения ИБ.  2. Разрабатывать требования, технические задания на подсистемы ИБ ИС.  3. Организовывать и координировать работы по разработке профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры. | |
| Знания:  1. Подходы к формированию требований и оценке безопасности ИС.  2. Принципы и методологию проектирования ИС.  3. Способы применения защитных механизмов программных и аппаратных средств организации. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Гибкость мышления  Дисциплинированность  Инициативность  Умение работать в команде | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | специалист по информационной безопасности | |
| 20. Карточка профессии "Специалист по информационной безопасности": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-007 | | |
| Наименование профессии: | Специалист по информационной безопасности | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: |  | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Планирование, контроль, мониторинг и обеспечение ИБ | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Рассмотрение процессов управления ИБ организации  2. Планирование процессов обеспечения ИБ  3. Осуществление мероприятий по обеспечению ИБ  4. Контроль процессов управления и обеспечения ИБ | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Рассмотрение процессов управления ИБ организации |  |  | |
| Навык 1:  Разработка (актуализация) нормативно- техническую документацию, регламентирующие процессы управления ИБ | Умения:  1. Координация аналитической работы по ИБ;  2. Анализ, выбор методик и методов оценки и реализации процессов управления ИБ охватывающие процессы управления рисками, активами; инцидентами, техническими уязвимостями, угрозами, техническим противодействиям угрозам, непрерывностью бизнеса;  3. Согласование НТД процессов управления ИБ;  4. Координация деятельности по разработке (актуализации) политики ИБ, НТД процессов управления ИБ и документов, регламентирующих процессы обеспечения ИБ;  5. Публикация и доведение утвержденной (актуализированной) политики ИБ организации до сведения сотрудников. | |
| Знания:  1. Базовые принципы регламентации бизнес- процессов;  2. Законодательство в сфере обеспечения информационной безопасности;  3. Национальные стандарты в области ИБ;  4. Принципы и методологии проектирования и эксплуатации ИС;  5. Принципы регламентации бизнес-процессов;  6. Методы управления проектами;  7. Методики оценки и управления рисками ИБ;  8. Методика анализа угроз и уязвимостей ИС;  9. Методы классификации, учета и маркировки активов, связанных с обработкой информации. | |
| Возможность признания навыка: | не требуется | |
| Навык 2:  Разработка (актуализация) НТД, регламентирующих процессы обеспечения ИБ | Умения:  1. Оценивать текущий уровень НТД, регламентирующих процессы обеспечения ИБ;  2. Разрабатывать (актуализировать) ТД, регламентирующие процессы обеспечения ИБ;  3. Разрабатывать профили защиты и задания по безопасности для ИС и компонентов информационно- коммуникационной инфраструктуры. | |
| Знания:  1. Принципы защитных механизмов программных и аппаратных средств организации;  2. Принципы построения системы управления ИБ;  3. Принципы и методология проектирования ИС. | |
| Возможность признания навыка: | не требуется | |
| Трудовая функция 2:  Планирование процессов обеспечения ИБ |  |  | |
| Навык 1:  Планирование мероприятий по обеспечению информационной безопасности | Умения:  1. Проводить инвентаризацию, классификацию, маркировку активов, связанных с автоматизированной обработкой информации;  2. Составлять отчҰтную документацию по результатам категоризации активов;  3. Выявлять недостатки в активах обеспечения ИБ. | |
| Знания:  1. Законодательство в сфере обеспечения ИБ;  2. Национальные стандарты в сфере обеспечения ИБ;  3. Принципы, методы и средства обеспечения ИБ при определении мероприятий по непрерывности бизнеса, регистрации и учету событий ИБ, резервному копированию, антивирусной защите, контролю доступа, работе со съемными носителями, мобильными устройствами, удаленного доступа, использованием криптографии и их носителей, лицензиях и версиях ПО. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Идентификация рисков, угроз и каналов утечек для бизнес-процессов и активов, связанных с автоматизированной обработкой информации | Умения:  1. Выявлять риски, угрозы и каналы утечек для бизнес-процессов и активов, связанных с автоматизированной обработкой информации;  2. Осуществлять мероприятия в рамках ТЗИ;  3. Проводить исследования на наличие ПЭМИН в средствах СВТ. | |
| Знания:  1. Методику и средства выявления каналов утечки информации;  2. НТД, методику выявления рисков и угроз ИБ;  3. Методы перехвата информации по ТКУИ;  4. Методику исследования средств СВТ на наличие ПЭМИН;  5. Методику проведения исследований средств СВТ на наличие незадекларированных технических возможностей. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 3:  Осуществление мероприятий по обеспечению ИБ |  |  | |
| Навык 1:  Реализация плана мероприятий по обеспечению ИБ | Умения:  1. Анализ защищенности бизнес-процессов и активов, связанных с автоматизированной обработкой информации;  2. Выбор инструментария и методов обеспечения ИБ;  3. Разработка мероприятий, направленных на реализацию политики ИБ организации;  4. Составление плана по обеспечению непрерывности бизнеса и восстановления после инцидентов ИБ и форс-мажорных ситуаций;  5. Разработка технических спецификаций, тендерной документации на закупаемые средства обеспечения ИБ;  6. Разработка требований, технических заданий на подсистемы ИБ ИС;  7. Организация и координация работ по разработке профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной  инфраструктуры. | |
| Знания:  1. Методика описания и формализации бизнес-процессов;  2. Принципы и методы выявления и блокирования каналов утечки информации;  3. Законодательство в сфере обеспечения ИБ;  4. Средства обеспечения ИБ, систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации, защитных механизмов систем;  5. Национальные стандарты в сфере обеспечения ИБ;  6. Подходы к формированию требований и оценке безопасности ИС;  7. Принципы и методологии проектирования ИС;  8. Способы применения защитных механизмов программных и аппаратных средств организации. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Контроль соответствия настроек функций безопасности компонентов ИС и ИКИ установленным требованиям | Умения:  1. Осуществлять контроль разделения сред разработки, тестирования и эксплуатации ИС;  2. Осуществлять текущий контроль технологического процесса обработки защищаемой информации;  3. Осуществлять контроль реализации профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры. | |
| Знания:  1. Базовые принципы и способы выполнения работ по разработке, тестированию и апробации средств и методов ИБ;  2. Правила эксплуатации программных средств, защитных механизмов, компонентов ИС и ИКИ;  3. Методы выявления нарушений в настройках. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 4:  Контроль процессов управления и обеспечения ИБ |  |  | |
| Навык 1:  Оценка соответствия процессов информационной безопасности | Умения:  1. Осуществление контроля реализации плана мероприятий по обеспечению ИБ;  2. Анализ результатов проверок исполнения требований документов, регламентирующих процессы обеспечения ИБ и НТД процессов управления ИБ в организации;  3. Участие в разработке соглашений о конфиденциальности или неразглашении информации с сотрудниками организации  подрядчиками и третьими сторонами. | |
| Знания:  1. Принципы и средства администрирования в ОС и встроенных в них механизмов защиты;  2. Принципы функционирования ПАС обеспечения ИБ;  3. Принципы построения и применения, систем мониторинга уязвимостей, систем мониторинга ИБ;  4. Системы предотвращения утечек информации;  5. Методы определения, предотвращения и устранения последствий инцидентов ИБ, критических (аварийных) ситуаций. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Администрирование и мониторинг функционирования СКУД и систем видеонаблюдения | Умения:  1. Администрировать СКУД и системы видеонаблюдения;  2. Проводить мониторинг функционирования СКУД и системы видеонаблюдения;  3. Формировать выводы о соответствии принятых решений максимальному уровню ИБ. | |
| Знания:  1. Назначение, технические характеристики, конструкцию, особенности СКУД;  2. Правила эксплуатации СКУД и систем видеонаблюдения;  3. Назначение, технические характеристики, конструкцию, особенности систем видеонаблюдения. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Умение работать в команде  Дисциплинированность  Инициативность  Организованность  Внимательность  Исполнительность  Планирование  Принятие решения  Ориентация на результат  Стремление к повышению профессионального уровня | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | Специалист по информационной безопасности | |
| 21. Карточка профессии "Инженер по защите информации": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-003 | | |
| Наименование профессии: | Инженер по защите информации | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: | Параграф 2 Приказа Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих"  Инженер по защите информации | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: | Высшее (или послевузовское) образование по соответствующему направлению подготовки кадров без предъявления требований к стажу работы или техническое и профессиональное, послесреднее (среднее специальное, среднее профессиональное) образование по соответствующей специальности (квалификации) и стаж работы в должности техника по защите информации I категории не менее 3 лет. | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Обеспечить работоспособность прикладного и системного программного обеспечения средствами защиты информации | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Создание системы защиты информации в организации  2. Ввод в эксплуатацию системы защиты информации в организации | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Создание системы защиты информации в организации |  |  | |
