

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
Министра цифрового развития,
инноваций и аэрокосмической

Профессиональный стандарт: "Деятельность в области кибербезопасности"

Сноска. Стандарт – в редакции приказа и.о. Министра искусственного интеллекта и цифрового развития РК от 7.07.2026 № 392/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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) Системное мышление – Умение специалиста объединять (обобщать) частные факты в общую картину, строить иерархические уровни для понимания различных ситуаций (экономических, политических, деловых) и принятия долгосрочных решений. Важным качеством является понимание того, как изменение одного элемента может отразиться на других элементах;

2) Кибербезопасность (далее – КБ) – состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности или доступности;

3) Цифровые технологии (далее – ЦТ) – совокупность методов работы с электронными информационными ресурсами и методов информационного взаимодействия, осуществляемых с применением аппаратно-программного комплекса и сети телекоммуникаций.

3. В настоящем профессиональном стандарте применяются следующие сокращения:

- 1) ТКУИ – Технические каналы утечки информации;
- 2) КС – Квалификационные справочники;
- 3) ПАС – Программно-аппаратные средства;
- 4) ПО – Программное обеспечение;
- 5) ЕТКС – Единый тарифно-квалификационный справочник;
- 6) ПД – Персональные данные;
- 7) СВТ – Средства вычислительной техники;

- 8) ПЭМИН – Побочные электромагнитные излучения и наводки;
- 9) ТОО – Товарищество с ограниченной ответственностью;
- 10) ОЮЛ – Объединение юридических лиц;
- 11) НАО – Некоммерческое акционерное общество;
- 12) КБ – Кибербезопасность;
- 13) ЗРК – Закон Республики Казахстан;
- 14) СУБД – Система управления базами данных;
- 15) НПА – Нормативно-правовые акты;
- 16) НТД – Нормативно-техническая документация;
- 17) ОС – Операционная система;
- 18) НД – Несанкционированный доступ;
- 19) ОРК – Отраслевая рамка квалификаций;
- 20) ЦС – Цифровые системы;
- 21) ЦТ – Цифровые технологии;
- 22) ЭМК – Электронные медицинские карты;
- 23) ACL – Access Control List;
- 24) API – Application Programming Interface;
- 25) BASH – Bourne Again SHell;
- 26) BDA – Battle Damage Assessment;
- 27) CARVER – Методика анализа целей;
- 28) COA – Course of Action;
- 29) DoS – Denial of Service;
- 30) HIDS – Host Intrusion Detection System;
- 31) HIPS – Host Intrusion Prevention System;
- 32) ICS – Industrial Control Systems;
- 33) IDS – Intrusion detection system;
- 34) IoT – Internet of Things;
- 35) IPS – Intrusion prevention system;
- 36) ISO – International Organization for Standardization;
- 37) JS – JavaScript;
- 38) KPI – Key Performance Indicators;
- 39) KRI – Key Risk Indicators;
- 40) NIDS – Network Intrusion Detection System;
- 41) NIPS – Network Intrusion Prevention System;
- 42) SIEM – Security Information and Event Management;
- 43) SQL – Structured Query Language;
- 44) SQLi – SQL injection;
- 45) TLP – Traffic Light Protocol;
- 36) TTPs – Tactics, Techniques, and Procedures;

47) VPN – Virtual Private Network;

48) XSS – Cross-Site Scripting.

Глава 2. Паспорт профессионального стандарта

4. Название профессионального стандарта: Деятельность в области кибербезопасности

5. Код профессионального стандарта: J62092101

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. 2 Деятельность в области кибербезопасности

7. Краткое описание профессионального стандарта: Профессиональный стандарт "Деятельность в области кибербезопасности" разработан в соответствии со статьей 5 Закона Республики Казахстан "О профессиональных квалификациях"

8. Перечень карточек профессий:

1) Администратор по информационной безопасности - 7 уровень ОРК

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

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

4) Специалист по защите информации - 7 уровень ОРК

5) Аудитор по информационной безопасности - 7 уровень ОРК

6) Специалист по информационной безопасности - 7 уровень ОРК

7) Специалист по безопасности сервисов - 7 уровень ОРК

8) Шифровальщик данных - 7 уровень ОРК

9) Инженер по защите информации - 7 уровень ОРК

10) Менеджер по управлению рисками (Risk Manager-SP-RSK-001) - 6 уровень ОРК

11) Разработчик целей - 6 уровень ОРК

12) Оператор киберопераций - 6 уровень ОРК

13) Кибер-инструктор - 6 уровень ОРК

14) Специалист по исследованиям и разработкам - 6 уровень ОРК

15) Менеджер по ИТ инвестициям/портфелю - 6 уровень ОРК

16) Менеджер-программ - 6 уровень ОРК

17) Аналитик угроз и предупреждений - 6 уровень ОРК

18) Специалист по сетевым операциям - 6 уровень ОРК

19) Планировщик киберопераций - 6 уровень ОРК

- 20) Архитектор корпоративной инфраструктуры - 6 уровень ОРК
- 21) Специалист по информационной безопасности - 6 уровень ОРК
- 22) Кибер-юридический консультант - 6 уровень ОРК
- 23) Уполномоченный представитель/ответственный за авторизацию - 6 уровень ОРК
- 24) Специалист по информационной безопасности транспортной инфраструктуры - 6 уровень ОРК
- 25) Специалист-криминалист по цифровым технологиям - 6 уровень ОРК
- 26) Менеджер знаний - 6 уровень ОРК
- 27) Аналитик по правоохранительной/судебной экспертизе и контрразведке - 6 уровень ОРК
- 28) Шифровальщик данных - 6 уровень ОРК
- 29) Аудитор по информационной безопасности - 6 уровень ОРК
- 30) Специалист по безопасности сервисов - 6 уровень ОРК
- 31) Специалист по многоязычному анализу - 6 уровень ОРК
- 32) Специалист по информационной безопасности в области здравоохранения - 6 уровень ОРК
- 33) Инженер по защите информации - 6 уровень ОРК
- 34) Специалист по защите информации - 6 уровень ОРК
- 35) Специалист по вопросам безопасности (ИКТ) - 6 уровень ОРК

Глава 3. Карточки профессий

9. 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:	1. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 2 лет	
Связь с неформальным и информальным образованием:	Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности	
Другие возможные наименования профессии :		
Основная цель деятельности:	Администрировать механизмы безопасности и своевременно реагировать на нарушения КБ	
Описание трудовых функций		
Перечень трудовых функций:	Обязательные трудовые функции:	1. Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения КБ 2. Администрирование механизмов безопасности 3. Реагирование на инциденты КБ 4. Контроль и анализ эффективности применения ПАС защиты информации и обеспечения КБ
	Дополнительные трудовые функции:	
	Навык 1: 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 кибербезопасности 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
Навык 2: 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 кибербезопасности 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 развертывание обновлений, с целью повышения защищенности 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

Трудовая функция 1: Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения КБ		5. Технологии и инструменты, используемые в системах предотвращения вторжений
	Возможность признания навыка:	Не требуется
	Навык 3: 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
		Умения: 1. Эксплуатировать ПАС защиты информации и обеспечения КБ 2. Принимать от поставщика и/или исполнителя работ ПАС защиты информации и обеспечения КБ 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 КБ
		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. Цифровые объекты, подлежащие защите 4. Специализацию и направления деятельности организации и ее подразделений

Навык 4: Эксплуатация ПАС защиты информации и обеспечения КБ и техническое сопровождение	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 цифровых объектов 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 5:	Умения: 1. Эффективно осуществлять удаленную 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 ИТ-инфраструктуры 3. Проводить тонкую настройку антивирусных решений на рабочих станциях и серверах в удаленном 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

	Администрирование антивирусного ПО	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 кибербезопасности 2. Официальных методических рекомендаций производителей антивирусного ПО по его корректной установке, с учетом 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
Трудовая функция 2:	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
		Умения: 1. Управлять криптографическими ключами (генерация и распределение)

Администрирование механизмов безопасности	Навык 2: Настраивание политики безопасности ОС, СУБД, ППО	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. Требования 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
	Навык 1: Мониторинг событий и инцидентов КБ	Умения: 1. Собирать и анализировать события в системах, находящихся под мониторингом КБ 2. Классифицировать события, серийные события и сочетания событий как нарушения КБ 3. Настраивать процедуры обработки событий и обнаруживать события КБ 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
Трудовая функция 3: Реагирование на инциденты КБ	Возможность признания навыка:	Не требуется
		Умения: 1. Регистрировать и оповещать (информировать) об инциденте КБ

	Навык 2: Реагирование на инциденты КБ	2. Определять причины инцидента КБ 3. Принимать меры к ликвидации инцидента КБ и его последствий 4. Собирать доказательства об инциденте 5. Участвовать в проведении расследований инцидентов КБ 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 защиты информации и обеспечения КБ	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 КБ 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 ЦС и защищаемым информационным ресурсам Знания: 1. Методы, принципы и приемы осуществления контроля 2. Процедуры анализа журнала событий КБ (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 КБ
	Возможность признания навыка:	Не требуется
		Умения: 1. Анализировать журналы регистрации событий ПАС защиты информации и обеспечения КБ 2. Оценивать использование ресурсов ПАС защиты информации и обеспечения КБ

	Навык 2: Текущий и периодический контроль работы ПАС защиты информации и обеспечения КБ	3. Вырабатывать предложения по совершенствованию и повышению эффективности использования ПАС защиты информации и обеспечения КБ	
	Возможность признания навыка:	Знания: 1. Принцип работы и правил эксплуатации ПАС защиты информации 2. Критерии и показатели результативности использования ресурсов ПАС защиты информации и обеспечения КБ 3. Параметры контроля ПАС защиты информации и обеспечения КБ	
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 безопасности. 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:	
	-	-	
10. 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 образования: послевузовское образование (	Специальность:	

Уровень профессионального образования:	магистратура, резидентура)	Информационно-коммуникационные технологии	Квалификация: -
Требования к опыту работы:	1. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 2 лет		
Связь с неформальным и информальным образованием:			
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:		
	Навык 1: Формирование политик безопасности компьютерных систем и сетей	Умения: 1. Анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия 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, межгосударственные и международные стандарты в области защиты информации 6. Возможности используемых и планируемых к использованию средств защиты информации	

Трудовая функция 1: Оценивание уровня безопасности компьютерных систем и сетей		7. Нормативные правовые акты в области защиты информации 8. Организационные меры по защите информации
	Возможность признания навыка:	Не требуется
	Навык 2: 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, межгосударственные и международные стандарты в области защиты информации 10. Нормативные правовые акты в области защиты информации 11. Организационные меры по защите информации
	Возможность признания навыка:	Не требуется
		Умения:

	Навык 3: Проведение анализа безопасности компьютерных систем	1. Анализировать компьютерную систему с целью определения уровня защищенности и доверия 2. Прогнозировать возможные пути развития действий нарушителя кибербезопасности 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, межгосударственные и международные стандарты в области защиты информации 7. Нормативные правовые акты в области защиты информации 8. Руководящие и методические документы уполномоченных органов исполнительной власти по защите информации 9. Организационные меры по защите информации
	Возможность признания навыка:	Не требуется
		Умения: 1. Проводить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации 2. Применять отечественные стандарты в области защиты информации для проектирования средств защиты информации компьютерной системы 3. Разрабатывать архитектуру и интерфейсы средств защиты информации, процедуры восстановления работоспособности средств и систем защиты после сбоев 4. Подбирать и обобщать научно-техническую литературу, методические материалы по программным и аппаратным средствам и способам защиты информации, в том числе на английском языке Знания: 1. Методы и средства получения, обработки и передачи информации в операционных системах,

	Навык 1: Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей	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 кибербезопасности 11. Криптографические алгоритмы и особенности их программной реализации 12. Нормативные правовые акты в области защиты информации 13. Организационные меры по защите информации 14. Национальные, межгосударственные и международные стандарты в области защиты информации
	Возможность признания навыка:	Не требуется
Трудовая функция 2: Разработка системы безопасности компьютерных систем и сетей		Умения: 1. Обобщать научно-техническую литературу, нормативные и методические материалы в области защиты информации 2. Формировать модели угроз и модели нарушителя безопасности компьютерных систем 3. Выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы 4. Разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками 5. Применять национальные, межгосударственные и международные стандарты в области защиты информации для оценки защищенности компьютерной системы 6. Применять действующую законодательную базу в области обеспечения компьютерной безопасности

	Навык 2: Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей	7. Читать и понимать нормативные и методические документы по кибербезопасности на английском языке 8. 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 области защиты информации 11. Организационные меры по защите информации 12. Национальные, межгосударственные и международные стандарты в области защиты информации
	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 безопасности. 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	
	Уровень ОРК:	Наименование профессии:
	5	Специалист по защите информации

Связь с другими профессиями в рамках ОРК:	6	Специалист по защите информации	
	7	Специалист по защите информации	
11. 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:	1. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 2 лет		
Связь с неформальным и информальным 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 кибербезопасности 2. Анализ цифровых данных	
	Дополнительные трудовые функции:		
		Умения: 1. Выявлять потенциальные источники данных в организации 2. Разрабатывать план сбора данных	

Трудовая функция 1: Ц и ф р о в а я криминалистика и анализ инцидентов кибербезопасности		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
	Навык 1: Получение данных из потенциальных источников информации	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 кибербезопасности 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 (	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

	объектов-носителей) при компьютерных преступлениях	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 кибербезопасности 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. Составлять отчетные материалы 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 2. Законодательство в сфере обеспечения кибербезопасности 3. Архитектура, устройство и функционирование вычислительных систем 4. Принципы построения и функционирования систем и сетей передачи информации 5. Программные средства обработки информации 6. 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 27001-2023 Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. 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-криминалист по цифровым технологиям
12. 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:	Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 Параграф 3. Специалист по защите информации		
Уровень профессионального образования:	Уровень образования: послевузовское образование (магистратура, резидентура)	Специальность: Информационная безопасность	Квалификация: -
Требования к опыту работы:	1. 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; 2. 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; 3. Специалист по защите информации: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров без предъявления требования к стажу работы.		
Связь с неформальным и информальным 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:		
		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	

Трудовая функция 1: Разработка систем защиты информации ИС	Навык 1: Проектирование архитектуры кибербезопасности	5. Определять виды и типы средств защиты информации 6. Разрабатывать архитектуру системы защиты информации
		Знания: 1. Законодательство в сфере обеспечения кибербезопасности 2. Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей, и их компонентов 3. Особенности защиты информации в ЦС 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 кибербезопасности 7. Принципы формирования политики кибербезопасности 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 кибербезопасности ИС 3. Проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов 4. Разрабатывать модели ЦС и систем защиты информации ЦС 5. Исследовать модели ЦС и систем защиты безопасности ЦС 6. Анализировать программные, архитектурно-технические и схемотехнические решения компонентов ЦС 7. Оценивать информационные риски в ЦС и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите 8. Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в ЦС 9. Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в ЦС 10. Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации Знания:

		1. Основные методы управления кибербезопасностью 2. Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов 3. Основные методы управления проектами в области кибербезопасности 4. Национальные стандарты в сфере обеспечения кибербезопасности 5. Основные меры по защите информации в ЦС 6. Особенности защиты информации в ЦС управления технологическими процессами 7. Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в ЦС 8. Методы, способы, средства, последовательность и содержание этапов разработки ЦС и систем защиты информации ЦС 9. Программно-аппаратные средства обеспечения защиты информации в программном обеспечении ЦС 10. Основные средства, способы и принципы построения систем защиты информации ЦС
	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 ЦС 2. Выявлять уязвимости информационно-технологических ресурсов ЦС 3. Разрабатывать предложения по совершенствованию системы управления защиты информации ЦС 4. Выбирать программно-аппаратных средств обеспечения безопасности информации для использования их в составе ЦС 5. Классифицировать и оценивать угрозы безопасности информации для ЦС 6. Определять информационную инфраструктуру и информационных ресурсов ЦС, подлежащие защите 7. Разрабатывать модели угроз безопасности информации и нарушителей в ЦС 8. Определять эффективность применения средств цифровизации Знания: 1. Основные информационные технологии, используемые в ЦС 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 ЦС 5. Принципы построения средств защиты информации от "утечки" по техническим каналам 6. Национальные стандарты в сфере обеспечения кибербезопасности 7. Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения	
	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:	ҚР СТ ISO/IEC 27001-2023 "Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	6	Специалист по защите информации	
13. 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 образования: послевузовское образование	Специальность:	

Уровень профессионального образования:	магистратура, резидентура)	Информационная безопасность	Квалификация: -
Требования к опыту работы:	1. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 2 лет		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности		
Другие возможные наименования профессии :			
Основная цель деятельности:	Планировать и контролировать аудит КБ		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Планирование аудита КБ 2. Обеспечение аудита КБ 3. Контроль аудита КБ	
	Дополнительные трудовые функции:		
Трудовая функция 1: Планирование аудита КБ	Навык 1: Планирование работы подразделения аудита КБ	Умения:	1. Планировать работы подразделения аудита КБ 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 КБ
Знания:		1. Законодательство в сфере обеспечения кибербезопасности	

Трудовая функция 2: Обеспечение аудита КБ		2. Методологии, методики и технологии планирования аудита 3. Методики управления проектами
	Возможность признания навыка:	Не требуется
	Навык 1: Организационное обеспечение КБ	Умения: 1. Организовывать взаимодействие с представителями проверяемой организации (подразделения) по вопросам аудита КБ 2. Организовывать обучение и повышение квалификации аудиторов КБ 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 2: Стратегическое руководство и управление процессами кибербезопасности	Умения: 1. Формирование стратегии информационной безопасности, соответствующей бизнес-целям и угрозам 2. Разработка планов по интеграции инновационных технологий в процесс защиты информации 3. Проводить оценку долгосрочных угроз безопасности и создавать сценарии реагирования Знания: 1. Основные требования к системе менеджмента по кибербезопасности 2. Подходы к управлению и снижению рисков кибербезопасности 3. Принципы управления рисками и их минимизации в контексте кибербезопасности 4. Законодательство в сфере цифровизации
	Возможность признания навыка:	Не требуется
	Навык 3: Консультирование и инструктаж работников	Умения: 1. Консультировать работников проверяемой организации (подразделения) по вопросам, связанным с аудитом КБ 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:

	организации по вопросам аудита КБ	1. Национальный стандарт по управлению рисками кибербезопасности 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 КБ	Навык 1: Контроль профессиональных качеств аудитора	Умения: 1. Контролировать соблюдение аудиторами КБ правил независимости и принципов этики при выполнении аудиторских заданий 2. Анализировать и оценивать профессиональные знания и качество аудиторов КБ 3. Работать с аудиторами КБ для совершенствования их профессиональных навыков Знания: 1. Национальные стандарты контроля качества аудита 2. Нормативно-правовые акты аудита по обеспечению КБ 3. Требования по ведению аудита по КБ
	Возможность признания навыка:	Не требуется
	Навык 2: 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
		Умения: 1. Проводить комплексные проверки системы безопасности с целью выявления уязвимостей 2. Использовать методы тестирования на проникновение (penetration testing) для оценки защищенности системы

	Навык 3: Проведение тестов на проникновение для оценки безопасности системы	3. Применять средства мониторинга для постоянного отслеживания эффективности защиты информации	
	Возможность признания навыка:	Знания: 1. Инструменты и методы тестирования на проникновение (например, Metasploit, Nessus, Burp Suite) 2. Технологии обнаружения и предотвращения атак (IDS, IPS) 3. Принципы проведения аудитинга безопасности на основе реальных сценариев угроз	
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 27001-2023 Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. 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	Аудитор по информационной безопасности	
14. 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:	1. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 2 лет	
Связь с неформальным и информальным 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 КБ организации	
Описание трудовых функций		
Перечень трудовых функций:	Обязательные трудовые функции:	1. Координирование процессов обеспечения КБ 2. Анализ и контроль мероприятий по управлению и обеспечению КБ
	Дополнительные трудовые функции:	
Трудовая функция 1: Координирование процессов обеспечения КБ	Навык 1: Планирование процессов управления и обеспечения КБ организации	Умения: 1. Оценивать текущий уровень НТД, регламентирующих процессы обеспечения КБ 2. Разрабатывать (актуализировать) ТД, регламентирующие процессы обеспечения КБ 3. Разрабатывать профили защиты и задания по безопасности для ЦС и компонентов информационно-коммуникационной инфраструктуры
		Знания: 1. Принципы защитных механизмов программных и аппаратных средств организации 2. Научные исследования в сфере обеспечения КБ 3. Принципы и методологию проектирования ИС
	Возможность признания навыка:	Не требуется
	Навык 2: Постановка задач и контроль их выполнения в сфере обеспечения КБ	
Знания:		

