Приложение № 11 к приказу
исполняющего обязанности
Председателя Правления
Национальной палаты
предпринимателей Республики
Казахстан «Атамекен» № 222 от
05.12.2022г.

Профессиональный стандарт: «Специалисты-профессионалы по безопасности информационной инфраструктуры и ИТ»

Глава 1. Общие положения

1. Область применения профессионального стандарта:
2. В настоящем профессиональном стандарте применяются следующие термины и определения:

1) Отраслевая рамка квалификаций – составная часть (подсистема) национальной системы квалификаций, представляющая собой рамочную структуру дифференцированных уровней квалификации, признаваемых в отрасли

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

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

4) Профессиональная задача (задача) – элементы трудовой функции, позволяющая декомпозировать функцию на единичные действия

5) Профессия – основной род занятий трудовой деятельности человека, требующий владения комплексом специальных теоретических знаний, умений и практических навыков, приобретаемых в результате специальной подготовки, подтверждаемых соответствующими документами об образовании и/или опыта работы

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

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

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

9) Умения – контролируемые работником действия, соответствующие требованиям норм трудовой деятельности

10) Компетенция – способность работника применять знания, умения и опыт в профессиональной и трудовой деятельности

11) Квалификация – официальное признание ценности освоенных компетенций для рынка труда и дальнейшего образования и обучения, дающее право на осуществление трудовой деятельности

12) Уровень квалификации – степень соответствия требованиям к знаниям, умениям и личностным и профессиональным компетенциям работников, дифференцируемые по параметрам сложности, нестандартности решения профессиональных задач, ответственности и самостоятельности

3. В настоящем профессиональном стандарте применяются следующие сокращения:

1) ОРК – отраслевая рамка квалификации
2) ПС – профессиональный стандарт
3) ПО – программное обеспечение
4) ИС – информационная система
5) ИКТ – информационно-коммуникационные технологии
6) IPsec – Internet Protocol Security VPN - Virtual Private Network NGFW - Next-Generation Firewall DLP - Data Loss Prevention
7) IDS – Intrusion Detection System
8) IPS – Intrusion Prevention Systems
9) TCP/IP – Transmission Control Protocol/Internet Protocol
10) ИТ (IT) – Информационные технологии
11) ЕСКД – Единая система конструкторской документации ЕСТД - Единая система технологической документации ЕСПД - Единая система программной документации
12) ЕТКС или КС – Единый тарифно-квалификационный справочник работ и профессий рабочих или Квалификационный справочник должностей руководителей, специалистов и других служащих
13) ОКЭД – Общий классификатор видов экономической деятельности
14) ПАС – Программно-аппаратные средства
15) БД – Базы данных
16) МСКО – Международная стандартная классификация образования
17) НПА – нормативные правовые акты
18) НТД – нормативно-техническая документация

Глава 2. Паспорт профессионального стандарта

4. Название профессионального стандарта: Специалисты-профессионалы по безопасности информационной инфраструктуры и ИТ

5. Код профессионального стандарта: J62090011

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

J Информация и связь

62 Компьютерное программирование, консультационные и другие сопутствующие услуги

62.0 Компьютерное программирование, консультационные и другие сопутствующие услуги

62.09 Другие виды деятельности в области информационных технологий и информационных систем

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

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

8. Перечень карточек профессий:

1) Инженер по защите информации - 4 уровень ОРК
2) Специалист по информационной безопасности - 4 уровень ОРК
3) Администратор по информационной безопасности - 4 уровень ОРК
4) Специалист по безопасности сервисов - 5 уровень ОРК
5) Инженер по защите информации - 5 уровень ОРК
6) Администратор по информационной безопасности - 5 уровень ОРК
7) Специалист по информационной безопасности - 5 уровень ОРК
8) Специалист по безопасности сервисов - 6 уровень ОРК
9) Аудитор по информационной безопасности - 6 уровень ОРК
10) Инженер по защите информации - 6 уровень ОРК
11) Специалист по информационной безопасности - 6 уровень ОРК
12) Аудитор по информационной безопасности - 7 уровень ОРК

Глава 3. Карточки профессий

9. 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:	4		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 185 Техник-программист		
Уровень профессионального образования:	Уровень образования: ТиПО (специалист среднего звена)	Специальность: Вычислительная техника и информационные сети (по видам)	Квалификация:
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:	Администратор по информационной безопасности Специалист по информационной безопасности		
Основная цель деятельности:	Устанавливать и настраивать средства защиты информации		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации 2. Проведение контроля защищенности информации	
	Дополнительные трудовые функции:		
Трудовая функция 1:			

Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации	Навык 1: Установка и монтаж технических средств защиты информации от утечки	Умения:
		1. Производить установку и монтаж технических средств защиты информации 2. Использовать нормативные правовые акты, методические документы, национальные стандарты в области защиты информации
		Знания:
		1. Технических средств защиты информации 2. Средств контроля эффективности защиты информации 3. Технических описаний и инструкции (руководства) по эксплуатации технических средств защиты информации
	Возможность признания навыка:	-
	Навык 2: Настройка и испытания технических средств защиты информации	Умения:
		1. Проводить настройку и испытания технических средств защиты информации 2. Использовать нормативные правовые акты, методические документы, национальные стандарты в области защиты информации
		Знания:
		1. Технических средств защиты информации 2. Технических описаний и инструкции (руководства) по эксплуатации технических средств защиты информации
	Возможность признания навыка:	-
Трудовая функция 2: Проведение контроля защищенности информации	Навык 1: Проведение контроля защищенности информации	Умения:
		1. Проводить контроль защищенности информации 2. Рассчитывать показатели защищенности информации
		Знания:
		1. Нормативно- правовых актов, методических документов, национальных стандартов в области защиты информации 2. Методов, средств и систем защиты информации 3. Технических средств защиты информатизации 4. Методов контроля защищенности информации
	Возможность признания навыка:	-
	Навык 2: Подготовка отчетных материалов по результатам контроля защищенности информации	Умения:
		1. Формировать, вести, хранить рабочую документацию 2. Готовить итоговый документ, формируемый по результатам контроля защищенности информации 3. Оформлять протоколы оценки защищенности информации 4. Оформлять отчет по результатам контроля
		Знания:
		1. Отчетные документы, оформляемые по результатам контроля защищенности информации 2. Принципов формирования и ведения рабочей и отчетной документации. 3. Методов систематизации и обобщения результатов аудита.
	Возможность признания навыка:	-

Требования к личностным компетенциям:	Ответственность Гибкость мышления Умение работать в команде Дисциплинированность Инициативность Организованность Внимательность Исполнительность Высокая обучаемость Ориентация на результат		
Список технических регламентов и национальных стандартов:			
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	5	Инженер по защите информации	
10. 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:	4		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 185. Техник-программист		
Уровень профессионального образования:	Уровень образования: ТиПО (специалист среднего звена)	Специальность: Вычислительная техника и информационные сети (по видам)	Квалификация: -
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:	Администратор по информационной безопасности Инженер по защите информации		
Основная цель деятельности:	Обеспечивать информационную безопасность организации		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Планирование процессов управления и обеспечения ИБ организации 2. Планирование мероприятий по обеспечению ИБ организации 3. Контроль процессов управления и обеспечения ИБ организации	
	Дополнительные трудовые функции:		
Трудовая функция 1: Планирование процессов управления и обеспечения ИБ организации	Навык 1: Описание бизнес-процессов, связанных с автоматизированной обработкой информации	Умения:	
		1. Пользоваться методами автоматизированной обработки информации 2. Выявлять и описывать бизнес- процессы, связанные с автоматизированной обработкой информации.	

		Знания:
		1. Базовых знаний о принципах и применении ИТ для автоматизации бизнес-процессов. 2. Методики описания бизнес-процессов. 3. Общих представлений о принципах и этапах проектирования, создания и эксплуатации ИС.
	Возможность признания навыка:	-
	Навык 2: Разработка (актуализация) шаблонов (макетов) документов, регламентирующих процессы обеспечения ИБ	Умения:
		1. Разрабатывать (актуализировать) шаблоны (макеты) документов, регламентирующих процессы обеспечения ИБ в организации 2. Управлять лицензиями и версионностью ПО, учетом носителей конфиденциальной информации.
		Знания:
		1. Основных принципов, методов и средств обеспечения ИБ. 2. Основных НПА РК в сфере информатизации, ИБ. 3. Национальных, международных и межгосударственных НТД по вопросам обеспечения ИБ. 4. Порядка разработки, оформления, согласования и утверждения ТД.
	Возможность признания навыка:	-
Трудовая функция 2: Планирование мероприятий по обеспечению ИБ организации	Навык 1: Инвентаризация активов, связанных с автоматизированной обработкой информации	Умения:
		1. Выполнять процедуры инвентаризации активов, связанных с автоматизированной обработкой информации. 2. Формировать отчет по инвентаризации
		Знания:
		1. НТД и методов классификации, учета и маркировки активов, связанных с обработкой информации. 2. Порядка оформления технической и отчетной документации.
	Возможность признания навыка:	-
Трудовая функция 3: Контроль процессов управления и обеспечения ИБ организации	Навык 1: Проверка соблюдения требований документов, регламентирующих процессы обеспечения ИБ сотрудниками, подрядчиками и третьими сторонами	Умения:
		1. Контролировать полноту, своевременности и фактов ознакомления сотрудниками с документами, регламентирующими процессы обеспечения ИБ. 2. Проводить проверку соблюдения требований документов, регламентирующих процессы обеспечения ИБ сотрудниками, подрядчиками и третьими сторонами. 3. Составлять и оформлять акты контрольных проверок выполнения требований документов, регламентирующих процессы обеспечения ИБ.

	Знания:
	1. Основных способов контроля выполнения планов и мероприятий по контролю процессов управления и обеспечения ИБ организации. 2. ТД организации по ИБ. 3. Принципов и методов обеспечения ИБ в части регистрации и учета событий ИБ, резервного копирования, антивирусной защиты, контроля доступа, обеспечения ИБ при работе со съемными носителями, мобильными устройствами, почтовыми службами и Интернетом, реагирования на инциденты ИБ, использования средств криптографии и их носителей, управления лицензиями и версионностью ПО.
Возможность признания навыка:	-
Навык 2: Тестирование (апробация) аппаратно- программных средств обеспечения ИБ	Умения:
	1. Осуществлять тестирование (апробацию) аппаратно-программных средств обеспечения ИБ. 2. Проверять состояние аппаратно- программных средств обеспечения ИБ, поступивших из ремонта.
	Знания:
	1. Базовых знаний и представления об ОС и встроенных в них механизмах защиты. 2. Назначений, технических характеристик, конструкций, особенностей и правил эксплуатации ПАС обеспечения ИБ. 3. Порядка оформления документации по приемке и постановке на учет в организации приобретаемых ПАС защиты информации. 4. Языков программирования
Возможность признания навыка:	-
Навык 3: Техническое сопровождение (регламентные и профилактические работы) аппаратно- программных средств обеспечения и мониторинга состояния ИБ	Умения:
	1. Осуществлять техническое сопровождение (регламентные и профилактические работы) аппаратно- программных средств обеспечения ИБ. 2. Осуществлять техническое сопровождение (регламентные и профилактические работы) систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации. 3. Анализировать журналы СКУД и записей систем видеонаблюдения.
	Знания:
	1. Назначений, технических характеристик, конструкций, особенностей ПАС обеспечения ИБ. 2. Правил эксплуатации ПАС обеспечения ИБ. 3. Общих представлений о назначении, сферах применения и принципах построения систем мониторинга уязвимостей, мониторинга ИБ и предотвращения утечек информации. 4. НТД, регламентирующих вопросы технического обслуживания оборудования. 5. Приемов и способов выполнения технического обслуживания оборудования. 6. Методики и рекомендаций производителя средств защиты информации и обеспечения ИБ по их обслуживанию. 7. Языков программирования
Возможность признания навыка:	-

	Навык 4: Восстановление работоспособности аппаратно- программных средств обеспечения ИБ	Умения:	
		1. Выполнять работы по обеспечению послеаварийного восстановления работоспособности аппаратно-рограммных средств обеспечения ИБ. 2. Вести и формировать отчетную документации по результатам проведенных работ по обеспечению ИБ.	
		Знания:	
		1. Технических характеристик, конструкции, особенностей ПАС обеспечения ИБ. 2. Правил эксплуатации ПАС обеспечения ИБ. 3. Принципов формирования и ведения технической и отчетной документации.	
	Возможность признания навыка:	-	
	Навык 5: Управлять носителями конфиденциальной информации	Умения:	
		1. Обеспечивать учет, хранение и передачу носителей с конфиденциальной информацией, не содержащую государственных секретов.	
		Знания:	
		1. Принципов и способов обеспечения конфиденциальности информации; 2. Технологии и типов носителей информации.	
	Возможность признания навыка:	-	
Требования к личностным компетенциям:	Ответственность Гибкость мышления Умение работать в команде Дисциплинированность Организованность Внимательность Исполнительность Ориентация на результат Высокая обучаемость		
Список технических регламентов и национальных стандартов:			
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	4	Администратор по информационной безопасности	
	5	Специалист по информационной безопасности	
	5		
11. 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:	4		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. Техник-программист		
Уровень профессионального образования:	Уровень образования: ТиПО (специалист среднего звена)	Специальность: Вычислительная техника и информационные сети (по видам)	Квалификация:

Требования к опыту работы:		
Связь с неформальным и информальным образованием:		
Другие возможные наименования профессии:	Специалист по информационной безопасности Инженер по защите информации	
Основная цель деятельности:	Поддерживать и администрировать ПАС защиты информации	
Описание трудовых функций		
Перечень трудовых функций:	Обязательные трудовые функции:	1. Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения ИБ 2. Администрирование механизмов безопасности 3. Реагирование на инциденты ИБ 4. Контроль и анализ эффективности применения ПАС зашиты информации и обеспечения ИБ
	Дополнительные трудовые функции:	
Трудовая функция 1: Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения ИБ	Навык 1: Эксплуатация ПАС защиты информации и обеспечения ИБ и техническое сопровождение	Умения:
		1. Эксплуатировать ПАС защиты информации и обеспечения ИБ. 2. Принимать от поставщика и/или исполнителя работ ПАС защиты информации и обеспечения ИБ. 3. Учитывать и хранить носители конфиденциальной информации. 4. Эксплуатировать ПАС защиты конфиденциальной информации. 5. Проводить регламентные и профилактические работы по техническому обслуживанию средств защиты информации и обеспечения ИБ
		Знания:
		1. Принципов работы и правил эксплуатации ПАС защиты информации и обеспечения ИБ. 2. Принципов и способов обеспечения конфиденциальности информации. 3. Технологий и типов носителей информации. 4. Рекомендаций производителя средств защиты информации и обеспечения ИБ по их эксплуатации. 5. НТД, регламентирующих вопросы технического обслуживания оборудования. 6. Видов, методов, приемов и способов технического обслуживания оборудования. 7. Регламента технического обслуживания средств защиты информации и обеспечения ИБ. 8. Методик и рекомендаций производителя средств защиты информации и обеспечения ИБ по их обслуживанию.
	Возможность признания навыка:	-
	Навык 2: Администрирование антивирусного ПО	Умения:
		1. Удаленно устанавливать, обновлять антивирусные программы и антивирусные базы 2. Создавать и копировать на серверы сети дистрибутивы для централизованной установки антивирусов. 3. Удаленно настраивать антивирусные программы, установленные на рабочие станции и серверы. 4. Планировать задания для немедленного или отложенного запуска на компьютерах сети.

		Знания:
		1. Назначений, видов и принципов действия антивирусных программ. 2. Рекомендаций производителя антивирусного ПО по его установке и эксплуатации.
	Возможность признания навыка:	-
	Навык 3: Администрирование системы обнаружения/ предотвращения вторжений	Умения:
		1. Осуществлять мониторинг, применять политики обнаружения/предотвращения вторжений 2. Управлять пользователями и осуществлять разграничения прав доступа, сегментирование и фильтрацию. 3. Осуществлять настройки парольной политики и блокировок пользователей. 4. Выполнять конфигурирование параметров сетевого доступа. 5. Устанавливать разрешение доступа с ограниченного количества хостов/подсетей. 6. Управлять обновлениями ПО.
		Знания:
		1. Назначений, принципов действия, архитектур систем обнаружения/ предотвращения вторжений. 2. Стандартов, регламентирующих функционирование систем обнаружения вторжений. 3. Рекомендаций производителя системы обнаружения/ предотвращения вторжений по ее установке и эксплуатации.
	Возможность признания навыка:	-
	Навык 4: Конфигурирование и настройка межсетевого экрана	Умения:
		1. Настраивать режимы работы межсетевого экрана и политик фильтрации. 2. Осуществлять создание учетной записи администратора, разграничение прав доступа. 3. Выполнять резервное копирование и восстановление. 4. Осуществлять настройку сервисов (DNS, DHCP и других внутренних сетевых сервисов). 5. Настраивать логирование и мониторинг событий. 6. Настраивать и отлаживать маршрутизации. 7. Настраивать виртуальные домены и сети 8. Настраивать защищенные соединения IPsec VPN. 9. Настраивать политику аутентификации. 10. Управлять и применять криптографические сертификаты
		Знания:
		1. Назначений, базовых принципов функционирования межсетевых экранов и работы стека протоколов TCP/IP. 2. Сетевых оборудований и ПО к ним
	Возможность признания навыка:	-
	Навык 5: Ведение отчетной документации	Умения:
		1. Назначений, базовых принципов функционирования межсетевых экранов и работы стека протоколов TCP/IP. 2. Сетевых оборудований и ПО к ним

		Знания:
		1. Принципов формирования и ведения отчетной документации. 2. Программного обеспечения по формированию отчетной документации.
	Возможность признания навыка:	-
Трудовая функция 2: Администрирование механизмов безопасности	Навык 1: Управление процессами по администрированию	Умения:
		1. Составлять и поддерживать в актуальном состоянии список прав доступа и полномочий сотрудников по доступу к защищаемой информации. 2. Мониторить выходы обновлений и управлять версиями ППО, СУБД, ОС серверного и сетевого оборудования. 3. Взаимодействовать с другими администраторами для обеспечения согласованной работы по обновлению версий ПО и списков прав доступа.
		Знания:
		1. Технологии межличностной и групповой коммуникации в деловом взаимодействии. 2. Основ администрирования систем 3. Инструментальных средств администрирования ИБ 4. Языков программирования
	Возможность признания навыка:	-
	Навык 2: Настраивание политики безопасности ОС, СУБД, ППО	Умения:
		1. Управлять криптографическими ключами (генерация и распределение). 2. Управлять шифрованием (Устанавливать и синхронизация криптографических параметров). 3. Управлять аутентификацией (распределение информации, необходимой для аутентификации - паролей, ключей и т.п.). 4. Управлять доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.). 5. Устанавливать и настраивать контролеры доменов сети.
		Знания:
		1. Встроенных механизмов безопасности ОС, СУБД и принципов настройки их политик. 2. Принципов и особенностей построения ОС для решения задач защиты информации и обеспечения ИБ. 3. Основных видов политик управления доступом и информационными потоками.
	Возможность признания навыка:	-
Трудовая функция 3: Реагирование на инциденты ИБ	Навык 1: Мониторинг событий и инцидентов ИБ	Умения:
		1. Собирать и анализировать события в системах, находящихся под мониторингом ИБ. 2. Классифицировать события, серийные события и сочетания событий как нарушения ИБ. 3. Настраивать процедуры обработки событий и обнаруживать события ИБ.

		Знания:
		1. НТД и ТД, регламентирующих управление инцидентами ИБ. 2. ПАС и систем управления инцидентами ИБ. 3. Понятий событий и инцидентов ИБ, принципов.
	Возможность признания навыка:	-
	Навык 2: Реагирование на инциденты ИБ	Умения:
		1. Регистрировать и оповещать (информировать) об инциденте ИБ. 2. Определять причины инцидента ИБ. 3. Принимать меры к ликвидации инцидента ИБ и его последствий. 4. Собирать доказательства об инциденте. 5. Участвовать в проведении расследований инцидентов ИБ. 6. Взаимодействовать с компетентными органами (CERT, органы внутренних дел и другие).
		Знания:
		1. Процедур управления инцидентами ИБ. 2. Компетенций полномочных организаций в области ИБ.
	Возможность признания навыка:	-
Трудовая функция 4: Контроль и анализ эффективности применения ПАС зашиты информации и обеспечения ИБ	Навык 1: Текущий контроль технологического процесса обработки защищаемой информации	Умения:
		1. Составлять и поддерживать в актуальном состоянии документации по размещению и конфигурации ПАС зашиты информации и обеспечения ИБ. 2. Контролировать целостности настроек механизмов безопасности ППО, СУБД, ОС серверного и телекоммуникационного оборудования. 3. Анализировать журналы регистрации событий системного и прикладного ПО с целью выявления попыток НСД к ИС и защищаемым информационным ресурсам.
		Знания:
		1. Методов, принципов и приемов осуществления контроля. 2. Процедур анализа журнала событий ИБ (выполнение задач анализа, проведение расследования и анализ нестандартных событий, документирование выполнения процедур и сбор доказательств, формировать отчетности для руководства). 3. Программных средств анализа
	Возможность признания навыка:	-
	Навык 2: Текущий и периодический контроль работы ПАС защиты информации и обеспечения ИБ	Умения:
		1. Анализировать журналы регистрации событий ПАС защиты информации и обеспечения ИБ 2. Оценивать полноту использования ресурсов ПАС защиты информации и обеспечения ИБ.
		Знания:
		1. Принципов работы и правил эксплуатации ПАС защиты информации 2. Критериев и показателей результативности использования ресурсов ПАС защиты информации и обеспечения ИБ.

	Возможность признания навыка:	-	
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:			
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	4	Специалист по информационной безопасности	
	5	Администратор по информационной безопасности	
12. 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:	5		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 185. Техник-программист		
Уровень профессионального образования:	Уровень образования: послесреднее образование (прикладной бакалавриат)	Специальность: Вычислительная техника и информационные сети (по видам)	Квалификация: -
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:			
Основная цель деятельности:	Проверять устойчивость приложений к внешнему несанкционированному доступу		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Проверка устойчивости веб- приложений компании к атакам 2. Поиск и устранение уязвимостей программного кода критичных сервисов 3. Внедрение контроля безопасности сервисов (аудит кода, сканирование на уязвимости и т.п.);	
	Дополнительные трудовые функции:		
Трудовая функция 1: Проверка устойчивости веб-приложений компании к атакам			

	Навык 1: Анализ и проверка безопасности архитектуры Web- сервера	Умения:
		1. Проверять состояние физической безопасности Web-сервера. 2. Проверять характеристики безопасности объекта аудита, связанных с архитектурой Web- сервера. 3. Проверять характеристики безопасности, связанных с конфигурацией встроенных механизмов ИБ серверного и сетевого оборудования Web-сервера.
		Знания:
		1. Методов предотвращения сетевых атак. 2. Методов анализа защищенности внешнего периметра корпоративной сети. 3. Методов анализа защищенности внутренней ИТ-инфраструктуры объекта аудита. 4. Методов и порядка проведения тестирования ПО.
	Возможность признания навыка:	-
	Навык 2: Описание векторов атаки и оценка рисков	Умения:
		1. Собирать и изучать проектную и эксплуатационную документации на Web-приложение, интервьюировть сотрудников и регистрировать сведения. 2. Оценивать применимость НПА и НТД к Web-приложению. 3. Оценивать соответствие принятых организационных и программно- технических решений обеспечения ИБ требованиям НПА и НТД. 4. Определять и оценивать вероятных угроз безопасности в отношении ресурсов Web-приложения и уязвимостей защиты. 5. Анализировать риски, связанные с возможностью осуществления угроз безопасности в отношении ресурсов Web-приложения. 6. Выявлять узкие места в системе защиты и архитектуре Web- приложения.
		Знания:
		1. Методов предотвращения сетевых атак. 2. Методов анализа защищенности внешнего периметра корпоративной сети. 3. Методов анализа защищенности внутренней ИТ-инфраструктуры объекта аудита. 4. Методов и порядка проведения тестирования ПО. 5. Языков программирования
	Возможность признания навыка:	-
Трудовая функция 2: Поиск и устранение уязвимостей программного кода критичных сервисов	Навык 1: Выявление, оценка и устранение всех возможных уязвимостей сервисов	Умения:
		1. Идентифицировать и инвентаризировать ресурсы Web- приложении. 2. Идентифицировать и учитывать сервисы и информационные потоки Web-приложении. 3. Сканировать уязвимости уровня операционной системы. 4. Идентифицировать и учитывать настройки безопасности Web- приложении.

		Знания:
		1. Программных средств обнаружения недостатков Web-приложении 2. Методов статического анализа программного кода. 3. Методов динамического анализа программного кода. 4. Инструментальных средств анализа защищенности и уязвимостей. 5. Языков программирования; 6. Основных технологий создания веб- сервисов: WSDL и RESTFull.
	Возможность признания навыка:	-
	Навык 2: Предоставление рекомендаций по улучшению информационной безопасности сервисов	Умения:
		1. Представлять рекомендации по улучшению ИБ серверов 2. Находить новейшие ПО по ИБ для серверов
		Знания:
		1. Методов систематизации и обобщения результатов аудита. 2. Программных средств ИБ. 3. Оборудований ИБ. 4. Языков программирования. 5. Основных технологий создания веб- сервисов: WSDL и RESTFull.
	Возможность признания навыка:	-
	Навык 3: Документирование процесса аудита безопасности сервисов компании	Умения:
		1. Формировать, вести, хранить рабочую документацию аудиторского задания. 2. Формировать итоговый документ, формируемый по результатам аудиторского задания.
		Знания:
		1. Принципов формирования и ведения рабочей и отчетной документации. 2. Методов систематизации и обобщения результатов аудита
	Возможность признания навыка:	-
Трудовая функция 3: Внедрение контроля безопасности сервисов (аудит кода, сканирование на уязвимости и т.п.);	Навык 1: Контроль выполнения 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. Методик контроля качества аудиторских заданий. 2. НТД по аудиторской деятельности.
	Возможность признания навыка:	-
	Навык 2: Текущий и периодический контроль работы сервисов	Умения:
		1. Анализировать журналы регистрации событий по работе сервисов 2. Оценивать полноту использования ресурсов сервисов.

		Знания:	
		1. Критериев и показателей результативности использования ресурсов сервисов.	
	Возможность признания навыка:	-	
	Навык 3: Контроль результатов аудиторского задания	Умения:	
		1. Анализировать результаты аудита сервиса. 2. Утверждать итоговый документ, формируемый по результатам аудита сервиса.	
		Знания:	
		1. Методики оценки эффективности применения организационных и технических средств обеспечения ИБ	
	Возможность признания навыка:	-	
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:			
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	5	Специалист по информационной безопасности	
13. 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:	5		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 185 Техник - программист		
Уровень профессионального образования:	Уровень образования: послесреднее образование (прикладной бакалавриат)	Специальность: Вычислительная техника и информационные сети (по видам)	Квалификация:
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:			
Основная цель деятельности:	Обеспечить техническое обслуживание средств защиты информации		
Описание трудовых функций			

Перечень трудовых функций:	Обязательные трудовые функции:	1. Обслуживание средств защиты информации прикладного и системного программного обеспечения 2. Обслуживание программно- аппаратных средств защиты информации в операционных системах
	Дополнительные трудовые функции:	
Трудовая функция 1: Обслуживание средств защиты информации прикладного и системного программного обеспечения	Навык 1: Установка программного обеспечения	Умения:
		1. Устанавливать программное обеспечение в соответствии с технической документацией 2. Использовать техническую документацию
		Знания:
		1. Порядка настройки программного обеспечения, систем управления базами данных 2. Порядка настройки программного обеспечения, систем управления базами данных и средств электронного документооборота
	Возможность признания навыка:	-
	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
		Знания:
		1. Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота 2. Методы, средства и системы защиты информации
	Возможность признания навыка:	-
Трудовая функция 2: Обслуживание программно-аппаратных средств защиты информации в операционных системах	Навык 1: Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	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. Обеспечивать безопасность информации при эксплуатации программного обеспечения
		Знания:
		1. Порядка настройки программного обеспечения, систем управления базами данных 2. Порядка настройки программного обеспечения средств электронного документооборота 3. Порядка эксплуатации средств антивирусной защиты 4. Порядка обеспечения безопасности информации при эксплуатации программного обеспечения
	Возможность признания навыка:	-

	Навык 2: Настройка встроенных средств защиты информации программного обеспечения по заданным шаблонам	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
		Знания:
		1. Порядка настройки программного обеспечения, систем управления базами данных и средств электронного документооборота 2. Порядка обеспечения безопасности информации при эксплуатации программного обеспечения 3. Языков программирования
	Возможность признания навыка:	-
Требования к личностным компетенциям:	Ответственность Гибкость мышления Умение работать в команде Дисциплинированность Инициативность Организованность Высокая обучаемость Внимательность Исполнительность Ориентация на результат	
Список технических регламентов и национальных стандартов:		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
	4	Инженер по защите информации
	4	Администратор по информационной безопасности
	6	Инженер по защите информации

14. 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:	5		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 185 Техник-программист		
Уровень профессионального образования:	Уровень образования: послесреднее образование (прикладной бакалавриат)	Специальность: Вычислительная техника и информационные сети (по видам)	Квалификация:
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:	Специалист по информационной безопасности Инженер по защите информации		
Основная цель деятельности:	Администрировать механизмы безопасности и своевременно реагировать на нарушения ИБ		

Описание трудовых функций		
Перечень трудовых функций:	Обязательные трудовые функции:	1. Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения ИБ 2. Администрирование механизмов безопасности 3. Реагирование на инциденты ИБ 4. Контроль и анализ эффективности применения ПАС зашиты информации и обеспечения ИБ
	Дополнительные трудовые функции:	
Трудовая функция 1: Администрирование, эксплуатация и поддержка работоспособности ПАС защиты информации и обеспечения ИБ	Навык 1: Эксплуатация ПАС защиты информации и обеспечения ИБ	Умения:
		1. Устанавливать и эксплуатировать ПАС защиты информации и обеспечения ИБ. 2. Проверять и оценивать соответствие реальных характеристик ПАС защиты информации и обеспечения ИБ, заявленным в ТД. 3. Эксплуатировать и поддерживать работоспособность ПАС защиты конфиденциальной информации. 4. Консультировать и инструктировать работников организации по вопросам, связанным с функционированием и правилами эксплуатации ПАС защиты информации и обеспечения ИБ.
		Знания:
		1. Принципов работы и правил эксплуатации ПАС защиты информации и обеспечения ИБ. 2. Принципов и способов обеспечения конфиденциальности информации. 3. Технологий и типов носителей информации. 4. Рекомендаций производителя средств защиты информации и обеспечения ИБ по их эксплуатации. 5. Методов и приемов консультирования и обучения.
	Возможность признания навыка:	-
	Навык 2: Техническое сопровождение (регламентные, восстановительные и профилактические работы)	Умения:
		1. Определять причины отказов в работе технических средств защиты информации и обеспечения ИБ. 2. Определять необходимые ресурсы, условий и факторы риска восстановления отказов технических средств защиты информации и обеспечения ИБ. 3. Устранять отказы и восстанавливать работоспособность систем защиты информации и обеспечения ИБ.
		Знания:
		1. Назначений, технических характеристик, конструкций, особенностей технических средств защиты информации и обеспечения ИБ. 2. Правил эксплуатации технических средств защиты информации и обеспечения ИБ. 3. Архитектур технических средств защиты информации
	Возможность признания навыка:	-

Навык 3: Администрирование антивирусного ПО	Умения:
	1. Удаленно устанавливать, обновлять, настраивать антивирусные программы и антивирусные базы. 2. Создавать и копировать на серверы сети дистрибутивы для централизованной установки антивирусов. 3. Обнаруживать новые рабочие станции, подключенные к корпоративной сети, с последующей автоматической установкой на эти станции антивирусных программ. 4. Планировать задания для немедленного или отложенного запуска на компьютерах сети. 5. Отображать в реальном времени процессы работы антивирусов на рабочих станциях и серверах сети.
	Знания:
	1. Назначений, видов и принципов действия антивирусных программ. 2. ТД, регламентирующих процесс антивирусной защиты. 3. Рекомендаций производителя антивирусного ПО по его установке и эксплуатации
Возможность признания навыка:	-
Навык 4: Администрирование системы управления событиями ИБ	Умения:
	1. Выполнять построение сетевой иерархии. 2. Использовать административные инструменты для управления профилями устройств, индексами, множествами ссылок. 3. Настраивать аккаунты пользователей и удаленную аутентификацию. 4. Настраивать резервное копирование, восстановления данных. 5. Настраивать политику удаления данных. 6. Управлять источниками журналов и сетевых пакетов. 7. Интегрировать агенты для сбора журналов. 8. Создавать собственные источники журналов. 9. Настраивать ложные срабатывания.
	Знания:
	1. Назначений, принципов действия, архитектур систем управления событиями ИБ. 2. Стандартов, регламентирующих функционирование систем управления событиями ИБ. 3. Функциональных возможностей средств для резервного копирования и ПО для ИБ 4. Языков программирования
Возможность признания навыка:	-
Навык 5: Администрирование системы обнаружения/ предотвращения вторжений	Умения:
	1. Выбирать объекты мониторинга, управлять блокировками, устанавливать пороговые значения. 2. Управлять и формировать политику доступа. 3. Управлять и разграничивать, сегментировать и фильтровать, ограничивать права доступа пользователей. 4. Управлять администраторами. 5. Конфигурировать параметры сетевого доступа. 6. Разрешать доступ с ограниченного количества хостов/подсетей. 7. Управлять обновлениями ПО.

	Знания:
	1. Назначений, принципов действия, архитектур систем обнаружения/ предотвращения вторжений. 2. Стандартов, регламентирующих функционирование систем обнаружения вторжений. 3. Рекомендаций производителя системы обнаружения/ предотвращения вторжений по ее установке и эксплуатации.
Возможность признания навыка:	-
Навык 6: Конфигурирование и настройка межсетевого экрана	Умения:
	1. Настраивать режимы работы межсетевого экрана. 2. Создавать учетную запись администратора, разграничивать права доступа. 3. Настраивать резервное копирование и восстановление. 4. Осуществлять настройку сервисов (DNS, DHCP и других внутренних сетевых сервисов). 5. Настраивать логирование и мониторинг событий. 6. Настраивать политику управления доступом и управлять информационными потоками (списки доступа, сегментирование сети, управлять сервисами). 7. Настраивать и отлаживать маршрутизации. 8. Настраивать виртуальные домены и сети. 9. Развертывать и настраивать отказоустойчивые решения. 10. Настраивать защищенные соединения IPsec VPN. 11. Настраивать политики аутентификации. 12. Управлять и применять криптографические сертификаты. 13. Настраивать и применять режимы диагностики. 14. Настраивать NGFW (антивируса, прокси-сервера, DLP, IDS, IPS).
	Знания:
	1. Назначений, базовых принципов функционирования межсетевых экранов 2. Работы стека протоколов TCP/IP. 3. Основ криптографии и шифрования
Возможность признания навыка:	-
Навык 7: Настройка системы защиты от утечек конфиденциальной информации	Умения:
	1. Устанавливать и настраивать серверную часть системы: - настраивать взаимодействие компонент системы; - настраивать интеграцию со SPAN- портом коммутатора, с почтовым сервером, с прокси-сервером, с ActiveDirectory; - настраивать базы контентной фильтрации; - настраивать правила и политику реакции системы. 2. Устанавливать клиентские компоненты на АРМ. 3. Устанавливать модули для контроля информации в общедоступных сетевых хранилищах.
	Знания:
	1. Назначений, принципов действия и архитектур систем защиты от утечек конфиденциальной информации. 2. Стандартов, регламентирующих системы защиты от утечек конфиденциальной информации. 3. Рекомендаций производителя системы защиты от утечек конфиденциальной информации.

	Возможность признания навыка:	-
	Навык 8: Ведение отчетной документации	Умения:
		1. Формировать требований к отчетной документации. 2. Вести отчетную документацию по результатам проведенных работ в процессе эксплуатации и технического сопровождения ПАС защиты информации и обеспечения ИБ
		Знания:
		1. Принципов формирования и ведения отчетной документации. 2. Программного обеспечения по формированию отчетной документации
	Возможность признания навыка:	-
Трудовая функция 2: Администрирование механизмов безопасности	Навык 1: Управление процессами по администрированию	Умения:
		1. Вырабатывать правила подбора механизмов безопасности (при наличии альтернатив). 2. Комбинировать механизмов для реализации сервисов безопасности. 3. Управлять сегментированием 4. Управлять взаимодействием с другими администраторами для обеспечения согласованной работы.
		Знания:
		1. Принципов функционирования и применения ПАС защиты информации и обеспечения ИБ. 2. Основных видов политик управления доступом и информационными потоками. 3. Технологии межличностной и групповой коммуникации в деловом взаимодействии. 4. Языков программирования
	Возможность признания навыка:	-
	Навык 2: Настройка политики безопасности ОС, СУБД, ППО	Умения:
		1. Управлять криптографическими ключами (генерация и распределение). 2. Управлять шифрованием (Устанавливать и синхронизировать криптографические параметры). 3. Управлять аутентификацией 4. Управлять доступом 5. Устанавливать и настраивать контролеры доменов сети. 6. Управлять трафиком 7. Управлять маршрутизацией 8. Управлять конфиденциальностью при хранении, передаче и обработке. 9. Управлять целостностью при хранении, передаче и обработке. 10. Управлять безотказностью отправления и получения информации.
		Знания:
		1. Встроенных механизмов безопасности ОС, СУБД 2. Принципов настроек политик ОС, СУБД 3. Принципов и особенностей построения ОС
	Возможность признания навыка:	-
Трудовая функция 3: Реагирование на инциденты		

ИБ	Навык 1: Мониторинг событий и инцидентов ИБ	Умения:
		1. Управлять инцидентами ИБ. 2. Собирать и анализировать события в системах, находящихся по мониторингом ИБ. 3. Классифицировать события, серийные события и сочетания событий как нарушения ИБ. 4. Настраивать процедуры обработки событий и обнаружение событий ИБ.
		Знания:
		1. НТД и ТД, регламентирующих 2. ПАС защиты информации и систем управления инцидентами ИБ. 3. Понятий событий и инцидентов ИБ, принципов.
	Возможность признания навыка:	-
	Навык 2: Реагирование на инциденты ИБ	Умения:
		1. Регистрировать и оповещать (информировать) об инциденте ИБ. 2. Определять причины инцидента ИБ. 3. Принимать меры к ликвидации инцидента ИБ и его последствий. 4. Собирать доказательства об инциденте. 5. Участвовать в проведении расследований инцидентов ИБ. 6. Взаимодействовать с компетентными органами (CERT, органы внутренних дел и другие).
		Знания:
		1. Процедур управления инцидентами ИБ. 2. Компетенций полномочных организаций в области ИБ.
	Возможность признания навыка:	-
Трудовая функция 4: Контроль и анализ эффективности применения ПАС зашиты информации и обеспечения ИБ	Навык 1: Текущий контроль технологического процесса обработки защищаемой информации	Умения:
		1. Контролировать целостность настроек механизмов безопасности ОС, СУБД, ППО на серверном и телекоммуникационном оборудовании. 2. Анализировать журналы регистрации событий системного и прикладного ПО с целью выявление попыток НСД к ИС и защищаемым информационным ресурсам. 3. Анализировать журналы регистрации событий системного и прикладного ПО с целью контроля действий администраторов ЛВС, ОС, СУБД, ППО. Контролировать за резервированием и дублированием ресурсов ИС и БД.
		Знания:
		1. Методов, принципов и приемов осуществления контроля. 2. Процедуры анализа журнала событий ИБ: выполнение задач анализа событий, проведение расследования, документирование выполнения процедур и сбор доказательств, формирование отчетности. 3. Программных средств анализа журналов событий ИБ.
	Возможность признания навыка:	-

	Навык 2: Текущий и периодический контроль работы ПАС защиты информации и обеспечения ИБ	Умения:	
		1. Анализировать журналы регистрации событий ПАС защиты информации и обеспечения ИБ. 2. Оценивать использование ресурсов ПАС зашиты информации и обеспечения ИБ. 3. Вырабатывать предложения по совершенствованию и повышению эффективности использования ПАС зашиты информации и обеспечения ИБ.	
		Знания:	
		1. Методов оценки эффективности применения организационных и технических средств обеспечения ИБ. 2. Критериев и показателей результативности использования ресурсов ПАС защиты информации и обеспечения ИБ.	
	Возможность признания навыка:	-	
Требования к личностным компетенциям:	Ответственность Гибкость мышления Умение работать в команде Дисциплинированность Организованность Внимательность Исполнительность		
Список технических регламентов и национальных стандартов:			
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	4	Администратор по информационной безопасности	
	5	Специалист по информационной безопасности	
	6	Инженер по защите информации	
15. 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:	5		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 185. Техник-программист		
Уровень профессионального образования:	Уровень образования: послесреднее образование (прикладной бакалавриат)	Специальность: Вычислительная техника и информационные сети (по видам)	Квалификация:
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:	Администратор по информационной безопасности Инженер по защите информации		
Основная цель деятельности:	Обеспечивать защиту данных организации		
Описание трудовых функций			

Перечень трудовых функций:	Обязательные трудовые функции:	1. Документирование процесса управления и обеспечения ИБ 2. Реализация мероприятий по автоматизации обработки информации 3. Контроль процессов управления и обеспечения ИБ организации 4. Использование ПАС обеспечения ИБ
	Дополнительные трудовые функции:	
Трудовая функция 1: Документирование процесса управления и обеспечения ИБ	Навык 1: Разработка (актуализация) нормативно- техническую документацию, регламентирующие процессы управления ИБ	Умения:
		1. Разрабатывать ТД процессов управления ИБ, охватывающие процессы управления (оценки) рисками, активами, инцидентами, техническими уязвимостями, угрозами, техническим противодействиям угрозам, непрерывностью бизнеса. 2. Разрабатывать шаблоны (макеты) политики ИБ
		Знания:
		1. НПА и НТД РК в сфере информатизации и ИБ. 2. Принципов оценки и управления рисками ИБ. 3. Способов анализа угроз и уязвимостей ИС.
	Возможность признания навыка:	-
	Навык 2: Разработка (актуализация) НТД, регламентирующих процессы обеспечения ИБ	Умения:
		1. Разрабатывать (актуализировать) ТД, регламентирующие процессы обеспечения ИБ 2. Разрабатывать профили защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры.
		Знания:
		1. Принципов защитных механизмов программных и аппаратных средств организации. 2. Общих представлений о современном отечественном и зарубежном опыте, инструментарии, методах и средствах обеспечения ИБ 3. Принципов и методологии проектирования ИС
	Возможность признания навыка:	-
Трудовая функция 2: Реализация мероприятий по автоматизации обработки информации	Навык 1: Категоризация активов, связанных с автоматизированной обработкой информации	Умения:
		1. Проводить инвентаризацию, классификацию, маркировку активов, связанных с автоматизированной обработкой информации
		Знания:
		1. НТД и методов классификации, учета и маркировки активов, связанных с обработкой информации
	Возможность признания навыка:	-
	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
		Знания:
		1. Методики и средства выявления каналов утечки информации. 2. НТД, методик выявления рисков и угроз ИБ.
	Возможность признания навыка:	-

	Навык 3: Анализировать рынок программно- технических средств обеспечения ИБ	Умения:
		1. Проводить маркетинговые исследования 2. Анализировать рынок программно- технических средств обеспечения ИБ
		Знания:
		1. Подходов к формированию требований и оценке безопасности ИС
	Возможность признания навыка:	-
Трудовая функция 3: Контроль процессов управления и обеспечения ИБ организации	Навык 1: Контролировать соблюдения исполнения требований ТД процессов управления ИБ	Умения:
		1. Контролировать соблюдения требований ТД процессов управления ИБ. 2. Составлять и оформлять акты контрольных проверок выполнения требований ТД процессов управления ИБ.
		Знания:
		1. ТД организации по ИБ. 2. Методов оценки результатов применения организационных и технических решений по обеспечению ИБ. 3. Основных способов контроля выполнения планов и мероприятий по обеспечению ИБ.
	Возможность признания навыка:	-
	Навык 2: Контролировать соответствия настроек функций безопасности компонентов ИС и ИКИ установленным требованиям	Умения:
		1. Осуществлять контроль разделения сред разработки, тестирования и эксплуатации ИС; 2. Осуществлять текущий контроль технологического процесса обработки защищаемой информации. 3. Контролировать реализацию профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры.
		Знания:
		1. Базовых принципов и способов выполнения работ по разработке, тестирования 2. Правил эксплуатации программных средств защитных механизмов компонентов ИС и ИКИ.
	Возможность признания навыка:	-
	Навык 3: Консультирование и инструктаж работников организации по вопросам, связанным с обеспечением ИБ	Умения:
		1. Консультировать работников организации по вопросам, связанным с обеспечением ИБ. 2. Инструктировать работников организации по вопросам, связанным с обеспечением ИБ.
		Знания:
		1. Методик и приемов консультирования и обучения.
	Возможность признания навыка:	-
Трудовая функция 4: Использование ПАС обеспечения ИБ		

	Навык 1: Эксплуатация ПАС обеспечения ИБ и систем мониторинга	Умения:
		1. Устанавливать и настраивать, обеспечивать работоспособность аппаратно-программные средства обеспечения ИБ. 2. Конфигурировать аппаратно- программные средства обеспечения ИБ. 3. Администрировать систему мониторинга уязвимостей, систему мониторинга ИБ и систему предотвращения утечек информации, антивирусной защиты, обновления антивирусных баз. 4. Проводить мониторинг событий ИБ и инцидентов ИБ. 5. Оповещать о критических (аварийных) ситуациях и событиях ИБ.
		Знания:
		1. Принципов и средств администрирования в ОС и встроенных в них механизмов защиты. 2. Принципов функционирования ПАС обеспечения ИБ. 3. Принципов построения и применения, систем мониторинга уязвимостей, систем мониторинга ИБ 4. Систем предотвращения утечек информации. 5. Методов определения, предотвращения и устранения последствий инцидентов ИБ, критических (аварийных) ситуаций.
	Возможность признания навыка:	-
	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.
		Знания:
		1. Назначений, технических характеристик, конструкций, особенностей СКУД и систем видеонаблюдения. 2. Правил эксплуатации СКУД и систем видеонаблюдения.
	Возможность признания навыка:	-
	Навык 3: Ведение отчетной документации	Умения:
		1. Формировать отчетную документацию по результатам проведенных работ по обеспечению ИБ.
		Знания:
		1. Принципов формирования и ведения технической и отчетной документации.
	Возможность признания навыка:	-
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:		
Связь с другими	Уровень ОРК:	Наименование профессии:

профессиями в рамках ОРК:	4	Специалист по информационной безопасности	
	5	Администратор по информационной безопасности	
	6	Специалист по информационной безопасности	
16. 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:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 140 Инженер-программист (программист)		
Уровень профессионального образования:	Уровень образования: высшее образование (бакалавриат, специалитет, ординатура)	Специальность: Информационная безопасность	Квалификация: -
	Уровень образования: высшее образование (бакалавриат, специалитет, ординатура)	Специальность: Информационно-коммуникационные технологии	Квалификация: -
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:			
Основная цель деятельности:	Производить поиск и обнаруживать уязвимые места системы для несанкционированного доступа		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Взаимодействие с разработчиками и менеджерами сервисов для устранения обнаруженных уязвимостей 2. Выступление консультантом и заказчиком новой функциональности, связанной с информационной безопасностью 3. Проведение семинаров и участие в исследовательской работе	
	Дополнительные трудовые функции:		
Трудовая функция 1: Взаимодействие с разработчиками и менеджерами сервисов для устранения обнаруженных уязвимостей	Навык 1: Сбор и анализ информации об обнаруженных уязвимостях сервисов	Умения:	
		1. Собирать и хранить информацию 2. Обрабатывать количественные данные 3. Вести реестр вопросов потенциальных пользователей сервисов	
		Знания:	
		1. Основ маркетинга 2. Методов проведения количественных и качественных исследований потребителя 3. Принципов взаимодействия с пользователями сервисов 4. Технических средств сбора, обработки и хранения текстовой информации	
	Возможность признания навыка:	-	

	Навык 2: Постановка и прием задачи по устранению обнаруженных уязвимостей сервисов	Умения:
		1. Сформулировать задачи 2. Разрабатывать требования 3. Разрабатывать бизнес-планы 4. Создавать концепции
		Знания:
		1. Основ информационных технологий 2. Методов системного анализа
	Возможность признания навыка:	-
Трудовая функция 2: Выступление консультантом и заказчиком новой функциональности, связанной с информационной безопасностью	Навык 1: Подготовка и размещение публикаций и сообщений о сервисах в средствах массовой информации и других открытых доступных источниках	Умения:
		1. Владеть компьютерной техникой и средствами ввода 2. Писать тексты литературным, техническим и рекламным языком. 3. Владеть текстовым редактором и навыками работы с множеством документов, стилями, таблицами, списками, заголовками и другими элементами форматирования
		Знания:
		1. Стандартов распространенных форматов текстовых и табличных данных 2. Методов создания рекламных текстов 3. Законодательства РК в области интеллектуальной собственности. 4. Правил использования информационных материалов в Интернет
	Возможность признания навыка:	-
	Навык 2: Проведение демонстрации возможностей продукта	Умения:
		1. Владеть инструментами подготовки презентаций. 2. Проводить публичные презентации. 3. Организовывать презентации. 4. Проводить консультации.
		Знания:
		1. Устройства и возможности продукта 2. Теории управления программами 3. Теории показателей эффективности
	Возможность признания навыка:	-
Трудовая функция 3: Проведение семинаров и участие в исследовательской работе	Навык 1: Проведение семинаров	Умения:
		1. Проводить публичные выступления 2. Проводить совещания 3. Организовывать обучающие семинары
		Знания:
		1. Принципов и способов проведения совещаний и презентаций 2. Принципов и методик управления конфликтами 3. Методов и технологий обучения
	Возможность признания навыка:	-

	Навык 2: Участие в исследовательской работе	Умения:	
		1. Проводить исследования 2. Оформлять результаты исследований в соответствии с международными и национальными стандартами (IEEE, ГОСТ, СТ РК).	
		Знания:	
		1. Основ информационных технологий 2. Методов статистического моделирования 3. Основ криптографии 4. Языков программирования 5. Основ математического и компьютерного моделирования	
	Возможность признания навыка:	-	
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:			
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	5	Специалист по информационной безопасности	
	6	Аудитор по информационной безопасности	
17. 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:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 140 Инженер-программист (программист)		
Уровень профессионального образования:	Уровень образования: высшее образование (бакалавриат, специалитет, ординатура)	Специальность: Информационная безопасность	Квалификация: -
	Уровень образования: высшее образование (бакалавриат, специалитет, ординатура)	Специальность: Информационно-коммуникационные технологии	Квалификация: -
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:			

Основная цель деятельности:	Проводить аудиторскую проверку по определению уровней безопасности	
Описание трудовых функций		
Перечень трудовых функций:	Обязательные трудовые функции:	1. Планирование задач аудиторского задания 2. Обеспечение задач аудиторского задания 3. Выполнение задач аудиторского задания
	Дополнительные трудовые функции:	
Трудовая функция 1: Планирование задач аудиторского задания	Навык 1: Планирование работы аудитора ИБ	Умения:
		1. Планировать работы аудитора ИБ. 2. Оценивать применимость методик проведения аудита.
		Знания:
		1. Методологических основ аудиторской деятельности. 2. Методов организации аудиторских проверок. 3. Способов, методов и техники проведения аудита.
	Возможность признания навыка:	-
	Навык 2: Планирование аудиторской проверки	Умения:
		1. Определять объемы, масштабы аудита. 2. Определять ресурсы, необходимые для выполнения аудиторского задания. 3. Готовить и согласовывать план и программы выполнения аудиторского задания.
		Знания:
		1. НТД аудиторской деятельности. 2. Методологии, методики и технологии планирования аудита. 3. Стандартов (республиканских и международных) по аудиторской деятельности
	Возможность признания навыка:	-
Трудовая функция 2: Обеспечение задач аудиторского задания	Навык 1: Методическое обеспечение аудита ИБ	Умения:
		1. Участвовать в разработке (актуализации) методических и организационно-распорядительных документов, регламентирующих аудиторскую деятельность. 2. Поводить презентации методических и организационно-распорядительных документов 3. Проводить ознакомление сотрудников с регламентирующей документацией
		Знания:
		1. Порядка разработки, оформления и утверждения методических и организационно-распорядительных документов. 2. НТД (Республики Казахстан и международные стандарты) по аудиторской деятельности.
	Возможность признания навыка:	-
	Навык 2: Организационное обеспечение аудита ИБ	Умения:
		1. Участвовать в организации взаимодействия с представителями проверяемой организации (подразделения) по вопросам аудита ИБ. 2. Проводить аудит ИБ
		Знания:
		1. Этапов и форм деловой коммуникации. 2. Принципов и правил общения в деловой среде

	Возможность признания навыка:	-
	Навык 3: Консультирование и инструктаж работников организации по вопросам аудита ИБ	Умения:
		1. Консультировать работников проверяемой организации (подразделения) по вопросам, связанным с аудиторским заданием. 2. Проводить инструктаж работников по вопросам аудита
		Знания:
		1. НТД по аудиторской деятельности. 2. Методики проведения аудита. 3. Основных принципов, методов и средства обеспечения ИБ. 4. Основных НПА Республики Казахстан в сфере информатизации, ИБ. 5. национальных, международных и межгосударственных НТД по вопросам обеспечения ИБ. 6. Методов контроля и анализа защищенности объектов аудита.
	Возможность признания навыка:	-
Трудовая функция 3: Выполнение задач аудиторского задания	Навык 1: Проверка и анализ соответствия проектной, эксплуатационной, ТД по ИБ требованиям НПА и НТД в сфере ИКТ и обеспечения ИБ объекта аудита ИБ	Умения:
		1. Оценивать применимость НПА и НТД к объекту аудита ИБ. 2. Оценивать соответствие принятых организационных и программно- технических решений обеспечения ИБ требованиям НПА и НТД.
		Знания:
		1. НПА и НТД в сфере ИКТ и обеспечения ИБ. 2. Методики проведения испытаний и экспертизы ТД.
	Возможность признания навыка:	-
	Навык 2: Проверка и анализ фактического соблюдения требований НПА и НТД в сфере ИКТ и обеспечения ИБ в процессах обеспечения ИБ объекта аудита ИБ	Умения:
		1. Собирать и изучать проектную и эксплуатационную документации на ИС, интервьюировать сотрудников и регистрировать сведения. 2. Оценивать применимость НПА и НТД к объекту аудита ИБ. 3. Оценивать соответствия принятых организационных и программно- технических решений обеспечения ИБ требованиям НПА и НТД. 4. Определять и оценивать вероятные угрозы безопасности в отношении ресурсов объекта аудита и уязвимостей защиты. 5. Анализировать риски, связанные с возможностью осуществления угроз безопасности в отношении ресурсов объекта аудита ИБ. 6. Выявлять узкие места в системе защиты и архитектуре объекта аудита ИБ.
		Знания:
		1. НПА и НТД в сфере ИКТ и обеспечения ИБ. 2. НТД, методик, программных средств выявления рисков и угроз ИБ. 3. Методов, процедур и порядка сбора аудиторских свидетельств.
	Возможность признания навыка:	-

Навык 3: Проверка и анализ текущего состояния защищенности объекта аудита ИБ	Умения:
	1. Проверять состояние физической безопасности объекта аудита. 2. Проверять характеристики безопасности объекта аудита, связанные с архитектурой. 3. Проверять характеристики безопасности, связанные с конфигурацией встроенных механизмов ИБ серверного и сетевого оборудования объекта аудита. 4. Проверять конфигурации ПО на наличие эксплуатационных уязвимостей.
	Знания:
	1. Методов предотвращения сетевых атак. 2. Методов анализа защищенности внешнего периметра корпоративной сети. 3. Методов анализа защищенности внутренней ИТ-инфраструктуры объекта аудита. 4. Методов и порядка проведения тестирования ПО.
Возможность признания навыка:	-
Навык 4: Выявление уязвимостей программного обеспечения объекта аудита	Умения:
	1. Проводить статический анализ исходного кода ПО 2. Проводить динамический анализ исходного кода
	Знания:
	1. Программных средств обнаружения недостатков ПО. 2. Методов статического анализа программного кода. 3. Методов динамического анализа программного кода. 4. Инструментальных средств анализа защищенности и уязвимостей. 5. Языков программирования
Возможность признания навыка:	-
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 поведения 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. Методов и программных средств анализа защищенности и уязвимостей. 2. Методов и программных средств для проведения нагрузочного тестирования. 3. Методов и программных средств для проведения отладки программ. 4. Языков программирования
Возможность признания навыка:	-

	Навык 6: Выявление уязвимостей оборудования сети объекта аудита	Умения:
		1. Идентифицировать и инвентаризовать ресурсы сети. 2. Идентифицировать и учитывать сервисы и информационные потоки сети. 3. Сканировать уязвимости уровня ОС хостов сети в сегментах сети. 4. Идентифицировать и учитывать настройки безопасности сегментов сети. 5. Создавать и анализировать отчеты о соответствии стандартам ИБ.
		Знания:
		1. Методов и программных средств анализа защищенности и уязвимостей. 2. Техники инвентаризации ресурсов сети
	Возможность признания навыка:	-
	Навык 7: Документирование процесса и результата выполнения задачи аудиторского задания	Умения:
		1. Формировать, вести, хранить рабочую документацию аудиторского задания. 2. Готовить итоговый документ, формируемый по результатам аудиторского задания
		Знания:
		1. Принципов формирования и ведения рабочей и отчетной документации. 2. Методов систематизации и обобщения результатов аудита.
	Возможность признания навыка:	-
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:		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
	7	Аудитор по информационной безопасности
18. 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:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 140 Инженер-программист (программист)	

Уровень профессионального образования:	Уровень образования: высшее образование (бакалавриат, специалитет, ординатура)	Специальность: Информационная безопасность	Квалификация: -
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
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 3. Сопровождение системы защиты информации в ходе ее эксплуатации	
	Дополнительные трудовые функции:		
Трудовая функция 1: Создание системы защиты информации в организации	Навык 1: Определение перечня информации (сведений) ограниченного доступа, подлежащих защите в организации	Умения:	
		1. Определять перечень информации (сведений) ограниченного доступа 2. Определять степень участия персонала в обработке (обсуждении, передаче, хранении) информации	
		Знания:	
		1. Нормативно-правовых актов, методических документов, национальных стандартов в области защиты информации 2. Организационно-распорядительной документации по защите информации	
	Возможность признания навыка:	-	
	Навык 2: Анализ данных о назначении, функциях, условиях функционирования технических средств обработки информации ограниченного доступа	Умения:	
		1. Определять степень участия персонала в обработке (обсуждении, передаче, хранении) информации 2. Анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем	
		Знания:	
		1. Эксплуатационной документации на систему защиты информации 2. Типов, категорий, видов и уровней градации (категорирования) информации	
	Возможность признания навыка:	-	
	Навык 3: Разработка модели угроз безопасности информации в организации	Умения:	
		1. Разрабатывать модели угроз безопасности информации в организации 2. Использовать программные средства разработки модели угроз 3. Разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации 4. Разрабатывать проекты систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием	

		Знания:
		1. Нормативно-правовых актов, методических документов, национальных стандартов в области защиты информации ограниченного доступа 2. Методов и методик контроля эффективности защиты информации 3. Организационно-распорядительной документация по защите информации
	Возможность признания навыка:	-
	Навык 4: Разработка технического задания на создание системы защиты информации	Умения:
		1. Разрабатывать эксплуатационную документацию на объект информатизации и средства защиты информации 2. Разрабатывать техническое задание системы
		Знания:
		1. Программных (программно- технических) средств защиты 2. Современных информационных технологий (операционные системы, базы данных, вычислительные сети) 3. Стандартов ЕСКД, ЕСТД и ЕСПД 4. Методов, средств и систем защиты информации
	Возможность признания навыка:	-
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-правовых актов, методических документов, национальных стандартов в области защиты информации 2. Методов, средств и систем защиты информации 3. Архитектуры технических средств защиты информации
	Возможность признания навыка:	-
	Навык 2: Организация проведения инструктажа руководящего состава и обучения персонала по вопросам технической защиты информации	Умения:
		1. Организовывать обучение персонала использованию технических, программных (программно- технических) средств защиты информации 2. Проводить инструктаж по вопросам технической защиты информации
		Знания:
		1. Организационно-распорядительных документов 2. Методики инструктирования персонала
	Возможность признания навыка:	-

	Навык 3: Организация опытной эксплуатации и доработки системы защиты информации	Умения:
		1. Разрабатывать программы и методики предварительных испытаний 2. Организовывать опытную эксплуатацию и доработку системы защиты информации 3. Разрабатывать программы и методики предварительных испытаний системы защиты информации
		Знания:
		1. Нормативно-правовых актов, методических документы, национальных стандартов в области защиты информации 2. Стандартов ЕСКД, ЕСТД и ЕСПД 3. Методов, средств и систем защиты информации 4. Языков программирования
	Возможность признания навыка:	-
	Навык 4: Ввод системы защиты информации в эксплуатацию	Умения:
		1. Разрабатывать программы и методики предварительных испытаний 2. Организовывать приемочные испытания системы защиты информации 3. Организовывать ввод системы защиты информации в эксплуатацию
		Знания:
		1. Нормативно-правовых актов, методических документов, национальных стандартов в области защиты информации 2. Стандартов ЕСКД, ЕСТД и ЕСПД 3. Современных информационных технологий 4. Типов, категорий, видов и уровней градации (категорирования) информации
	Возможность признания навыка:	-
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. Современных информационных технологий 2. Нормативно-правовых актов, методических документов, национальных стандартов в области защиты информации 3. Методов, средств и систем защиты информации
	Возможность признания навыка:	-

	Навык 2: Организация мероприятий техническому обслуживанию и по выводу из эксплуатации систем информатизации и утилизации их элементов	Умения:	
		1. Организовать работы по техническому обслуживанию технических и программно- технических средств защиты информации 2. Организовывать проведение и руководить выполнением работ по выводу из эксплуатации 3. Утилизировать ПО и технические средства, выведенные из эксплуатации	
		Знания:	
		1. Нормативно-правовых актов, методических документов, национальных стандартов в области защиты информации	
	Возможность признания навыка:	-	
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:			
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:	
	5	Инженер по защите информации	
19. Карточка профессии «Специалист по информационной безопасности»:			
Код группы:	2524-0		
Код наименования занятия:	2524-0-007		
Наименование профессии:	Специалист по информационной безопасности		
Уровень квалификации по ОРК:	6		
подуровень квалификации по ОРК:			
Уровень квалификации по ЕТКС, КС и др типовых квалификационных характеристик:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. 140 Инженер-программист (программист)		
Уровень профессионального образования:	Уровень образования: высшее образование (бакалавриат, специалитет, ординатура)	Специальность: Информационная безопасность	Квалификация: -
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:	Администратор по информационной безопасности Инженер по защите информации		
Основная цель деятельности:	Контролировать процесс управления и обеспечения ИБ организации		
Описание трудовых функций			

Перечень трудовых функций:	Обязательные трудовые функции:	1. Координирование процессов управления и обеспечения ИБ организации 2. Управление мероприятием по обеспечению ИБ организации 3. Анализ и контроль мероприятий по управлению и обеспечению ИБ 4. Обеспечение ИБ
	Дополнительные трудовые функции:	
Трудовая функция 1: Координирование процессов управления и обеспечения ИБ организации	Навык 1: Методическое обеспечение процессов управления и обеспечения ИБ организации	Умения:
		1. Координировать деятельность по разработке (актуализации) политики ИБ, ТД процессов управления ИБ и документов, регламентирующих процессы обеспечения ИБ. 2. Публиковать и доводить утвержденную (актуализированной) политику ИБ организации до сведения сотрудников. 3. Участвовать в разработке соглашений о конфиденциальности или неразглашении информации с сотрудниками организации, подрядчиками и третьими сторонами
		Знания:
		1. Базовых принципов регламентации бизнес-процессов. 2. НПА РК в сфере информатизации, ИБ. 3. Национальных, международных, межгосударственных НТД в области ИТ, ИБ, защиты информации и криптографии.
	Возможность признания навыка:	-
	Навык 2: Риск-менеджмент при планировании процессов управления и обеспечения ИБ организации	Умения:
		1. Координировать аналитическую работу по ИБ. 2. Анализировать, выбирать методику и методы оценки и реализации процессов управления ИБ.
		Знания:
		1. Методики оценки и управления рисками ИБ. 2. Методик анализа угроз и уязвимостей ИС
	Возможность признания навыка:	-
Трудовая функция 2: Управление мероприятием по обеспечению ИБ организации	Навык 1: Подготовка планов мероприятий по обеспечению ИБ организации	Умения:
		1. Анализировать защищенности бизнес- процессов и активов, связанных с автоматизированной обработкой информации. 2. Выбирать инструментарий и методы обеспечения ИБ. 3. Разрабатывать мероприятия, направленные на реализацию политики ИБ организации. 4. Составлять план по обеспечению непрерывности бизнеса и восстановления после инцидентов ИБ и форс-мажорных ситуаций.

		Знания:
		1. Основных тенденции развития отечественного и зарубежного рынка инструментария и средств обеспечения ИБ. 2. Принципов и методов выявления и блокирования каналов утечки информации. 3. НТД и методов классификации, учета и маркировки активов, связанных с обработкой информации. 4. НТД в сфере обеспечения непрерывности бизнес-процессов
	Возможность признания навыка:	-
	Навык 2: Подготовка технической документации для осуществления закупок оборудования, программных средств и систем (подсистем)	Умения:
		1. Разрабатывать технические спецификации, тендерную документацию на закупаемые средства обеспечения ИБ. 2. Разрабатывать требования, технические задания на подсистемы ИБ ИС. 3. Организовывать и координировать работы по разработке профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры.
		Знания:
		1. Подходов к формированию требований и оценке безопасности ИС. 2. Принципов и методологии проектирования ИС. 3. Способов применения защитных механизмов программных и аппаратных средств организации.
	Возможность признания навыка:	-
Трудовая функция 3: Анализ и контроль мероприятий по управлению и обеспечению ИБ	Навык 1: Контроль процессов управления и обеспечения ИБ организации	Умения:
		1. Анализировать процессы управления и обеспечения ИБ 2. Осуществлять контроль реализации плана мероприятий по обеспечению ИБ. 3. Анализировать результаты проверок исполнения требований документов, регламентирующих процессы обеспечения ИБ и ТД процессов управления ИБ в организации.
		Знания:
		1. Методики оценки результатов применения организационных и технических решений по обеспечению ИБ. 2. Методики контроля выполнения планов и мероприятий по контролю процессов управления и обеспечения ИБ организации.
	Возможность признания навыка:	-
Трудовая функция 4: Обеспечение ИБ	Навык 1: Оценка эффективности применяемых средств обеспечения и мониторинга ИБ	Умения:
		1. Оценивать эффективность применяемых аппаратно-программных средств обеспечения ИБ, систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации, антивирусной защиты. 2. Анализировать эффективность применения методов обеспечения ИБ. 3. Контролировать выполнение планов технического противодействия угрозам информации организации. 4. Разрабатывать предложения по совершенствованию (развитию) и повышению эффективности применяемых средств и методов обеспечения ИБ.

		Знания:
		1. Методов оценки эффективности применения организационных и технических средств обеспечения ИБ. 2. Принципов построения и применения ПАС обеспечения ИБ, систем мониторинга уязвимостей, систем мониторинга информационной безопасности и систем предотвращения утечек информации. 3. Способов анализа процессов обеспечения ИБ организации.
	Возможность признания навыка:	-
	Навык 2: Управлять процессами мониторинга событий ИБ	Умения:
		1. Разрабатывать политики для систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации. 2. Реагировать на инциденты ИБ организации.
		Знания:
		1. Методик оценки эффективности применения организационных и технических средств обеспечения ИБ. 2. Принципов функционирования и администрирования ОС и встроенных в них механизмов защиты. 3. Принципов анализа методов определения, предотвращения и устранения последствий инцидентов ИБ, критических (аварийных) ситуаций. 4. Порядка реагирования и проведения расследования инцидента ИБ, принципов и способов регистрации событий и инцидентов ИБ.
	Возможность признания навыка:	-
	Навык 3: Организация взаимодействия с полномочными организациями по вопросам ИБ.	Умения:
		1. Организовывать взаимодействии с полномочными организациями по вопросам ИБ.
		Знания:
		1. Компетенций полномочных организаций по вопросам ИБ. 2. Этапов и форм деловой коммуникации. 3. Принципов и правил общения в деловой среде.
	Возможность признания навыка:	-
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:		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
	5	Специалист по информационной безопасности
	5	Администратор по информационной безопасности
20. 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:	Квалификационный справочник должностей руководителей, специалистов и иных служащих Приказ Министра труда и социальной защиты населения Республики Казахстан от 30 декабря 2020 года № 553 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих". Зарегистрирован в Министерстве юстиции Республики Казахстан 31 декабря 2020 года № 22003. Инженер-программист (программист)		
Уровень профессионального образования:	Уровень образования: послевузовское образование (магистратура, резидентура)	Специальность: Информационная безопасность	Квалификация: -
	Уровень образования: послевузовское образование (магистратура, резидентура)	Специальность: Информационно-коммуникационные технологии	Квалификация: -
Требования к опыту работы:			
Связь с неформальным и информальным образованием:			
Другие возможные наименования профессии:			
Основная цель деятельности:	Планировать и контролировать аудит ИБ		
Описание трудовых функций			
Перечень трудовых функций:	Обязательные трудовые функции:	1. Планирование аудита ИБ 2. Обеспечение аудита ИБ 3. Контроль аудита ИБ 4. Выполнение аудиторского задания	
	Дополнительные трудовые функции:		
Трудовая функция 1: Планирование аудита ИБ	Навык 1: Планирование работы подразделения аудита ИБ	Умения:	
		1. Планировать работы подразделения аудита ИБ. 2. Анализировать, выбирать (разрабатывать) методику проведения аудита. 3. Управлять проектами.	
		Знания:	
		1. Методологических основ аудиторской деятельности. 2. Методов организации аудиторских проверок. 3. Способов, методов и техники проведения аудита.	
	Возможность признания навыка:	-	
	Навык 2: Планирование аудиторской проверки	Умения:	
		1. Определять объемы, масштабы аудита. 2. Определять ресурсы, необходимые для выполнения аудита. 3. Подбирать (назначать) членов аудиторской группы. 4. Распределять аудиторские задания и устанавливать конкретные сроки их выполнения. 5. Готовить и согласовывать план и программу проведения аудита ИБ.	

		Знания:
		1. НТД по аудиторской деятельности. 2. Методологии, методики и технологии планирования аудита. 3. Методики управления проектами.
	Возможность признания навыка:	-
Трудовая функция 2: Обеспечение аудита ИБ	Навык 1: Методическое обеспечение аудита ИБ	Умения:
		1. Разрабатывать (актуализировать), согласовывать методические и организационно-распорядительные документы, регламентирующие аудиторскую деятельность. 2. Управлять разработкой методических документов
		Знания:
		1. Порядка разработки, оформления, согласования и утверждения методических и организационно-распорядительных документов. 2. НТД по аудиторской деятельности.
	Возможность признания навыка:	-
	Навык 2: Организационное обеспечение ИБ	Умения:
		1. Организовывать взаимодействие с представителями проверяемой организации (подразделения) по вопросам аудита ИБ. 2. Организовывать обучение и повышение квалификации аудиторов ИБ. 3. Управлять аудиторской деятельностью
		Знания:
		1. Этапов и форм деловой коммуникации. 2. Принципов и правил общения в деловой среде. 3. Форм и методов обучения и повышения квалификации персонала на рабочем месте. 4. Этапов процесса обучения и повышения квалификации персонала
	Возможность признания навыка:	-
	Навык 3: Консультирование и инструктаж работников организации по вопросам аудита ИБ	Умения:
		1. Консультировать работников проверяемой организации (подразделения) по вопросам, связанным с аудитом ИБ. 2. Консультировать участников аудиторской группы по нерешенным сложным и спорным вопросам, связанным с выполнением аудиторского задания. 3. Инструктировать аудиторскую группу перед заданием с целью уяснения и понимания ее членами целей и задач.
		Знания:
		1. НТД по аудиторской деятельности. 2. Методики проведения аудита. 3. Основных принципов, методов и средства обеспечения ИБ. 4. Основных НПА Республики Казахстан в сфере информатизации, ИБ. 5. Национальных, международных и межгосударственных НТД по вопросам обеспечения ИБ. 6. Методов контроля и анализа защищенности объектов аудита.

	Возможность признания навыка:	-
Трудовая функция 3: Контроль аудита ИБ	Навык 1: Контроль аудиторского задания	Умения:
		1. Контролировать сроки выполнения процедур аудиторского задания. 2. Контролировать качество выполнения процедур аудиторского задания. 3. Контролировать соблюдение аудиторами организационно- распорядительных документов, регламентирующих аудиторскую деятельность.
		Знания:
		1. Методики контроля качества аудиторских заданий. 2. НТД по аудиторской деятельности.
	Возможность признания навыка:	-
	Навык 2: Контроль профессиональных качеств аудитора	Умения:
		1. Контролировать соблюдение аудиторами ИБ правил независимости и принципов этики при выполнении аудиторских заданий. 2. Анализировать и оценивать профессиональные знания и качество аудиторов ИБ.
		Знания:
		1. Международных стандартов контроля качества аудита. 2. Нормативно-правовых акты аудита
	Возможность признания навыка:	-
	Навык 3: Контроль результатов аудиторского задания	Умения:
		1. Анализировать результаты аудита ИБ. 2. Утверждать итоговый документ, формируемый по результатам аудита ИБ.
		Знания:
		1. Методов оценки эффективности применения организационных и технических средств обеспечения ИБ
	Возможность признания навыка:	-
Трудовая функция 4: Выполнение аудиторского задания	Навык 1: Проверка и анализ соответствия проектной, эксплуатационной ТД по ИБ требованиям НПА и НТД в сфере ИКТ и обеспечения ИБ объекта аудита ИБ	Умения:
		1. Оценивать применимость НПА и НТД к объекту аудита ИБ. 2. Оценивать соответствие принятых организационных и программно- технических решений обеспечения ИБ требованиям НПА и НТД.
		Знания:
		1. НПА и НТД в сфере ИКТ и обеспечения ИБ. 2. Методов проведения испытаний и экспертизы ТД.
	Возможность признания навыка:	-
	Навык 2: Проверка и анализ фактического соблюдения требований НПА и НТД в сфере ИКТ и обеспечения ИБ в процессах обеспечения ИБ объекта аудита ИБ	Умения:
		1. Собирать и изучать проектную и эксплуатационную документацию на ИС, интервьюировать сотрудников и регистрировать сведения. 2. Оценивать применимость НПА и НТД к объекту аудита ИБ. 3. Оценивать соответствие принятых организационных и программно- технических решений обеспечения ИБ требованиям НПА и НТД.

		Знания:
		1. НПА и НТД в сфере ИКТ и обеспечения ИБ. 2. НТД, методик, программных средств выявления рисков и угроз ИБ. 3. Методов, процедур и порядка сбора аудиторских свидетельств.
	Возможность признания навыка:	-
	Навык 3: Проверка и анализ текущего состояния защищенности объекта аудита ИБ	Умения:
		1. Проверять состояние физической безопасности объекта аудита. 2. Проверять характеристики безопасности объекта аудита, связанные с архитектурой и конфигурацией встроенных механизмов ИБ серверного и сетевого оборудования объекта аудита. 3. Определять и оценивать вероятные угрозы безопасности в отношении ресурсов объекта аудита и уязвимостей защиты. 4. Анализировать риски, связанные с возможностью осуществления угроз безопасности в отношении ресурсов объекта аудита ИБ. 5. Выявлять узкие места в системе защиты и архитектуре объекта аудита ИБ.
		Знания:
		1. Методов предотвращения сетевых атак. 2. Методов анализа защищенности внешнего периметра корпоративной сети. 3. Методов анализа защищенности внутренней ИТ-инфраструктуры объекта аудита
	Возможность признания навыка:	-
	Навык 4: Выявление уязвимостей программного обеспечения объекта аудита	Умения:
		1. Проводить статический анализ исходного кода ПО. 2. Проводить верификацию исходного кода
		Знания:
		1. Программных средств обнаружения недостатков ПО. 2. Методов статического анализа программного кода. 3. Методов динамического анализа программного кода. 4. Инструментальных средств верификации 5. Языков программирования
	Возможность признания навыка:	-
	Навык 5: Тестирование ПО на работоспособность в различных режимах нагрузки	Умения:
		1. Составлять сценарии тестирования ПО по принципам «черного ящика» и «белого ящика».. 2. Выполнять сценарии тестирования ПО в тестовой и 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. Принципов тестирования 2. Сценариев тестирования 3. Методов и программных средств для проведения нагрузочного тестирования. 4. Методов и программных средств для проведения отладки программ. 5. Языков программирования
	Возможность признания навыка:	-
	Навык 6: Выявление уязвимостей оборудования сети объекта аудита	Умения:
		1. Идентификация и инвентаризация ресурсов сети. 2. Идентификация и учет сервисов и информационных потоков сети. 3. Сканирование уязвимостей уровни операционной системы хостов сети в сегментах сети. 4. Идентификация и учет настроек безопасности сегментов сети. 5. Создание и анализ отчетов о соответствии стандартам ИБ.
		Знания:
		1. Характеристик ресурсов сети 2. Методов и программных средств анализа защищенности и уязвимостей. 3. Языков программирования
	Возможность признания навыка:	-
	Навык 7: Документирование процесса и результата аудиторской проверки	Умения:
		1. Формировать, вести, хранить рабочую документацию аудита. 2. Готовить итоговый документ, формируемый по результатам аудита ИБ, содержащего аргументированные (подкрепленные результатами анализа). 3. Оценивать эффективность системы защиты объекта аудита
		Знания:
		1. Принципов формирования и ведения рабочей и отчетной документации. 2. Методов систематизации и обобщения результатов аудита.
	Возможность признания навыка:	-
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:		
Связь с другими профессиями в рамках ОРК:	Уровень ОРК:	Наименование профессии:
	6	Аудитор по информационной безопасности

Глава 4. Технические данные профессионального стандарта

21. Наименование государственного органа:
Министерство искусственного интеллекта и цифрового развития Республики Казахстан
Исполнитель:

, ,
22. Организации (предприятия) участвующие в разработке:

23. Отраслевой совет по профессиональным квалификациям:
24. Национальный орган по профессиональным квалификациям: -
25. Национальная палата предпринимателей Республики Казахстан «Атамекен»: -
26. Номер версии и год выпуска: версия 2, 2022 г.
27. Дата ориентировочного пересмотра: 05.12.2025 г.