| Навык 1:  Определение перечня информации (сведений) ограниченного доступа, подлежащих защите в организации | Умения:  1. Выполнять работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и технических мер защиты информационных систем;  2. Проводить исследования для выбора наиболее целесообразных практических решений;  3. Осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации;  4. Участвовать в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации;  5. Составлять методики расчетов и программы экспериментальных исследований по технической защите информации, выполнять расчеты в соответствии с разработанными методиками и программами;  6. Проводить сопоставительный анализ данных исследований и испытаний, изучать возможные источники и каналы утечки информации;  7. Осуществлять разработку технического обеспечения системы защиты информации, техническое обслуживание средств защиты информации, 8. Принимать участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов;  9. Составлять информационные обзоры по технической защите информации;  10. Выполнять оперативные задания, связанные с обеспечением контроля технических средств и механизмов системы защиты информации, участвовать в проведении проверок организаций по выполнению требований нормативно-технической документации по защите информации, в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию;  11. Готовить предложения по заключению соглашений и договоров с иными организациями, предоставляющими услуги в области технических средств защиты информации, составлять заявки на необходимые материалы, оборудование, приборы;  12. Участвовать в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности;  13. Проводить контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности принимаемых мер;  14. Изучать и обобщать опыт работы иных организаций по использованию технических средств и способов защиты информации;  15. Выполнять работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ. | |
| Знания:  1. Законодательство в области информатизации;  2. Специализацию организации и особенности его деятельности;  3. Методы и средства получения, обработки и передачи информации;  4. Технические средства защиты информации, программно-математические средства защиты информации;  5. Каналы возможной утечки информации;  6. Методы анализа и защиты информации;  7. Организацию работ по защите информации;  8. Инструкции по соблюдению режима проведения специальных работ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Анализ данных о назначении, функциях, условиях функционирования технических средств обработки информации ограниченного доступа | Умения:  1. Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота;  2. Работать с программным обеспечением с соблюдением действующих требований по защите информации;  3. Осуществлять настройку резервирования данных. | |
| Знания:  1. Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота;  2. Методы, средства и системы защиты информации;  3. Требования к защите информации во время эксплуатации средств защиты информации. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Ввод в эксплуатацию системы защиты информации в организации |  |  | |
| Навык 1:  Разработка и реализация организационных мер, обеспечивающих эффективность системы защиты информации | Умения:  1. Организовывать проведение специальных исследований и специальных проверок технических средств обработки информации ограниченного доступа;  2. Устанавливать и настраивать технические, программные (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации;  3. Разрабатывать организационно- распорядительные документы. | |
| Знания:  1. Нормативно-правовые акты в сфере обеспечения ИБ;  2. Методы, средства и системы защиты информации;  3. Архитектуры технических средств защиты информации;  4. Национальные стандарты в сфере обеспечения ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Организация проведения инструктажа руководящего состава и обучения персонала по вопросам технической защиты информации | Умения:  1. Оценивать текущие настройки встроенных средств защиты информации программного обеспечения  2. Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота  3. Работать с программным обеспечением с соблюдением действующих требований по защите информации | |
| Знания:  1. Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота  2. Порядок обеспечения безопасности информации при эксплуатации программного обеспечения  3. Языки программирования (Python, Bash, PowerShell, JS, SQL) | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Гибкость мышления  Умение работать в команде  Дисциплинированность  Инициативность  Организованность  Внимательность  Исполнительность  Ориентация на результат  Высокая обучаемость | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | Инженер по защите информации | |
| 22. Карточка профессии "Инженер по защите информации": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-003 | | |
| Наименование профессии: | Инженер по защите информации | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: |  | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: | Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих"  Инженер по защите информации | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: | Высшее (или послевузовское) образование по соответствующему направлению подготовки кадров без предъявления требований к стажу работы или техническое и профессиональное, послесреднее (среднее специальное, среднее профессиональное) образование по соответствующей специальности (квалификации) и стаж работы в должности техника по защите информации I категории не менее 3 лет. | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: | 2524-0-006 - Специалист по защите информации | | |
| Основная цель деятельности: | Обеспечивать работоспособность прикладного и системного программного обеспечения средствами защиты информации | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Создание системы защиты информации в организации  2. Ввод в эксплуатацию системы защиты информации в организации  3. Сопровождение системы защиты информации в ходе ее эксплуатации | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Создание системы защиты информации в организации |  |  | |
| Навык 1:  Нормативное регулирование, угрозы, методы и средства защиты информации | Умения:  1. Выполнять работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и технических мер защиты информационных систем;  2. Проводить исследования с целью нахождения и выбора наиболее целесообразных практических решений в пределах поставленной задачи;  3. Осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации;  4. Участвовать в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации;  5. Составлять методики расчетов и программы экспериментальных исследований по технической защите информации, выполняет расчеты в соответствии с разработанными методиками и программами;  6. Проводить сопоставительный анализ данных исследований и испытаний, изучает возможные источники и каналы утечки информации;  7. Осуществлять разработку технического обеспечения системы защиты информации, техническое обслуживание средств защиты информации, принимать участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов;  8. Составлять информационные обзоры по технической защите информации;  9. Выполнять оперативные задания, связанные с обеспечением контроля технических средств и механизмов системы защиты информации, участвовать в проведении проверок организаций по выполнению требований нормативно-технической документации по защите информации, в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию;  10. Готовить предложения по заключению соглашений и договоров с иными организациями, предоставляющими услуги в области технических средств защиты информации, составлять заявки на необходимые материалы, оборудование, приборы;  11. Участвовать в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности;  12. Проводить контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности принимаемых мер;  13. Изучать и объединить опыт работы иных организаций по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по ее защите и сохранению в режиме секретности;  14. Выполнять работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ. | |
| Знания:  1. Законодательные, иные нормативные правовые акты и методические материалы по вопросам, связанным с обеспечением технической защиты информации;  2. Специализацию организации и особенности его деятельности;  3. Методы и средства получения, обработки и передачи информации;  4. Научно-техническую и иную специальную литературу по техническому обеспечению защиты информации;  5. Технические средства защиты информации, программно-математические средства защиты информации;  6. Порядок оформления технической документации по защите информации;  7. Каналы возможной утечки информации;  8. Методы анализа и защиты информации;  9. Организацию работ по защите информации;  10. Инструкции по соблюдению режима проведения специальных работ;  11. Отечественный и зарубежный опыт в области технической разведки и защиты информации;  12. Основы экономики, организации производства, труда и управления;  Трудовое законодательство, порядок внутреннего трудового распорядка, по безопасности и охране труда, производственной санитарии, требования пожарной безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Анализ данных о назначении, функциях, условиях функционирования технических средств обработки информации ограниченного доступа | Умения:  1. Оценивать текущее состояние средств обеспечения ИБ;  2. Определять степень участия персонала в обработке (обсуждении, передаче, хранении) информации;  3. Анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем. | |