Трудовая функция 2: Анализ и контроль мероприятий по управлению и обеспечению КБ		1. Базовые принципы регламентации бизнес-процессов 2. Законодательства в сфере обеспечения КБ 3. Национальные стандарты в сфере обеспечения КБ
	Возможность признания навыка:	Не требуется
	Навык 1: Подготовка планов мероприятий по обеспечению КБ организации	Умения: 1. Анализировать защищенности бизнес- процессов и активов, связанных с автоматизированной обработкой информации 2. Выбирать инструментарий и методы обеспечения КБ 3. Разрабатывать мероприятия, направленные на реализацию политики КБ организации 4. Составлять план по обеспечению непрерывности бизнеса и восстановления после инцидентов КБ и форс-мажорных ситуаций Знания: 1. Основные тенденции развития отечественного и зарубежного рынка инструментариев и средств обеспечения КБ 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 КБ 2. Разрабатывать требования, технические задания на подсистемы КБ ИС 3. Организовывать и координировать работы по разработке профилей защиты и задания по безопасности для ЦС 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
	Гибкость мышления	

Требования к личностным компетенциям:	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 безопасности. 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	
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:	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:	1. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 2 лет		
Связь с неформальным и информальным 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 кибербезопасности
	Дополнительные трудовые функции:	
Трудовая функция 1: Оценка и анализ рисков безопасности при проектировании и внедрении сервисов	Навык 1: Проведение тестирования 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 КБ, 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 кибербезопасностью	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 кибербезопасности 6. Обнаруживать и предотвращать дезинформационные атаки, направленные на сервис Знания: 1. Основы кибербезопасности – 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 1: Участие в расследовании инцидентов и разработке мер по их предотвращению	
	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 безопасности. 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	
16. 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:	1. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 2 лет	
Связь с неформальным и информальным 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 кибербезопасности
	Дополнительные трудовые функции:	
	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 кибербезопасности 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

Трудовая функция 1: Разработка программно-аппаратных систем шифрования данных		5. Основные характеристики технических средств шифрования данных 6. Функционирование современных систем шифрования данных 7. Национальные стандарты в сфере обеспечения кибербезопасности
	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 кибербезопасности
	Возможность признания навыка:	Не требуется
		Умения: 1. Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для систем шифрования данных

Трудовая функция 2: Проведение шифрование и расшифровки данных в соответствии с регламентами и требованиями кибербезопасности	Навык 1: Разработка эксплуатационной документации на системы шифрования данных	2. Разрабатывать технические задания на создание подсистем КБ 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
	Навык 2:	Умения: 1. Тестировать 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. Разрабатывать и оформлять контрольные примеры для проверки работоспособности программного обеспечения

	Тестирование разработанных систем шифрования данных	5. Подготавливать наборы 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	
Требования к личностным компетенциям:	Ответственность Структурное мышление Усидчивость, 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 управления 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 Информационные технологии. Аудит систем управления информационной безопасностью организации 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	
17. 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	Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих Приказ Министра труда и социальной		

квалификационных характеристик:	защиты населения Республики Казахстан от 30 декабря 2020 года № 553 Параграф 2. 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 информальным 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:		
		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	

Навык 1:
Нормативное
регулирование, угрозы,
методы и средства
защиты информации

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,

Трудовая функция 1: Создание системы защиты информации в организации		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 13. 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 КБ 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 КБ 2. Эксплуатационной документации на систему защиты информации 3. Типов, категорий, видов и уровней градации (категорирования) информации
	Возможность признания навыка:	Не требуется
		Умения: 1. Разрабатывать модели угроз безопасности информации в организации 2. Использовать программные средства разработки модели угроз

	Навык 3: Разработка модели угроз безопасности информации в организации	3. Разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации 4. Разрабатывать проекты систем и подсистем управления кибербезопасности 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 цифровой объект 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
	Навык 1: 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 кибербезопасности 2. Стандарты ЕСКД, ЕСТД и ЕСПД 3. Современные информационных технологии 4. Типы, категории, виды и уровни градации (категорирования) информации
	Возможность признания навыка:	Не требуется
		Умения:

Трудовая функция 2: Ввод в эксплуатацию системы защиты информации в организации	Навык 2: Разработка и реализация организационных мер, обеспечивающих эффективность системы защиты информации	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 кибербезопасности 2. Методы, средства и системы защиты информации 3. Архитектуру технических средств защиты информации
	Возможность признания навыка:	Не требуется
	Навык 3: 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 4: 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

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 цифровизации 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 безопасности. 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	
18. Карточка профессии "Менеджер по управлению рисками (Risk Manager-SP-RSK-001)":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-026		
Наименование профессии :	Менеджер по управлению рисками (Risk Manager-SP-RSK-001)		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) управленческого образования		
Другие возможные наименования профессии :	1229-0-002 - Руководитель по риск-менеджменту		
Основная цель деятельности:	Идентифицирует, оценивает и минимизирует риски в области кибербезопасности.		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Обеспечение КБ и работа с данными 2. Идентификация рисков в области кибербезопасности 3. Оценка рисков в области кибербезопасности	
	Дополнительные трудовые функции:	1. Минимизация рисков в области кибербезопасности	
	Навык 1: Комплексное обеспечение	Умения: 1. Собирать и анализировать артефакты, логи, дампы памяти, системные следы 2. Управлять политикой паролей, групп безопасности, многофакторной аутентификацией 3. Применять групповые политики, права пользователей, правила межсетевых экранов 4. Проводить аудит и тестирование систем КБ	
		Знания:	

Трудовая функция 1: Обеспечение КБ и работа с данными	кибербезопасности и администрирование защищенных систем	1. Основ администрирования и защиты информационных систем 2. Методов и средств обеспечения безопасности 3. Принципов анализа, аудита и тестирования систем безопасности 4. Языков программирования
	Возможность признания навыка:	Требуется
	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	Умения: 1. Выявлять и классифицировать инциденты кибербезопасности 2. Анализировать журналы событий, сетевой трафик и другие источники данных 3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства) Знания: 1. Основ классификации инцидентов кибербезопасности и их особенностей 2. Методов сбора и корреляции данных об инцидентах КБ 3. Основ расследования инцидентов и цифровой криминалистики 4. Нормативных требований к фиксации и обработке инцидентов КБ
	Возможность признания навыка:	Требуется
Трудовая функция 2: Идентификация рисков в области кибербезопасности	Навык 1: Сбор и анализ информации о потенциальных угрозах	Умения: 1. Проводить аудит систем и процессов для выявления уязвимостей 2. Использовать инструменты мониторинга для обнаружения аномалий в сетевом трафике 3. Интервьюировать сотрудников и заинтересованных сторон для сбора данных о рисках 4. Документировать идентифицированные угрозы в реестре рисков Знания: 1. Основных типов киберугроз (вирусы, фишинг, DDoS-атаки) 2. Методов анализа уязвимостей (CVSS, OWASP) 3. Нормативных требований к кибербезопасности в РК и мире 4. Инструментов для сканирования уязвимостей (Nessus, OpenVAS)
	Возможность признания навыка:	Не требуется
		Умения: 1. Категорировать риски по уровням воздействия

	Навык 2: Классификация и сортировка рисков	2. Применять матрицы рисков для оценки вероятности и последствий 3. Интегрировать данные из внешних в анализ рисков КБ 4. Обновлять реестр рисков на основе новых данных Знания: 1. Моделей классификации рисков 2. Факторов, влияющих на бизнес-критичность активов 3. Источников информации о угрозах 4. Принципов непрерывного мониторинга рисков
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Оценка рисков в области кибербезопасности	Навык 1: Количественная и качественная оценка рисков	Умения: 1. Рассчитывать ожидаемые потери от рисков 2. Проводить сценарийный анализ для моделирования последствий угроз 3. Оценивать эффективность существующих мер контроля 4. Формировать отчеты с рекомендациями Знания: 1. Методик количественной оценки 2. Качественных подходов 3. Стандартов оценки рисков (NIST SP 800-30, FAIR) 4. Экономических аспектов рисков
	Возможность признания навыка:	Не требуется
	Навык 2: Интеграция оценки рисков в бизнес-процессы	Умения: 1. Координировать оценку рисков с другими отделами 2. Разрабатывать планы тестирования на проникновение (pentesting) 3. Анализировать влияние рисков на бизнес-цели 4. Отслеживать изменения в оценке рисков Знания: 1. Интеграции риск-менеджмента в SDLC (Secure Software Development Lifecycle). 2. Ролей заинтересованных сторон в оценке 3. Инструментов для моделирования рисков 4. Регуляторных рамок для оценки
	Возможность признания навыка:	Не требуется
		Умения: 1. Проектировать стратегии минимизации рисков 2. Внедрять технические меры минимизации рисков в области КБ

Дополнительная трудовая функция 1: Минимизация рисков в области кибербезопасности	Навык 1: Разработка мер по снижению рисков	3. Обучать персонал по вопросам кибербезопасности 4. Оценивать эффективность внедренных мер
	Возможность признания навыка:	Знания: 1. Стратегий минимизации рисков КБ 2. Технических контрмер 3. Программ повышения осведомленности 4. Метрик эффективности Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты ISO/IEC 27005:2018 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление рисками информационной безопасности (Information security risk management) ISO 31000:2018 — Управление рисками. Принципы и руководство (Risk management) ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Связь с менеджментом ИБ ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Контрольные меры (кодекс практики) Национальные стандарты РК: СТ РК ISO/IEC 27005-2013 ("Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности") СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
19. Карточка профессии "Разработчик целей":		
Код группы:	2524-0	
Код наименования занятия:	2524-0-024	
Наименование профессии:	Разработчик целей	
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности и кибер-разведки при наличии базового (высшего) образования в области кибербезопасности		
Другие возможные наименования профессии :			
Основная цель деятельности:	Проводит анализ целей и разрабатывает планы операций в киберпространстве		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Анализ и выбор объектов воздействия в киберпространстве 2. Разработка пакетов целеуказания 3. Поддержка планирования и проведения киберопераций	
	Дополнительные трудовые функции:	1. Оценка эффективности проведенной кибероперации	
Трудовая функция 1: Анализ и выбор объектов воздействия в киберпространстве	Навык 1: Построение сетевой карты и профиля цели	Умения: 1. Строить топологию сети цели и выявлять критические узлы 2. Определять программно-аппаратный стек цели (версии ОС, СУБД, веб-серверов и т.д.) 3. Выявлять уязвимости и возможные векторы атаки 4. Оценивать критичность активов цели	
		Знания: 1. Методик анализа целевой системы и киберцепочки поражения 2. Баз данных уязвимостей и их эксплуатации 3. Принципов оценки критичности активов в киберпространстве 4. Инструментов визуализации сетей в связке с разведанными	
	Возможность признания навыка:	Требуется	
		Умения: 1. Проводить OSINT и HUMINT о сетевой инфраструктуре цели 2. Выполнять пассивную и активную разведку с использованием специализированных инструментов 3. Структурировать и верифицировать полученные данные о цели	

	Навык 2: Сбор и обработка разведывательной информации о цели	4. Оформлять разведывательные сводки в установленном формате
	Возможность признания навыка:	Знания: 1. Методов и инструментов OSINT и HUMINT 2. Принципов сетевых протоколов и архитектуры корпоративных сетей 3. Основ оперативной безопасности при проведении разведки 4. Методов противодействия обнаружению в сетевой и реальной среде
Трудовая функция 2: Разработка пакетов целеуказания	Навык 1: Формирование номенклатуры целей и обоснование выбора	Умения: 1. Определять приоритетность цели по стратегической, оперативной и тактической значимости 2. Обосновывать выбор цели с использованием модели CARVER или аналогичных 3. Согласовывать пакет целеуказания с вышестоящим руководством 4. Подготавливать презентации и брифинги по разработанным целям Знания: 1. Матрицы CARVER и других методик приоритизации целей 2. Принципов эффектов киберопераций 3. Требований к оформлению пакета целеуказания 4. Основ военной доктрины применения сил в киберпространстве
	Возможность признания навыка:	Не требуется
	Навык 2: Разработка детализированного досье на цель	Умения: 1. Составлять электронное досье цели 2. Включать в досье временные окна уязвимости, зависимости и сопутствующие риски 3. Моделировать возможные пути доступа и этапы эксплуатации 4. Обновлять досье в реальном времени по мере поступления новых разведанных Знания: 1. Стандартов обмена разведанными 2. Принципов моделирования атак 3. Методов оценки сопутствующего ущерба в киберпространстве 4. Инструментов совместной работы
	Возможность признания навыка:	Не требуется
		Умения: 1. Предлагать технически осуществимые варианты действий (COA) на основе разработанных целей

Трудовая функция 3: Поддержка планирования и проведения киберопераций	Навык 1: Участие в разработке курсов действий	2. Оценивать риски и вероятность успеха каждого варианта действий (COA) 3. Участвовать в военных играх и упражнениях на кибертренажере 4. Корректировать цели под выбранный вариант действий (COA)
		Знания: 1. Процессов планирования операций в киберпространстве 2. Методик анализа и сравнения вариантов действий (COA) 3. Принципов матрицы синхронизации в кибероперациях 4. Основ теории игр в киберконфликтах
	Возможность признания навыка:	Не требуется
	Навык 2: Обеспечение целеуказания в режиме реального времени	Умения: 1. Отслеживать состояние цели в ходе операции 2. Оперативно корректировать параметры доступа при изменении инфраструктуры 3. Передавать уточненные данные группам эксплуатации/доступа 4. Фиксировать достигнутые эффекты и остаточные уязвимости Знания: 1. Принципов командования и управления в кибероперациях 2. Протоколов и форматов передачи целеуказания в режиме реального времени 3. Методов измерения эффектов от киберопераций 4. Инструментов единой кибероперационной обстановки
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Оценка эффективности проведенной кибероперации	Навык 1: Сбор и анализ данных о достигнутых результатах кибероперации	Умения: 1. Собирать телеметрию и логи с закладных устройств и эксплойтов 2. Оценивать степень достижения желаемых результатов 3. Выявлять причины отрицательных результатов 4. Готовить отчеты об оценке нанесенного ущерба (BDA) в киберпространстве Знания: 1. Методик оценки нанесенного ущерба (BDA) и рекомендаций для повторной атаки 2. Индикаторов достижения результатов атаки в киберпространстве 3. Инструментов анализа трафика и логов 4. Принципов полученного опыта в кибероперациях

	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение быстро принимать решения Умение работать в команде Целеустремленность Дисциплинированность Аналитическое мышление Концентрация и управление вниманием Инициативность	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры (кодекс практики) обеспечения информационной безопасности ISO/IEC 27033 — Информационные технологии. Методы обеспечения безопасности. Безопасность сетей ISO/IEC 27005 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление рисками информационной безопасности Национальные стандарты РК: СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла") СТ РК 4009-2025 ("Информационные технологии. Криптографическая защита информации. Алгоритм блочного симметричного шифрования")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
20. Карточка профессии "Оператор киберопераций":		
Код группы:	2524-0	
Код наименования занятия:	2524-0-033	
Наименование профессии:	Оператор киберопераций	
Уровень квалификации по ОРК:	6	
подуровень квалификации по ОРК:		
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:		
	Уровень образования:	Специальность:

Уровень профессионального образования:	высшее образование (бакалавриат, специалитет, ординатура)	Информационная безопасность	Квалификация: -
Требования к опыту работы:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности и киберопераций при наличии базового (высшего) образования в области кибербезопасности		
Другие возможные наименования профессии:			
Основная цель деятельности:	Проводит наступательные и оборонительные кибероперации, выявляя уязвимости и нейтрализуя угрозы		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Выявление уязвимостей в информационных системах 2. Проведение оборонительных киберопераций 3. Проведение наступательных киберопераций	
	Дополнительные трудовые функции:	1. Оценка эффективности проведенной кибероперации	
Трудовая функция 1: Выявление уязвимостей в информационных системах	Навык 1: Тестирование на проникновение и эксплуатация уязвимостей	Умения: 1. Выполнять сканирование уязвимостей с использованием специализированных инструментов 2. Эксплуатировать выявленные уязвимости для получения доступа 3. Проводить пост-эксплуатацию для оценки глубины компрометации 4. Оценивать уровень риска от обнаруженных уязвимостей	
		Знания: 1. Баз данных уязвимостей 2. Инструментов тестирования на проникновение 3. Этапов пентеста 4. Методик оценки уязвимостей	
	Возможность признания навыка:	Требуется	
Навык 2: Сбор разведанных о цели		Умения: 1. Проводить разведку для сбора информации о цели 2. Использовать инструменты сканирования сети для выявления открытых портов и сервисов 3. Анализировать публичные источники на предмет утечек конфиденциальной информации 4. Документировать результаты разведки в отчетах	
		Знания: 1. Методов получения разведывательных данных о цели кибероперации 2. Принципов работы сетевых протоколов и сервисов	

		3. Инструментов кибер-разведки 4. Нормативных ограничений на получение данных о пользователе сети
	Возможность признания навыка:	Требуется
Трудовая функция 2: Проведение оборонительных киберопераций	Навык 1: Мониторинг и обнаружение угроз	Умения: 1. Настраивать системы обнаружения вторжений 2. Анализировать логи и трафик для выявления аномалий 3. Реагировать на сигналы тревоги в реальном времени 4. Проводить корреляцию событий из различных источников Знания: 1. Принципов работы SIEM-систем 2. Паттернов атак 3. Инструментов мониторинга сети 4. Методов обнаружения угроз
	Возможность признания навыка:	Не требуется
	Навык 2: Нейтрализация угроз и восстановление системы	Умения: 1. Изолировать скомпрометированные в сети узлы 2. Удалять вредоносное ПО и восстанавливать системы из резервных копий 3. Проводить форензик-анализ инцидентов 4. Внедрять временные меры защиты до полного устранения угрозы Знания: 1. Процессов реагирования на инциденты КБ 2. Инструментов цифровой криминалистики 3. Методов устранения и ликвидации угрозы КБ 4. Принципов резервного копирования и восстановления
	Возможность признания навыка:	Не требуется
	Навык 1: Планирование и подготовка киберопераций	Умения: 1. Разрабатывать правила применения сил для киберопераций 2. Координировать действия команды в рамках кибероперации 3. Подготавливать специализированные инструменты 4. Оценивать потенциальные эффекты от кибероперации Знания: 1. Этапов киберопераций 2. Правовых и этических аспектов наступательных киберопераций 3. Инструментов создания эксплойтов

Трудовая функция 3: Проведение наступательных киберопераций		4. Тактики, техники и процедуры наступательных киберопераций
	Возможность признания навыка:	Не требуется
	Навык 2: Выполнение и контроль киберопераций	Умения: 1. Получать и поддерживать доступ к целевым системам 2. Выполнять перемещение внутри сети 3. Маскировать действия во избежание обнаружения 4. Оценивать эффективность операции в реальном времени Знания: 1. Методов закрепления и повышения привелегий 2. Техник проведения киберопераций без обнаружения 3. Инструментов C2 инфраструктуры
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Оценка эффективности проведенной кибероперации	Навык 1: Сбор и анализ данных о достигнутых результатах операции	Умения: 1. Собирать телеметрию и логи с закладных устройств эксплойтов 2. Оценивать степень достижения желаемых результатов 3. Выявлять причины недостижения результатов 4. Готовить отчеты об оценке нанесенного ущерба (BDA) в киберпространстве Знания: 1. Методик оценки нанесенного ущерба (BDA) и рекомендаций для повторной атаки 2. Индикаторов достижения результатов атаки в киберпространстве 3. Инструментов анализа трафика и логов 4. Принципов полученного опыта в кибероперациях
	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
	Международные стандарты: ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий (Common Criteria) ISO/IEC 27033 — Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность ISO/IEC 27035 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление инцидентами информационной безопасности (Incident management) ISO/IEC 27031 —	

Список технических регламентов и национальных стандартов:	Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по готовности к непрерывности деятельности (Continuity readiness) Национальные стандарты ПК: СТ ПК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ ПК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ ПК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ ПК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
21. Карточка профессии "Кибер-инструктор":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-020		
Наименование профессии :	Кибер-инструктор		
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: Педагогика и психология	Квалификация: -
Требования к опыту работы:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) педагогического образования		
Другие возможные наименования профессии :			
Основная цель деятельности:	Разрабатывает и проводит тренинговые программы для повышения навыков и осведомленности в области кибербезопасности		
Описание трудовых функций			
		1. Обеспечение КБ и работа с данными	