| Знания:  1. Основных параметров технических средств ИБ;  2. Эксплуатационной документации на систему защиты информации;  3. Типов, категорий, видов и уровней градации (категорирования) информации. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Разработка модели угроз безопасности информации в организации | Умения:  1. Разрабатывать модели угроз безопасности информации в организации;  2. Использовать программные средства разработки модели угроз;  3. Разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации;  4. Разрабатывать проекты систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием. | |
| Знания:  1. Нормативно-правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа;  2. Методы и методики контроля эффективности защиты информации;  3. Организационно-распорядительную документацию по защите информации. | |
| Возможность признания навыка: | Не требуется | |
| Навык 4:  Разработка технического задания на создание системы защиты информации | Умения:  1. Разрабатывать эксплуатационную документацию на объект информатизации и средства защиты информации;  2. Разрабатывать техническое задание системы;  3. Разрабатывать конструкторско-технологическую документацию на систему защиты информации. | |
| Знания:  1. Программные (программно- технических) средства защиты;  2. Современные информационные технологии (операционные системы, базы данных, вычислительные сети);  3. Стандарты ЕСКД, ЕСТД и ЕСПД;  4. Методы, средства и системы защиты информации. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Ввод в эксплуатацию системы защиты информации в организации |  |  | |
| Навык 1:  Разработка и реализация организационных мер, обеспечивающих эффективность системы защиты информации | Умения:  1. Организовывать проведение специальных исследований и специальных проверок технических средств обработки информации ограниченного доступа;  2. Устанавливать и настраивать технические, программные (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации;  3. Разрабатывать организационно- распорядительные документы. | |
| Знания:  1. Законодательство в сфере обеспечения информационной безопасности;  2. Методы, средства и системы защиты информации;  3. Архитектуру технических средств защиты информации. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Организация проведения инструктажа руководящего состава и обучения персонала по вопросам технической защиты информации | Умения:  1. Организовывать обучение персонала использованию технических, программных (программно- технических) средств защиты информации;  2. Проводить инструктаж по вопросам технической защиты информации;  3. Проводить занятия с персоналом. | |
| Знания:  1. Организационно-распорядительных документов;  2. Методик инструктирования персонала;  3. Правил проведения учебных занятий. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Организация опытной эксплуатации и доработки системы защиты информации | Умения:  1. Разрабатывать программы и методики предварительных испытаний;  2. Организовывать опытную эксплуатацию и доработку системы защиты информации;  3. Разрабатывать программы и методики предварительных испытаний системы защиты информации. | |
| Знания:  1. Нормативно-правовые акты, методические документы, национальные стандарты в области защиты информации;  2. Стандарты ЕСКД, ЕСТД и ЕСПД;  3. Методы, средства и системы защиты информации;  4. Языки программирования (Python, Bash, PowerShell, JS, SQL). | |
| Возможность признания навыка: | Не требуется | |
| Навык 4:  Ввод системы защиты информации в эксплуатацию | Умения:  1. Разрабатывать программы и методики предварительных испытаний;  2. Организовывать приемочные испытания системы защиты информации;  3. Организовывать ввод системы защиты информации в эксплуатацию. | |
| Знания:  1. Национальные стандарты в сфере обеспечения информационной безопасности;  2. Стандарты ЕСКД, ЕСТД и ЕСПД;  3. Современные информационных технологии;  4. Типы, категории, виды и уровни градации (категорирования) информации. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 3:  Сопровождение системы защиты информации в ходе ее эксплуатации |  |  | |
| Навык 1:  Разработка предложений по совершенствованию организационных и технических мероприятий | Умения:  1. Проводить контроль (мониторинг) состояния системы защиты информации;  2. Контролировать состояние системы защиты информации;  3. Управлять разработкой предложений по совершенствованию организационных и технических мероприятий по технической защите информации;  4. Оценивать эффективность и совершенствовать систему технической защиты информации в организации. | |
| Знания:  1. Современные информационные технологии;  2. Нормативно-правовые акты, методические документы, национальные стандарты в области защиты информации;  3. Методы, средства и системы защиты. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Организация мероприятий техническому обслуживанию и по выводу из эксплуатации систем информатизации и утилизации их элементов | Умения:  1. Организовать работы по техническому обслуживанию технических и программно- технических средств защиты информации;  2. Организовывать проведение и руководить выполнением работ по выводу из эксплуатации;  3. Утилизировать ПО и технические средства, выведенные из эксплуатации. | |
| Знания:  1. Нормативно-правовые акты, методические документы, национальные стандарты в области защиты информации;  2. Методов гарантированного уничтожения печатной информации;  3. Методов гарантированного уничтожения различных машинных носителей информации. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Гибкость мышления  Дисциплинированность  Инициативность  Умение работать в команде | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | инженер по защите информации | |
| 23. Карточка профессии "Специалист по безопасности сервисов": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-004 | | |
| Наименование профессии: | Специалист по безопасности сервисов | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: | 2524-0-005 - Специалист по вопросам безопасности (ИКТ)  2524-0-006 - Специалист по защите информации | | |
| Основная цель деятельности: | Производить поиск и обнаруживать уязвимые места системы для несанкционированного доступа | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Оценка и анализ рисков безопасности при проектировании и внедрении сервисов  2. Выступление консультантом и заказчиком новой функциональности, связанной с информационной безопасностью | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Оценка и анализ рисков безопасности при проектировании и внедрении сервисов |  |  | |
| Навык 1:  Проведение тестирование на уязвимости | Умения:  1. Использовать инструменты сканирования уязвимостей;  2. Анализировать логи и сетевой трафик для выявления атак;  3. Искать информацию об уязвимостях в базах данных и на специализированных ресурсах;  4. Определять критичность уязвимостей и оценивать их влияние на безопасность системы;  5. Подготавливать отчеты и рекомендации по устранению уязвимостей. | |
| Знания:  1. Понимание основных типов атак;  2. Методологии оценки уязвимостей;  3. Логирование и анализ событий – работа с SIEM-системами;  4. Протоколы и архитектура сервисов;  5. Языки программирования (Python, Bash, PowerShell, JS, SQL);  6. Работа с публичными базами уязвимостей. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Мониторинг и реагирование на инциденты ИБ, связанные с сервисами | Умения:  1. Формулировать четкие задачи разработчикам и администраторам по устранению уязвимостей;  2. Проверять исправления путем повторного тестирования;  3. Автоматизировать процессы устранения уязвимостей с помощью;  4. Вести документацию по уязвимостям, описывать их природу и способы устранения;  5. Работать с командами разработчиков и системных администраторов, объясняя требования безопасности. | |
| Знания:  1. Жизненный цикл разработки ПО и безопасная разработка;  2. Методы исправления уязвимостей – обновление ПО, патчинг, изменение конфигураций, настройка WAF;  3. Контроль версий и управление уязвимостями – Git, Jira, ServiceNow, Tenable;  4. Методы тестирования на безопасность;  5. Языки программирования (Python, Bash, PowerShell, JS, SQL). | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Выступление консультантом и заказчиком новой функциональности, связанной с информационной безопасностью |  |  | |
| Навык 1:  Участие в расследовании инцидентов и разработке мер по их предотвращению | Умения:  1. Анализировать публикации на предмет наличия конфиденциальной информации и скрытых угроз;  2. Проверять файлы перед публикацией на наличие метаданных, способных раскрыть информацию;  3. Грамотно формулировать сообщения с учетом принципов безопасности, минимизируя риски;  4. Использовать защищенные каналы связи при передаче информации (шифрование, цифровые подписи);  5. Оценивать возможные последствия публикации с точки зрения угроз информационной безопасности;  6. Обнаруживать и предотвращать дезинформационные атаки, направленные на сервис. | |
| Знания:  1. Основы информационной безопасности – понимание рисков, связанных с публикацией информации, в том числе утечек данных и киберугроз;  2. Знание того, как злоумышленники могут использовать открытые источники для сбора информации;  3. Понимание, какие данные могут остаться в публикациях (скрытые метаданные файлов, геолокация, информация об устройстве);  4. Законодательство в сфере защиты информации – правила обработки и распространения данных;  5. Социальная инженерия – знание методов, которыми злоумышленники могут использовать опубликованные сведения для атак. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Организация и проведение аудита | Умения:  1. Подготавливать демонстрационные стенды с учетом требований безопасности, исключая возможность компрометации данных;  2. Показывать сценарии атак и защиты в контролируемых условиях, не нарушая работу боевых систем;  3. Работать с инструментами мониторинга безопасности в реальном времени;  4. Проводить тестирование безопасности на демонстрационных сервисах, выявляя уязвимости в режиме реального времени;  5. Настраивать доступ к демонстрационным средам с учетом принципа минимальных привилегий;  6. Объяснять технические аспекты безопасности понятным языком для разных аудиторий (разработчики, менеджеры, клиенты). | |
| Знания:  1. Методы тестирования безопасности сервисов;  2. Угрозы и атаки на сервисы ;  3. Безопасные среды для демонстрации ;  4. Методы защиты при проведении онлайн-демонстраций – безопасные соединения, защита от перехвата данных. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Гибкость мышления  Дисциплинированность  Инициативность  Ответственность  Умение работать в команде | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | специалист по защите информации | |
| 24. Карточка профессии "Шифровальщик данных": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-009 | | |
| Наименование профессии: | Шифровальщик данных | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: | 4419-9-003 - Кодировщик | | |
| Основная цель деятельности: | Разработка и эксплуатация систем шифрования данных | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Разработка программно-аппаратных систем шифрования данных  2. Проведение шифрование и расшифровки данных в соответствии с регламентами и требованиями информационной безопасности | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Разработка программно-аппаратных систем шифрования данных |  |  | |
| Навык 1:  Разработка проектных решений для систем шифрования данных | Умения:  1.Применять действующую нормативную базу в области функционирования систем шифрования данных;  2.Применять нормативные документы по противодействию технической разведке;  3.Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;  4.Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты ;  5.Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в системах шифрования данных;  6.Определять структуру систем шифрования данных в соответствии с требованиями нормативных правовых документов в области шифрования данных. | |
| Знания:  1.Законодательство в сфере обеспечения информационной безопасности;  2.Принципы построения и функционирования, примеры реализаций современных систем шифрования данных;  3.Критерии оценки эффективности и надежности средств шифрования данных;  4.Принципы организации и структура систем шифрования данных;  5.Основные характеристики технических средств шифрования данных;  6.Функционирование современных систем шифрования данных;  7.Национальные стандарты в сфере обеспечения информационной безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Реализация программных, программно-аппаратных систем шифрования данных | Умения:  1.Оценивать сложность криптографических алгоритмов и вычислений;  2.Разрабатывать технические задания по созданию систем, ЕСКД и ЕСПД;  3.Анализировать программные, архитектурно-технические и схемотехнические решения компонентов систем шифрования данных с целью выявления потенциальных уязвимостей безопасности в системах шифрования данных;  4.Проводить комплексное тестирование аппаратных и программных средств. | |
| Знания:  1.Основные информационные технологии и технические средства, используемые в системах шифрования данных;  3.Средства и способы обеспечения безопасности информации, принципы построения систем шифрования данных;  4.Основные криптографические методы, алгоритмы, протоколы, используемые в системах шифрования данных;  5.Современные технологии программирования;  6.Эталонная модель взаимодействия открытых систем;  7.Принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;  8.Принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения;  9.Методы тестирования и отладки программного и аппаратного обеспечения;  10.Законодательство в сфере обеспечения информационной безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Проведение шифрование и расшифровки данных в соответствии с регламентами и требованиями информационной безопасности |  |  | |
| Навык 1:  Тестирование разработанных систем шифрования данных | Умения:  1.Тестирование процедуры проверки работоспособности программного обеспечения на выбранном языке программирования;  2.Применять методы и средства тестирования;  3.Использовать выбранную среду программирования для разработки процедур проверки работоспособности программного обеспечения на выбранном языке программирования;  4.Разработка и оформление контрольных примеров для проверки работоспособности программного обеспечения;  5.Подготовка наборов данных, используемых в процессе проверки работоспособности программного обеспечения. | |
| Знания:  1.Методы автоматической и автоматизированной проверки работоспособности программного обеспечения;  2.Основные виды диагностических данных и способы их представления;  3.Утилиты и среды программирования, и средства пакетного выполнения процедур;  4.Методы создания и документирования контрольных примеров и тестовых наборов данных;  5.Правила, алгоритмы и технологии создания тестовых наборов данных;  6. Структуры и форматы хранения тестовых наборов данных, криптографических алгоритмов. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Разработка эксплуатационной документации на системы шифрования данных | Умения:  1.Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для систем шифрования данных;  2.Разрабатывать технические задания на создание подсистем ИБ систем шифрования данных;  3.Проектировать подсистемы систем шифрования данных с учетом действующих нормативных и методических документов;  4.Анализировать программные, архитектурно-технические и схемотехнические решения компонентов систем шифрования данных с целью выявления потенциальных уязвимостей систем шифрования данных;  5.Оценивать информационные риски в системах шифрования данных и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите ;  6.Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств в системах шифрования данных с целью обеспечения требуемого уровня защищенности;  7.Исследовать эффективность проектных решений программно-аппаратных средств в системах шифрования данных. | |
| Знания:  1.Методы автоматической и автоматизированной проверки работоспособности программного обеспечения;  2.Основные виды диагностических данных и способы их представления;  3.Утилиты и среды программирования, и средства пакетного выполнения процедур;  4.Методы создания и документирования контрольных примеров и тестовых наборов данных;  5.Правила, алгоритмы и технологии создания тестовых наборов данных;  6. Структуры и форматы хранения тестовых наборов данных, криптографических алгоритмов. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Структурное мышление  Усидчивость и внимательность  Аналитический ум  Способность к самообучению  Математические способности | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК 1073-2007 Средства криптографической защиты информации. Общие технические требования | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | шифровальщик данных | |
| 25. Карточка профессии "Специалист-криминалист по цифровым технологиям": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-008 | | |
| Наименование профессии: | Специалист-криминалист по цифровым технологиям | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Цифровая криминалистика и анализ инцидентов информационной безопасности  2. Анализ цифровых данных | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Цифровая криминалистика и анализ инцидентов информационной безопасности |  |  | |
| Навык 1:  Получение данных из потенциальных источников информации | Умения:  1.Выявлять потенциальные источники данных в организации;  2.Разрабатывать план сбора данных;  3.Осуществлять получение данных и проверку целостности полученных данных;  4.Осуществлять ведение журнала, для сбора данных, включая информацию о каждом инструменте, используемом в процессе;  5.Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;  6.Определять принципы деления программного обеспечения на группы. | |
| Знания:  1.Виды потенциальных источников данных;  2.Носители компьютерной информации;  3.Методы обеспечения сохранности, целостности и конфиденциальности полученной информации;  4.Принципы построения и функционирования систем и сетей передачи информации;  5.Законодательство в сфере обеспечения информационной безопасности;  6.Архитектура, устройство и функционирование вычислительных систем;  7.Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации;  8.Технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов;  9.Порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Экспертное исследование собранной информации (объектов-носителей) при компьютерных преступлениях | Умения:  1.Осуществлять извлечение/считывание информации с носителей;  2.Осуществлять декодирование информации и вычленение из нее той, которая относится к делу;  3.Использовать автоматизированные средства исследования информации;  4.Обеспечивать целостность и сохранность информации с исследуемых носителей;  5.Применять действующую законодательную базу в области обеспечения защиты информации;  6.Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа. | |
| Знания:  1.Методы извлечения/считывания данных с компьютерных носителей информации;  2.Методы обеспечения сохранности, целостности и конфиденциальности полученной информации;  3.Программные средства исследования и фильтрации данных;  4.Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации;  5.Принципы построения и функционирования систем и сетей передачи информации;  6.Нормативные правовые акты в области цифровой криминалистики;  7.Технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов;  8.Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Анализ цифровых данных |  |  | |