Перечень трудовых функций:	Обязательные трудовые функции:	2. Проектирование образовательных программ по кибербезопасности 3. Проведение учебных занятий и оценка обучающихся
	Дополнительные трудовые функции:	1. Актуализация учебных материалов на основе поиска новых угроз
Трудовая функция 1: Обеспечение КБ и работа с данными	Навык 1: Комплексное обеспечение кибербезопасности и администрирование защищенных систем	Умения: 1. Собирать и анализировать артефакты, логи, дампы памяти, системные следы 2. Управлять политикой паролей, групп безопасности, многофакторной аутентификацией 3. Применять групповые политики, права пользователей, правила межсетевых экранов 4. Проводить аудит и тестирование систем КБ Знания: 1. Основ администрирования и защиты информационных систем 2. Методов и средств обеспечения безопасности 3. Принципов анализа, аудита и тестирования систем безопасности 4. Языки программирования
	Возможность признания навыка:	Требуется
	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	Умения: 1. Выявлять и классифицировать инциденты кибербезопасности 2. Анализировать журналы событий, сетевой трафик и другие источники данных 3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства) Знания: 1. Основ классификации инцидентов кибербезопасности и их особенностей 2. Методов сбора и корреляции данных об инцидентах КБ 3. Основ расследования инцидентов и цифровой криминалистики 4. Нормативных требований к фиксации и обработке инцидентов КБ
	Возможность признания навыка:	Требуется
		Умения: 1. Анализировать требования к образовательным модулям по кибербезопасности 2. Формировать цели и результаты обучения 3. Создавать структуру программы с учетом уровня аудитории 4. Разрабатывать планы проведения занятий

Трудовая функция 2: Проектирование образовательных программ по кибербезопасности	Навык 1: Разработка учебных программ	5. Проектировать сценарии практических заданий и лабораторных работ Знания: 1. Основ педагогического проектирования 2. Принципов модульного построения учебных программ 3. Методов разработки образовательных программ 4. Необходимых компетенций в области кибербезопасности 5. Требований к учебной документации
	Возможность признания навыка:	Не требуется
	Навык 2: Подготовка учебных материалов	Умения: 1. Разрабатывать УМК 2. Формировать кейсы на основе реальных киберинцидентов 3. Подготавливать контент для онлайн-платформ 4. Использовать эффективные инструменты визуализации 5. Применять адаптивные подходы к подаче материала
		Знания: 1. Типов учебных материалов 2. Основ визуальной коммуникации 3. Инструментов разработки электронных курсов 4. Принципов адаптивного обучения 5. Требований к академическим и прикладным учебным материалам
	Возможность признания навыка:	Не требуется
	Навык 3: Оценка учебных материалов	Умения: 1. Проводить экспертную оценку учебных материалов 2. Использовать контрольные и измерительные методы 3. Анализировать обратную связь с обучающимися 4. Оценивать практическую эффективность практических лабораторных заданий 5. Корректировать материалы на основе результатов анализа
		Знания: 1. Методов педагогической экспертизы 2. Критериев качества учебных материалов 3. Стандартов оценки образовательных материалов 4. Психометрических методов контроля знаний 5. Подходов к ко всем видам контроля и оценивания знаний обучающихся
	Возможность признания навыка:	Не требуется

Трудовая функция 3: Проведение учебных занятий и оценка обучающихся	Навык 1: Проведение аудиторных и онлайн-занятий	Умения: 1. Проводить аудиторные и онлайн-занятия 2. Управлять динамикой группы 3. Объяснять сложные материалы доступным языком 4. Мотивировать обучающихся к активному участию 5. Управлять временем и структурой занятия Знания: 1. Методов активного обучения 2. Основ публичных коммуникаций 3. Психологии педагогического процесса 4. Методов групповой работы 5. Приёмов упрощённого объяснения
	Возможность признания навыка:	Не требуется
	Навык 2: Проведение практических занятий в сфере КБ	Умения: 1. Организовывать практические занятия на симуляционных платформах 2. Проводить моделирование кибератак 3. Формировать задачи по реагированию на инциденты КБ 4. Настраивать виртуальные практические окружения 5. Анализировать действия обучающихся Знания: 1. Кибергигиены 2. Методов моделирования кибератак 3. Принципов построения киберполигонов 4. Основ цифровой криминалистики 5. Инструментов управления инцидентами КБ
	Возможность признания навыка:	Не требуется
	Навык 3: Контроль и оценка результатов обучения	Умения: 1. Разрабатывать материал для проверки знаний 2. Оценивать выполнение практических заданий 3. Использовать автоматизированные системы тестирования 4. Проводить итоговую оценку навыков 5. Анализировать и обрабатывать результаты оценивания Знания: 1. Стандартов и критериев оценивания 2. Типов контрольных и тестовых заданий 3. Методов анализа результатов тестирования 4. Принципов объективного оценивания 5. Автоматизированных систем для проведение тестирований и оценки результатов

	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Актуализация учебных материалов на основе поиска новых угроз	Навык 1: Анализ актуальных угроз	Умения: 1. Отслеживать изменения киберугроз 2. Анализировать отчёты компаний и CERT-центров 3. Выделять угрозы, значимые для обучающихся 4. Сопоставлять полученные данные с содержанием учебных материалов 5. Использовать аналитические инструменты Знания: 1. Основных источников данных о киберугрозах 2. Типологии атак и уязвимостей 3. Принципов анализа киберугроз 4. Текущих трендов в кибербезопасности 5. Методов оценки рисков
	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры (кодекс практики) обеспечения информационной безопасности ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий (Common Criteria) ISO/IEC 27033 — Информационные технологии. Методы обеспечения безопасности. Обучение построению безопасной сети Национальные стандарты РК: СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определённые пакеты требований безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
22. Карточка профессии "Специалист по исследованиям и разработкам":		

Код группы:	2524-0		
Код наименования занятия:	2524-0-029		
Наименование профессии:	Специалист по исследованиям и разработкам		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) технического образования		
Другие возможные наименования профессии:	2153-2-009 - Инженер-разработчик по телекоммуникациям 1233-0-001 - Главный конструктор (по научным исследованиям и разработкам)		
Основная цель деятельности:	Разрабатывает инновации в области кибербезопасности, исследует новые технологии и методологии для борьбы с возникающими угрозами		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Обеспечение КБ и работа с данными 2. Проведение научно-исследовательских и опытно-конструкторских работ в сфере КБ 3. Осуществление тестирования систем КБ в процессе исследований и разработок	
	Дополнительные трудовые функции:		
	Навык 1: Комплексное обеспечение информационной безопасности и администрирование защищенных систем	Умения: 1. Собирать и анализировать артефакты, логи, дампы памяти, системные следы 2. Управлять политикой паролей, групп безопасности, многофакторной аутентификацией 3. Применять групповые политики, права пользователей, правила межсетевых экранов 4. Проводить аудит и тестирование систем КБ	
		Знания: 1. Основ администрирования и защиты информационных систем 2. Методов и средств обеспечения безопасности	

Трудовая функция 1: Обеспечение КБ и работа с данными		3. Принципов анализа, аудита и тестирования систем безопасности 4. Языков программирования
	Возможность признания навыка:	Требуется
	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	Умения: 1. Выявлять и классифицировать инциденты кибербезопасности 2. Анализировать журналы событий, сетевой трафик и другие источники данных 3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства) Знания: 1. Основ классификации инцидентов кибербезопасности и их особенностей 2. Методов сбора и корреляции данных об инцидентах КБ 3. Основ расследования инцидентов и цифровой криминалистики 4. Нормативных требований к фиксации и обработке инцидентов КБ
	Возможность признания навыка:	Требуется
	Навык 1: Проведение патентных исследований в области КБ	Умения: 1. Обосновывать меры по обеспечению патентной чистоты 2. Обосновывать меры по беспрепятственному производству и реализации 3. Оценивать патентоспособность вновь созданных решений в области КБ 4. Использовать методы анализа применимости исследований объектов интеллектуальной собственности в области КБ 5. Определять показатели технического уровня решения Знания: 1. Охранных документов: патентов, заявок 2. Сопоставительного анализа объекта патента с охраняемыми объектами в сфере КБ 3. Методов определения патентной чистоты 4. Правовых основ охраны объектов исследований
	Возможность признания навыка:	Не требуется
	Навык 2:	Умения: 1. Осуществлять разработку планов и методических программ проведения исследований и разработок 2. Организовывать сбор и изучение научно-технической информации

Трудовая функция 2: Проведение научно-исследовательских и опытно-конструкторских работ в сфере КБ	Проведение работ по обработке и анализу научно-технической информации и результатов исследований	3. Проведение анализа научных данных, результатов экспериментов и наблюдений 4. Осуществление теоретического обобщения научных данных, результатов экспериментов и наблюдений Знания: 1. НПА и НТД в сфере КБ 2. Методов анализа научных данных 3. Методов и средств планирования и организации исследований и разработок
	Возможность признания навыка:	Не требуется
	Навык 3: Управление группой работников при проведении исследований в области КБ	Умения: 1. Разрабатывать элементы планов и методических программ проведения исследований и разработок 2. Внедрять результаты исследований и разработок в соответствии с установленными полномочиями 3. Проверять правильности результатов, полученных сотрудниками 4. Осуществлять повышение квалификации собственных сотрудников Знания: 1. Актуальной нормативной документации в области труда и менеджмента 2. Методов организации труда и управления персоналом 3. Методов внедрения результатов исследований и разработок
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Осуществление тестирования систем КБ в процессе исследований и разработок	Навык 1: Комплексное тестирование кибербезопасности	Умения: 1. Проведение пентестов 2. Анализ исходного кода 3. Сканирование уязвимостей 4. Эксплуатация уязвимостей Знания: 1. Разведки, сканирования, эксплуатации и пост-эксплуатации при проведении пентеста 2. Типичных ошибок в коде 3. Техник эксплуатации уязвимостей
	Возможность признания навыка:	Не требуется
	Навык 2: Проведение исследований в области	Умения: 1. Тестировать человеческий фактор через методы социальной инженерии 2. Планировать, координировать и документировать процесс тестирования 3. Управлять временем и ресурсами Знания:

	социальной инженерии, в применении к КБ	1. Методов социальной инженерии 2. Тайм менеджмента 3. Порядка проведения и ведения этапов исследований	
	Возможность признания навыка:	Не требуется	
Требования к личностным компетенциям:	Самостоятельность и ответственность Системное мышление Стрессоустойчивость Умение работать в команде Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность		
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 15408-1:2018 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Overview and general model ISO/IEC 15408-2/3 — части, охватывающие функциональные требования и требования обеспечения безопасности. Национальные стандарты РК: СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла") СТ РК 4009-2025 ("Информационные технологии. Криптографическая защита информации. Алгоритм блочного симметричного шифрования")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
23. Карточка профессии "Менеджер по ИТ инвестициям/портфелю":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-022		
Наименование профессии:	Менеджер по ИТ инвестициям/портфелю		
Уровень квалификации по ОРК:	6		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:			
	Уровень образования:	Специальность:	Квалификация:

Уровень профессионального образования:	высшее образование (бакалавриат, специалитет, ординатура)	Информационная безопасность	-
Требования к опыту работы:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) финансового образования		
Другие возможные наименования профессии:	2412-0-003 - Консультант по инвестициям		
Основная цель деятельности:	Гарантирует, что инвестиции в ИТ соответствуют стратегическим целям организации и учитывают потребности в кибербезопасности		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Обеспечение КБ и работа с данными 2. Стратегическое управление ИТ-инвестициями 3. Финансово-аналитическое сопровождение ИТ-инвестиций	
	Дополнительные трудовые функции:	1. Управление соответствием в ИТ-инвестициях	
Трудовая функция 1: Обеспечение КБ и работа с данными	Навык 1: Комплексное обеспечение кибербезопасности и администрирование защищенных систем	Умения: 1. Собирать и анализировать артефакты, логи, дампы памяти, системные следы 2. Управлять политикой паролей, групп безопасности, многофакторной аутентификацией 3. Применять групповые политики, права пользователей, правила межсетевых экранов 4. Проводить аудит и тестирование систем КБ Знания: 1. Основ администрирования и защиты информационных систем 2. Методов и средств обеспечения безопасности 3. Принципов анализа, аудита и тестирования систем безопасности 4. Языки программирования	
	Возможность признания навыка:	Требуется	
	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	Умения: 1. Выявлять и классифицировать инциденты кибербезопасности 2. Анализировать журналы событий, сетевой трафик и другие источники данных 3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства) Знания: 1. Основ классификации инцидентов кибербезопасности и их особенностей	

Трудовая функция 2: Стратегическое управление ИТ-инвестициями		2. Методов сбора и корреляции данных об инцидентах КБ 3. Основ расследования инцидентов и цифровой криминалистики 4. Нормативных требований к фиксации и обработке инцидентов КБ
	Возможность признания навыка:	Требуется
	Навык 1: Формирование стратегического плана ИТ-инвестиций	Умения: 1. Анализировать стратегию организации и формировать долгосрочные ориентиры для ИТ-инвестиций 2. Определять приоритеты финансирования ИТ-инициатив на основе бизнес-требований и рисков 3. Оценивать влияние ИТ-инвестиций на достижение корпоративных целей 4. Обосновывать необходимость инвестиций для руководства и заинтересованных сторон Знания: 1. Принципов стратегического и финансового планирования 2. Методов анализа бизнес-приоритетов и факторов стоимости 3. Основ корпоративного управления ИТ 4. Принципов интеграции требований кибербезопасности в стратегию ИТ
	Возможность признания навыка:	Не требуется
	Навык 2: Управление портфелем ИТ-проектов	Умения: 1. Консолидировать данные о портфеле ИТ-инициатив и инвестиционных потребностях 2. Оценивать ценность, сложность и риск ИТ-проектов 3. Балансировать портфель между инновационными, операционными и защитными инициативами 4. Согласовывать решения о составе портфеля с руководством Знания: 1. Подходов к оценке инвестиционной привлекательности проектов 2. Методов классификации ИТ-инициатив 3. Основ инвестиционного и проектного управления 4. Подходов управления рисками и кибербезопасностью
	Возможность признания навыка:	Не требуется
		Умения: 1. Разрабатывать критерии оценки результативности инвестиций

	Навык 3: Оценка эффективности ИТ-инвестиций	2. Проводить анализ фактических затрат и выгод ИТ-проектов 3. Формировать отчеты по эффективности ИТ-инвестиций 4. Выявлять области для повышения отдачи от ИТ-инвестиций
	Возможность признания навыка:	Знания: 1. Методов постпроектного анализа 2. Финансовых моделей оценки эффективности 3. Методов сбора и анализа показателей KPI/KRI 4. Основ контроля исполнения бюджета
Трудовая функция 3: Финансово-аналитическое сопровождение ИТ-инвестиций	Навык 1: Финансовое моделирование ИТ-инвестиций	Умения: 1. Разрабатывать финансовые модели оценки инвестиционных сценариев 2. Рассчитывать прогнозные финансовые результаты ИТ-инвестиций 3. Сравнивать инвестиций по стоимости и ценности 4. Подготавливать презентационные материалы
	Возможность признания навыка:	Знания: 1. Методов инвестиционного анализа и финансового моделирования 2. Основ сценарного анализа 3. Требований к финансовым данным и их качеству 4. Принципов формирования прогнозируемых денежных потоков
	Возможность признания навыка:	Не требуется
	Навык 2: Бюджетирование и планирование ИТ-инвестиций	Умения: 1. Разрабатывать и актуализировать бюджет ИТ-инвестиций 2. Проводить анализ отклонений и прогнозирование затрат 3. Подготавливать финансовые обоснования инвестиционных заявок 4. Согласовывать бюджетные заявки с финансовыми подразделениями
	Возможность признания навыка:	Знания: 1. Методов бюджетирования 2. Основ управленческого учета 3. Принципов распределения ИТ-инвестиций 4. Финансовые требования к оформлению инвестиционных проектов
		Умения: 1. Анализировать законодательные и отраслевые требования

Дополнительная трудовая функция 1: Управление соответствием в ИТ-инвестициях	Навык 1: Контроль соответствия ИТ-инвестиций нормативным требованиям	2. Оценивать соответствие ИТ-инициатив нормативным стандартам 3. Разрабатывать рекомендации по устранению несоответствий 4. Подготавливать отчеты по исполнению требований регуляторов
	Возможность признания навыка:	Знания: 1. Нормативных правовых актов в сфере ИТ и КБ 2. Требований к обработке персональных данных 3. Стандартов регулирования закупок и инвестиций 4. Подходов к документированию процессов соответствия Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27005 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление рисками информационной безопасности ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры (кодекс практики) обеспечения информационной безопасности ISO 31000 — Управление рисками. Принципы и руководство Национальные стандарты РК: СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 27005-2013 ("Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
24. Карточка профессии "Менеджер-программ":		
Код группы:	2524-0	
Код наименования занятия:	2524-0-021	
Наименование профессии:	Менеджер-программ	
Уровень квалификации по ОРК:	6	

подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др т и п о в ы х квалификационных характеристик:			
У р о в е н ь профессионального образования:	Уровень образования: высшее образование (бакалавриат, специалитет , ординатура)	Специальность: Информационная безопасность	Квалификация: -
Требования к опыту работы:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) управленческого образования		
Другие возможные наименования профессии :	2512-1-003 - Менеджер проектов ИКТ		
Основная цель деятельности:	Осуществляет контроль над проектами по кибербезопасности, обеспечивая их соответствие организационным целям, соблюдению сроков и бюджета		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Обеспечение КБ и работа с данными 2. Управление проектами в области КБ на основе полученных планов 3. Планирование и завершение проектов в области КБ на основе договорных обязательств	
	Дополнительные трудовые функции:	1. Обучение сотрудников методам управления	
Трудовая функция 1: Обеспечение КБ и работа с данными	Навык 1: Комплексное обеспечение кибербезопасности и администрирование защищённых систем	Умения: 1. Собирать и анализировать артефакты, логи, дампы памяти, системные следы 2. Управлять политикой паролей, групп безопасности, многофакторной аутентификацией 3. Применять групповые политики, права пользователей, правила межсетевых экранов 4. Проводить аудит и тестирование систем КБ	
		Знания: 1. Основ администрирования и защиты информационных систем 2. Методов и средств обеспечения безопасности 3. Принципов анализа, аудита и тестирования систем безопасности 4. Языки программирования	
	Возможность признания навыка:	Требуется	
		Умения: 1. Выявлять и классифицировать инциденты кибербезопасности	

	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	2. Анализировать журналы событий, сетевой трафик и другие источники данных 3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства) Знания: 1. Основ классификации инцидентов кибербезопасности и их особенностей 2. Методов сбора и корреляции данных об инцидентах КБ 3. Основ расследования инцидентов и цифровой криминалистики 4. Нормативных требований к фиксации и обработке инцидентов КБ
	Возможность признания навыка:	Требуется
	Навык 1: Мониторинг выполнения договоров в проектах по системам защиты информации в соответствии с полученным планом	Умения: 1. Разрабатывать документы 2. Осуществлять коммуникации 3. Составлять отчетность 4. Анализировать входные данные 5. Контролировать исполнение договорных обязательств по срокам поставок и платежей Знания: 1. Основ делопроизводства 2. Технологий межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии 3. Инструментов и методов контроля исполнения договорных обязательств 4. Инструментов и методов осуществления платежей
Трудовая функция 2: Управление проектами в области КБ на основе полученных планов	Возможность признания навыка:	Не требуется
	Навык 2: Организация исполнения работ проекта в соответствии с полученным планом	Умения: 1. Назначать членов команды проекта на выполнение работ по проекту в соответствии с полученными планами проекта 2. Получать и управлять необходимыми ресурсами для выполнения проекта 3. Получать и контролировать отчетность об исполнении от членов команды проекта по факту выполнения работ 4. Контролировать подтверждение выполнения работ Знания: 1. Матрица RACI (Responsible, Accountable, Consulted, Informed) для распределения ролей