| Навык 1:  Обработка экспертных данных | Умения:  1.Анализировать собранную на предыдущих этапах расследования информацию;  2.Производить анализ интерпретированных данных, полученных из различных источников, данных;  3.Определять тип компьютерных файлов, в том числе без расширения;  4.Производить реконструкцию событий компьютерного инцидента, объединяя различные источники компьютерной информации;  5.Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа. | |
| Знания:  1. Методы обеспечения сохранности, целостности и конфиденциальности полученной информации;  2.Архитектура, устройство и функционирование вычислительных систем;  3.Принципы построения и функционирования систем и сетей передачи информации;  4.Программные средства обработки информации;  5.Законодательство в сфере обеспечения информационной безопасности;  6.Форматы хранения информации в анализируемой компьютерной системе;  7.Основные форматы файлов, используемые в компьютерных системах;  8.Особенности хранения конфигурационной и системной информации в компьютерных системах;  9.Уязвимости компьютерных систем и сетей;  10.Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Оформление результатов анализа и исследований в соответствии с законодательными требованиями представления информации | Умения:  1.Составление отчетных материалов по итогам анализа;  2.Актуализировать информации по анализу;  3.Разрабатывать рекомендации по предотвращению компьютерных инцидентов и преступлений. | |
| Знания:  1.Методы обеспечения сохранности, целостности и конфиденциальности полученной информации;  3.Законодательство в сфере обеспечения информационной безопасности;  4.Архитектура, устройство и функционирование вычислительных систем;  5.Принципы построения и функционирования систем и сетей передачи информации;  6.Программные средства обработки информации;  7.Порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Стрессоустойчивость  Аналитическое мышление  Критический анализ  Организованность  Обучаемость  Уметь работать в команде | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2015 "Информационная технология. Методы и средства обеспечения безопасности Системы менеджмента информационной безопасностью" СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | специалист-криминалист по цифровым технологиям | |
| 26. Карточка профессии "Администратор по информационной безопасности": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-001 | | |
| Наименование профессии: | Администратор по информационной безопасности | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: |  | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Администрировать механизмы безопасности и своевременно реагировать на нарушения ИБ | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения ИБ  2. Администрирование механизмов безопасности  3. Реагирование на инциденты ИБ  4. Контроль и анализ эффективности применения ПАС зашиты информации и обеспечения ИБ | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения ИБ |  |  | |
| Навык 1:  Эксплуатация ПАС защиты информации и обеспечения ИБ и техническое сопровождение | Умения:  1. Эксплуатировать ПАС защиты информации и обеспечения ИБ.  2. Принимать от поставщика и/или исполнителя работ ПАС защиты информации и обеспечения ИБ.  3. Учитывать и хранить носители конфиденциальной информации.  4. Эксплуатировать ПАС защиты конфиденциальной информации.  5. Проводить регламентные и профилактические работы по техническому обслуживанию средств защиты информации и обеспечения ИБ | |
| Знания:  1. Законодательные и иные нормативные правовые акты, регулирующие деятельность по защите государственной тайны и иной информации ограниченного доступа;  2. Нормативные и методические документы по вопросам, связанным с обеспечением технической защиты информации;  3. Объекты информатизации, подлежащие защите;  4. Специализацию и направления деятельности организации и ее подразделений;  5. Применяемые информационные технологии и системы;  6. Структуру управления, связи, автоматизации;  7. Средства технической разведки и методы оценки их возможностей;  8. Угрозы безопасности информации и классификацию (категории) нарушений;  9. Оснащенность объектов информатизации основными и вспомогательными техническими средствами и системами, комплексами и средствами технической защиты информации, сервисами и механизмами безопасности автоматизированных систем управления;  10. Подсистемы разграничения доступа;  11. Подсистемы обнаружения атак;  12. Подсистемы защиты от преднамеренного воздействия;  13. Методы контроля целостности информации, перспективы их развития и модернизации;  14. Методы оценки состояния систем безопасности, выявления каналов утечки информации, контроля процесса резервирования и дублирования критичных вычислительных и информационных ресурсов;  15. Порядок работы с техническими, программными, программно-аппаратными средствами защиты информации и контроля, сервисами и механизмами безопасности автоматизированных систем управления и аудита их состояния. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Администрирование антивирусного ПО | Умения:  1. Эффективно осуществлять удалҰнную установку и обновление антивирусного программного обеспечения и вирусных баз данных с применением централизованных систем управления, обеспечивая своевременную защиту информационных ресурсов;  2. Организовывать и поддерживать репозитории дистрибутивов антивирусных решений на сетевых серверах, обеспечивая их актуальность и доступность для централизованной установки на все объекты IT-инфраструктуры;  3. Проводить тонкую настройку антивирусных решений на рабочих станциях и серверах в удалҰнном режиме, оптимизируя уровень защиты в соответствии с политикой безопасности организации;  4. Разрабатывать и планировать задания на выполнение сканирования, обновлений и других операций на устройствах сети, с возможностью немедленного или отложенного запуска, повышая эффективность и автоматизацию процессов администрирования. | |
| Знания:  1. Назначения, классификации и принципов работы антивирусных программ, включая сигнатурные, эвристические, поведенческие методы обнаружения угроз, а также технологий проактивной защиты и интеграции с другими средствами информационной безопасности;  2. Официальных методических рекомендаций производителей антивирусного ПО по его корректной установке, с учҰтом особенностей операционных систем, политик безопасности и корпоративной инфраструктуры, а также требований по предварительной подготовке среды;  3. Рекомендаций разработчиков антивирусных решений по их настройке, администрированию и сопровождению, включая управление политиками безопасности, автоматизацию обновлений, организацию отчетности, мониторинг инцидентов и своевременное реагирование на угрозы. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Администрирование системы обнаружения/ предотвращения вторжений | Умения:  1. Осуществлять комплексный мониторинг безопасности сети с применением систем обнаружения и предотвращения вторжений (IDS/IPS), обеспечивая своевременное реагирование на потенциальные угрозы и реализацию политик информационной безопасности;  2. Администрировать учетные записи пользователей с реализацией строгого разграничения прав доступа, применяя методы ролевого доступа (RBAC), а также реализуя сегментирование сетевой инфраструктуры и фильтрацию трафика в соответствии с принципами Zero Trust;  3. Настраивать и сопровождать парольную политику организации, включая требования к сложности паролей, периодичность их смены, а также реализуя механизмы автоматической блокировки учетных записей при нарушении правил аутентификации;  4. Выполнять конфигурирование параметров сетевого доступа, включая настройку VPN, сетевых экранов, NAT, DHCP, ACL и других компонентов, обеспечивая безопасное и контролируемое подключение к ресурсам сети;  5. Ограничивать доступ к критически важным ресурсам по IP-адресам, хостам и подсетям, минимизируя поверхность атаки и исключая несанкционированный доступ извне;  6. Управлять процессом обновления программного обеспечения в корпоративной среде, включая тестирование, планирование и централизованное развҰртывание обновлений, с целью повышения защищҰнности и стабильности ИТ-инфраструктуры; | |
| Знания:  1. Назначение, принципы действия, архитектуру систем обнаружения/предотвращения вторжений;  2. Стандарты, регламентирующие функционирование систем обнаружения вторжений;  3. Рекомендации производителя системы обнаружения/предотвращения вторжений по ее установке и эксплуатации;  4. Типы и методы обнаружения вторжений;  5. Технологии и инструменты, используемые в системах предотвращения вторжений; | |
| Возможность признания навыка: | Не требуется | |
| Навык 4:  Конфигурирование и настройка межсетевого экрана | Умения:  1. Настраивать режимы работы межсетевого экрана и политик фильтрации;  2. Осуществлять создание учетной записи администратора, разграничение прав доступа;  3. Выполнять резервное копирование и восстановление;  4. Осуществлять настройку сервисов (DNS, DHCP и других внутренних сетевых сервисов);  5. Настраивать логирование и мониторинг событий;  6. Настраивать и отлаживать маршрутизации;  7. Настраивать виртуальные домены и сети;  8. Настраивать защищенные соединения IPsec VPN;  9. Настраивать политику аутентификации;  10. Управлять и применять криптографические сертификаты. | |
| Знания:  1. Правила фильтрации и порядок их применения;  2. Типы и функции межсетевых экранов;  3. Использование NAT;  4. Мониторинг и журналирование событий;  5. Обновления и патчинг системы. | |
| Возможность признания навыка: | Не требуется | |
| Навык 5:  Ведение отчетной документации | Умения:  1. Составлять отчеты по инцидентам безопасности, включая описание происшествия, действия, предпринятые для устранения угрозы, анализ причин, а также результаты расследования;  2. Регулярно обновлять и вести журналы событий безопасности, включая информацию о попытках доступа, несанкционированных действиях и других событиях;  3. Создавать и поддерживать документации по политикам и процедурам безопасности, включая политику доступа, шифрования данных и использования паролей;  4. Вести отчетность по уязвимостям и патч-менеджменту и своевременно составлять отчеты о текущих уязвимостях и патчах;  5. Документировать процедуры реагирования на инциденты включая пошаговые инструкции по ликвидации угроз, восстановлению данных и минимизации ущерба. | |
| Знания:  1. Стандартов и требований к отчетности в области информационной безопасности;  2. Понимание структуры и форматов отчетности, порядка их составления;  3. Методов анализа и обработки данных безопасности, интерпретации данных из журналов событий безопасности и других источников;  4. Принципов ведения журналов событий и инцидентов, включая регистрацию всех значимых событий;  5. Принципов и процессов управления изменениями и инцидентами в инфраструктуре безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Администрирование механизмов безопасности |  |  | |
| Навык 1:  Управление процессами по администрированию | Умения:  1. Составлять и поддерживать в актуальном состоянии список прав доступа и полномочий сотрудников по доступу к защищаемой информации;  2. Мониторить выходы обновлений и управлять версиями ППО, СУБД, ОС серверного и сетевого оборудования;  3. Взаимодействовать с другими администраторами для обеспечения согласованной работы по обновлению версий ПО и списков прав доступа. | |
| Знания:  1. Жизненный цикл управления ИТ-процессов : планирование, проектирование, внедрение, эксплуатацию, поддержку и завершение;  2. Принципы и модели для управления ИТ-услугами;  3. Управление изменениями и конфигурациями без риска для работы системы;  4. Контроль и мониторинга производительности системы с помощью различных инструментов;  5. Управление рисками и инцидентами безопасности или сбоями в работе системы. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Настраивание политики безопасности ОС, СУБД, ППО | Умения:  1. Управлять криптографическими ключами (генерация и распределение);  2. Управлять шифрованием (Устанавливать и синхронизация криптографических параметров);  3. Управлять аутентификацией (распределение информации, необходимой для аутентификации - паролей, ключей и т.п.);  4. Управлять доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.);  5. Устанавливать и настраивать контролеры доменов сети. | |
| Знания:  1. Принципы разработки политик безопасности, включая определение целей, рисков и требований;  2. Типы политики безопасности, включая: политику управления доступом; политику использования паролей; политику обработки данных; политику управления инцидентами;  3. Требований к безопасности, установленные различными нормативными актами и стандартами;  4. Процесс реализации и внедрения политики, включая обучение сотрудников, создание системы контроля и обеспечения соблюдения политики;  5. Мониторинг и пересмотр политики безопасности в ответ на изменения в организационной структуре, новые угрозы или изменения в законодательстве. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 3:  Реагирование на инциденты ИБ |  |  | |
| Навык 1:  Мониторинг событий и инцидентов ИБ | Умения:  1. Собирать и анализировать события в системах, находящихся под мониторингом ИБ;  2. Классифицировать события, серийные события и сочетания событий как нарушения ИБ;  3. Настраивать процедуры обработки событий и обнаруживать события ИБ. | |
| Знания:  1. Процесс мониторинга безопасности, включая использование систем управления, которые собирают, анализируют и отслеживают данные о событиях безопасности в реальном времени;  2. Типы событий безопасности и их классификацию;  3. Принципы анализа инцидентов и выявления угрозы, включая использование машинного обучения и аналитики больших данных;  4. Порядок ведения журналов событий безопасности и созданию отчетов для анализа тенденций и выявления рисков. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Реагирование на инциденты ИБ | Умения:  1. Регистрировать и оповещать (информировать) об инциденте ИБ;  2. Определять причины инцидента ИБ;  3. Принимать меры к ликвидации инцидента ИБ и его последствий;  4. Собирать доказательства об инциденте;  5. Участвовать в проведении расследований инцидентов ИБ;  6. Взаимодействовать с компетентными органами (CERT, органы внутренних дел и другие). | |
| Знания:  1. Процессы реагирования на инциденты и основные этапы процесса;  2. Классификации инцидентов безопасности по типам и серьезности;  3. Инструменты для расследования инцидентов, которые помогают собирать доказательства и анализировать происходящее;  4. Роли коммуникации в процессе реагирования;  5. Порядок документирования и анализ инцидентов для улучшения безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 4:  Контроль и анализ эффективности применения ПАС зашиты информации и обеспечения ИБ |  |  | |
| Навык 1:  Текущий контроль технологического процесса обработки защищаемой информации | Умения:  1. Составлять и поддерживать в актуальном состоянии документации по размещению и конфигурации ПАС защиты информации и обеспечения ИБ;  2. Контролировать целостность настроек механизмов безопасности ППО, СУБД, ОС серверного и телекоммуникационного оборудования;  3. Анализировать журналы регистрации событий системного и прикладного ПО с целью выявления попыток НСД к ИС и защищаемым информационным ресурсам. | |
| Знания:  1. Методы, принципы и приемы осуществления контроля;  2. Процедуры анализа журнала событий ИБ (выполнение задач анализа, проведение расследования и анализ нестандартных событий, документирование выполнения процедур и сбор доказательств, формировать отчетности для руководства);  3. Программные средства анализа журналов событий ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Текущий и периодический контроль работы ПАС защиты информации и обеспечения ИБ | Умения:  1. Анализировать журналы регистрации событий ПАС защиты информации и обеспечения ИБ;  2. Оценивать использование ресурсов ПАС зашиты информации и обеспечения ИБ;  3. Вырабатывать предложения по совершенствованию и повышению эффективности использования ПАС зашиты информации и обеспечения ИБ. | |
| Знания:  1. Принцип работы и правил эксплуатации ПАС защиты информации;  2. Критерии и показатели результативности использования ресурсов ПАС защиты информации и обеспечения ИБ;  3. Параметры контроля ПАС защиты информации и обеспечения ИБ. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Гибкость мышления  Умение работать в команде  Дисциплинированность  Инициативность | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| - | - | |
| 27. Карточка профессии "Специалист по защите информации": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-006 | | |
| Наименование профессии: | Специалист по защите информации | | |
| Уровень квалификации по ОРК: | 7 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: | Параграф 3 Приказа Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих"  Специалист по защите информации | | |
| Уровень профессионального образования: | Уровень образования:  послевузовское образование (магистратура, резидентура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: | Специалист по защите информации I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по защите информации II категории не менее 3 лет; специалист по защите информации II категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по защите информации без категории не менее 3 лет; специалист по защите информации: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров без предъявления требования к стажу работы. | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: |  | | |
| Основная цель деятельности: | Администрирование систем защиты информации ИС | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Разработка систем защиты информации ИС  2. Обеспечение защиты информации и информационных систем | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Разработка систем защиты информации ИС |  |  | |
| Навык 1:  Проектирование архитектуры информационной безопасности | Умения:  1.Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;  2.Проводить анализ информационной системы и оценку угроз безопасности;  3.Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в ИС;  4.Выбирать меры защиты информации, подлежащие реализации в системе защиты информации ИС;  5.Определять виды и типы средств защиты информации;  6.Разрабатывать архитектуру системы защиты информации. | |
| Знания:  1.Законодательство в сфере обеспечения информационной безопасности;  2.Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей, и их компонентов;  3.Особенности защиты информации в ИС управления технологическими процессами;  4.Критерии оценки эффективности и надежности средств защиты информации программного обеспечения ИС;  5.Принципы организации и структура систем защиты информации программного обеспечения ИС;  6.Национальные стандарты в сфере обеспечения информационной безопасности;  7.Принципы формирования политики информационной безопасности в ИС. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Разработка эксплуатационной документации на системы защиты информации ИС | Умения:  1.Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в ИС;  2.Разрабатывать технические задания на создание подсистем информационной безопасности ИС;  3.Проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов;  4.Разрабатывать модели ИС и систем защиты информации ИС;  5.Исследовать модели ИС и систем защиты безопасности ИС;  6.Анализировать программные, архитектурно-технические и схемотехнические решения компонентов ИС;  7.Оценивать информационные риски в ИС и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите;  8.Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в ИС;  9.Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в ИС ;  10.Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации. | |