		2. Порядка организации приёма, хранения и использования ТМЦ 3. Отчётной документации в области кибербезопасности 4. Отчётной документации в области договорных обязательств
	Возможность признания навыка:	Не требуется
	Навык 3: Аудит конфигураций системы КБ в соответствии с полученным планом	Умения: 1. Проводить формальный физический аудит конфигурации системы защиты информации 2. Проводить формальный функциональный аудит конфигурации системы защиты информации 3. Осуществлять оценку технического задания на систему защиты данных 4. Работать с углубленными параметрами и терминологией в области КБ Знания: 1. Инструменты и методы физического аудита конфигурации системы защиты информации 2. Инструменты и методы функционального аудита конфигурации системы защиты информации 3. Конфигураций технических заданий 4. Углублённая терминология и технические параметры систем защиты данных
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Планирование и завершение проектов в области КБ на основе договорных обязательств	Навык 1: Планирование проекта в соответствии с полученным заданием	Умения: 1. Составлять план управления проектом и частных планов в его составе 2. Разрабатывать иерархические структуры работ проекта в соответствии с полученным заданием 3. Разрабатывать расписание проекта в соответствии с полученным заданием 4. Разрабатывать смету расходов проекта в соответствии с полученным заданием 5. Разрабатывать план финансирования проекта в соответствии с полученным заданием Знания: 1. Знание структуры и содержания плана управления проектом 2. Знание принципов построения и правил декомпозиции работ 3. Знание методов сетевого планирования 4. Знание методов оценки стоимости 5. Знание принципов распределения и планирования финансовых потоков проекта
	Возможность признания навыка:	Не требуется
		Умения:

	Навык 2: Завершение проекта в соответствии с полученным заданием	1. Доносить результаты проекта заказчику согласно договору и проектной документации 2. Архивировать данные проекта 3. Разрабатывать отчет о проекте 4. Инициировать корректировки в систему менеджмента на основе полученного опыта
	Возможность признания навыка:	Знания: 1. Инструментов и методов коммуникаций 2. Каналов коммуникаций 3. Моделей коммуникаций 4. Дисциплин управления проектами 5. Порядка подготовки финализирующих документов по проекту
Дополнительная трудовая функция 1: Обучение сотрудников методам управления	Навык 1: Проведение обучающих занятий по методам управления	Умения: 1. Разрабатывать программу обучения с учетом уровня подготовки сотрудников 2. Проводить тренинги, лекционные и практические занятия по управленческим методикам 3. Использовать интерактивные методы обучения
	Возможность признания навыка:	Знания: 1. Современных методологий управления 2. Принципов организации и проведения занятий 3. Методов оценки вовлеченности слушателей
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements ISO/IEC 27002:2022 — Code of practice for information security controls ISO/IEC 27005:2018 — Information security risk management Национальные стандарты РК: СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла") СТ РК 4009-2025 ("	

	Информационные технологии. Криптографическая защита информации. Алгоритм блочного симметричного шифрования")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
25. Карточка профессии "Аналитик угроз и предупреждений":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-023		
Наименование профессии:	Аналитик угроз и предупреждений		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) образования по направлению кибербезопасности		
Другие возможные наименования профессии:			
Основная цель деятельности:	Разрабатывает оценки угроз на основе анализа возможностей и намерений противника.		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Сбор, обработка и агрегация данных об угрозах и потенциальных противниках 2. Анализ возможностей и намерений противника, разработка оценок угроз 3. Формирование предупреждений, рекомендаций и отчетности по противодействию угрозам	
	Дополнительные трудовые функции:		
		Умения: 1. Настраивать правила корреляции в SIEM для выявления цепочек подготовки атак 2. Анализировать телеметрию EDR/XDR на предмет аномального поведения	

Трудовая функция 1: Сбор, обработка и агрегация данных об угрозах и потенциальных противниках	Навык 1: Мониторинг и выявление признаков подготовки и реализации целевых атак	3. Выявлять признаки разведки, создания инструмента атаки и первоначального доступа 4. Отслеживать изменения в инфраструктуре противника (С2, домены, IP) 5. Формировать и актуализировать списки Знания: 1. Моделей фреймворков кибербезопасности 2. Типовых TTPs АРТ-групп и киберпреступных сообществ 3. Методов активного и пассивного сканирования инфраструктуры 4. Признаков эксплуатации уязвимостей нулевого дня 5. Основ поведенческого анализа и UEBA
	Возможность признания навыка:	Требуется
	Навык 2: Сбор и первичная обработка индикаторов компрометации и данных об угрозах	Умения: 1. Формировать запросы к открытым, коммерческим и закрытым источникам угроз 2. Осуществлять парсинг и нормализацию индикаторов компрометации 3. Проводить первичную верификацию и оценку достоверности получаемых данных 4. Классифицировать источники по уровню доверия и актуальности 5. Автоматизировать сбор данных с использованием API и скриптовых средств Знания: 1. Основных платформ и видов threat intelligence (MISP, OTX, STIX/TAXII, VirusTotal и др.) 2. Форматов представления индикаторов (STIX 2.x, OpenIOC, YARA, Sigma) 3. Классификации источников threat intelligence (OSINT, HUMINT, коммерческие, закрытые) 4. Принципов оценки достоверности данных 5. Нормативных документов по категориям актуальных угроз
	Возможность признания навыка:	Требуется
	Навык 1: Проведение многоаспектного анализа	Умения: 1. Строить профили угроз 2. Оценивать технические и ресурсные возможности противника 3. Определять вероятные цели и приоритеты атакующего субъекта 4. Проводить сравнительный анализ TTPs разных группировок 5. Формировать гипотезы о следующих шагах противника Знания:

Трудовая функция 2: Анализ возможностей и намерений противника, разработка оценок угроз	возможностей и мотивации субъекта угроз	1. Классификации субъектов угроз (государственные, киберпреступные, хактивисты, инсайдеры) 2. Методик оценки возможностей нарушителя (ISO 27005) 3. Моделей зрелости киберугроз (CMMI-подобные для АРТ) 4. Факторов мотивации и экономических моделей киберпреступности 5. Методов сценарного прогнозирования развития угроз
	Возможность признания навыка:	Не требуется
	Навык 2: Разработка и актуализация оценок угроз	Умения: 1. Определять актуальность угроз для конкретной организации / отрасли 2. Рассчитывать вероятность и возможные последствия реализации угрозы 3. Формировать матрицы угроз и уязвимостей (threat × vulnerability) 4. Подготавливать обоснованные выводы о приоритетности угроз 5. Готовить материалы для обновления модели угроз Знания: 1. Методик оценки угроз 2. Подходов к качественной и количественной оценке рисков 3. Шкал вероятности и ущерба, используемых в мире 4. Требований к моделям угроз для ГИС, КВОИКИ 5. Нормативных требований к актуализации оценок угроз
	Возможность признания навыка:	Не требуется
	Навык 1: Подготовка и распространение предупреждений (advisory / warning)	Умения: 1. Составлять структурированные предупреждения (формат TLP, Traffic Light Protocol) 2. Определять уровень критичности и срочности оповещения 3. Адаптировать содержание под разные целевые аудитории 4. Обеспечивать конфиденциальность распространения информации 5. Отслеживать обратную связь и эффективность предупреждений Знания: 1. Системы цветовой маркировки TLP (WHITE / GREEN / AMBER / RED) 2. Требований к оформлению и распространению предупреждений

Трудовая функция 3: Формирование предупреждений, рекомендаций и отчетности по противодействию угрозам		3. Правил работы с ограниченной информацией в сфере КБ 4. Каналов и форматов оповещения (email, мессенджеры, порталы) 5. Метрик эффективности коммуникаций по КБ
	Возможность признания навыка:	Не требуется
	Навык 2: Разработка и обоснование рекомендаций по противодействию угрозам	Умения: 1. Формировать приоритизированный перечень мер противодействия 2. Оценивать применимость и стоимость предлагаемых мер 3. Подготавливать дорожную карту реализации рекомендаций 4. Обосновывать рекомендации нормативными требованиями и лучшими практиками 5. Участвовать в согласовании мер с владельцами процессов Знания: 1. Иерархии мер защиты (технические, организационные, правовые) 2. Лучших практик противодействия (CIS Controls, NIST CSF) 3. Принципов defense-in-depth и zero trust 4. Методов оценки эффективности мер защиты 5. Требований регуляторов к мерам компенсации выявленных угроз
	Возможность признания навыка:	Не требуется
Требования к личным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Дисциплинированность Аналитическое мышление Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27005 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление рисками информационной безопасности (Risk management) ISO/IEC 27035 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление инцидентами информационной безопасности (Information security incident management) ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Анализ требований безопасности (Common Criteria) Национальные стандарты РК: СТ РК ISO/IEC 27005-2013 ("Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность,	

	кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
26. Карточка профессии "Специалист по сетевым операциям":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-031		
Наименование профессии :	Специалист по сетевым операциям		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) ИТ-образования		
Другие возможные наименования профессии :			
Основная цель деятельности:	Управляет и защищает сетевую инфраструктуру, включая маршрутизаторы, коммутаторы и межсетевые экраны, обеспечивая надежную и безопасную работу сети		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Мониторинг и эксплуатация сетевой инфраструктуры 2. Обеспечение безопасности сетевой инфраструктуры 3. Устранение неисправностей и оптимизация сети	
	Дополнительные трудовые функции:	1. Оценка рисков и обеспечение соответствия нормативным требованиям в ИТ-архитектуре	
		Умения: 1. Конфигурировать маршрутизаторы и коммутаторы	

Трудовая функция 1: Мониторинг и эксплуатация сетевой инфраструктуры	Навык 1: Эксплуатация сетевого оборудования	2. Управлять виртуальными локальными сетями и механизмами коммутации 3. Обновлять встроенное программное обеспечение и применять исправления безопасности 4. Выполнять резервное копирование и восстановление конфигураций
		Знания: 1. Командных интерфейсов сетевого оборудования ведущих производителей 2. Эталонной модели OSI и модели TCP/IP 3. Протоколов динамической маршрутизации 4. Протоколов и механизмов коммутации и агрегации каналов
	Возможность признания навыка:	Не требуется
	Навык 2: Мониторинг состояния сети	Умения: 1. Настраивать и эксплуатировать системы сетевого мониторинга 2. Анализировать показатели производительности сети (пропускная способность, задержки, потери пакетов) 3. Выявлять аномалии сетевого трафика в режиме реального времени 4. Настраивать оповещения и уведомления о нарушениях в работе сети
		Знания: 1. Протоколов сетевого мониторинга и телеметрии 2. Платформ и инструментов мониторинга сетевой инфраструктуры 3. Ключевых показателей производительности сети 4. Принципов проактивного мониторинга и раннего обнаружения инцидентов
	Возможность признания навыка:	Не требуется
	Навык 1: Защита от сетевых угроз	Умения: 1. Выявлять и противодействовать атакам отказа в обслуживании 2. Реализовывать сегментацию и микросегментацию сети 3. Анализировать журналы событий безопасности 4. Настраивать разграничение доступа на основе ролей пользователей
		Знания: 1. Основных типов сетевых атак и методов их реализации 2. Международных и отраслевых стандартов кибербезопасности 3. Нормативных требований РК в области КБ 4. Инструментов анализа сетевого трафика и расследования инцидентов

Трудовая функция 2: Обеспечение безопасности сетевой инфраструктуры	Возможность признания навыка:	Не требуется
	Навык 2: Настройка средств сетевой защиты	Умения: 1. Конфигурировать межсетевые экраны нового поколения 2. Разрабатывать и применять правила фильтрации сетевого трафика и трансляции адресов 3. Внедрять защищенные виртуальные частные сети 4. Настраивать системы обнаружения и предотвращения вторжений Знания: 1. Принципов работы межсетевых экранов с отслеживанием состояний соединений 2. Архитектуры и функциональности NGFW 3. Криптографических протоколов защиты сетевых соединений 4. Подходов Zero Trust и контролируемого сетевого доступа
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Устранение неисправностей и оптимизация сети	Навык 1: Диагностика и восстановление работоспособности сети	Умения: 1. Проводить диагностику связности и маршрутизации 2. Анализировать сетевые пакеты для выявления причин сбоев 3. Восстанавливать работоспособность сети при отказах 4. Взаимодействовать с поставщиками оборудования при эскалации инцидентов Знания: 1. Инструментов сетевой диагностики 2. Методологий поиска и устранения неисправностей 3. Принципов высокой доступности и резервирования 4. Уровней сервиса и приоритизации инцидентов
	Возможность признания навыка:	Не требуется
	Навык 2:	Умения: 1. Проводить аудит сети и планирование емкости 2. Настраивать механизмы приоритизации трафика 3. Оптимизировать маршрутизацию и балансировку нагрузки 4. Проводить нагрузочное и стресс-тестирование сети Знания: 1. Технологий обеспечения качества обслуживания 2. Протоколов резервирования и балансировки

	Оптимизация производительности сети	3. Методов управления пропускной способностью 4. Инструментов нагрузочного тестирования сетей
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Оценка рисков и обеспечение соответствия нормативным требованиям в ИТ-архитектуре	Навык 1: Анализ рисков КБ	Умения: 1. Моделировать угрозы и нарушителей 2. Проводить качественную и количественную оценку рисков 3. Приоритизировать риски для архитектурных решений 4. Разрабатывать компенсирующие меры контроля
		Знания: 1. Методологии управления рисками 2. НПА РК в области защиты информации 3. Международных стандартов
	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27033 — Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность (Network security) ISO/IEC 27031 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по готовности к непрерывности деятельности (Continuity readiness) ISO/IEC 27001 / ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности и средства управления информационной безопасностью Национальные стандарты РК: СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
27. Карточка профессии "Планировщик киберопераций":		
Код группы:	2524-0	

Код наименования занятия:	2524-0-032		
Наименование профессии:	Планировщик киберопераций		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности и кибер-разведки при наличии базового (высшего) образования в области кибербезопасности		
Другие возможные наименования профессии:			
Основная цель деятельности:	Разрабатывает и координирует планы киберопераций, гарантируя соответствие ресурсов и стратегии		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Планирование киберопераций на стратегическом и оперативном уровне 2. Разработка и сравнение вариантов действий (COA) 3. Разработка планов и распорядительных документов киберопераций 4. Координация и контроль проведения киберопераций	
	Дополнительные трудовые функции:	1. Оценка эффективности проведенной кибероперации	
	Навык 1:	Умения: 1. Формулировать цели и желаемые эффекты кибероперации 2. Разрабатывать замысел кибероперации с учетом политических и правовых ограничений 3. Согласовывать замысел с вышестоящим руководством и смежными видами сил 4. Оформлять замысел в виде приказа на проведение кибероперации	
		Знания:	

Трудовая функция 1: Планирование киберопераций на стратегическом и оперативном уровне	Разработка замысла и концепции кибероперации	1. Доктрины применения сил и средств в киберпространстве РК и противника 2. Методик подхода, ориентированного на эффект (ЕВА) 3. Правовых основ международного права в киберпространстве 4. Структуры и порядка разработки оперативных планов
	Возможность признания навыка:	Не требуется
	Навык 2: Приоритизация и распределение ресурсов киберопераций	Умения: 1. Проводить приоритизацию целей с использованием матрицы CARVER или аналогичной 2. Распределять ограниченные ресурсы между операциями 3. Рассчитывать требуемое количество сил и средств для достижения эффекта 4. Формировать заявки на дополнительные технические средства и персонал Знания: 1. Методики CARVER или еЎ аналогов 2. Принципов управления ограниченными ресурсами в киберпространстве 3. Структуры и возможностей национального арсенала киберсредств 4. Основ теории принятия решений в условиях неопределѐнности
	Возможность признания навыка:	Не требуется
Трудовая функция 2:	Навык 1: Разработка вариантов действий (COA)	Умения: 1. Разрабатывать не менее трѐх технически реализуемых вариантов действий (COA) на одну цель/группу целей 2. Моделировать этапы проведения каждого варианта в рамках киберцепочки поражения 3. Учитывать временные окна, риски обнаружения и сопутствующий ущерб 4. Оформлять варианты действий (COA) в виде схем и матриц Знания: 1. Процесса планирования, адаптированного под кибероперации 2. Методик разработки и сравнения вариантов действий (COA) 3. Принципов построения матрицы синхронизации действий 4. Инструментов моделирования киберопераций
	Возможность признания навыка:	Не требуется

Разработка и сравнение вариантов действий (COA)	Навык 2: Анализ и сравнение вариантов действий (COA)	Умения: 1. Проводить сравнительный анализ вариантов действий (COA) по критериям эффективность/риски/ресурсы/время 2. Рассчитывать вероятность успеха и риски каждого варианта действий 3. Презентовать результаты анализа руководству для принятия решения 4. Корректировать выбранный вариант действия (COA) Знания: 1. Методик многокритериального анализа и сравнения вариантов действий (COA) 2. Основ теории игр и моделирования конфликтов в киберпространстве 3. Критериев оценки рисков в кибероперациях 4. Порядка утверждения выбранного варианта действий (COA)
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Разработка планов и распорядительных документов киберопераций	Навык 1: Составление плана кибероперации и матрицы синхронизации	Умения: 1. Разрабатывать детальный план кибероперации с разбивкой по фазам 2. Составлять матрицу синхронизации действий всех задействованных сил и средств 3. Разрабатывать резервные и экстренные варианты действий 4. Оформлять приложения к плану (схемы управления, правила применения сил и др.) Знания: 1. Структуры и требований к плану кибероперации 2. Принципов построения матрицы синхронизации в киберпространстве 3. Цикла проведения операций в киберпространстве 4. Требований к оформлению распорядительных документов
	Возможность признания навыка:	Не требуется
	Навык 2:	Умения: 1. Проектировать устойчивую инфраструктуру командования и управления для операции 2. Определять основные и резервные каналы командования и управления 3. Разрабатывать правила перехода на резервные схемы командования и управления 4. Проводить тестирование системы командования и управления перед началом операции Знания:

	Разработка командования и управления в кибероперациях	1. Принципов построения отказоустойчивых систем командования и управления в условиях активного противодействия 2. Современных протоколов и инструментов управления эксплойтами и закладными устройствами 3. Методик противодействия нарушению командования и управления противником 4. Требований к защите каналов командования и управления
	Возможность признания навыка:	Не требуется
Трудовая функция 4: Координация и контроль проведения киберопераций	Навык 1: Координация взаимодействия участников операции	Умения: 1. Координировать действия групп разработки целей , доступа, эксплуатации и поддержки 2. Обеспечивать своевременную передачу целеуказания и разведданных 3. Организовывать совместную работу в единой кибероперативной обстановке 4. Разрешать конфликтные ситуации по приоритетам и ресурсам между группами Знания: 1. Принципов межведомственного взаимодействия в киберпространстве 2. Структуры единой кибероперативной обстановки и инструментов еѸ ведения 3. Порядка согласования действий с другими структурами 4. Методики управления конфликтами интересов при распределении ресурсов
	Возможность признания навыка:	Не требуется
	Навык 2: Контроль хода операции и корректировка плана	Умения: 1. Вести непрерывное отслеживание хода операции в реальном времени 2. Проводить оперативную оценку нанесѸнного ущерба (BDA) 3. Принимать решения о корректировке или прекращении операции 4. Готовить промежуточные и итоговые доклады руководству Знания: 1. Методик оперативного контроля и управления кибероперациями 2. Порядка проведения оценки нанесѸнного ущерба в киберпространстве 3. Критериев успеха/неудачи кибероперации 4. Порядка подготовки выводов по кибероперации
	Возможность признания навыка:	Не требуется

Дополнительная трудовая функция 1: Оценка эффективности проведенной кибероперации	Навык 1: Сбор и анализ данных о достигнутых результатах операции	Умения: 1. Собирать телеметрию и логи с закладных устройств эксплойтов 2. Оценивать степень достижения желаемых результатов 3. Выявлять причины недостижения результатов 4. Готовить отчеты об оценке нанесенного ущерба (BDA) в киберпространстве
	Возможность признания навыка:	Знания: 1. Методик оценки нанесенного ущерба (BDA) и рекомендаций для повторной атаки 2. Индикаторов достижения результатов атаки в киберпространстве 3. Инструментов анализа трафика и логов 4. Принципов полученного опыта в кибероперациях
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение быстро принимать решения Умение работать в команде Целеустремленность Дисциплинированность Аналитическое мышление Концентрация и управление вниманием Инициативность	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 15408 (Common Criteria) — критерии оценки ИТ-безопасности ISO/IEC 27031:2011 — Guidelines for ICT readiness for business continuity ISO/IEC 27033 (серия) — Network security Национальные стандарты РК: СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла") СТ РК 4009-2025 ("Информационные технологии. Криптографическая защита информации. Алгоритм блочного симметричного шифрования")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
28. Карточка профессии "Архитектор корпоративной инфраструктуры":		
Код группы:	2524-0	
Код наименования занятия:	2524-0-028	
Наименование профессии:	Архитектор корпоративной инфраструктуры	

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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) ИТ-образования		
Другие возможные наименования профессии :	2521-2-001 - Архитектор ИТ-инфраструктуры		
Основная цель деятельности:	Обеспечивает интеграцию требований безопасности в ИТ, архитектуру организации, согласовывая бизнес-цели с безопасными технологическими решениями		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Анализ требований и разработка целевой архитектуры с учетом КБ 2. Проектирование и интеграция решений кибербезопасности в корпоративную инфраструктуру 3. Оценка рисков и обеспечение соответствия нормативным требованиям в ИТ-архитектуре	
	Дополнительные трудовые функции:	1. Мониторинг эффективности архитектуры КБ	
	Навык 1: Анализ целей и требований к корпоративной инфраструктуре	Умения: 1. Проводить интервью для выявления бизнес-потребностей 2. Моделировать бизнес-процессы с учетом рисков безопасности 3. Определять ключевые требования к ИТ-инфраструктуре 4. Согласовывать бизнес-цели с возможностями технологий	
		Знания: 1. Методологии построения корпоративной архитектуры 2. Бизнес-анализа и моделирования процессов 3. Основ управления рисками 4. Принципов интеграции ИТ и бизнеса	

Трудовая функция 1: Анализ требований и разработка целевой архитектуры с учетом	Возможность признания навыка:	Не требуется
	Навык 2: Разработка целевой архитектуры	Умения: 1. Разрабатывать модели корпоративной архитектуры 2. Интегрировать требования безопасности на этапе проектирования 3. Создавать дорожную карту перехода от текущей к целевой архитектуре 4. Визуализировать полученные данные Знания: 1. Фреймворков корпоративной инфраструктуры 2. Стандартов моделирования IT-решений 3. Принципов внедрения систем КБ в инфраструктуру 4. Технологий корпоративной инфраструктуры
	Возможность признания навыка:	Не требуется
Трудовая функция 2: Проектирование и интеграция решений кибербезопасности в корпоративную инфраструктуру	Навык 1: Проектирование защищенной IT-инфраструктуры	Умения: 1. Разрабатывать архитектуру с интегрированной системой КБ 2. Интегрировать средства защиты 3. Проектировать безопасные облачные и гибридные инфраструктуры 4. Моделировать потоки данных с учетом контроля доступа Знания: 1. Моделей угроз 2. Стандартов КБ 3. Технологий безопасности 4. Принципов безопасной разработки
	Возможность признания навыка:	Не требуется
	Навык 2: Выбор и обоснование технологических решений	Умения: 1. Сравнивать поставщиков и решения по критериям безопасности 2. Обосновывать стоимость и рентабельность безопасных решений 3. Разрабатывать технические спецификации Знания: 1. Рынка средств КБ (продуктов и ведущих производителей) 2. Методов оценки эффективности защитных мер 3. Принципов разработки технической спецификации
	Возможность признания навыка:	Не требуется
		Умения:

	Навык 3: Интеграция КБ в существующие системы	1. Оценивать текущую инфраструктуру на уязвимости 2. Планировать миграцию с сохранением уровня безопасности 3. Координировать внедрение защитных мер в проекты 4. Тестировать интеграцию на соответствие требованиям Знания: 1. Методов оценки систем КБ 2. Инструментов интеграции 3. Нормативных требований к системам КБ 4. Фреймворков облачной безопасности
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Оценка рисков и обеспечение соответствия нормативным требованиям в ИТ-архитектуре	Навык 1: Обеспечение регуляторного и нормативного соответствия ИТ-архитектуры	Умения: 1. Проводить анализ на соответствие нормативным требованиям 2. Разрабатывать политики и процедуры кибербезопасности 3. Подготавливать документацию для проведения аудитов 4. Координировать процессы сертификации информационных систем Знания: 1. НПА РК в области кибербезопасности 2. Стандартов аудита КБ 3. Процессов подготовки документов для аудита 4. Требований к КВОИКИ
	Возможность признания навыка:	Не требуется
	Навык 2: Анализ рисков КБ	Умения: 1. Моделировать угрозы и нарушителей 2. Проводить качественную и количественную оценку рисков 3. Приоритизировать риски для архитектурных решений 4. Разрабатывать компенсирующие меры контроля Знания: 1. Методологии управления рисками 2. НПА РК в области защиты информации 3. Международных стандартов
	Возможность признания навыка:	Не требуется
		Умения: 1. Настраивать метрики и показатели эффективности (KPI) в области безопасности 2. Анализировать инциденты безопасности и их влияние на архитектуру

Дополнительная трудовая функция 1: Мониторинг эффективности архитектуры КБ	Навык 1: Мониторинг эффективности архитектуры КБ	3. Проводить периодические обзоры архитектуры 4. Формировать рекомендации по улучшению на основе результатов мониторинга
	Возможность признания навыка:	Знания: 1. Метрик кибербезопасности (CIS Controls) 2. Инструментов мониторинга (SIEM, сканеры уязвимостей) 3. Принципов непрерывного улучшения (PDCA) 4. Трендов угроз (CVE, аналитика угроз)
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27033 — Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры (кодекс практики) обеспечения информационной безопасности ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Вопросы оценки безопасности архитектурных компонентов (Common Criteria) Национальные стандарты РК: СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
29. 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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные курсы повышения квалификации в области кибербезопасности		
Другие возможные наименования профессии:			
Основная цель деятельности:	Планирование, контроль, мониторинг и обеспечение КБ		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Рассмотрение процессов управления КБ организации 2. Планирование процессов обеспечения КБ 3. Осуществление мероприятий по обеспечению КБ 4. Контроль процессов управления и обеспечения КБ	
	Дополнительные трудовые функции:		
	Навык 1: Разработка (актуализация) нормативно-технической	Умения: 1. Координировать аналитическую работу по КБ 2. Анализировать, выбирать методики и методы оценки и реализации процессов управления КБ охватывающие процессы управления рисками, активами, инцидентами, техническими уязвимостями, угрозами, техническим противодействиям угрозам, непрерывностью бизнеса 3. Согласовывать НТД процессов управления КБ 4. Координировать деятельность по разработке (актуализации) политики КБ, НТД процессов управления КБ и документов, регламентирующих процессы обеспечения КБ 5. Публиковать и доводить утвержденную (актуализированную) политику КБ организации до сведения сотрудников	
		Знания:	

Трудовая функция 1: Рассмотрение процессов управления КБ организации	документации, регламентирующей процессы управления КБ	1. Базовые принципы регламентации бизнес-процессов 2. Законодательство в сфере обеспечения кибербезопасности 3. Национальные стандарты в области КБ 4. Принципы и методологии проектирования и эксплуатации ИС 5. Принципы регламентации бизнес-процессов 6. Методы управления проектами 7. Методики оценки и управления рисками КБ 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) Н Т Д , регламентирующей процессы обеспечения КБ	Умения: 1. Оценивать текущий уровень НТД, регламентирующих процессы обеспечения КБ 2. Разрабатывать (актуализировать) ТД, регламентирующие процессы обеспечения КБ 3. Разрабатывать профили защиты и задания по безопасности для ЦС и компонентов информационно-коммуникационной инфраструктуры Знания: 1. Принципы защитных механизмов программных и аппаратных средств организации 2. Принципы построения системы управления КБ 3. Принципы и методология проектирования ИС
	Возможность признания навыка:	не требуется
	Навык 1: Планирование мероприятий по обеспечению кибербезопасности	Умения: 1. Проводить инвентаризацию, классификацию, маркировку активов, связанных с автоматизированной обработкой информации 2. Составлять отчетную документацию по результатам категоризации активов 3. Выявлять недостатки в активах обеспечения КБ Знания: 1. Законодательство в сфере обеспечения КБ 2. Национальные стандарты в сфере обеспечения КБ 3. Принципы, методы и средства обеспечения КБ при определении мероприятий по непрерывности бизнеса, регистрации и учету событий КБ, резервному копированию, антивирусной защите, контролю доступа, работе со съемными носителями, мобильными устройствами, удаленного доступа, использованием криптографии и их носителей, лицензиях и версиях ПО

Трудовая функция 2: Планирование процессов обеспечения КБ	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 КБ 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:	Навык 1: Реализация плана мероприятий по обеспечению КБ	Умения: 1. Анализ защищенности бизнес-процессов и активов, связанных с автоматизированной обработкой информации 2. Выбор инструментария и методов обеспечения КБ 3. Разработка мероприятий, направленных на реализацию политики КБ организации 4. Составление плана по обеспечению непрерывности бизнеса и восстановления после инцидентов КБ и форс-мажорных ситуаций 5. Разработка технических спецификаций, тендерной документации на закупаемые средства обеспечения КБ 6. Разработка требований, технических заданий на подсистемы КБ ИС 7. Организация и координация работ по разработке профилей защиты и задания по безопасности для ЦС 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 КБ 4. Средства обеспечения КБ, систем мониторинга уязвимостей, систем мониторинга КБ и систем

Осуществление мероприятий по обеспечению КБ		предотвращения утечек информации, защитных механизмов систем 5. Национальные стандарты в сфере обеспечения КБ 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 ЦС и ЦИ 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 ЦС и компонентов информационно-коммуникационной инфраструктуры Знания: 1. Базовые принципы и способы выполнения работ по разработке, тестированию и апробации средств и методов КБ 2. Правила эксплуатации программных средств, защитных механизмов, компонентов ЦС и ЦИ 3. Методы выявления нарушений в настройках
	Возможность признания навыка:	Не требуется
Трудовая функция 4:	Навык 1: Оценка соответствия процессов кибербезопасности	Умения: 1. Осуществление контроля реализации плана мероприятий по обеспечению КБ 2. Анализ результатов проверок исполнения требований документов, регламентирующих процессы обеспечения КБ и НТД процессов управления КБ 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 КБ 3. Принципы построения и применения, систем мониторинга уязвимостей, систем мониторинга КБ 4. Системы предотвращения утечек информации 5. Методы определения, предотвращения и устранения последствий инцидентов КБ, критических (аварийных) ситуаций

Контроль процессов управления и обеспечения КБ	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 КБ 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 безопасности. 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
30. Карточка профессии "Кибер-юридический консультант":		
Код группы:	2524-0	
Код наименования занятия:	2524-0-019	
Наименование профессии:	Кибер-юридический консультант	
Уровень квалификации по ОРК:	6	

подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др т и п о в ы х квалификационных характеристик:			
У р о в е н ь профессионального образования:	Уровень образования: высшее образование (бакалавриат, специалитет, ординатура)	Специальность: Информационная безопасность	Квалификация: -
Требования к опыту работы:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) юридического образования		
Другие возможные наименования профессии :	2611 - Юристы		
Основная цель деятельности:	Обеспечение экспертизы в правовых и нормативных аспектах кибербезопасности, соблюдение законов, политических и этических норм		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Разработка и правовая экспертиза документов в области КБ 2. Представительство интересов организаций и физических лиц по вопросам КБ 3. Работа с данными в области КБ	
	Дополнительные трудовые функции:	1. Обучение сотрудников правовой грамотности в вопросах кибербезопасности	
	Навык 1: Использование современных электронных ресурсов	Умения: 1. Использовать современные технологии и открытые ресурсы для проверки действительности документов 2. Использовать современные технологии и открытые ресурсы для формирования документов и запросов 3. Применять аналитические системы проверки контрагентов	
		Знания: 1. Правил пользования электронными площадками, а также ограничений на получаемые данные 2. Необходимых данных для эффективного использования электронных ресурсов 3. Требования законодательства к содержанию различных типов документов	
	Возможность признания навыка:	Не требуется	
		Умения:	

Трудовая функция 1: Разработка и правовая экспертиза документов в области КБ	Навык 2: Подготовка юридических заключений и правовых рекомендаций	1. Выявлять в документах положения, противоречащие законодательству, в т.ч. в области КБ 2. Выявлять в документах положения, нарушающие баланс интересов сторон 3. Оценивать текст юридических документов, касающихся КБ, на предмет соответствия фактическому результату 4. Составлять протоколы разногласий в ходе переговоров о заключении сделок
	Возможность признания навыка:	Знания: 1. Гражданское законодательство и практика его применения в части положений о лицах, сделках, вещных правах, а также общих положений об обязательствах 2. Гражданское законодательство и практика его применения в части положений о заключении, исполнении, расторжении, а также о последствиях нарушения договоров 3. Гражданское законодательство и практика его применения в части положений об отдельных видах обязательств
	Навык 3: Разработки документов в области кибербезопасности	Умения: 1. Разрабатывать и проверять договоры, оформляющие отношения в сфере кибербезопасности 2. Разрабатывать локальные акты, относящиеся к сфере кибербезопасности, законодательства о защите персональных данных 3. Вести деловую переписку
	Возможность признания навыка:	Знания: 1. Административного законодательства и практики его применения в части регулирования сферы кибербезопасности 2. Требований к составлению правовых документов; перечень необходимых реквизитов 3. Требования законодательства к содержанию различных типов документов 4. Правила документооборота
	Навык 1: Осуществление переговорных функций	Умения: 1. Выявлять юридические и технические риски в ходе переговоров 2. Применять переговорные техники для отстаивания своей позиции 3. Протоколировать ход переговоров
		Знания:

Трудовая функция 2: Представительство интересов организаций и физических лиц по вопросам КБ		1. Процессуальное законодательство и практика его применения 2. Правила расчета сроков исковой давности 3. Правила направления претензий и ответов на претензии
	Возможность признания навыка:	Не требуется
	Навык 2: Работа с исковыми документами в области кибербезопасности	Умения: 1. Составлять претензии, заявления, отзывы, жалобы, иные процессуальные документы 2. Рассчитывать суммы неустоек, возмещения убытков 3. Собирать документы, подтверждающие основания и размер заявленных требований 4. Подготавливать устное выступление для усиления позиции Знания: 1. Правил искового, производства 2. Правил производства по пересмотру судебных актов 3. Законодательства об исполнительном производстве и практике его применения 4. Техники переговоров и устных выступлений
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Работа с данными в области КБ	Навык 1: Обеспечение безопасности персональных и конфиденциальных данных	Умения: 1. Идентифицировать персональные и конфиденциальные данные в цифровых системах 2. Применять меры защиты в соответствии с законодательством и внутренними политиками 3. Оценивать риски нарушения конфиденциальности и предлагать способы их минимизации 4. Участвовать в разработке и сопровождении внутренних регламентов и политик по защите данных Знания: 1. Законодательство о защите персональных данных 2. Методы и средства защиты информации 3. Классификация и категорирование информации 4. Угрозы безопасности персональных и конфиденциальных данных
	Возможность признания навыка:	Требуется
		Умения: 1. Выявлять и классифицировать инциденты кибербезопасности 2. Анализировать журналы событий, сетевой трафик и другие источники данных

	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства)
	Возможность признания навыка:	Знания: 1. Основы классификации инцидентов кибербезопасности и их особенностей. 2. Методы сбора и корреляции данных об инцидентах 3. Основы расследований инцидентов и цифровой криминалистики 4. Нормативные требования к фиксации и обработке инцидентов
Дополнительная трудовая функция 1: Обучение сотрудников правовой грамотности в вопросах кибербезопасности	Навык 1: Обучение сотрудников правовой грамотности в вопросах кибербезопасности	Умения: 1. Разрабатывать программы обучения по кибербезопасности для сотрудников на темы управления паролями, безопасности электронной почты, фишинговых атак, социальной инженерии, защиты от вредоносных программ и защиты данных 2. Проводить тренинги для сотрудников, используя различные методы как презентации, обучающие программы и практические занятия 3. Контролировать и оценивать эффективность программ обучения
	Возможность признания навыка:	Знания: 1. Способы и принципы проведения презентаций 2. Различные техники обучения 3. Методов оценки профессионального уровня и аттестации специалистов Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и	Международные стандарты: ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры (кодекс практики) обеспечения информационной безопасности ISO/IEC 27005 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования к управлению рисками информационной безопасности ISO/IEC 29100 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Privacy framework. Конфиденциальность и защита персональных данных Национальные стандарты РК: СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы	

национальных стандартов:	менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
31. Карточка профессии "Уполномоченный представитель/ответственный за авторизацию":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-027		
Наименование профессии:	Уполномоченный представитель/ответственный за авторизацию		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) управленческого образования		
Другие возможные наименования профессии:			
Основная цель деятельности:	Оценивает и утверждает ИТ-системы для эксплуатации на приемлемом уровне риска, обеспечивая соответствие стандартам безопасности перед развертыванием		
Описание трудовых функций			
	Обязательные трудовые функции:	1. Обеспечение КБ и работа с данными 2. Оценка механизмов авторизации в ИТ-системах для обеспечения приемлемого уровня риска	

Перечень трудовых функций:		3. Утверждение ИТ-систем на основе оценки авторизации и соответствия стандартам безопасности
	Дополнительные трудовые функции:	1. Минимизация рисков в области кибербезопасности
Трудовая функция 1: Обеспечение КБ и работа с данными	Навык 1: Комплексное обеспечение кибербезопасности и администрирование защищенных систем	Умения: 1. Собирать и анализировать артефакты, логи, дампы памяти, системные следы 2. Управлять политикой паролей, групп безопасности, многофакторной аутентификацией 3. Применять групповые политики, права пользователей, правила межсетевых экранов 4. Проводить аудит и тестирование систем КБ Знания: 1. Основ администрирования и защиты информационных систем 2. Методов и средств обеспечения безопасности 3. Принципов анализа, аудита и тестирования систем безопасности 4. Языков программирования
	Возможность признания навыка:	Требуется
	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	Умения: 1. Выявлять и классифицировать инциденты кибербезопасности 2. Анализировать журналы событий, сетевой трафик и другие источники данных 3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства) Знания: 1. Основ классификации инцидентов кибербезопасности и их особенностей 2. Методов сбора и корреляции данных об инцидентах КБ 3. Основ расследования инцидентов и цифровой криминалистики 4. Нормативных требований к фиксации и обработке инцидентов КБ
	Возможность признания навыка:	Требуется
	Навык 1:	Умения: 1. Определять распространенные ошибки при реализации авторизации 2. Оценивать влияние вариативности требований на риски несанкционированного доступа 3. Проверять наличие механизмов аудита доступа в системах с динамической авторизацией

Трудовая функция 2: Оценка механизмов авторизации в ИТ-системах для обеспечения приемлемого уровня риска	Выявление рисков, связанных с реализацией авторизации	4. Анализировать потенциальные уязвимости, возникающие при наличии избыточных прав Знания: 1. Ошибок, возникающих при проектировании и реализации авторизации 2. Принципов обеспечения аудируемости 3. Рисков, связанных с производительностью и масштабируемостью моделей авторизации 4. Требований к минимальным правам и учУту для минимизации рисков
	Возможность признания навыка:	Не требуется
	Навык 2: Анализ моделей управления доступом	Умения: 1. Определять различия между моделями авторизации (RBAC, ABAC, PBAC, MAC, DAC) 2. Оценивать пригодность выбранной модели авторизации для конкретных бизнес-требований ИТ-системы 3. Выявлять комбинации моделей авторизации для сложных систем 4. Проверять разделение авторизации и бизнес-логики при проектировании системы Знания: 1. Основных моделей авторизации и их принципов (RBAC, ABAC/PBAC, MAC, DAC) 2. Преимуществ и недостатков динамических моделей 3. Требований к минимальной достаточности прав и отзыву доступа 4. Влияния моделей авторизации на производительность системы
	Возможность признания навыка:	Не требуется
	Навык 1: Проверка соответствия авторизации требованиям безопасности	Умения: 1. Оценивать интеграцию авторизации с требованиями бизнеса и кибербезопасности 2. Проверять наличие аудита и мониторинга доступа перед утверждением системы 3. Определять баланс между гибкостью (PBAC) и производительностью (ACL) в предлагаемых решениях 4. Выявлять необходимость дополнительных журналов для динамических моделей авторизации Знания: 1. Практик выбора и комбинации моделей авторизации 2. Требований к аудиту и мониторингу в системах авторизации 3. Влияния авторизации на общую безопасность ИТ-системы

Трудовая функция 3: Утверждение ИТ-систем на основе оценки авторизации и соответствия стандартам безопасности		4. Стандартов оценки готовности системы к эксплуатации
	Возможность признания навыка:	Не требуется
	Навык 2: Принятие решения об утверждении эксплуатации ИТ-системы с учетом рисков авторизации	Умения: 1. Оценивать приемлемость остаточных рисков, связанных с механизмами авторизации 2. Формулировать условия утверждения эксплуатации 3. Координировать корректировки в механизмах авторизации для снижения рисков 4. Документировать обоснование принятия риска на основе анализа авторизации Знания: 1. Принципов оценки приемлемого уровня риска в контексте управления доступом 2. Роли авторизации в процессе утверждения ИТ-системы 3. Методов минимизации рисков авторизации 4. Требований к документации и мониторингу ИТ-системы после утверждения
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Минимизация рисков в области кибербезопасности	Навык 1: Разработка мер по снижению рисков	Умения: 1. Проектировать стратегии минимизации рисков 2. Внедрять технические меры минимизации рисков в области КБ 3. Обучать персонал по вопросам кибербезопасности 4. Оценивать эффективность внедренных мер Знания: 1. Стратегий минимизации рисков КБ 2. Технических контрмер 3. Программ повышения осведомленности 4. Метрик эффективности
	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
	Международные стандарты: ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Контроль доступа и идентификация (кодекс практики по	

Список технических регламентов и национальных стандартов:	мерам обеспечения информационной безопасности) ISO/IEC 24760 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление идентификацией и доступом Национальные стандарты РК: СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
32. Карточка профессии "Специалист по информационной безопасности транспортной инфраструктуры":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-016		
Наименование профессии :	Специалист по информационной безопасности транспортной инфраструктуры		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) ИТ-образования		
Другие возможные наименования профессии :	2524-0-007 - Специалист по информационной безопасности		
Основная цель деятельности:	Обеспечение защиты объектов транспортного комплекса с целью исключения несанкционированного воздействия. Команд и нарушений в области воздушного, наземного и речного транспорта		
Описание трудовых функций			
		1. Тестирование систем безопасности, сетевых устройств при управлении и контроле над процессом осуществления перевозок	

Перечень трудовых функций:	Обязательные трудовые функции:	2. Разработка и внедрение стандартов кибербезопасности с учетом критических особенностей транспортной отрасли 3. Реагирование на инциденты кибербезопасности
	Дополнительные трудовые функции:	1. Обучение сотрудников политике и процедурам кибербезопасности
	Навык 1: Проверка программного обеспечения	Умения: 1. Планировать и выполнять регулярное сканирование (включая инструменты SIEM) уязвимостей, эксплойтов для выявления слабых мест в системе безопасности организации 2. Проводить пентест систем безопасности 3. Использовать результаты сканирования уязвимостей для оценки уровня рисков 4. Разрабатывать рекомендации по устранению уязвимостей или рисков Знания: 1. Основы проведения пентеста и языков программирования как Python, BASH, Java, Ruby и Perl 2. Текущая организационная политика и процедуры по реагированию на НД 3. Стандартные отраслевые средства обнаружения и предотвращения НД 4. Идентификационные характеристики аномальной активности 5. Установки и настройки NIDS, NIPS, HIDS и HIPS 6. Необходимая документация для составления отчетов об обнаружении НД 7. Управления информацией о новых уязвимостях для сохранения еѸ конфиденциальности до устранения известных уязвимостей 8. Правильное размещение датчиков при проектировании NIDS/NIPS продуктов в архитектурах и сетях предприятий 9. Обслуживание и настройка систем обнаружения НД 10. Выполнение сканирования уязвимостей с помощью инструментов SIEM 11. Обнаружение аномальной активности в сети или системе, используя защитный мониторинг 12. Программные инструменты и методы анализа защищенности систем и уязвимостей с учетом особенностей в транспортной отрасли 13. Понимание правовых, инженерно-технических, организационных вопросов функционирования объектов транспортного комплекса
	Возможность признания навыка:	Не требуется
		Умения:

Трудовая функция 1: Тестирование систем безопасности, сетевых устройств при управлении и контроле над процессом осуществления перевозок	Навык 2: Мониторинг сетей, раннее выявление угроз безопасности	1. Выполнять комплексное наблюдение и мониторинг для обнаружения угроз 2. Использовать результаты анализа данных об угрозах для поиска и обнаружения потенциальных нарушений 3. Осуществлять установку, эксплуатацию и обслуживание систем обнаружения и предотвращения НД включая круглосуточный защитный мониторинг 4. Анализировать и характеризовать данные сетевого трафика с целью выявления аномальной активности и потенциальных угроз для сетевых ресурсов
	Возможность признания навыка:	Знания: 1. Стандартные отраслевые средства обнаружения и предотвращения НД 2. Текущая организационная политика и процедуры по реагированию на НД 3. Идентификационные характеристики аномальной активности 4. Обнаружение аномальной активности в сети или системе, используя защитный мониторинг 5. Управление информацией о новых уязвимостях для сохранения еѸ конфиденциальности до устранения известных уязвимостей 6. Программные инструменты и методы анализа защищенности систем и уязвимостей с учетом особенностей в транспортной отрасли
	Навык 3:	Умения: 1. Настраивать и эксплуатировать межсетевые экраны и IDS/IPS для защиты транспортных сетей 2. Мониторить и анализировать сетевой трафик с использованием специализированных инструментов 3. Управлять системами контроля доступа и видеонаблюдения, адаптированными под транспортные объекты 4. Внедрять и сопровождать криптографическое оборудование и технологии шифрования 5. Конфигурировать и поддерживать сетевую сегментацию и VPN для безопасного обмена данными 6. Использовать SIEM-систем для анализа и реагирования на инциденты кибербезопасности 7. Проводить диагностику и тестирование безопасности специализированного оборудования 8. Обеспечивать резервирование и отказоустойчивость систем безопасности транспортной инфраструктуры 9. Документировать процедуры и результаты технического обслуживания оборудования

	Анализ и оценка уязвимостей, специфичных для транспортной инфраструктуры	Знания: 1. Принципы работы и архитектура межсетевых экранов (firewalls) промышленного уровня, адаптированных для транспортных систем 2. Особенности систем обнаружения и предотвращения вторжений (IDS/IPS) в транспортных сетях 3. Технологии контроля доступа и видеонаблюдения на транспортных объектах 4. Протоколы мониторинга сетевого трафика и анализа (NetFlow, SNMP, Wireshark) с учетом специфики транспортных коммуникаций 5. Принципы криптографической защиты и оборудования для шифрования данных в транспортной инфраструктуре 6. Работа с системами управления событиями безопасности (SIEM) и их интеграция в транспортные ИТ-системы 7. Методы сегментации и изоляции сетей (VLAN, VPN) в распределенных инфраструктурах 8. Технические решения для обеспечения отказоустойчивости и резервирования критичных компонентов 9. Стандарты и нормативы по КБ в транспортной сфере
	Возможность признания навыка:	Не требуется
	Навык 1: Удаленная установка и обновление системы сетевой безопасности, предназначенной для предотвращения НД	Умения: 1. Проводить регулярное обновление программного и аппаратного обеспечения систем 2. Осуществлять установку и обновление антивирусных программ 3. Осуществлять настройку межсетевого экрана промышленных узлов сети 4. Тестировать обновления на совместимость с промышленным ПО перед внедрением Знания: 1. Работы промышленных сетевых узлов предприятия 2. Шифрование и криптография 3. Политики, требования принципов установки и обновлений ПО 4. Функционирование, применение и конфигурации межсетевого экрана 5. Настройка критериев ACL для определения разрешенного трафика в межсетевом экран
	Возможность признания навыка:	Не требуется
		Умения:

Трудовая функция 2: Разработка и внедрение стандартов кибербезопасности с учетом критических особенностей транспортной отрасли	Навык 2: Разработка, внедрение и поддержка протоколов и процедур безопасности для снижения рисков	1. Определять текущие организационные процедуры кибербезопасности и требования, специфичные для транспортных объектов 2. Проводить анализ эффективности существующих киберопераций транспортной инфраструктуры в соответствии с внутренними и отраслевыми стандартами 3. Документировать результаты анализа с учетом требований и нормативов, действующих в транспортной сфере 4. Внедрять и сопровождать системы кибербезопасности, обеспечивающие защиту транспортных ИТ-средств и сетей 5. Выявлять и документировать необходимые обновления процедур безопасности, нарушения обслуживания и задачи для эффективного осуществления киберопераций в транспортной инфраструктуре 6. Внедрять операционные и аналитические процессы, а также процедуры отчетности по инцидентам с учетом особенностей транспортной отрасли Знания: 1. Подготовка и ведение технической, производственной и организационной документации, адаптированной под транспортные объекты и системы 2. Создание документации с детальным анализом, выводами и рекомендациями, оформленными согласно установленным стандартам транспортной отрасли 3. Глубокие отраслевые и технические знания в области транспортных систем с учетом их специфики и особенностей эксплуатации 4. Владение языками программирования (C, C++, PHP, Python, JavaScript) для разработки и поддержки транспортных ИТ-решений и систем безопасности
---	--	--

	Навык 3: Внедрение безопасности для систем IoT	6. Выполнять регулярное обслуживание процессов обнаружения проблем безопасности IoT 7. Проектировать и разрабатывать информационные панели мониторинга и отчетности по IoT 8. Сканировать критические уязвимости на всех уровнях IoT 9. Выполнять резервное копирование и шифрование устройств безопасности Знания: 1. Разработка информационной панели мониторинга 2. Языки программирования и визуализации данных (Python, R, SQL, NodeJS) 3. Основы шифрования и криптографии 4. Организационная политика, процедуры и руководства по поддержанию КБ 5. Процедуры обмена данными для документирования и внедрения процедур КБ 6. Спектр стандартных шаблонов и инструментов, доступных для мониторинга безопасности 7. Фундаментальные топологии сети, устройств, конфигурации и возможности подключения в системах IoT 8. Различные контексты безопасности IoT и уровни, охвата, включая устройства, облака, коммуникации, базы данных и приложения 9. Рутинные операционные процедуры реагирования на инциденты кибербезопасности IoT 10. Устранение уязвимостей и инцидентов кибербезопасности IoT 11. Внедрение повышения уровня кибербезопасности в системах IoT 12. Протоколы аудита систем, выявления и анализов аномалий в системах IoT
	Возможность признания навыка:	Не требуется
	Навык 1: Распознавание и реагирование на	Умения: 1. Установить и подтвердить возникновение и характер инцидента кибербезопасности 2. Определить законодательные требования, организационные политики, процедуры и планы реагирования на инциденты кибербезопасности 3. Проводить анализ и оценку источников, влияния и последствий инцидента 4. Активировать план реагирования на инцидент и подтвердить, что кибер-инцидент локализован 5. Проводить оценку ущерба критической системной инфраструктуры организации или утечки данных 6. Документировать инцидент кибербезопасности, предпринятые действия, решения и результаты Знания:

Трудовая функция 3:
Реагирование на
инциденты
кибербезопасности

инциденты в соответствии с организационными процедурами безопасности	1. Ключевые особенности планов реагирования на инциденты кибербезопасности, а также их источники и причины 2. Различные типы атак, включая отказ в обслуживании (DoS), инъекции SQL (SQLi), атаки межсайтового скриптинга (XSS), аппаратные атаки, атаки на WiFi 3. Методология обнаружения инцидентов кибербезопасности, предупредительные меры и методы смягчения последствий 4. Процессы документирования и анализа журнала событий КБ 5. Организационная политика и процедуры реагирования на инциденты кибербезопасности (определения характера и местонахождения инцидентов, их локализации, установка исправлений безопасности и отключение доступа к сети, уведомления и предоставления отчетов необходимому персоналу)
Возможность признания навыка:	Не требуется
Навык 2: Внедрение существующих стандартов кибербезопасности, политики и руководства для организации	Умения: 1. Внедрять политику и руководство по кибербезопасности, которые соответствуют миссии и целям организации 2. Применять существующие стандарты безопасности для защиты данных и систем организации от злоумышленников 3. Разрабатывать и поддерживать планы и процедуры реагирования на инциденты для эффективного управления инцидентами 4. Оценивать риски кибербезопасности организации и разрабатывать стратегии по снижению этих рисков 5. Отслеживать и анализировать тенденции в области безопасности и возникающие угрозы для обеспечения актуальности политики и рекомендаций по кибербезопасности организации Знания: 1. Продвинутые функции сетевой безопасности 2. Организационные бизнес-процессы, применимые к внедрению стандартов кибербезопасности с учетом особенностей транспортной отрасли 3. Документирование установленных стандартов и требований 4. Установление требований и характеристик инфраструктуры сетевой безопасности 5. Установление процессов технического обслуживания и оповещения 6. Проведение плановых проверок инфраструктуры сетевой безопасности 7. Методы и процедуры тестирования КБ

		8. Риски безопасности и толерантность к риску в организации 9. Отраслевые стандарты и правила по внедрению инфраструктуры сетевой безопасности в организации 10. Понимание правовых, инженерно-технических, организационных вопросов функционирования объектов транспорта
	Возможность признания навыка:	Не требуется
	Навык 3: Осуществление оценки и доклада об инцидентах кибербезопасности	Умения: 1. Собирать, передавать и сохранять доказательства, связанные с кибератакой, включая журналы, кэш, файлы и другие цифровые артефакты 2. Работать с внутренними заинтересованными сторонами, включая исполнительное руководство, кибер-криминалистов и ИТ-команды 3. Передавать информацию о кибератаках в правоохранительные органы Знания: 1. Внутренние протоколы для сообщения об инцидентах кибербезопасности правоохранительным органам 2. Работа с чувствительными данными (сбор, шифрование, хранение и передача свидетельств о кибератаках)
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Обучение сотрудников политике и процедурам кибербезопасности	Навык 1: Обучение сотрудников политике и процедурам кибербезопасности	Умения: 1. Разрабатывать программы обучения по кибербезопасности для сотрудников на темы управления паролями, безопасности электронной почты, фишинговых атак, социальной инженерии, защиты от вредоносных программ и защиты данных 2. Проводить тренинги для сотрудников используя различные методы, такие как презентации, обучающие программы и практические занятия 3. Контролировать и оценивать эффективность программ обучения Знания: 1. Способы и принципы проведения презентаций 2. Различные техники обучения 3. Методов проведения научных исследований, разработок по технической защите информации 4. Методов оценки профессионального уровня, аттестации специалистов по обеспечению безопасности информации

		5. Трудового законодательства, порядок внутреннего трудового распорядка, по безопасности и охране труда, производственной санитарии, требований пожарной безопасности
	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Аналитическое мышление Инициативность	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры (кодекс практики) обеспечения информационной безопасности ISO/IEC 27033 — Информационные технологии. Методы обеспечения безопасности. Безопасность сетей ISO/IEC 27005 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление рисками информационной безопасности ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий (Common Criteria) Национальные стандарты РК: СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла") СТ РК 4009-2025 ("Информационные технологии. Криптографическая защита информации. Алгоритм блочного симметричного шифрования")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
33. 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: Информационно-коммуникационные технологии	Квалификация: -
Требования к опыту работы:	Не требуется		
Связь с неформальным и информальным образованием:			
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:		
		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	
	Навык 1:	Знания: 1. Основные виды компьютерных преступлений 2. Способы доступа злоумышленников в сеть организации 3. Основные угрозы безопасности информации и модели нарушителя в ЦС организации 4. Принципы построения и функционирования систем и сетей передачи информации	

Трудовая функция 1: Расследование компьютерных преступлений	Первичное реагирование на компьютерные преступления	5. Национальные, межгосударственные и международные стандарты в области защиты информации 6. Технические каналы "утечки" информации 7. Нормативные правовые акты в области защиты информации 8. Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей 9. Основные методы организации и проведения технического обслуживания технических средств цифровизации 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 Нормы уголовного и административного права в сфере компьютерной информации
	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: полнодисковое шифрование, удаленное хранение информации и др. 4. Осуществлять сбор доказательной базы и ее оформление/хранение 5. Моделировать реальную атаку на организацию и тренировать навыки принятия мер по минимизации ущерба от нее Знания: 1. Принципы построения и функционирования систем и сетей передачи информации 2. Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей 3. Национальные, межгосударственные и международные стандарты в области защиты информации

		4. Основные угрозы безопасности информации и модели нарушителя в ЦС 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. Основные принципы изъятия компьютерной техники 10. Методы сокрытия уликовых данных от обнаружения 11. Документирование информации по расследованию
	Возможность признания навыка:	Не требуется
	Навык 1: Криминалистическая экспертиза компьютеров	Умения: 1. Расследовать инциденты кибербезопасности 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 Знания: 1. Базовые знания о файловых системах 2. Базовые знания об операционных системах 3. Основные принципы кибербезопасности и методы работы средств защиты

Трудовая функция 2:
Криминалистическая
экспертиза цифровых
устройств и
оборудования

	4. Инструментарий компьютерной криминалистики 5. Устройство жестких дисков и других накопителей 6. Архитектура 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
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. Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей 3. Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях 4. Основные принципы проведения сетевой криминалистики 5. Регламент действий сотрудников с целью получения максимально подробной информации для проведения анализа 6. Типовые источники данных для проведения сетевой криминалистики и их исследование 7. Особенности инструментария для создания дампа сетевого трафика
Возможность признания навыка:	Не требуется
	Умения: 1. Осуществлять идентификацию устройства мобильной связи

	Навык 3: Криминалистическая экспертиза мобильных устройств	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 7. 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. Базовые знания об мобильных операционных системах 5. Базовые знания о файловых системах мобильных устройств 6. Устройство карт памяти
	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 27001-2023 Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы управления информационной безопасностью. Требования СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 информационные технологии. Аудит систем управления информационной безопасностью организации	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
34. Карточка профессии "Менеджер знаний ":		
Код группы:	2524-0	
Код наименования занятия:	2524-0-030	

Наименование профессии :	Менеджер знаний		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области создания и разработки баз данных при наличии базового (высшего) педагогического образования		
Другие возможные наименования профессии :			
Основная цель деятельности:	Разрабатывает системы для сбора, обмена и управления знаниями внутри организации, обеспечивая доступ сотрудников к критически важной информации		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Сбор и обновление базы основных знаний компании 2. Разработка и поддержка базы знаний и управление входящей информацией 3. Организация и координация передачи и обмена знаниями	
	Дополнительные трудовые функции:	1. Мониторинг эффективности системы управления знаниями	
	Навык 1: Сбор и обновление базы основных знаний	Умения: 1. Обнаруживать и собирать ключевые регламенты, шаблоны и справочники из разных источников 2. Обеспечивать актуализацию основных документов 3. Вести реестр подрядчиков и партнеров с контактными данными 4. Контролировать целостность и отсутствие дублирования информации	
		Знания: 1. Методов идентификации и классификации основных знаний организации 2. Принципов версионирования документов и контроля изменений	

Трудовая функция 1: Сбор и обновление базы основных знаний компании		3. Стандартов хранения корпоративной документации (ISO 15489) 4. Инструментов для редактирования и хранения файлов
	Возможность признания навыка:	Не требуется
	Навык 2: Сбор и обновление базы динамичных знаний	Умения: 1. Организовывать процессы регулярного сбора динамичных знаний 2. Проводить периодический аудит актуальности динамичной информации 3. Внедрять механизмы уведомлений об устаревших материалах 4. Автоматизировать частичный сбор и обновление данных через формы и интеграции Знания: 1. Методов получения динамичных знаний 2. Принципов жизненного цикла знаний 3. Инструментов мониторинга изменений в процессах и процедурах 4. Подходов к вовлечению сотрудников в регулярное обновление контента
	Возможность признания навыка:	Не требуется
Трудовая функция 2: Разработка и поддержка базы знаний и управление входящей информацией	Навык 1: Разработка и оптимизация структуры базы знаний для удобства использования	Умения: 1. Проектировать логическую структуру разделов и подразделов базы знаний 2. Внедрять системы тегов, метаданных и полнотекстового поиска 3. Проводить тестирование удобства с представителями целевых отделов 4. Оптимизировать структуру на основе аналитики использования Знания: 1. Принципов информационной архитектуры и баз данных; 2. Методов построения таксономии, онтологии и тегирования 3. Стандартов навигации и поиска в корпоративных системах 4. Требований к доступности информации для разных ролей сотрудников
	Возможность признания навыка:	Не требуется
		Умения: 1. Разрабатывать и внедрять правила модерации и утверждения контента 2. Настраивать права доступа в зависимости от роли пользователя

	Навык 2: Обеспечение качества и доступности информации в базе знаний	3. Анализировать статистику просмотров и поиска для выявления закономерностей 4. Собирать и учитывать отзывы сотрудников по удобству системы знаний Знания: 1. Принципов управления качеством контента 2. Политик разграничения доступа и конфиденциальности 3. Инструментов аналитики баз данных 4. Методов обратной связи от пользователей системы знаний
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Организация и координация передачи и обмена знаниями	Навык 1: Организация процессов передачи знаний	Умения: 1. Разрабатывать программы менторства и парного обучения 2. Организовывать сессии передачи знаний при смене сотрудников 3. Создавать шаблоны для фиксации передаваемых знаний 4. Координировать назначение менторов новичкам Знания: 1. Моделей передачи знаний 2. Принципов построения программ адаптации 3. Подходов к мотивации передачи знаний от опытных сотрудников новичкам
	Возможность признания навыка:	Не требуется
	Навык 2: Проведение обучающих мероприятий	Умения: 1. Организовывать занятия на информационных платформах 2. Разрабатывать материалы для проверки знаний 3. Оценивать изменение уровня компетенций после обучения. 4. Создавать видеоуроки и интерактивные материалы Знания: 1. Интерактивных обучающих платформ 2. Методов оценки результатов обучения 3. Принципов создания усваиваемого материала
	Возможность признания навыка:	Не требуется
	Навык 1:	Умения: 1. Настраивать и анализировать результаты использования базы знаний 2. Проводить регулярные опросы сотрудников о качестве системы 3. Выявлять узкие места и разрабатывать планы улучшений

Дополнительная трудовая функция 1: Мониторинг эффективности системы управления знаниями	Оценка и улучшение системы управления знаниями организации	4. Внедрять новые функции и инструменты на основе анализа
		Знания: 1. Ключевых метрик эффективности 2. Методов сбора обратной связи и аналитики поведения пользователей 3. Моделей управления знаниями 4. Современных трендов в области управления знаниями и ИИ-инструментов
	Возможность признания навыка:	Не требуется
Требования к личным компетенциям:	Системное мышление Стрессоустойчивость Умение работать в команде Целеустремленность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью (кодекс практики по мерам обеспечения информационной безопасности) ISO/IEC 27004 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Измерение и метрики информационной безопасности (Information security measurement and metrics) ISO/IEC 27003 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по внедрению систем менеджмента информационной безопасности (Implementation guidance) Национальные стандарты РК: СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 27002-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью") (если адаптирован) СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки")	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
35. Карточка профессии "Аналитик по правоохранительной/судебной экспертизе и контрразведке":		
Код группы:	2524-0	
Код наименования занятия:	-	
Наименование профессии:	Аналитик по правоохранительной/судебной экспертизе и контрразведке	

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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) юридического образования.		
Другие возможные наименования профессии:	2611-1-003 - Юрист		
Основная цель деятельности:	Сбор и анализ цифровых доказательства для поддержки юридических расследований и контрразведывательных операций		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Подготовка заключения специалиста и анализ инцидентов кибербезопасности 2. Технический и контрразведывательный анализ цифровых данных и информационных систем 3. Работа с данными в области КБ	
	Дополнительные трудовые функции:	1. Обучение сотрудников правовой грамотности в вопросах кибербезопасности	
Трудовая функция 1:	Навык 1: Процессуально-правовые основы цифровой экспертизы и заключений специалиста	Умения: 1. Проводить сбор, учет и хранение цифровых доказательств без нарушения их целостности 2. Подготавливать заключения специалиста и представлять результаты расследований в суде 3. Разрабатывать и внедрять процедуры цифровой экспертизы и заключений специалиста 4. Доводить результаты расследований в логической и юридически корректной форме Знания: 1. Уголовного, процессуального и административного законодательства РК 2. Принципов и стандартов судебной цифровой экспертизы/заключения специалиста 3. Международных стандартов и этических норм в цифровой криминалистике	
		Возможность признания навыка:	Требуется

Подготовка заключения специалиста и анализ инцидентов кибербезопасности	Навык 2: Анализ и обработка данных инцидентов кибербезопасности	Умения: 1. Выявлять и классифицировать инциденты кибербезопасности 2. Анализировать журналы событий, сетевой трафик и другие источники данных 3. Формировать отчеты и рекомендации по результатам анализа инцидентов 4. Использовать специализированные инструменты (SIEM, IDS/IPS, forensic-средства) Знания: 1. Основ классификации инцидентов кибербезопасности и их особенностей 2. Методов сбора и корреляции данных об инцидентах 3. Основ расследования инцидентов и цифровой криминалистики 4. Нормативных требований к фиксации и обработке инцидентов
	Возможность признания навыка:	Требуется
Трудовая функция 2: Технический и контрразведывательный	Навык 1: Технический анализ цифровых носителей и систем	Умения: 1. Анализировать цифровые носители с использованием программных и технических инструментов 2. Извлекать данные из мобильных устройств 3. Разрабатывать временные шкалы событий 4. Использовать инструменты анализа данных, полученных с носителей Знания: 1. Основ криминалистики и правовой информатики 2. Принципов работы операционных систем (Windows, Linux, macOS, Android, iOS). 3. Структуры файловых систем (NTFS, FAT, ext4, APFS и др.). 4. Методов анализа жестких дисков, мобильных устройств и сетевых данных
	Возможность признания навыка:	Не требуется
	Навык 2: Реализация контрразведывательных мероприятий средствами цифровой криминалистики	Умения: 1. Восстанавливать и интерпретировать удаленные или зашифрованные данные 2. Проводить анализ вредоносных файлов и скриптов 3. Работать с инструментами криптоанализа и дешифрования 4. Определять источники кибератак в цифровом и материальном пространстве Знания: 1. Принципов кибербезопасности и контрразведки

анализ цифровых данных и информационных систем		2. Методов восстановления удаленных или зашифрованных данных 3. Основ реверс-инжиниринга и анализа вредоносного ПО 4. Методов криптографической защиты и дешифрования данных
	Возможность признания навыка:	Не требуется
	Навык 3: Аналитическая и контрразведывательная деятельность	Умения: 1. Проводить анализ сетевых журналов и событий безопасности 2. Проводить корреляцию данных из разных источников (логов, переписок, метаданных) 3. Использовать методы OSINT для выявления связей между субъектами 4. Применять методики контрразведывательного анализа Знания: 1. Сетевых протоколов и методов их анализа (TCP/IP, HTTP/S, DNS и т.д.) 2. Методов противодействия анонимизации и защиты данных 3. Принципов работы SIEM-систем 4. Основ OSINT, HUMINT, TECHINT анализа
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Работа с данными в области КБ	Навык 1: Работа с данными	Умения: 1. Собирать и обрабатывать данные из различных источников 2. Удалять и преобразовывать данные 3. Проводить анализ и интерпретировать результаты 4. Визуализировать и презентовать данные Знания: 1. Основ статистики и математического анализа данных 2. Методов сбора, подготовки и удаления данных 3. Инструментов анализа и визуализации 4. Баз и структуры данных
	Возможность признания навыка:	-
	Навык 2: Обеспечение безопасности	Умения: 1. Идентифицировать персональные и конфиденциальные данные в информационных системах 2. Применять меры защиты в соответствии с законодательством и внутренними политиками 3. Оценивать риски нарушения конфиденциальности и предлагать способы их минимизации

	персональных и конфиденциальных данных	4. Участвовать в разработке и сопровождении внутренних регламентов и политик по защите данных
		Знания: 1. Законодательство о защите персональных данных 2. Методы и средства защиты информации 3. Классификация и категорирование информации 4. Угрозы безопасности персональных и конфиденциальных данных
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Обучение сотрудников правовой грамотности в вопросах кибербезопасности	Навык 1: Обучение сотрудников правовой грамотности	Умения: 1. Разрабатывать программы обучения по кибербезопасности для сотрудников на темы управления паролями, безопасности электронной почты, фишинговых атак, социальной инженерии, защиты от вредоносных программ и защиты данных 2. Проводить тренинги для сотрудников используя различные методы, такие как презентации, обучающие программы и практические занятия 3. Контролировать и оценивать эффективность программ обучения
		Знания: 1. Способы и принципы проведения презентаций 2. Различные техники обучения 3. Методов оценки профессионального уровня, аттестации специалистов
	Возможность признания навыка:	Не требуется
Требования к личным компетенциям:	Самостоятельность и ответственность Системное мышление Стрессоустойчивость Умение работать в команде Аналитическое мышление Концентрация и управление вниманием Инициативность	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий (Common Criteria) ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27037 / ISO/IEC 27038 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Цифровая криминалистика. Рекомендации по сбору, анализу и сохранению цифровых доказательств Национальные стандарты РК: СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности")	

	СТ РК ISO/IEC 27001-2023 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
36. 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:	Не требуется		
Связь с неформальным и информальным 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:		
		Умения: 1. Выполнять задачи по получению, хранению, учету, выдаче, приему и утилизации специальных документов, применяемых в процессе эксплуатации систем шифрования данных	

Трудовая функция 1: Эксплуатация систем шифрования данных	Навык 1: Ведение специального делопроизводства и технических документов в процессе эксплуатации	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 кибербезопасности 3. Организационные меры по защите информации в системах шифрования данных 4. Законодательство в сфере обеспечения кибербезопасности 5. Устройство и функционирование современных систем шифрования данных
	Возможность признания навыка:	Не требуется
	Навык 2: Управление функционированием систем 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 кибербезопасности 8. Устройство и функционирование современных систем шифрования данных
	Возможность признания навыка:	Не требуется
	Трудовая функция 2: Оценивание уровня безопасности 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 недokumentированных 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 КБ 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, 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 безопасности. 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	
37. 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:	Не требуется		
Связь с неформальным и информальным 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 кибербезопасности 2. Обеспечение задач аудиторского задания 3. Выполнение задач аудиторского задания
	Дополнительные трудовые функции:	
Трудовая функция 1: Оценка и анализ рисков кибербезопасности	Навык 1: Применение методов анализа рисков для идентификации и оценки угроз	Умения: 1. Использовать методики анализа рисков для идентификации и оценки угроз 2. Разрабатывать комплексные стратегии по минимизации рисков и устранению уязвимостей в информационных системах 3. Оценивать воздействие потенциальных угроз на организацию, разрабатывать планы 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. Разрабатывать политики безопасности, стандарты и процедуры защиты информации для организации 2. Внедрять стандартизированные процессы безопасности, адаптируя их под нужды организации 3. Формировать и поддерживать культуру безопасности в организации через регулярное обновление политик Знания: 1. Принципы и подходы к разработке политики кибербезопасности 2. Национальный стандарт в области разработки и внедрения политики безопасности 3. Технологии защиты информации на уровне корпоративной инфраструктуры
	Возможность признания навыка:	Не требуется
		Умения: 1. Участвовать в разработке (актуализации) методических и организационно-распорядительных документов, регламентирующих аудиторскую деятельность 2. Проводить презентации методических и организационно-распорядительных документов

Трудовая функция 2: Обеспечение задач аудиторского задания	Навык 1: Методическое обеспечение аудита КБ	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 кибербезопасности 3. Эффективных методов ознакомления персонала с методическими документами обеспечения аудита КБ
	Возможность признания навыка:	Не требуется
	Навык 2: Организационное обеспечение аудита КБ	Умения: 1. Участвовать в организации взаимодействия с представителями проверяемой организации (подразделения) по вопросам аудита КБ 2. Осуществлять сбор руководящих документов (приказы, распоряжения, инструкции) по вопросам хранения, порядка доступа и передачи информации 3. Проводить аудит КБ Знания: 1. Этапы и формы деловой коммуникации 2. Принципы и правила общения в деловой среде 3. Порядков проведения аудита КБ
	Возможность признания навыка:	Не требуется
	Навык 3: Консультирование по вопросам безопасности на всех уровнях организации.	Умения: 1. Обучать сотрудников методам защиты данных и созданию безопасной рабочей среды 2. Консультировать по вопросам соблюдения политик безопасности, составлять рекомендации по безопасному использованию информационных технологий 3. Проводить регулярные консультации 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
		Умения: 1. Создавать отчеты с выводами и рекомендациями по улучшению системы защиты данных

Навык 1: Подготовка отчета и представление результатов внешним и внутренним аудиторам	2. Обсуждать и представлять результаты аудита с внутренними и (или) внешними аудиторами 3. Проводить визуализацию данных для улучшения восприятия отчета и принятия решений Знания: 1. Основы отчетности и метрики эффективности безопасности 2. Законодательство в сфере цифровизации 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 ЦТ и обеспечения КБ в процессах обеспечения КБ объекта аудита КБ	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 КБ 3. Оценивать соответствие принятых организационных и программно-технических решений обеспечения КБ 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 КБ 6. Выявлять узкие места в системе защиты и архитектуре объекта аудита КБ Знания: 1. Законодательство в сфере обеспечения кибербезопасности 2. Методики, программных средств выявления рисков и угроз КБ 3. Методов, процедур и порядка сбора аудиторских свидетельств
Возможность признания навыка:	Не требуется
Навык 3: Проверка и анализ текущего состояния защищенности объекта аудита КБ	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 КБ серверного и сетевого оборудования объекта аудита 4. Проверять конфигурации ПО на наличие эксплуатационных уязвимостей Знания:

Трудовая функция 3:
Выполнение задач
аудиторского задания

	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, floodи 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
	Умения:

	Навык 6: Выявление уязвимостей оборудования сети объекта аудита	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 КБ	Знания: 1. Методы и программные средства анализа защищенности и уязвимости 2. Техники инвентаризации ресурсов сети 3. Принципы формирования отчетов КБ
	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 безопасности. 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	
38. 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:	Не требуется		
Связь с неформальным и информальным 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 кибербезопасности	
	Дополнительные трудовые функции:		
		Умения: 1. Применять инструменты и методы сбора информации об уязвимостях 2. Анализировать полученные данные об уязвимостях	

Трудовая функция 1: Взаимодействие с разработчиками и менеджерами сервисов для устранения обнаруженных уязвимостей	Навык 1: Сбор и анализ информации об обнаруженных уязвимостях сервисов	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
	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 кибербезопасности 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:

Трудовая функция 2: Выступление консультантом и заказчиком новой функциональности, связанной с кибербезопасности		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 кибербезопасности
	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 безопасности. 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	
	Уровень ОРК:	Наименование профессии:

Связь с другими профессиями в рамках ОРК:	7	Специалист по безопасности сервисов	
39. Карточка профессии "Специалист по многоязычному анализу":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-025		
Наименование профессии :	Специалист по многоязычному анализу		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) лингвистического образования		
Другие возможные наименования профессии :			
Основная цель деятельности:	Использует лингвистическую и культурную экспертизу для поддержки операций в области кибербезопасности, особенно в анализе международных угроз		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Идентификация и обработка иностранных источников информации 2. Лингвистический анализ в области кибербезопасности 3. Подготовка аналитических материалов и отчетов по результатам многоязычного анализа	
	Дополнительные трудовые функции:	1. Социолингвистический анализ программного кода	
		Умения: 1. Выполнять точный перевод технических текстов по кибербезопасности 2. Адаптировать перевод с учетом контекста 3. Проверять точность перевода на наличие искажений смысла (пасхальных яиц)	

Трудовая функция 1: Идентификация и обработка иностранных источников информации	Навык 1: Перевод и адаптация материалов в области кибербезопасности	4. Работать с глоссариями специализированной терминологии
	Возможность признания навыка:	Знания: 1. Методов перевода технических и специализированных текстов в области кибербезопасности 2. Специфической лексики в области кибербезопасности на иностранных языках 3. Принципов сохранения смысла при переводе идиоматических выражений 4. Стандартов качества перевода
	Навык 2: Распознавание и классификация иностранных текстов и аудиоматериалов	Умения: 1. Определять язык и диалект источника информации 2. Извлекать существенные фрагменты из информации в области КБ иностранных источников 3. Использовать специализированные инструменты для обработки языковых данных Знания: 1. Основ фонетики, морфологии и синтаксиса основных иностранных языков 2. Методов идентификации языков и диалектов 3. Принципов работы с инструментами автоматического распознавания речи и текста 4. Терминологии в области кибербезопасности на иностранных языках
	Возможность признания навыка:	Не требуется
Трудовая функция 2:	Навык 1: Анализ культурного контекста иноязычных источников	Умения: 1. Выявлять культурные особенности в коммуникациях 2. Интерпретировать скрытые смыслы и подтексты в иностранных текстах 3. Оценивать влияние культурных факторов на сферу кибербезопасности 4. Сопоставлять культурные особенности с кибератаками Знания: 1. Культурных особенностей регионов, представляющих потенциальные угрозы 2. Социолингвистических аспектов коммуникации 3. Влияния культуры на сферу кибербезопасности 4. Методов культурного анализа текстов
	Возможность признания навыка:	Не требуется
		Умения: 1. Связывать данные с геополитическими событиями

Лингвистический анализ в области кибербезопасности	Навык 2: Оценка геополитического и регионального источника угрозы	2. Выявлять индикаторы происхождения угрозы по языковым признакам 3. Анализировать региональные особенности в кибератаках 4. Прогнозировать развитие угроз на основе культурно-лингвистических данных Знания: 1. Геополитических особенностей кибербезопасности 2. Региональных особенностей языкового воспроизведения в области кибербезопасности 3. Источников открытой информации по международным отношениям 4. Методов интерпретации культурного контекста в сфере кибербезопасности
	Возможность признания навыка:	Не требуется
Трудовая функция 3: Подготовка аналитических материалов и отчетов по результатам многоязычного анализа	Навык 1: Подготовка отчетов и рекомендаций по противодействию угрозам КБ	Умения: 1. Составлять аналитические отчеты на основе многоязычных данных 2. Формулировать рекомендации по нейтрализации угроз 3. Презентовать результаты анализа заинтересованным сторонам 4. Адаптировать отчеты под разные уровни аудитории Знания: 1. Структуры аналитических отчетов в сфере кибербезопасности 2. Методов формулирования рекомендаций по противодействию угрозам КБ 3. Принципов презентации аналитической информации 4. Требований к оформлению отчетов в области кибербезопасности
	Возможность признания навыка:	Не требуется
	Навык 2: Сбор и систематизация аналитических данных	Умения: 1. Систематизировать результаты лингвистического анализа 2. Формировать базы данных по многоязычным источникам угроз 3. Визуализировать данные для аналитических отчетов 4. Обеспечивать конфиденциальность обработанной информации Знания: 1. Методов систематизации и хранения аналитических данных

		2. Инструментов для создания баз данных по угрозам 3. Принципов визуализации информации в кибербезопасности 4. Норм защиты информации при обработке данных
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Социолингвистический анализ программного кода	Навык 1: Идентификация и оценка социолингвистических особенностей программного кода	Умения: 1. Выявлять лингвистические особенности в комментариях и переменных кода 2. Анализировать использование идиоматических выражений в коде 3. Определять культурные отсылки в структуре программного кода 4. Проводить сравнительный анализ кода на разных языках программирования
		Знания: 1. Основ социолингвистики и её применения к цифровым данным 2. Терминологии программирования с учетом лингвистических особенностей 3. Культурных различий в стилях написания кода 4. Методов выявления скрытых социолингвистических индикаторов
	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Дисциплинированность Аналитическое мышление Концентрация и управление вниманием Инициативность Лидерство	
Список технических регламентов и национальных стандартов:	Международные стандарты: ISO/IEC 15408 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии обеспечения безопасности информационных технологий (Common Criteria) ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление контрольными мерами (кодекс практики по мерам обеспечения информационной безопасности) ISO/IEC 2382 & ISO/IEC 2383 — Информационные технологии. Терминология и общие понятия (2382), Анализ данных (2383). Поддерживающие стандарты в области ИКТ Национальные стандарты РК: СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК ISO/IEC 15408-5-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Заранее определенные пакеты требований безопасности") СТ РК ISO/IEC 27001-2023 (	

	"Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
40. Карточка профессии "Специалист по информационной безопасности в области здравоохранения":			
Код группы:	2524-0		
Код наименования занятия:	2524-0-017		
Наименование профессии:	Специалист по информационной безопасности в области здравоохранения		
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:	Не требуется		
Связь с неформальным и информальным образованием:	Дополнительные профессиональные программы повышения квалификации в области кибербезопасности при наличии базового (высшего) ИТ-образования		
Другие возможные наименования профессии:	2524-0-007 - Специалист по информационной безопасности		
Основная цель деятельности:	Обеспечение кибербезопасности объектов медицины с целью исключения несанкционированного воздействия на них и связанные с ними системы		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Тестирование систем безопасности, сетевых устройств, медицинского оборудования при управлении и контроле над системой здравоохранения, а также определение уязвимых мест 2. Разработка и внедрение стандартов кибербезопасности с учетом особенностей в системе здравоохранения 3. Реагирование на инциденты кибербезопасности	
	Дополнительные трудовые функции:	1. Обучение сотрудников политике и процедурам кибербезопасности	
		Умения:	

Навык 1: Особенности информационных систем здравоохранения, включая электронные медицинские карты и лабораторные системы	1. Работать с информационными системами здравоохранения (ИСЗ), включая настройку и защиту электронных медицинских карт (ЭМК) и лабораторных систем 2. Обеспечивать соблюдение требований законодательства РК и стандартов Минздрава при защите медицинской информации 3. Реализовывать меры по защите персональных данных и конфиденциальной медицинской информации, включая шифрование и разграничение доступа 4. Настраивать и администрировать системы контроля доступа и аутентификации пользователей в медицинских информационных системах 5. Внедрять и поддерживать сетевые средства защиты, включая VPN, антивирусные решения и средства шифрования данных 6. Конфигурировать и использовать системы обнаружения вторжений (IDS/IPS), проводить мониторинг безопасности для своевременного выявления угроз 7. Организовывать процессы резервного копирования и восстановления медицинских данных для обеспечения непрерывности работы систем 8. Анализировать и противодействовать специфичным киберугрозам в здравоохранении, включая атаки на медицинское оборудование и системы Знания: 1. Нормативно-правовые требования в здравоохранении (Закон Республики Казахстан "Об охране здоровья граждан Республики Казахстан" (Закон РК № 193-V от 18 сентября 2009 года), Закон Республики Казахстан "О персональных данных и их защите" (Закон РК № 94-V от 21 мая 2013 года) 2. Методы защиты персональных данных и конфиденциальной медицинской информации 3. Технологии контроля доступа и аутентификации в медицинских системах 4. Отличительные основы сетевой безопасности информационных систем здравоохранения 5. Принципы работы систем обнаружения вторжений (IDS/IPS) и мониторинга безопасности 6. Организация резервного копирования и восстановления медицинских данных 7. Киберугрозы, специфичные для здравоохранения (например, атаки на медицинское оборудование)
Возможность признания навыка:	Требуется
	Умения:

Трудовая функция 1: Тестирование систем безопасности, сетевых устройств, медицинского оборудования при управлении и контроле над системой здравоохранения, а также определение уязвимых мест	Навык 2: Проверка программного обеспечения	1. Планировать и выполнять регулярное сканирование (включая инструменты SIEM) уязвимостей, эксплойтов для выявления слабых мест в системе безопасности организации 2. Проводить пентест систем безопасности 3. Использовать результаты сканирования уязвимостей для оценки уровня рисков 4. Разрабатывать рекомендации по устранению уязвимостей или рисков Знания: 1. Основы проведения пентеста и языков программирования, такие как Python, BASH, Java, Ruby и Perl 2. Текущая организационная политика и процедуры по реагированию на НД 3. Стандартные отраслевые средства обнаружения и предотвращения НД 4. Идентификационные характеристики аномальной активности 5. Установки и настройки NIDS, NIPS, HIDS и HIPS 6. Необходимая документация для составления отчетов об обнаружении НД 7. Управления информацией о новых уязвимостях для сохранения еѸ конфиденциальности до устранения известных уязвимостей 8. Правильное размещение датчиков при проектировании NIDS/NIPS продуктов в архитектурах и сетях предприятий 9. Обслуживание и настройка систем обнаружения НД 10. Выполнение сканирования уязвимостей с помощью инструментов SIEM 11. Обнаружение аномальной активности в сети или системе, используя защитный мониторинг 12. Программные инструменты и методы анализа защищенности систем и уязвимостей с учетом особенностей в области здравоохранения 13. Понимание правовых, инженерно-технических, организационных вопросов функционирования объектов здравоохранения
	Возможность признания навыка:	Требуется
		Умения: 1. Выполнять комплексное наблюдение и мониторинг для обнаружения угроз 2. Использовать результаты анализа данных об угрозах для поиска и обнаружения потенциальных нарушений 3. Осуществлять установку, эксплуатацию и обслуживание систем обнаружения и предотвращения НД включая круглосуточный защитный мониторинг

	Навык 3: Мониторинг сетей, раннее выявление угроз безопасности	4. Анализировать и характеризовать данные сетевого трафика с целью выявления аномальной активности и потенциальных угроз для сетевых ресурсов Знания: 1. Стандартные отраслевые средства обнаружения и предотвращения НД 2. Текущая организационная политика и процедуры по реагированию на НД 3. Идентификационные характеристики аномальной активности 4. Обнаружение аномальной активности в сети или системе, используя защитный мониторинг 5. Управление информацией о новых уязвимостях для сохранения еѸ конфиденциальности до устранения известных уязвимостей 6. Программные инструменты и методы анализа защищенности систем и уязвимостей с учетом особенностей в отрасли здравоохранения
	Возможность признания навыка:	Требуется
	Навык 1: Удаленная установка и обновление системы сетевой безопасности, предназначенной для предотвращения НД	Умения: 1. Проводить регулярное обновление программного и аппаратного обеспечения систем 2. Осуществлять установку и обновление антивирусных программ 3. Осуществлять настройку межсетевого экрана промышленных узлов сети 4. Тестировать обновления на совместимость с промышленным ПО перед внедрением Знания: 1. Работы промышленных сетевых узлов предприятия 2. Шифрование и криптография 3. Политики, требования принципов установки и обновлений ПО 4. Функционирование, применение и конфигурации межсетевого экрана 5. Настройка критериев ACL для определения разрешенного трафика в межсетевом экране
	Возможность признания навыка:	Не требуется
		Умения: 1. Определять существующие организационные операции безопасности и требования 2. Проводить анализ эффективности существующих киберопераций организации в сравнении с требованиями организации 3. Документировать результаты анализа в соответствии с организационными требованиями 4. Внедрять и обслуживать системы ICS

Трудовая функция 2: Разработка и внедрение стандартов кибербезопасности с учетом особенностей в системе здравоохранения	Навык 2: Разработка, внедрение и поддержка протоколов и процедур безопасности для снижения рисков безопасности	5. Определять и документировать необходимые обновления существующих организационных операций, нарушений обслуживания и задач для осуществления киберопераций 6. Внедрять необходимые операционные и аналитические процессы, процедуры отчетности об инцидентах
		Знания: 1. Техническая, производственная и организационная документация 2. Написание документации с подробным анализом, выводов и рекомендаций с использованием требуемой структур 3. Отраслевые и технические знания в области промышленных систем управления (ICS) с учетом особенностей в отрасли здравоохранения 4. Языки программирования, такие как C, C++, PHP, Python и JavaScript
	Возможность признания навыка:	Не требуется
		Умения: 1. Регистрировать, классифицировать и определять приоритеты инцидентов КБ, используя стандартные шаблоны и инструменты 2. Вести документацию по инцидентам безопасности 3. Определить инфраструктуру и подключения устройств IoT к электрическим сетям предприятия 4. Выявлять аномалии и инциденты безопасности IoT 5. Собирать информацию и выполнять глубокий анализ, диагностику и устранение проблем с безопасностью конечных точек IoT 6. Выполнять регулярное обслуживание процессов обнаружения проблем безопасности IoT 7. Проектировать и разрабатывать информационные панели мониторинга и отчетности по IoT 8. Сканировать критические уязвимости на всех уровнях IoT 9. Выполнять резервное копирование и шифрование устройств безопасности
	Навык 3: Внедрение безопасности для систем IoT	Знания: 1. Разработка информационной панели мониторинга 2. Языки программирования и визуализации данных (Python, R, SQL, NodeJS) 3. Основы шифрования и криптографии 4. Организационная политика, процедуры и руководства по поддержанию КБ 5. Процедуры обмена данными для документирования и внедрения процедур КБ

		6. Спектр стандартных шаблонов и инструментов, доступных для мониторинга безопасности 7. Фундаментальные топологии сети, устройств, конфигурации и возможности подключения в системах IoT 8. Различные контексты безопасности IoT и уровни охвата, включая устройства, облака, коммуникации, базы данных и приложения 9. Рутинные операционные процедуры реагирования на инциденты кибербезопасности IoT 10. Устранение уязвимостей и инцидентов кибербезопасности IoT 11. Внедрение повышения уровня кибербезопасности в системах IoT 12. Протоколы аудита систем, выявления и анализа аномалий в системах IoT
	Возможность признания навыка:	Не требуется
	Навык 1: Осуществление оценки и доклада об инцидентах кибербезопасности	Умения: 1. Собирать, передавать и сохранять доказательства, связанные с кибератакой, включая журналы, кэш, файлы и другие цифровые артефакты 2. Работать с внутренними заинтересованными сторонами, включая исполнительное руководство, кибер-криминалистов и ИТ-команды 3. Передавать информацию о кибератаках в правоохранительные органы Знания: 1. Внутренние протоколы для сообщения об инцидентах кибербезопасности правоохранительным органам 2. Работа с чувствительными данными (сбор, шифрование, хранение и передача свидетельств о кибератаках)
	Возможность признания навыка:	Не требуется
	Навык 2:	Умения: 1. Установить и подтвердить возникновение и характер инцидента кибербезопасности 2. Определить законодательные требования, организационные политики, процедуры и планы реагирования на инциденты кибербезопасности 3. Проводить анализ и оценку источников, влияний и последствий инцидента 4. Активировать план реагирования на инцидент и подтвердить, что кибер-инцидент локализован 5. Проводить оценку ущерба критической системной инфраструктуры организации или утечки данных 6. Документировать инцидент кибербезопасности, предпринятые действия, решения и результаты

Трудовая функция 3:
Реагирование на
инциденты
кибербезопасности

Распознавание и реагирование на инциденты в соответствии с организационными процедурами безопасности	Знания: 1. Ключевые особенности планов реагирования на инциденты кибербезопасности, а также их источники и причины 2. Различные типы атак, включая отказ в обслуживании (DoS), инъекции SQL (SQLi), атаки межсайтового скриптинга (XSS), аппаратные атаки, атаки на WiFi 3. Методология обнаружения инцидентов кибербезопасности, предупредительные меры и методы смягчения последствий 4. Процессы документирования и анализа журнала событий КБ 5. Организационная политика и процедуры реагирования на инциденты кибербезопасности (определения характера и местонахождения инцидентов, их локализация, установка исправлений безопасности и отключение доступа к сети, уведомления и предоставления отчетов необходимому персоналу)
Возможность признания навыка:	Не требуется
Навык 3: Внедрение существующих стандартов кибербезопасности, политики и руководства для организации	Умения: 1. Внедрять политику и руководство по кибербезопасности, которые соответствуют миссии и целям организации 2. Применять существующие стандарты безопасности для защиты данных и систем организации от злоумышленников 3. Разрабатывать и поддерживать планы и процедуры реагирования на инциденты для эффективного управления инцидентами 4. Оценивать риски кибербезопасности организации и разрабатывать стратегии по снижению этих рисков 5. Отслеживать и анализировать тенденции в области безопасности и возникающие угрозы для обеспечения актуальности политики и рекомендаций по кибербезопасности организации Знания: 1. Продвинутые функции сетевой безопасности 2. Организационные бизнес-процессы, применимые к внедрению стандартов кибербезопасности с учетом особенностей отрасли здравоохранения 3. Документирование установленных стандартов и требований 4. Установление требований и характеристик инфраструктуры сетевой безопасности 5. Установление процессов технического обслуживания и оповещения 6. Проведение плановых проверок инфраструктуры сетевой безопасности

		7. Методы и процедуры тестирования КБ 8. Риски безопасности и толерантность к риску в организации 9. Отраслевые стандарты и правила по внедрению инфраструктуры сетевой безопасности в организации
	Возможность признания навыка:	Не требуется
Дополнительная трудовая функция 1: Обучение сотрудников политике и процедурам кибербезопасности	Навык 1: Обучение сотрудников политике и процедурам кибербезопасности	Умения: 1. Разрабатывать программы обучения по кибербезопасности для сотрудников на темы управления паролями, безопасности электронной почты, фишинговых атак, социальной инженерии, защиты от вредоносных программ и защиты данных 2. Проводить тренинги для сотрудников, используя различные методы, такие как презентации, обучающие программы и практические занятия 3. Контролировать и оценивать эффективность программ обучения
		Знания: 1. Способы и принципы проведения презентаций 2. Различные техники обучения 3. Методов проведения научных исследований, разработок по технической защите информации достижения науки и техники в стране и за рубежом в области технической разведки и защиты информации 4. Методов оценки профессионального уровня, аттестации специалистов по обеспечению безопасности информации 5. Трудового законодательства, порядок внутреннего трудового распорядка, по безопасности и охране труда, производственной санитарии, требований пожарной безопасности
	Возможность признания навыка:	Не требуется
Требования к личностным компетенциям:	Системное мышление Стрессоустойчивость Аналитическое мышление Инициативность	
Список технических регламентов и	Международные стандарты: ISO/IEC 27001 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования ISO/IEC 27799 — Информационные технологии в здравоохранении (Health informatics). Управление информационной безопасностью в здравоохранении (Information security management in health) ISO/IEC 27002 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры (кодекс практики) обеспечения информационной безопасности ISO/IEC 27005 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление рисками информационной безопасности (Risk management) Национальные стандарты ПК: СТ ПК ISO/IEC 27001-2023 ("	

национальных стандартов:	Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования") СТ РК ISO/IEC 15408-4-2025 ("Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Структура спецификации методов и действий оценки") СТ РК 1073-2025 ("Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла")		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
41. 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:	Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 Параграф 2. 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 информальным 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:	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,

Создание системы защиты информации в организации		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 цифровизации 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: Настройка программного обеспечения с соблюдением требований по защите информации		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 КБ 2. Методы, средства и системы защиты информации 3. Архитектуры технических средств защиты информации 4. Национальные стандарты в сфере обеспечения КБ
	Возможность признания навыка:	Не требуется
	Навык 2: Настройка встроенных средств защиты информации программного обеспечения по заданным образцам	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	
42. 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:	Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 Параграф 3. Специалист по защите информации		
Уровень профессионального образования:	Уровень образования: высшее образование (бакалавриат, специалитет , ординатура)	Специальность: Информационная безопасность	Квалификация: -
Требования к опыту работы:	1. 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; 2. 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; 3. Специалист по защите информации: высшее (или послевузовское) образование по соответствующему направлению подготовки кадров без предъявления требования к стажу работы.		
Связь с неформальным и информальным 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 ЦС в процессе их эксплуатации 2. Внедрение систем защиты информации в ИС
	Дополнительные трудовые функции:	
	Навык 1: Диагностика систем защиты информации ЦС	Умения: 1. Классифицировать и оценивать угрозы кибербезопасности 2. Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в ЦС 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
	Возможность признания навыка:	Не требуется
		Умения: 1. Создавать, удалять и изменять учетные записи пользователей ЦС 2. Планировать политику безопасности программных компонентов ЦС 3. Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы 4. Использовать криптографические методы и средства защиты информации в ЦС

Трудовая функция 1: Обеспечение защиты информации в ЦС в процессе их эксплуатации	Навык 2: Администрирование систем защиты информации ИС	5. Регистрировать и анализировать события, связанные с защитой информации в ЦС
		Знания: 1. Принципы формирования политики КБ в ЦС 2. Программно-аппаратные средства защиты информации ЦС 3. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ЦС 4. Методы контроля эффективности защиты информации от "утечки" по техническим каналам 5. Критерии оценки эффективности и надежности средств защиты программного обеспечения ЦС 6. Технические средства контроля эффективности мер защиты информации 7. Принципы организации и структура систем защиты программного обеспечения ЦС 8. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности ЦС 9. Основные меры по защите информации в ЦС
	Возможность признания навыка:	Не требуется
	Навык 3: Управление защитой информации в ЦС	Умения: 1. Оценивать информационные риски в ЦС 2. Классифицировать и оценивать угрозы безопасности информации 3. Определять подлежащие защите информационные ресурсы автоматизированных систем 4. Разрабатывать предложения по совершенствованию системы управления защиты информации ЦС 5. Конфигурировать параметры системы защиты информации ЦС 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 ЦС 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
		Умения:

Трудовая функция 2:
Внедрение систем
защиты информации в
ЦС

Навык 1: Разработка организационно-распоря дительных документов по защите информации в ЦС	1. Классифицировать и оценивать угрозы кибербезопасности 2. Применять нормативные документы по противодействию технической разведке 3. Определять параметры настройки программного обеспечения системы защиты информации ЦС 4. Контролировать эффективность принятых мер по защите информации в ЦС Знания: 1. Содержание и порядок деятельности персонала по эксплуатации защищенных ЦС и систем защиты информации 2. Основные угрозы безопасности информации и модели нарушителя в ЦС 3. Основные криптографические методы, алгоритмы , протоколы, используемые для защиты информации в ЦС 4. Принципы построения средств защиты информации от "утечки" по техническим каналам 5. Нормативные правовые акты в сфере кибербезопасности
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 ЦС комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации 4. Осуществлять планирование и организацию работы персонала ЦС с учетом требований по защите информации 5. Конфигурировать аттестованную ЦС и системы защиты информации ЦС Знания: 1. Нормативные правовые акты в сфере обеспечения кибербезопасности 2. Методы, способы, средства, последовательность и содержание этапов разработки ЦС 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 безопасности. 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	
43. 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:	Не требуется		
Связь с неформальным и информальным 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:	
		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
	Навык 1: Администрирование средств защиты информации прикладного и системного 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 кибербезопасности программного обеспечения и меры по их предотвращению 7. Уязвимости используемого программного обеспечения и методы их эксплуатации

Трудовая функция 1: Администрирование средств защиты информации в компьютерных системах и сетях		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: 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. Противостоять 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 3: 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 кибербезопасности 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 кибербезопасности
	Возможность признания навыка:	Не требуется
	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

Трудовая функция 2: Оценка и управление рисками в области информационной безопасности		4. Принципы построения антивирусного программного обеспечения 5. Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению 6. Источники угроз кибербезопасности 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 ЦТ	Умения: 1. Выявлять и анализировать потенциальные риски, связанные с использованием ЦТ, 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 кибербезопасности 2. Методологии оценки рисков 3. Национальные стандарты в сфере обеспечения кибербезопасности 4. Законодательство в сфере обеспечения кибербезопасности
	Возможность признания навыка:	Не требуется
	Ответственность Системное мышление Аналитическое мышление	

Требования к личностным компетенциям:	Критический а 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 управления информационной безопасностью. Требования СТ РК ISO/IEC 27006-2017 Информационные технологии. Методы и средства безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности СТ РК 34.030-2008 Информационные технологии. Аудит систем управления информационной безопасностью организации	
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
	7	Специалист по вопросам безопасности (ИКТ)

Глава 4. Технические данные профессионального стандарта

44. Наименование государственного органа:

Министерство искусственного интеллекта и цифрового развития Республики Казахстан

Исполнитель:

Калим Ерболат Темирулы, +7 (700) 007 03 33, e.kalim@mdai.gov.kz

45. Организации (предприятия) участвующие в разработке:

ТОО "Институт проблем информационной безопасности"

Руководитель проекта:

Косяков Игорь Олегович

E-mail: heimmdal@topmail.kz

Номер телефона: +7 (702) 359 14 90

Министерство искусственного интеллекта и цифрового развития Республики Казахстан

Исполнители:

Советханова Ақжарқын Бакдәулетқызы, +7 (705) 508 72 05, a.sovetkhanova@mdai.gov.kz

ОЮЛ "Казахстанская ассоциация информационный безопасности"

Исполнители:

Покусов Виктор Владимирович, +7 (771) 716 18 16, v@viktor.kz

"Каспийский общественный университет"

Исполнители:

Сулейменов Нариман Сапарович, +7 (777) 827 33 31, narimanS1991@yandex.kz

НАО "Казахский национальный университет имени аль-Фараби"

Исполнители:

Мусиралиева Шынар Женисбековна, +7 (708) 010 03 72, mussiraliyevash@gmail.com

НАО "Евразийский национальный университет имени Л. Н. Гумилева"

Исполнители:

Сатыбалдина Дина Жагыпаровна, +7 (701) 538 40 75, satybaldina_dzh@enu.kz

ТОО "Astana IT University"

Исполнители:

Аманжолова Сауле Токсановна, +7 (777) 362 22 37, s.amanzholova@astanait.edu.kz

46. Отраслевой совет по профессиональным квалификациям: 10.03.2026 год.

47. Национальный орган по профессиональным квалификациям: 28.05.2026 год.

48. Национальная палата предпринимателей Республики Казахстан "Атамекен": -

49. Номер версии и год выпуска: версия, год.

50. Дата ориентировочного пересмотра: -

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