| Знания:  1.Основные методы управления информационной безопасностью;  2.Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов;  3.Основные методы управления проектами в области информационной безопасности;  4.Национальные стандарты в сфере обеспечения информационной безопасности;  5.Основные меры по защите информации в ИС;  6.Особенности защиты информации в ИС управления технологическими процессами;  7.Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в ИС;  8.Методы, способы, средства, последовательность и содержание этапов разработки ИС и систем защиты информации ИС;  9.Программно-аппаратные средства обеспечения защиты информации в программном обеспечении ИС;  10.Основные средства, способы и принципы построения систем защиты информации ИС. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Обеспечение защиты информации и информационных систем |  |  | |
| Навык 1:  Разработка архитектуры системы защиты информации ИС | Умения:  1.Определять комплекс мер для обеспечения безопасности информационной в ИС;  2.Выявлять уязвимости информационно-технологических ресурсов ИС;  3.Разрабатывать предложения по совершенствованию системы управления защиты информации ИС;  4.Выбирать программно-аппаратных средств обеспечения безопасности информации для использования их в составе ИС;  5.Классифицировать и оценивать угрозы безопасности информации для ИС;  6.Определять информационную инфраструктуру и информационных ресурсов ИС, подлежащие защите;  7.Разрабатывать модели угроз безопасности информации и нарушителей в ИС;  8.Определять эффективность применения средств информатизации. | |
| Знания:  1.Основные информационные технологии, используемые в ИС;  2.Способы и средства защиты информации от "утечки" по техническим каналам и контроля эффективности защиты информации;  3.Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации;  4.Программно-аппаратные средства обеспечения защиты информации ИС;  5.Принципы построения средств защиты информации от "утечки" по техническим каналам;  6.Национальные стандарты в сфере обеспечения информационной безопасности;  7.Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения. | |
| Возможность признания навыка: | - | |
| Требования к личностным компетенциям: | Ответственность  Системное мышление  Аналитическое мышление  Критический анализ  Организованность  Умение решать нестандартные задачи  Внимательность к деталям | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 6 | Специалист по защите информации | |
| 28. Карточка профессии "Специалист по вопросам безопасности (ИКТ)": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-005 | | |
| Наименование профессии: | Специалист по вопросам безопасности (ИКТ) | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: |  | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: |  | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: | 2524-0-004 - Специалист по безопасности сервисов  2524-0-006 - Специалист по защите информации  2524-0-007 - Специалист по информационной безопасности | | |
| Основная цель деятельности: | Противодействие вредоносному влиянию программно-технического воздействия на подсистемы, устройства, элементы и каналы инфокоммуникационных систем | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Администрирование средств защиты информации в компьютерных системах и сетях  2. Оценка и управление рисками в области информационной безопасности | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Администрирование средств защиты информации в компьютерных системах и сетях |  |  | |
| Навык 1:  Администрирование подсистем защиты информации в операционных системах | Умения:  1.Формулировать политики безопасности операционных систем;  2.Настраивать политики безопасности операционных систем;  3.Оценивать угрозы безопасности информации операционных систем;  4.Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем;  5.Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах;  6.Настраивать антивирусные средства защиты информации в операционных системах;  7.Устанавливать обновления программного обеспечения и средств антивирусной защиты;  8.Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах;  9.Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах;  10.Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах. | |
| Знания:  1.Архитектура и принципы построения операционных систем;  2.Программные интерфейсы операционных систем;  3.Виды политик управления доступом и информационными потоками применительно к операционным системам;  4.Архитектура подсистем защиты информации в операционных системах;  5.Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы;  6.Состав типовых конфигураций программно-аппаратных средств защиты информации;  7.Требования к составу и характеристикам подсистем защиты информации для операционных систем;  8.Порядок реализации методов и средств антивирусной защиты в операционных системах;  9.Программно-аппаратные средства и методы защиты информации в операционных системах;  10.Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации;  11.Нормативные правовые акты в области защиты информации. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Администрирование программно-аппаратных средств защиты информации в компьютерных сетях | Умения:  1.Оценивать угрозы безопасности информации в компьютерных сетях;  2.Настраивать правила фильтрации пакетов в компьютерных сетях;  3.Выбирать используемых программно-аппаратных средств защиты информации в компьютерных сетях;  4.Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях;  5.Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;  6.Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях;  7.Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях;  8.Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях. | |
| Знания:  1.Принципы построения компьютерных сетей;  2.Стек сетевых протоколов операционных систем;  3.Стек протоколов сетевого оборудования;  4.Порядок реализации методов и средств межсетевого экранирования;  5.Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы;  6.Виды политик управления доступом и информационными потоками в компьютерных сетях;  7.Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению;  8.Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;  9.Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;  10.Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации;  11.Программно-аппаратные средства и методы защиты информации в компьютерных сетях;  12.Нормативные правовые акты в сфере информационной безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Администрирование средств защиты информации прикладного и системного программного обеспечения | Умения:  1.Анализировать угрозы безопасности информации программного обеспечения  2.Формулировать правила безопасной эксплуатации программного обеспечения  3.Обосновывать правила безопасной эксплуатации программного обеспечения  4.Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия  5.Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации  6.Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения  7.Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации  8.Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения | |
| Знания:  1.Архитектура подсистем защиты информации в операционных системах  2.Принципы построения систем управления базами данных  3.Основные средства и методы анализа программных реализаций  4.Принципы построения антивирусного программного обеспечения  5.Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению  6.Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению  7.Уязвимости используемого программного обеспечения и методы их эксплуатации  8.Виды и формы функционирования вредоносного программного обеспечения  9.Характерные признаки наличия вредоносного программного обеспечения  10.Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения  11.Принципы функционирования программных средств криптографической защиты информации  12.Порядок обеспечения безопасности информации при эксплуатации программного обеспечения  13.Нормативные правовые акты в области защиты информации  14.Организационные меры по защите информации | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Оценка и управление рисками в области информационной безопасности |  |  | |
| Навык 1:  Администрирование средств защиты информации прикладного и системного программного обеспечения | Умения:  1.Анализировать угрозы безопасности информации программного обеспечения  2.Формулировать правила безопасной эксплуатации программного обеспечения  3.Обосновывать правила безопасной эксплуатации программного обеспечения  4.Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия  5.Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации  6.Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения  7.Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации  8.Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения | |
| Знания:  1.Архитектура подсистем защиты информации в операционных системах  2.Принципы построения систем управления базами данных  3.Основные средства и методы анализа программных реализаций  4.Принципы построения антивирусного программного обеспечения  5.Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению  6.Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению  7.Уязвимости используемого программного обеспечения и методы их эксплуатации  8.Виды и формы функционирования вредоносного программного обеспечения  9.Характерные признаки наличия вредоносного программного обеспечения  10.Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения  11.Принципы функционирования программных средств криптографической защиты информации  12.Порядок обеспечения безопасности информации при эксплуатации программного обеспечения  13.Нормативные правовые акты в области защиты информации  14.Организационные меры по защите информации | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Разработка и внедрение методик оценки рисков, связанных с использованием ИКТ | Умения:  1. Выявлять и анализировать потенциальные риски, связанные с использованием ИКТ, включая угрозы, уязвимости и последствия;  2. Разрабатывать и адаптировать методики оценки рисков с учетом специфики организации и ее информационных систем;  3. Документировать результаты оценки рисков и представлять их заинтересованным сторонам, включая руководство и технический персонал;  4. Формулировать рекомендации по снижению и управлению рисками, включая внедрение средств защиты и контрольных мероприятий. | |
| Знания:  1. Основы информационной безопасности;  2. Методологии оценки рисков;  3. Национальные стандарты в сфере обеспечения информационной безопасности;  4. Законодательство в сфере обеспечения информационной безопасности. | |
| Возможность признания навыка: | - | |
| Требования к личностным компетенциям: | Ответственность  Системное мышление  Аналитическое мышление  Критический анализ  Организованность  Умение решать нестандартные задачи  Внимательность к деталям | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2015 "Информационная технология. Методы и средства обеспечения безопасности Системы менеджмента информационной безопасностью" СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | Специалист по вопросам безопасности (ИКТ) | |
| 29. Карточка профессии "Специалист по защите информации": | | | |
| Код группы: | 2524-0 | | |
| Код наименования занятия: | 2524-0-006 | | |
| Наименование профессии: | Специалист по защите информации | | |
| Уровень квалификации по ОРК: | 6 | | |
| подуровень квалификации по ОРК: | - | | |
| Уровень квалификации по ЕТКС, КС и др. типовых квалификационных характеристик: | Параграф 5 Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих".  Специалист по защите информации | | |
| Уровень профессионального образования: | Уровень образования:  высшее образование (бакалавриат, специалитет, ординатура) | Специальность:  Информационная безопасность | Квалификация:  - |
| Требования к опыту работы: | Специалист по защите информации I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по защите информации II категории не менее 3 лет; Специалист по защите информации II категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по защите информации без категории не менее 3 лет; Специалист по защите информации: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров без предъявления требования к стажу работы. | | |
| Связь с неформальным и формальным образованием: | Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности | | |
| Другие возможные наименования профессии: | 2524-0-007 - Специалист по информационной безопасности  2524-0-005 - Специалист по вопросам безопасности (ИКТ)  2524-0-004 - Специалист по безопасности сервисов | | |
| Основная цель деятельности: | Администрирование систем защиты информации ИС | | |
| Описание трудовых функций | | | |
| Перечень трудовых функций: | Обязательные трудовые функции: | 1. Обеспечение защиты информации в ИС в процессе их эксплуатации  2. Внедрение систем защиты информации в ИС | |
| Дополнительные трудовые функции: |  | |
| Трудовая функция 1:  Обеспечение защиты информации в ИС в процессе их эксплуатации |  |  | |
| Навык 1:  Диагностика систем защиты информации ИС | Умения:  1.Классифицировать и оценивать угрозы информационной безопасности;  2.Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в ИС;  3.Контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем;  4.Контролировать события безопасности и действия пользователей автоматизированных систем;  5.Применять технические средства контроля эффективности мер защиты информации;  6.Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы. | |
| Знания:  1.Содержание и порядок деятельности персонала по эксплуатации защищенных ИС и подсистем безопасности ИС;  2.Основные угрозы безопасности информации и модели нарушителя в ИС;  3.Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС;  4.Программно-аппаратные средства обеспечения защиты информации ИС;  5.Методы защиты информации от "утечки" по техническим каналам;  6.Нормативные правовые акты в области защиты информации. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Администрирование систем защиты информации ИС | Умения:  1.Создавать, удалять и изменять учетные записи пользователей ИС;  2.Планировать политику безопасности программных компонентов ИС;  3.Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы;  4.Использовать криптографические методы и средства защиты информации в ИС;  5.Регистрировать и анализировать события, связанные с защитой информации в ИС. | |
| Знания:  1.Принципы формирования политики ИБ в ИС;  2.Программно-аппаратные средства защиты информации ИС;  3.Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС;  4.Методы контроля эффективности защиты информации от "утечки" по техническим каналам;  5.Критерии оценки эффективности и надежности средств защиты программного обеспечения ИС;  6.Технические средства контроля эффективности мер защиты информации;  7.Принципы организации и структура систем защиты программного обеспечения ИС;  8.Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности ИС;  9.Основные меры по защите информации в ИС. | |
| Возможность признания навыка: | Не требуется | |
| Навык 3:  Управление защитой информации в ИС | Умения:  1.Оценивать информационные риски в ИС;  2.Классифицировать и оценивать угрозы безопасности информации;  3.Определять подлежащие защите информационные ресурсы автоматизированных систем;  4.Разрабатывать предложения по совершенствованию системы управления защиты информации ИС;  5.Конфигурировать параметры системы защиты информации ИС;  6.Применять технические средства контроля эффективности мер защиты информации. | |
| Знания:  1.Основные методы управления защитой информации;  2.Основные угрозы безопасности информации и модели нарушителя в ИС;  3.Методы защиты информации от "утечки" по техническим каналам;  4.Нормативные правовые акты в области защиты информации;  5.Национальные стандарты в области защиты информации. | |
| Возможность признания навыка: | Не требуется | |
| Трудовая функция 2:  Внедрение систем защиты информации в ИС |  |  | |
| Навык 1:  Разработка организационно-распорядительных документов по защите информации в ИС | Умения:  1.Классифицировать и оценивать угрозы информационной безопасности;  2.Применять нормативные документы по противодействию технической разведке;  3.Определять параметры настройки программного обеспечения системы защиты информации ИС;  4.Контролировать эффективность принятых мер по защите информации в ИС. | |
| Знания:  1.Содержание и порядок деятельности персонала по эксплуатации защищенных ИС и систем защиты информации;  2.Основные угрозы безопасности информации и модели нарушителя в ИС;  3.Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС;  4.Принципы построения средств защиты информации от "утечки" по техническим каналам;  5.Нормативные правовые акты в сфере информационной безопасности. | |
| Возможность признания навыка: | Не требуется | |
| Навык 2:  Внедрение организационных мер по защите информации в автоматизированных системах | Умения:  1.Реализовывать правила разграничения доступа персонала к объектам доступа;  2.Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации;  3.Обучать персонал ИС комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации;  4.Осуществлять планирование и организацию работы персонала ИС с учетом требований по защите информации;  5.Конфигурировать аттестованную ИС и системы защиты информации ИС. | |
| Знания:  1.Нормативные правовые акты в сфере обеспечения информационной безопасности;  2.Методы, способы, средства, последовательность и содержание этапов разработки ИС и систем защиты автоматизированных систем;  3.Методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации;  4.Методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем. | |
| Возможность признания навыка: | Не требуется | |
| Требования к личностным компетенциям: | Ответственность  Системное мышление  Аналитическое мышление  Критический анализ  Организованность  Умение решать нестандартные задачи  Внимательность к деталям | | |
| Список технических регламентов и национальных стандартов: | СТ РК ISO/IEC 27001-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования" СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационная технология. Аудит систем управления информационной безопасностью организации | | |
| Связь с другими профессиями в рамках ОРК: | Уровень ОРК: | Наименование профессии: | |
| 7 | Специалист по защите информации | |

**Глава 4. Технические данные профессионального стандарта**

      30. Наименование государственного органа:

      Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан

      Исполнитель:

      Советханова Ақжарқын Бақдәулетқызы, +7 (717) 264 94 07, a.sovetkhanova@mdai.gov.kz

      31. Организации (предприятия) участвующие в разработке:

      Комитет по информационной безопасности

      Руководитель проекта:

      Қалим Ерболат Темірұлы

      E-mail: e.kalim@mdai.gov.kz

      Номер телефона: +7 (717) 264 93 96

      Исполнители:

      Советханова Ақжарқын Бақдәулетқызы, +7 (717) 264 94 07, a.sovetkhanova@mdai.gov.kz

      32. Отраслевой совет по профессиональным квалификациям: 3 , 04.12.2024 г.

      33. Национальный орган по профессиональным квалификациям: 02.06.2025 г.

      34. Национальная палата предпринимателей Республики Казахстан "Атамекен": 24.12.2024 г.

      35. Номер версии и год выпуска: версия 1, 2025 г.

      36. Дата ориентировочного пересмотра: 05.12.2028 г.

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан