Приложение № 34
к приказу Заместителя Председателя
Правления Национальной палаты
предпринимателей
Республики Казахстан «Атамекен»
от 24.12.2019г. № 259

Профессиональный стандарт
«Обеспечение безопасности информационной инфраструктуры и ИТ»

Глоссарий

В настоящем профессиональном стандарте применяются следующие термины и определения:

Информационная система (ИС) – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач.

Информационная технология (ИТ, IT) – это процесс, использующий совокупность средств и методов сбора, обработки и передачи данных для получения информации нового качества о состоянии объекта, процесса или явления. Информационные технологии (ИТ, от англ. Information technology, IT) — это класс областей деятельности, относящихся к технологиям управления и обработкой огромного потока информации с применением вычислительной техники.

IT-инфраструктура – это комплексная структура, объединяющая все информационные технологии и ресурсы, используемые конкретной организацией либо компанией. Информационно-технологическая инфраструктура включает все компьютеры, установленное ПО, системы связи, информационные центры, сети и базы данных.

Сопровождение ИС – обеспечение использования введенной в промышленную эксплуатацию ИС в соответствии с ее назначением, включающее мероприятия по проведению корректировки, модификации и устранению дефектов программного обеспечения, без проведения модернизации и реализации дополнительных функциональных требований и при условии сохранения ее целостности.

Архитектура информационной системы - концепция, определяющая модель, структуру, выполняемые функции и взаимосвязь компонентов информационной системы.

База данных (БД) – совокупность данных, организованных согласно концептуальной структуре, описывающей характеристики этих данных, а также взаимосвязей между их объектами.

Программное обеспечение - совокупность программ, программных кодов, а также программных продуктов с технической документацией, необходимой для их эксплуатации**.**

Программный интерфейс - система унифицированных связей, предназначенных для обмена информацией между компонентами вычислительной системы, задающих набор необходимых процедур, их параметров и способов обращения**.**

Программный продукт - самостоятельная программа или часть программного обеспечения, являющаяся товаром, которая независимо от ее разработчиков может использоваться в предусмотренных целях в соответствии с системными требованиями, установленными технической документацией.

ИКТ– Информационно-коммуникационные технологии;

ПО – Программное обеспечение;

МСКО – Международная стандартная классификация образования

1. Паспорт Профессионального стандарта

Название ПС:	Обеспечение безопасности информационной инфраструктуры и ИТ
Номер ПС:	

Названия секции, раздела, группы, класса, и подкласса согласно ОКЭД:	J Информация и связь 62 Компьютерное программирование, консультации и другие сопутствующие услуги 62.0 Компьютерное программирование, консультации и другие сопутствующие услуги 62.01 Деятельность в области компьютерного программирования 62.02 Консультационные услуги в области компьютерных технологий 62.02.0 Консультационные услуги в области компьютерных технологий
Краткое описание ПС:	Обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности

2. Карточки профессий

Перечень карточек профессий	Специалист по вопросам безопасности (ИКТ)	5-7-й уровни ОРК
	Специалист по защите информации	5-7-й уровни ОРК
	Специалист-криминалист по цифровым технологиям	6-7-й уровни ОРК
	Шифровальщик данных	5-7-й уровни ОРК

КАРТОЧКА ПРОФЕССИИ
«СПЕЦИАЛИСТ ПО ВОПРОСАМ БЕЗОПАСНОСТИ (ИКТ)»

Код:	2524-0-005	
Код группы:	2524-0	
Профессия:	Специалист по вопросам безопасности (ИКТ)	
Другие возможные названия профессии:	Техник по защите инфокоммуникационных систем Инженер по информационной безопасности инфокоммуникационных систем Эксперт в области информационной безопасности	
Квалификационный уровень по ОРК:	5	
Основная цель деятельности	Противодействие вредоносному влиянию программно-технического воздействия на подсистемы, устройства, элементы и каналы инфокоммуникационных систем	
Трудовые функции	Обязательные трудовые функции	1. Администрирование средств защиты информации в компьютерных системах и сетях
	Дополнительные трудовые функции	-
Трудовая функция 1: Администрирование средств защиты информации в компьютерных системах и сетях	**Задача 1** Администрирование подсистем защиты информации в операционных системах	**Умения:** 1. Настраивать компоненты подсистем защиты информации операционных систем 2. Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей 3. Применять программно-аппаратные средства защиты информации в операционных системах

		4. Применять антивирусные средства защиты информации в операционных системах 5. Работать в операционных системах с соблюдением действующих требований по защите информации 6. Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах 7. Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации 8. Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации 9. Контролировать целостность подсистем защиты информации операционных систем 10. Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации 11. Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации
		Знания:
		1. Архитектура и пользовательские интерфейсы операционных систем 2. Порядок обеспечения безопасности информации при эксплуатации операционных систем 3. Источники угроз информационной безопасности и меры по их предотвращению 4. Сущность и содержание понятия информационной безопасности, характеристики ее составляющих 5. Типовые средства защиты информации в операционных системах 6. Программно-аппаратные средства и методы защиты информации 7. Порядок эксплуатации средств антивирусной защиты в операционных системах 8. Формы и методы инструктажа пользователей по порядку работы в операционных системах

		9. Общие принципы функционирования программно-аппаратных средств криптографической защиты информации 10. Порядок оформления эксплуатационной документации 11. Нормативные правовые акты в области защиты информации Организационные меры по защите информации
	Задача 2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	**Умения:**
		1. Применять программно-аппаратные средства защиты информации в компьютерных сетях 2. Устанавливать межсетевые экраны в компьютерных сетях 3. Конфигурировать межсетевые экраны в соответствии с заданными правилами 4. Контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами 5. Работать в компьютерных сетях с соблюдением действующих требований по защите информации 6. Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях 7. Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации Формулировать предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях
		Знания:
		1. Топологии и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях 2. Состав и основные характеристики оборудования, применяемого при построении компьютерных сетей 3. Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях 4. Типовые сетевые атаки и способы защиты от них 5. Сущность и содержание понятия информационной безопасности, характеристики ее составляющих 6. Основные источники угроз информационной безопасности и меры

		по их предотвращению 7. Программно-аппаратные средства и методы защиты информации 8. Основные методы организации и проведения технического обслуживания коммутационного оборудования компьютерных сетей 9. Порядок оформления эксплуатационной документации 10. Общие принципы функционирования средств криптографической защиты информации в компьютерных сетях 11. Порядок обеспечения безопасности информации при эксплуатации компьютерных сетей 12. Формы и методы инструктажа пользователей по порядку работы в компьютерных сетях 13. Нормативные правовые акты в области защиты информации Организационные меры по защите информации
	Задача 3 Администрирование средств защиты информации прикладного и системного программного обеспечения	**Умения:**
		1. Устанавливать программное обеспечение в соответствии с технической документацией 2. Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота 3. Работать с программным обеспечением с соблюдением действующих требований по защите информации Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации
		Знания:
		1. Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота 2. Общие принципы функционирования вредоносного программного обеспечения 3. Принципы функционирования средств антивирусной защиты 4. Сущность и содержание понятия информационной безопасности, характеристики ее составляющих 5. Источники угроз информационной

		безопасности и меры по их предотвращению 6. Особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения 7. Признаки наличия вредоносного программного обеспечения 8. Типовые уязвимости программного обеспечения и методы их эксплуатации 9. Общие принципы функционирования средств защиты информации программного обеспечения, в том числе, средств криптографической защиты информации 10. Порядок эксплуатации средств антивирусной защиты 11. Порядок обеспечения безопасности информации при эксплуатации программного обеспечения 12. Нормативные правовые акты в области защиты информации Организационные меры по защите информации	
Требования к личностным компетенциям	Аналитическое мышление, Критический анализ, Ответственность Организованность, Системное мышление, Умение решать нестандартные задачи, Внимательность к деталям		
Связь с другими профессиями в рамках ОРК	5	Специалист по защите информации	
	6	Специалист по защите информации	
	7	Специалист по защите информации	
Связь с ЕТКС или КС	КС	185. Техник-программист 140 Инженер - программист	
Связь с системой образования и квалификации	Уровень образования: общее среднее ТиПО (5 уровень МСКО)	Специальность: 1304000 Вычислительная техника и программное обеспечение (по видам) 1305000 Информационные системы (по областям применения)	Квалификация: 130409 4 Прикладной бакалавр программист вычислительной техники 1305084 Прикладной бакалавр – программист

КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ ПО ВОПРОСАМ БЕЗОПАСНОСТИ (ИКТ)»	
Код:	2524-0-005
Код группы:	2524-0
Профессия:	Специалист по вопросам безопасности (ИКТ)
Другие возможные названия профессии:	Техник по защите инфокоммуникационных систем Инженер по информационной безопасности инфокоммуникационных систем Эксперт в области информационной безопасности

<table>
<tr><td>Квалификационный уровень по ОРК:</td><td colspan="2">6</td></tr>
<tr><td>Основная цель деятельности</td><td colspan="2">Противодействие вредоносному влиянию программно-технического воздействия на подсистемы, устройства, элементы и каналы инфокоммуникационных систем</td></tr>
<tr><td rowspan="2">Трудовые функции</td><td>Обязательные трудовые функции</td><td>1. Администрирование средств защиты информации в компьютерных системах и сетях</td></tr>
<tr><td>Дополнительные трудовые функции</td><td>-</td></tr>
<tr><td rowspan="4">Трудовая функция 1: Администрирование средств защиты информации в компьютерных системах и сетях</td><td rowspan="4">Задача 1 Администрирование подсистем защиты информации в операционных системах</td><td>Умения:</td></tr>
<tr><td>1. Формулировать политики безопасности операционных систем
2. Настраивать политики безопасности операционных систем
3. Оценивать угрозы безопасности информации операционных систем
4. Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем
5. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах
6. Настраивать антивирусные средства защиты информации в операционных системах
7. Устанавливать обновления программного обеспечения и средств антивирусной защиты
8. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах
9. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах
10. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах</td></tr>
<tr><td>Знания:</td></tr>
<tr><td>1. Архитектура и принципы построения операционных систем
2. Программные интерфейсы операционных систем
3. Виды политик управления доступом и информационными потоками</td></tr>
</table>

		применительно к операционным системам 4. Архитектура подсистем защиты информации в операционных системах 5. Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы 6. Состав типовых конфигураций программно-аппаратных средств защиты информации 7. Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам 8. Порядок реализации методов и средств антивирусной защиты в операционных системах 9. Программно-аппаратные средства и методы защиты информации в операционных системах 10. Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации 11. Нормативные правовые акты в области защиты информации 12. Организационные меры по защите информации
	Задача 2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	**Умения:** 1. Оценивать угрозы безопасности информации в компьютерных сетях 2. Настраивать правила фильтрации пакетов в компьютерных сетях 3. Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях 4. Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях 5. Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях 6. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях 7. Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях 8. Оценивать оптимальность выбора программно-аппаратных средств защиты

		информации и их режимов функционирования в компьютерных сетях
		Знания:
		1. Принципы построения компьютерных сетей 2. Стек сетевых протоколов операционных систем 3. Стек протоколов сетевого оборудования 4. Порядок реализации методов и средств межсетевого экранирования 5. Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы 6. Виды политик управления доступом и информационными потоками в компьютерных сетях 7. Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению 8. Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях 9. Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации 10. Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации 11. Программно-аппаратные средства и методы защиты информации в компьютерных сетях 12. Нормативные правовые акты в области защиты информации 13. Организационные меры по защите информации
	Задача 3 Администрирование средств защиты информации прикладного и системного программного обеспечения	**Умения:**
		1. Анализировать угрозы безопасности информации программного обеспечения 2. Формулировать правила безопасной эксплуатации программного обеспечения 3. Обосновывать правила безопасной эксплуатации программного

		обеспечения 4. Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия 5. Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации 6. Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения 7. Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации 8. Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения
		Знания:
		1. Архитектура подсистем защиты информации в операционных системах 2. Принципы построения систем управления базами данных 3. Основные средства и методы анализа программных реализаций 4. Принципы построения антивирусного программного обеспечения 5. Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению 6. Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению 7. Уязвимости используемого программного обеспечения и методы их эксплуатации 8. Виды и формы функционирования вредоносного программного обеспечения 9. Характерные признаки наличия вредоносного программного обеспечения 10. Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения 11. Принципы функционирования

		программных средств криптографической защиты информации 12. Порядок обеспечения безопасности информации при эксплуатации программного обеспечения 13. Нормативные правовые акты в области защиты информации 14. Организационные меры по защите информации	
Требования к личностным компетенциям	Аналитическое мышление, Критический анализ, Ответственность Организованность, Системное мышление, Умение решать нестандартные задачи, Внимательность к деталям		
Связь с другими профессиями в рамках ОРК	5	Специалист по защите информации	
	6	Специалист по защите информации	
	7	Специалист по защите информации	
Связь с ЕТКС или КС	КС	185. Техник-программист 140 Инженер - программист	
Связь с системой образования и квалификации	Уровень образования: Высшее (5В код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии	Квалификация: Бакалавр в области ИКТ
КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ ПО ВОПРОСАМ БЕЗОПАСНОСТИ (ИКТ)»			
Код:	2524-0-005		
Код группы:	2524-0		
Профессия:	Специалист по вопросам безопасности (ИКТ)		
Другие возможные названия профессии:	Техник по защите инфокоммуникационных систем Инженер по информационной безопасности инфокоммуникационных систем Эксперт в области информационной безопасности		
Квалификационный уровень по ОРК:	7		
Основная цель деятельности	Противодействие вредоносному влиянию программно-технического воздействия на подсистемы, устройства, элементы и каналы инфокоммуникационных систем		
Трудовые функции	Обязательные трудовые функции	1. Оценивание уровня безопасности компьютерных систем и сетей	
		2. Разработка системы безопасности компьютерных систем и сетей	
	Дополнительные трудовые функции	-	
Трудовая функция 1:	**Задача 1**	**Умения:**	

Оценивание уровня безопасности компьютерных систем и сетей	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	1. Определять параметры функционирования программно-аппаратных средств защиты информации 2. Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации 3. Оценивать эффективность защиты информации 4. Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации 5. Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия
		Знания:
		1. Принципы построения компьютерных систем и сетей 2. Методы и методики оценки безопасности программно-аппаратных средств защиты информации 3. Принципы построения программно-аппаратных средств защиты информации 4. Принципы построения подсистем защиты информации в компьютерных системах 5. Методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации 6. Методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации 7. Методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей 8. Способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности 9. Национальные, межгосударственные и международные стандарты в области защиты информации 10. Нормативные правовые акты в области защиты информации 11. Организационные меры по защите

		информации
	Задача 2 Формирование политик безопасности компьютерных систем и сетей	**Умения:**
		1. Анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия 2. Разрабатывать профили защиты компьютерных систем 3. Формулировать задания по безопасности компьютерных систем 4. Выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации
		Знания:
		1. Принципы построения компьютерных систем и сетей 2. Модели безопасности компьютерных систем 3. Виды политик безопасности компьютерных систем и сетей 4. Принципы построения средств криптографической защиты информации 5. Национальные, межгосударственные и международные стандарты в области защиты информации 6. Возможности используемых и планируемых к использованию средств защиты информации 7. Нормативные правовые акты в области защиты информации 8. Организационные меры по защите информации
	Задача 3 Проведение анализа безопасности компьютерных систем	**Умения:**
		1. Анализировать компьютерную систему с целью определения уровня защищенности и доверия 2. Прогнозировать возможные пути развития действий нарушителя информационной безопасности 3. Производить анализ политики безопасности на предмет адекватности 4. Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах 5. Составлять и оформлять аналитический отчет по результатам проведенного анализа 6. Разрабатывать предложения по устранению выявленных уязвимостей
		Знания:

		1. Принципы построения компьютерных систем и сетей 2. Уязвимости компьютерных систем и сетей 3. Криптографические методы защиты информации 4. Принципы построения систем управления базами данных 5. Средства анализа конфигураций 6. Национальные, межгосударственные и международные стандарты в области защиты информации 7. Нормативные правовые акты в области защиты информации 8. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации 9. Организационные меры по защите информации
Трудовая функция 2: Разработка системы безопасности компьютерных систем и сетей	**Задача 1** Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей	**Умения:** 1. Обобщать научно-техническую литературу, нормативные и методические материалы в области защиты информации 2. Формировать модели угроз и модели нарушителя безопасности компьютерных систем 3. Выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы 4. Разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками 5. Применять национальные, межгосударственные и международные стандарты в области защиты информации для оценки защищенности компьютерной системы 6. Применять действующую законодательную базу в области обеспечения компьютерной безопасности 7. Читать и понимать нормативные и методические документы по информационной безопасности на английском языке 8. Осуществлять принятие решений о необходимости использования программно-аппаратных средств защиты

		информации
		Знания:
		1. Порядок организации работ по защите информации 2. Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях 3. Методы анализа безопасности компьютерных систем 4. Виды атак и механизмы их реализации в компьютерных системах 5. Методы выявления каналов утечки информации 6. Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных 7. Принципы построения средств защиты информации компьютерных систем 8. Формальные модели управления доступом 9. Криптографические алгоритмы и особенности их программной реализации 10. Нормативные правовые акты в области защиты информации 11. Организационные меры по защите информации 12. Национальные, межгосударственные и международные стандарты в области защиты информации
	Задача 2 Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей	**Умения:**
		1. Проводить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации 2. Применять отечественные стандарты в области защиты информации для проектирования средств защиты информации компьютерной системы 3. Разрабатывать архитектуру и интерфейсы средств защиты информации, процедуры восстановления работоспособности средств и систем защиты после сбоев 4. Подбирать и обобщать научно-техническую литературу, методические материалы по программным и аппаратным средствам и способам

		защиты информации, в том числе на английском языке
		Знания:
		1. Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях 2. Виды атак и механизмы их реализации в компьютерных системах 3. Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных 4. Принципы построения систем защиты информации компьютерных систем, в том числе антивирусного программного обеспечения 5. Методы анализа безопасности компьютерных систем 6. Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации 7. Формальные модели управления доступом 8. Принципы и методы проектирования программно-аппаратного обеспечения 9. Методологии и технологии разработки программного обеспечения 10. Принципы и методы управления проектами в области информационной безопасности 11. Криптографические алгоритмы и особенности их программной реализации 12. Нормативные правовые акты в области защиты информации 13. Организационные меры по защите информации 14. Национальные, межгосударственные и международные стандарты в области защиты информации
Требования к личностным компетенциям	Аналитическое мышление, Критический анализ, Ответственность Организованность, Системное мышление, Умение решать нестандартные задачи, Внимательность к деталям	
Связь с другими профессиями в рамках ОРК	5	Специалист по защите информации
	6	Специалист по защите информации
	7	Специалист по защите информации
Связь с ЕТКС или КС	КС	185. Техник-программист 140 Инженер - программист

Связь с системой образования и квалификации	Уровень образования: Послевузовское (6М код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии	Квалификация: Магистр в области ИКТ
КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ»			
Код:	2524-0-006		
Код группы:	2524-0		
Профессия:	Специалист по защите информации		
Другие возможные названия профессии:	Техник по защите информации Инженер по защите информации		
Квалификационный уровень по ОРК:	5		
Основная цель деятельности	Администрирование систем защиты информации ИС		
Трудовые функции	Обязательные трудовые функции	1. Обеспечение защиты информации в ИС в процессе их эксплуатации	
		2. Внедрение систем защиты информации в ИС	
	Дополнительные трудовые функции	-	
Трудовая функция 1: Обеспечение защиты информации в ИС в процессе их эксплуатации	**Задача 1** Диагностика систем защиты информации ИС	**Умения:**	
		1. Определять источники и причины возникновения инцидентов 2. Оценивать последствия выявленных инцидентов 3. Обнаруживать нарушения правил разграничения доступа 4. Устранять нарушения правил разграничения доступа 5. Осуществлять контроль обеспечения уровня защищенности в ИС Использовать криптографические методы и средства защиты информации в ИС	
		Знания:	
		1. Нормативные правовые акты в области защиты информации 2. Национальные, межгосударственные и международные стандарты в области защиты информации 3. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации 4. Организационные меры по защите информации 5. Принципы построения средств защиты	

		информации от "утечки" по техническим каналам 6. Критерии оценки защищенности автоматизированной системы 7. Технические средства контроля эффективности мер защиты информации 8. Регламент информирования персонала ИС о выявленных инцидентах 9. Регламент учета выявленных инцидентов 10. Регламент устранения инцидентов Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в ИС
	Задача 2 Администрирование систем защиты информации ИС	**Умения:**
		1. Конфигурировать параметры системы защиты информации ИС в соответствии с ее эксплуатационной документацией 2. Обнаруживать и устранять неисправности системы защиты информации ИС согласно эксплуатационной документации 3. Производить монтаж и диагностику компьютерных сетей Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи
		Знания:
		1. Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях 2. Базовая конфигурация системы защиты информации ИС 3. Особенности применения программных и программно-аппаратных средств защиты информации в ИС 4. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации 5. Нормативные правовые акты в области защиты информации Организационные меры по защите информации
Трудовая функция 2: Внедрение систем защиты информации в ИС	**Задача 1** Установка и настройка средств защиты информации в ИС	**Умения:**
		1. Администрировать программные средства системы защиты информации ИС 2. Устранять известные уязвимости ИС, приводящие к возникновению угроз безопасности информации 3. Применять нормативные документы по противодействию технической разведке

<table>
<tr><td></td><td></td><td colspan="2">4. Применять аналитические и компьютерные модели ИС и систем защиты информации
5. Проводить анализ структурных и функциональных схем защищенной ИС
6. Определять параметры настройки программного обеспечения системы защиты информации ИС</td></tr>
<tr><td></td><td></td><td colspan="2">Знания:</td></tr>
<tr><td></td><td></td><td colspan="2">1. Основные угрозы безопасности информации и модели нарушителя в ИС
2. Содержание эксплуатационной документации ИС
3. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации
4. Основные меры по защите информации в ИС
5. Нормативные правовые акты в области защиты информации</td></tr>
<tr><td>Требования к личностным компетенциям</td><td colspan="3">Аналитическое мышление, Критический анализ, Ответственность Организованность, Системное мышление, Умение решать нестандартные задачи, Внимательность к деталям</td></tr>
<tr><td rowspan="3">Связь с другими профессиями в рамках ОРК</td><td>5</td><td colspan="2">Специалист по вопросам безопасности (ИКТ)</td></tr>
<tr><td>6</td><td colspan="2">Специалист по вопросам безопасности (ИКТ)</td></tr>
<tr><td>7</td><td colspan="2">Специалист по вопросам безопасности (ИКТ)</td></tr>
<tr><td>Связь с ЕТКС или КС</td><td>КС</td><td colspan="2">185. Техник-программист
140 Инженер - программист</td></tr>
<tr><td>Связь с системой образования и квалификации</td><td>Уровень образования:
общее среднее ТиПО (5 уровень МСКО)</td><td>Специальность:
1304000 Вычислительная техника и программное обеспечение (по видам)
1305000 Информационные системы (по областям применения)</td><td>Квалификация:
130409 4 Прикладной бакалавр программист вычислительной техники
1305084 Прикладной бакалавр – программист</td></tr>
<tr><td colspan="4">КАРТОЧКА ПРОФЕССИИ
«СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ»</td></tr>
<tr><td>Код:</td><td colspan="3">2524-0-006</td></tr>
<tr><td>Код группы:</td><td colspan="3">2524-0</td></tr>
<tr><td>Профессия:</td><td colspan="3">Специалист по защите информации</td></tr>
<tr><td>Другие возможные названия профессии:</td><td colspan="3">Техник по защите информации
Инженер по защите информации</td></tr>
</table>

Квалификационный уровень по ОРК:	6	
Основная цель деятельности	Администрирование систем защиты информации ИС	
Трудовые функции	Обязательные трудовые функции	1. Обеспечение защиты информации в ИС в процессе их эксплуатации
		2. Внедрение систем защиты информации в ИС
	Дополнительные трудовые функции	-
Трудовая функция 1: Обеспечение защиты информации в ИС в процессе их эксплуатации	**Задача 1** Диагностика систем защиты информации ИС	**Умения:**
		1. Классифицировать и оценивать угрозы информационной безопасности 2. Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в ИС 3. Контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем 4. Контролировать события безопасности и действия пользователей автоматизированных систем 5. Применять технические средства контроля эффективности мер защиты информации 6. Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы
		Знания:
		1. Содержание и порядок деятельности персонала по эксплуатации защищенных ИС и подсистем безопасности ИС 2. Основные угрозы безопасности информации и модели нарушителя в ИС 3. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС 4. Программно-аппаратные средства обеспечения защиты информации ИС 5. Методы защиты информации от "утечки" по техническим каналам 6. Нормативные правовые акты в области защиты информации 7. Организационные меры по защите информации
	Задача 2	**Умения:**

	Администрирование систем защиты информации ИС	1. Создавать, удалять и изменять учетные записи пользователей ИС 2. Планировать политику безопасности программных компонентов ИС 3. Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации 4. Использовать криптографические методы и средства защиты информации в ИС 5. Регистрировать события, связанные с защитой информации в ИС 6. Анализировать события, связанные с защитой информации в ИС
		Знания:
		1. Принципы формирования политики информационной безопасности в ИС 2. Программно-аппаратные средства защиты информации ИС 3. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС 4. Методы контроля эффективности защиты информации от "утечки" по техническим каналам 5. Критерии оценки эффективности и надежности средств защиты программного обеспечения ИС 6. Технические средства контроля эффективности мер защиты информации 7. Принципы организации и структура систем защиты программного обеспечения ИС 8. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности ИС 9. Основные меры по защите информации в ИС
	Задача 3 Управление защитой информации в ИС	**Умения:**
		6-й уровень ОРК
		1. Оценивать информационные риски в ИС 2. Классифицировать и оценивать угрозы безопасности информации 3. Определять подлежащие защите информационные ресурсы автоматизированных систем 4. Применять нормативные документы по

		противодействию технической разведке 5. Разрабатывать предложения по совершенствованию системы управления защиты информации ИС 6. Конфигурировать параметры системы защиты информации ИС 7. Применять технические средства контроля эффективности мер защиты информации
		Знания:
		6-й уровень ОРК
		1. Основные методы управления защитой информации 2. Основные угрозы безопасности информации и модели нарушителя в ИС 3. Методы защиты информации от "утечки" по техническим каналам 4. Нормативные правовые акты в области защиты информации 5. Национальные, межгосударственные и международные стандарты в области защиты информации
Трудовая функция 2: Внедрение систем защиты информации в ИС	**Задача 1** Разработка организационно-распорядительных документов по защите информации в ИС	**Умения:**
		1. Классифицировать и оценивать угрозы информационной безопасности 2. Применять нормативные документы по противодействию технической разведке 3. Определять параметры настройки программного обеспечения системы защиты информации ИС 4. Контролировать эффективность принятых мер по защите информации в ИС
		Знания:
		1. Содержание и порядок деятельности персонала по эксплуатации защищенных ИС и систем защиты информации 2. Основные угрозы безопасности информации и модели нарушителя в ИС 3. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС 4. Принципы построения средств защиты информации от "утечки" по техническим каналам 5. Нормативные правовые акты в области защиты информации
	Задача 2 Внедрение организационных	**Умения:**
		1. Реализовывать правила разграничения

	мер по защите информации в автоматизированных системах	доступа персонала к объектам доступа 2. Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах 3. Обучать персонал ИС комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации 4. Осуществлять планирование и организацию работы персонала ИС с учетом требований по защите информации 5. Конфигурировать аттестованную информационную систему и системы защиты информации информационной системы
		Знания:
		1. Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации 2. Методы, способы, средства, последовательность и содержание этапов разработки ИС и систем защиты автоматизированных систем 3. Нормативные правовые акты в области защиты информации 4. Организационные меры по защите информации 5. Методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации 6. Методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем
Требования к личностным компетенциям	Аналитическое мышление, Критический анализ, Ответственность Организованность, Системное мышление, Умение решать нестандартные задачи, Внимательность к деталям	
Связь с другими профессиями в рамках ОРК	5	Специалист по вопросам безопасности (ИКТ)
	6	Специалист по вопросам безопасности

		(ИКТ)	
	7	Специалист по вопросам безопасности (ИКТ)	
Связь с ЕТКС или КС	КС	185. Техник-программист 140 Инженер - программист	
Связь с системой образования и квалификации	Уровень образования: Высшее (5В код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии	Квалификация: Бакалавр в области ИКТ
КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ»			
Код:	2524-0-006		
Код группы:	2524-0		
Профессия:	Специалист по защите информации		
Другие возможные названия профессии:	Техник по защите информации Инженер по защите информации		
Квалификационный уровень по ОРК:	7		
Основная цель деятельности	Администрирование систем защиты информации ИС		
Трудовые функции	Обязательные трудовые функции	1. Разработка систем защиты информации ИС	
	Дополнительные трудовые функции	-	
Трудовая функция 1: Разработка систем защиты информации ИС	**Задача 1** Разработка проектных решений по защите информации в ИС	**Умения:**	
		1. Применять действующую нормативную базу в области обеспечения защиты информации 2. Применять нормативные документы по противодействию технической разведке 3. Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности 4. Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты 5. Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в ИС 6. Выбирать меры защиты информации, подлежащие реализации в системе защиты информации ИС 7. Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты	

		информации 8. Определять структуру системы защиты информации ИС в соответствии с требованиями нормативных правовых документов в области защиты информации ИС
		Знания:
		1. Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации 2. Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей, и их компонентов 3. Особенности защиты информации в ИС управления технологическими процессами 4. Критерии оценки эффективности и надежности средств защиты информации программного обеспечения ИС 5. Принципы организации и структура систем защиты информации программного обеспечения ИС 6. Основные характеристики технических средств защиты информации от утечек по техническим каналам 7. Принципы формирования политики информационной безопасности в ИС
	Задача 2 Разработка эксплуатационной документации на системы защиты информации ИС	**Умения:**
		1. Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в ИС 2. Разрабатывать технические задания на создание подсистем информационной безопасности ИС 3. Проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов 4. Разрабатывать модели ИС и систем защиты информации ИС 5. Исследовать модели ИС и систем защиты безопасности ИС 6. Анализировать программные,

		архитектурно-технические и схемотехнические решения компонентов ИС с целью выявления потенциальных уязвимостей систем защиты информации ИС 7. Оценивать информационные риски в ИС и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите 8. Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в ИС с целью обеспечения требуемого уровня защищенности 9. Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в ИС с целью обеспечения требуемого уровня защищенности 10. Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации
		Знания:
		1. Основные методы управления информационной безопасностью 2. Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов 3. Основные методы управления проектами в области информационной безопасности 4. Национальные, межгосударственные и международные стандарты в области защиты информации 5. Основные меры по защите информации в ИС 6. Особенности защиты информации в ИС управления технологическими процессами 7. Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в ИС 8. Методы, способы, средства, последовательность и содержание этапов разработки ИС и систем защиты информации ИС 9. Программно-аппаратные средства обеспечения защиты информации в программном обеспечении ИС

		10. Основные средства, способы и принципы построения систем защиты информации ИС 11. Нормативные правовые акты в области защиты информации
	Задача 3 Разработка архитектуры системы защиты информации ИС	**Умения:**
		1. Определять комплекс мер для обеспечения безопасности информационной в ИС 2. Выявлять уязвимости информационно-технологических ресурсов ИС 3. Разрабатывать предложения по совершенствованию системы управления защиты информации ИС 4. Проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе ИС с целью обеспечения требуемого уровня защищенности ИС 5. Классифицировать и оценивать угрозы безопасности информации для ИС 6. Определять информационную инфраструктуру и информационные ресурсы ИС, подлежащие защите 7. Разрабатывать модели угроз безопасности информации и нарушителей в ИС 8. Определять эффективность применения средств информатизации
		Знания:
		1. Основные информационные технологии, используемые в ИС 2. Способы и средства защиты информации от "утечки" по техническим каналам и контроля эффективности защиты информации 3. Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации 4. Программно-аппаратные средства обеспечения защиты информации ИС 5. Принципы построения средств защиты информации от "утечки" по техническим каналам 6. Национальные, межгосударственные и международные стандарты в области защиты информации 7. Методы тестирования и отладки,

		принципы организации документирования разработки, процесса сопровождения программного обеспечения	
Требования к личностным компетенциям	Аналитическое мышление, Критический анализ, Ответственность Организованность, Системное мышление, Умение решать нестандартные задачи, Внимательность к деталям		
Связь с другими профессиями в рамках ОРК	5	Специалист по вопросам безопасности (ИКТ)	
	6	Специалист по вопросам безопасности (ИКТ)	
	7	Специалист по вопросам безопасности (ИКТ)	
Связь с ЕТКС или КС	КС	185. Техник-программист 140 Инженер - программист	
Связь с системой образования и квалификации	Уровень образования: Послевузовское (6М код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии	Квалификация: Магистр в области ИКТ

КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ-КРИМИНАЛИСТ ПО ЦИФРОВЫМ ТЕХНОЛОГИЯМ»		
Код:		2524-0-008
Код группы:		2524-0
Профессия:		Специалист-криминалист по цифровым технологиям
Другие возможные названия профессии:		Цифровой криминалист Специалист по компьютерной криминалистике
Квалификационный уровень по ОРК:		6
Основная цель деятельности		Анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства
Трудовые функции:	Обязательные трудовые функции:	1. Расследование компьютерных преступлений
		2. Проведение цифровой криминалистической экспертизы
	Дополнительные трудовые функции:	-
Трудовая функция 1: Расследование компьютерных преступлений	**Задача 1:** Первичное реагирование на компьютерные преступления	**Умения:**
		1. Определять источники и причины возникновения инцидентов 2. Оценивать последствия выявленных инцидентов

		3. Идентифицировать проникновения в корпоративную сеть 4. Устранять все установленные способы доступа злоумышленников в сеть организации 5. Анализировать структуру механизма возникновения и обстоятельства события 6. Определять причину и условия изменения программного обеспечения 7. Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику 8. Выявлять несоответствия имеющейся информации ее расположению в системе
		Знания:
		1. Основные виды компьютерных преступлений 2. Способы доступа злоумышленников в сеть организации 3. Основные угрозы безопасности информации и модели нарушителя в ИС организации 4. Принципы построения и функционирования систем и сетей передачи информации 5. Национальные, межгосударственные и международные стандарты в области защиты информации 6. Технические каналы "утечки" информации 7. Нормативные правовые акты в области защиты информации 8. Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей 9. Основные методы организации и проведения технического обслуживания технических средств информатизации 10. Организационные меры по защите информации 11. Регламент учета выявленных инцидентов 12. Форматы хранения информации в анализируемой компьютерной системе 13. Основные форматы файлов, используемые в компьютерных системах 14. Порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов Нормы уголовного и административного права в сфере компьютерной информации

	Задача 2: Планирование мер по предотвращению взломов и несанкционированного доступа	15. **Умения:** 1. Разрабатывать меры по предотвращению и своевременному обнаружению взломов 2. Производить поиск уликовой информации на компьютерах 3. Выявлять методы и средства контр-криминалистики: полнодисковое шифрование, удаленное хранение информации и др. 4. Осуществлять сбор доказательной базы и ее оформление/хранение 16. Моделировать реальную атаку на организацию и тренировать навыки принятия мер по минимизации ущерба от нее 17. **Знания:** 1. Принципы построения и функционирования систем и сетей передачи информации 2. Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей 3. Национальные, межгосударственные и международные стандарты в области защиты информации 4. Основные угрозы безопасности информации и модели нарушителя в ИС организации 5. Методы и средства контр-криминалистики 6. Принципы построения средств защиты информации от "утечки" по техническим каналам 7. Нормативные правовые акты в области защиты информации 8. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ИС 9. Основные принципы изъятия компьютерной техники 10. Методы сокрытия уликовых данных от обнаружения. 18. Документирование информации по расследованию
Трудовая функция 2: Криминалистическая экспертиза цифровых устройств и оборудования	**Задача 1** Криминалистическая экспертиза компьютеров	**Умения:** 1. Расследовать инциденты информационной безопасности 2. Фиксировать время инцидента 3. Проводить первичную диагностику компьютерного устройства

		4. Работать с аппаратными блокираторами записи и дубликаторами носителей информации 5. Работать с дистрибутивами для криминалистического анализа. 6. Производить снятие образа (идентичной копии) жесткого диска (НМЖД) и других носителей информации, включая снятие образа с раздела или отдельного сектора жесткого диска 7. Производить обработку сформированных образов дисков 8. Осуществлять сбор данных с жестких дисков 9. Осуществлять анализ файлов, найденных на жестких дисках. 10. Производить извлечение данных из файлов. 11. Производить исследование дампов оперативной памяти. 12. Производить поиск артефактов на жестком диске и периферии 13. Работать с системными логами и журналами операционных систем и прикладных программ 14. Восстанавливать удаленные данные 15. Осуществлять сбор доказательной базы и ее оформление/хранение
		Знания:
		1. Базовые знания о файловых системах 2. Базовые знания об операционных системах 3. Основные принципы информационной безопасности и методы работы средств защиты 4. Инструментарий компьютерной криминалистики 5. Устройство жестких дисков и других накопителей 6. Архитектура и пользовательские интерфейсы операционных систем 7. Архитектура, устройство и функционирование вычислительных систем 8. Инструментарий для работы с файловой системой, включая восстановление данных 9. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации
	Задача 2 Криминалистическая экспертиза сетевых	**Умения:**
		1. Производить анализ сетевого стека и браузеров.

	устройств	2. Производить анализ email-сообщений и устанавливать принадлежность адреса электронной почты. 3. Работать с инструментарием для создания дампа сетевого трафика 4. Осуществлять перехват и исследование сетевого трафика 5. Осуществлять исследование логов web-серверов 6. Устанавливать принадлежность и расположение IP-адреса 7. Устанавливать принадлежность доменного имени
		Знания:
		1. Принципы построения и функционирования систем и сетей передачи информации 2. Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей 3. Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях 4. Основные принципы проведения сетевой криминалистики. 5. Регламент действий сотрудников с целью получения максимально подробной информации для проведения анализа 6. Типовые источники данных для проведения сетевой криминалистики и их исследование 7. Особенности инструментария для создания дампа сетевого трафика
	Задача 3 Криминалистическая экспертиза мобильных устройств	**Умения:**
		1. Осуществлять идентификацию устройства мобильной связи 2. Осуществлять клонирование всех данных с цифрового устройства, периферийного оборудования и накопителей информации 3. Осуществлять получение информации с мобильных телефонов 4. Осуществлять получение информации с SIM-карты 5. Осуществлять получение информации с встроенной и внешней карты памяти 6. Осуществлять контроль почтовых отправлений, телеграфных и иных сообщений

		7. Работать с программными и аппаратными инструментальными средствами для доступа к данным мобильного телефона	
		Знания:	
		1. Принципы и устройства мобильной связи 2. Программно-аппаратный инструментарий для доступа к данным мобильного телефона 3. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации 4. Базовые знания об мобильных операционных системах 5. Базовые знания о файловых системах мобильных устройств 6. Устройство карт памяти	
Требования к личностным компетенциям	Аналитическое мышление, Критический анализ, Стрессоустойчивость, Ответственность, Организованность, Обучаемость, Уметь работать в команде		
Связь с другими профессиями в рамках ОРК	-		
Связь с ЕТКС или КС	КС	140 Инженер - программист 284. Инженер - проектировщик	
Связь с системой образования и квалификации	Уровень образования: Высшее (5В код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии	Квалификация: Бакалавр в области ИКТ
КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ-КРИМИНАЛИСТ ПО ЦИФРОВЫМ ТЕХНОЛОГИЯМ»			
Код:		2524-0-008	
Код группы:		2524-0	
Профессия:		Специалист-криминалист по цифровым технологиям	
Другие возможные названия профессии:		Цифровой криминалист Специалист по компьютерной криминалистике	
Квалификационный уровень по ОРК:		7	
Основная цель деятельности		Анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства	
Трудовые функции:	Обязательные	1. Расследование компьютерных преступлений	

	трудовые функции:	2. Проведение анализа экспертных данных
	Дополнительные трудовые функции:	-
Трудовая функция 1: Расследование компьютерных преступлений	**Задача 1** Получение данных из потенциальных источников информации	**Умения:**
		1. Выявлять потенциальные источники данных в организации 2. Разрабатывать план сбора данных 3. Осуществлять получение данных и проверку целостности полученных данных 4. Осуществлять ведение подробного журнала каждого шага, который был предпринят для сбора данных, включая информацию о каждом инструменте, используемом в процессе 5. Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику 6. Определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой
		Знания:
		1. Виды потенциальных источников данных 2. Носители компьютерной информации 3. Методы обеспечения сохранности, целостности и конфиденциальности полученной информации 4. Принципы построения и функционирования систем и сетей передачи информации 5. Нормативные правовые акты в области цифровой криминалистики 6. Основные принципы изъятия компьютерной техники 7. Документирование информации по расследованию 8. Базовые знания о файловых системах 9. Базовые знания об операционных системах 10. Архитектура, устройство и функционирование вычислительных систем 11. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации 12. Технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов

		13. Порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов
	Задача 4 Экспертное исследование собранной информации (объектов-носителей) при компьютерных преступлениях	**Умения:**
		1. Осуществлять извлечение/считывание информации с носителей 2. Осуществлять декодирование информации и вычленение из нее той, которая относится к делу 3. Использовать автоматизированные средства исследования информации 4. Обеспечивать целостность и сохранность информации с исследуемых носителей 5. Применять действующую законодательную базу в области обеспечения защиты информации 6. Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа
		Знания:
		1. Методы извлечения/считывания данных с компьютерных носителей информации 2. Методы обеспечения сохранности, целостности и конфиденциальности полученной информации 3. Программные средства исследования и фильтрации данных 4. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации 5. Базовые знания о файловых системах 6. Базовые знания об операционных системах 7. Принципы построения и функционирования систем и сетей передачи информации 8. Нормативные правовые акты в области цифровой криминалистики 9. Технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов 10. Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов
Трудовая функция 3: Проведение анализа экспертных данных	**Задача 1** Обработка экспертных данных	**Умения:**
		1. Анализировать собранную на предыдущих этапах расследования информацию. 2. Производить анализ интерпретированных данных, полученных из различных

		источников, данных 3. Определять тип компьютерных файлов, в том числе без расширения 4. Производить реконструкцию событий компьютерного инцидента, объединяя различные источники компьютерной информации 5. Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа
		Знания:
		1. Носители компьютерной информации 2. Методы обеспечения сохранности, целостности и конфиденциальности полученной информации 3. Базовые знания о файловых системах 4. Базовые знания об операционных системах 5. Архитектура, устройство и функционирование вычислительных систем 6. Принципы построения и функционирования систем и сетей передачи информации 7. Программные средства обработки информации 8. Нормативные правовые акты в области цифровой криминалистики 9. Форматы хранения информации в анализируемой компьютерной системе 10. Основные форматы файлов, используемые в компьютерных системах 11. Особенности хранения конфигурационной и системной информации в компьютерных системах 12. Уязвимости компьютерных систем и сетей 13. Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов
	Задача 2 Оформление результатов исследования и анализа в установленной законом и понятной неспециалистам форме	**Умения:**
		1. Формировать отчетную документацию в установленном законом и понятной неспециалистам форме 2. Актуализировать информацию для выявления полезной информации, полученной из данных, которые могут позволить аналитику собирать новые источники информации 3. На основе отчетных данных разрабатывать рекомендации по предотвращению

		компьютерных инцидентов и преступлений
		Знания:
		1. Методика составления отчетной и служебной документации 2. Методы обеспечения сохранности, целостности и конфиденциальности полученной информации 3. Нормативные правовые акты в области цифровой криминалистики 4. Архитектура, устройство и функционирование вычислительных систем 5. Принципы построения и функционирования систем и сетей передачи информации 6. Программные средства обработки информации 7. Порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем 8. Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов
Требования к личностным компетенциям	Аналитическое мышление, Критический анализ, Стрессоустойчивость, Ответственность, Организованность, Обучаемость, Уметь работать в команде	
Связь с другими профессиями в рамках ОРК	-	
Связь с ЕТКС или КС	КС	140 Инженер - программист 284. Инженер - проектировщик
Связь с системой образования и квалификации	Уровень образования: Послевузовское (6М код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии Квалификация: Магистр в области ИКТ

КАРТОЧКА ПРОФЕССИИ «ШИФРОВАЛЬЩИК ДАННЫХ»	
Код:	2524-0-009
Код группы:	2524-0
Профессия:	Шифровальщик данных
Другие возможные названия профессии:	Кодировщик
Квалификационный	5

уровень по ОРК:		
Основная цель деятельности	Разработка и эксплуатация систем шифрования данных	
Трудовые функции:	Обязательные трудовые функции:	1. Эксплуатация систем шифрования данных.
		2. Оценивание уровня безопасности систем шифрования данных
	Дополнительные трудовые функции:	-
Трудовая функция 1: Эксплуатация систем шифрования данных	**Задача 1:** Техническое обслуживание программных, программно-аппаратных систем шифрования данных	**Умения:**
		1. Проводить диагностику систем шифрования данных. 2. Обнаруживать неисправности в системе шифрования данных. 3. Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт систем шифрования данных 4. Проводить работы по техническому обслуживанию, в том числе по обновлению версий программного обеспечения систем шифрования данных 5. Устранять неисправности систем шифрования данных, если это предусмотрено технической документацией.
		Знания:
		1. Организация и содержание диагностики и технического обслуживания систем шифрования данных. 2. Правила ведения эксплуатационной документации программных, программно-аппаратных систем шифрования данных 3. Устройство и функционирование современных систем шифрования данных 4. Методики и приемы ремонта систем шифрования данных. 5. Базовые понятия и теории кодирования и шифрования данных.
	Задача 2: Администрирование систем шифрования данных	**Умения:**
		1. Планировать политику безопасности программных компонентов систем

		шифрования данных 2. Устанавливать и настраивать компьютерные сети и программные системы с учетом требований к системам шифрования данных 3. Регистрировать события, связанные с системой шифрования данных. 4. Анализировать события, связанные с функционированием систем шифрования данных
		Знания:
		1. Принципы формирования политики информационной безопасности в системах шифрования данных. 2. Программно-аппаратные средства шифрования данных 3. Основные криптографические методы, алгоритмы, протоколы, используемые в системах шифрования данных 4. Методы контроля эффективности и криптостойкости систем шифрования данных 5. Критерии оценки эффективности и надежности систем шифрования данных 6. Программно-технические средства контроля эффективности и надежности систем шифрования данных 7. Принципы организации и структура систем шифрования данных Содержание и порядок деятельности персонала по эксплуатации систем шифрования данных
Трудовая функция 2: Оценивание уровня безопасности систем шифрования данных	**Задача 1:** Мониторинг функционирования систем шифрования данных.	**Умения:**
		1. Использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных систем шифрования данных 2. Проводить контроль функционирования систем шифрования данных. 3. Определять технические характеристики систем шифрования данных 4. Осуществлять проверки программных, программно-аппаратных систем шифрования данных 5. Проводить документационное обеспечение функционирования систем шифрования данных

		Знания:
		1. Методы контроля функционирования систем шифрования данных. 2. Принципы построения современных систем шифрования данных. 3. Функциональное назначение и основные характеристики средств контроля функционирования систем шифрования данных. 4. Организация и содержание мониторинга функционирования систем шифрования данных. 5. Нормативные правовые акты в области систем шифрования данных и защиты информации.
	Задача 2: Аудит защищенности систем шифрования данных.	**Умения:**
		1. Классифицировать и оценивать угрозы безопасности информации для систем шифрования данных. 2. Разрабатывать предложения по совершенствованию управлением информационной безопасностью систем шифрования данных 3. Разрабатывать политики безопасности информации систем шифрования данных. 4. Применять инструментальные средства контроля защищенности информации в системах шифрования данных
		Знания:
		1. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в системах шифрования данных. 2. Принципы построения систем шифрования данных 3. Нормативные правовые акты в области защиты информации. 4. Организационные меры по защите информации 5. Принципы организации и структура систем шифрования данных. 6. Устройство и функционирование современных систем шифрования данных 7. Требования по сохранению государственной и коммерческой тайны
Требования к	Структурное мышление, Усидчивость и внимательность	

личностным компетенциям	Аналитический ум, Способность к самообучению, Ответственность, Математические способности		
Связь с другими профессиями в рамках ОРК	-	-	
Связь с ЕТКС или КС	КС	185. Техник-программист	
Связь с системой образования и квалификации	Уровень образования: общее среднее ТиПО (5 уровень МСКО)	Специальность: 1304000 Вычислительная техника и программное обеспечение (по видам) 1305000 Информационные системы (по областям применения)	Квалификация: 130409 4 Прикладной бакалавр программист вычислительной техники 1305084 Прикладной бакалавр – программист
КАРТОЧКА ПРОФЕССИИ «ШИФРОВАЛЬЩИК ДАННЫХ»			
Код:	2524-0-009		
Код группы:	2524-0		
Профессия:	Шифровальщик данных		
Другие возможные названия профессии:	Кодировщик		
Квалификационный уровень по ОРК:	6		
Основная цель деятельности	Разработка и эксплуатация систем шифрования данных		
Трудовые функции:	Обязательные трудовые функции:	1. Эксплуатация систем шифрования данных.	
		2. Оценивание уровня безопасности систем шифрования данных	
	Дополнительные трудовые функции:	-	
Трудовая функция 1: Эксплуатация систем шифрования данных	**Задача 1:** Управление функционированием системам шифрования данных	**Умения:**	
		1. Осуществлять организацию бесперебойного функционирования систем шифрования данных. 2. Устанавливать и настраивать параметры сетевых протоколов, реализованных в системах шифрования данных. 3. Разрабатывать предложения по совершенствованию и повышению эффективности принимаемых технических мер и проводимых организационных мероприятий по защите систем шифрования данных. 4. Организовывать работы по	

		выполнению требований режима защиты информации ограниченного доступа к системам шифрования данных Разрабатывать методические материалы и организационно-распорядительные документы по системам шифрования данных
		Знания:
		1. Архитектура, устройство и функционирование вычислительных систем. 2. Сетевые протоколы и их параметры настройки. 3. Особенности применения программных, программно-аппаратных и технических средств в системах шифрования данных. 4. Методы комплексного обеспечения защиты систем шифрования данных. 5. Показатели эффективности применяемых программных, программно-аппаратных и технических средств в системах шифрования данных 6. Нормативные правовые акты в области защиты информации ограниченного доступа 7. Национальные, межгосударственные и международные стандарты в области защиты информации 8. Устройство и функционирование современных систем шифрования данных Требования по сохранению государственной и коммерческой тайны
	Задача 2: Ведение специального делопроизводства и технических документов в процессе эксплуатации	**Умения:**
		1. Выполнять задачи по получению, хранению, учету, выдаче, приему и утилизации специальных документов, применяемых в процессе эксплуатации систем шифрования данных. 2. Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт систем шифрования данных. 9. Вести эксплуатационную документацию систем шифрования данных.
		Знания:

		1. Правила ведения специального делопроизводства и технических документов систем обеспечения данных. 2. Нормативные правовые акты по организации защиты государственной тайны, конфиденциальной информации и деятельности органов защиты государственной тайны. 3. Организационные меры по защите информации в системах шифрования данных 4. Нормативные правовые акты в области защиты информации. 10. Устройство и функционирование современных систем шифрования данных
Трудовая функция 2: Оценивание уровня безопасности систем шифрования данных	**Задача 1:** Проведение контрольных проверок работоспособности и эффективности систем шифрования данных	**Умения:** 1. Определять параметры функционирования программно-аппаратных средств системы шифрования данных. 2. Разрабатывать методики оценки эффективности программно-аппаратных средств систем шифрования данных. 3. Оценивать эффективность программно-аппаратных средств систем шифрования данных. 4. Анализировать программно-аппаратные средства систем шифрования данных с целью определения уровня обеспечиваемой ими защищенности и доверия
		Знания: 1. Методы и методики оценки эффективности программно-аппаратных средств систем шифрования данных. 2. Принципы построения программно-аппаратных средств систем шифрования данных. 3. Методы и средства оценки корректности и эффективности программных реализаций алгоритмов шифрования информации. 4. Методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей 5. Национальные, межгосударственные и

		международные стандарты в области защиты информации 6. Нормативные правовые акты в области защиты информации 7. Организационные меры по защите информации 8. Устройство и функционирование современных систем шифрования данных
	Задача 2: Проведение анализа безопасности систем шифрования данных	**Умения:**
		1. Анализировать системы шифрования данных с целью определения уровня защищенности и доверия. 2. Прогнозировать возможные пути развития действий нарушителя информационной безопасности. 3. Производить анализ политики безопасности на предмет адекватности. 4. Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств в системах шифрования данных. 5. Составлять и оформлять аналитический отчет по результатам проведенного анализа 6. Разрабатывать предложения по устранению выявленных уязвимостей
		Знания:
		1. Уязвимости компьютерных систем и сетей. 2. Криптографические методы защиты информации. 3. Средства анализа конфигураций 4. Национальные, межгосударственные и международные стандарты в области защиты информации 5. Нормативные правовые акты в области защиты информации 6. Организационные меры по защите информации 7. Устройство и функционирование современных систем шифрования данных 8. Требования по сохранению государственной и коммерческой тайны
Требования к личностным компетенциям	Структурное мышление, Усидчивость и внимательность Аналитический ум, Способность к самообучению, Ответственность, Математические способности	
Связь с другими	-	-

профессиями в рамках ОРК			
Связь с ЕТКС или КС	КС	185. Техник-программист	
Связь с системой образования и квалификации	Уровень образования: Высшее (5В код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии	Квалификация: Бакалавр в области ИКТ
КАРТОЧКА ПРОФЕССИИ «ШИФРОВАЛЬЩИК ДАННЫХ»			
Код:	2524-0-009		
Код группы:	2524-0		
Профессия:	Шифровальщик данных		
Другие возможные названия профессии:	Кодировщик		
Квалификационный уровень по ОРК:	7		
Основная цель деятельности	Разработка и эксплуатация систем шифрования данных		
Трудовые функции:	Обязательные трудовые функции:	1. Разработка программных, программно-аппаратных систем шифрования данных	
	Дополнительные трудовые функции:	-	
Трудовая функция 1: Разработка программных, программно-аппаратных систем шифрования данных	**Задача 1** Разработка проектных решений для систем шифрования данных	**Умения:**	
		1. Применять действующую нормативную базу в области функционирования систем шифрования данных 2. Применять нормативные документы по противодействию технической разведке 3. Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности 4. Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты 5. Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в системах шифрования данных 6. Определять структуру систем шифрования данных в соответствии с требованиями нормативных правовых документов в области шифрования данных	
		Знания:	
		1. Нормативные правовые акты и национальные стандарты по	

		лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации 2. Принципы построения и функционирования, примеры реализаций современных систем шифрования данных 3. Критерии оценки эффективности и надежности средств шифрования данных 4. Принципы организации и структура систем шифрования данных 5. Основные характеристики технических средств шифрования данных 6. Устройство и функционирование современных систем шифрования данных 7. Требования по сохранению государственной и коммерческой тайны
	Задача 2 Реализация программных, программно-аппаратных систем шифрования данных	**Умения:**
		1. Оценивать сложность криптографических алгоритмов и вычислений 2. Разрабатывать технические задания на создание систем шифрования данных с учетом требований нормативных документов, ЕСКД и ЕСПД 3. Анализировать программные, архитектурно-технические и схемотехнические решения компонентов систем шифрования данных с целью выявления потенциальных уязвимостей безопасности в системах шифрования данных 4. Проводить комплексное тестирование аппаратных и программных средств
		Знания:
		1. Профессиональная и криптографическая терминология в области безопасности информации и шифрования данных 2. Основные информационные технологии и технические средства, используемые в системах шифрования данных 3. Средства и способы обеспечения безопасности информации, принципы построения систем шифрования данных

		4. Основные криптографические методы, алгоритмы, протоколы, используемые в системах шифрования данных 5. Современные технологии программирования 6. Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей 7. Принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры 8. Принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения 9. Методы тестирования и отладки программного и аппаратного обеспечения 10. Нормативные правовые акты в области защиты информации 11. Требования по сохранению государственной и коммерческой тайны
	Задача 3 Тестирование разработанных систем шифрования данных	**Умения:**
		1. Писать программный код процедур проверки работоспособности программного обеспечения на выбранном языке программирования 2. Применять методы и средства тестирования 3. Использовать выбранную среду программирования для разработки процедур проверки работоспособности программного обеспечения на выбранном языке программирования 4. Разработка и оформление контрольных примеров для проверки работоспособности программного обеспечения 5. Подготовка наборов данных, используемых в процессе проверки работоспособности программного обеспечения
		Знания:
		1. Методы автоматической и автоматизированной проверки

		работоспособности программного обеспечения 2. Основные виды диагностических данных и способы их представления 3. Языки, утилиты и среды программирования, и средства пакетного выполнения процедур 4. Методы создания и документирования контрольных примеров и тестовых наборов данных 5. Правила, алгоритмы и технологии создания тестовых наборов данных 6. Требования к структуре и форматам хранения тестовых наборов данных 7. Криптографические алгоритмы и особенности их программной реализации 8. Основные инструментальные средства искусственного интеллекта
	Задача 4 Разработка эксплуатационной документации на системы шифрования данных	**Умения:**
		1. Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для систем шифрования данных 2. Разрабатывать технические задания на создание подсистем информационной безопасности систем шифрования данных 3. Проектировать подсистемы систем шифрования данных с учетом действующих нормативных и методических документов 4. Анализировать программные, архитектурно-технические и схемотехнические решения компонентов систем шифрования данных с целью выявления потенциальных уязвимостей систем шифрования данных 5. Оценивать информационные риски в системах шифрования данных и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите 6. Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств в системах шифрования данных с целью обеспечения требуемого уровня защищенности 7. Исследовать эффективность

		проектных решений программно-аппаратных средств в системах шифрования данных с целью обеспечения требуемого уровня защищенности	
		Знания:	
		1. Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов, криптографии 2. Основные методы управления проектами в области систем шифрования данных 3. Национальные, межгосударственные и международные стандарты в области защиты информации 4. Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в системах шифрования данных 5. Методы, способы, средства, последовательность и содержание этапов разработки систем шифрования данных 6. Основные средства, способы и принципы построения систем шифрования данных 7. Нормативные правовые акты в области защиты информации 8.Требования по сохранению государственной и коммерческой тайны	
Требования к личностным компетенциям	Структурное мышление, Усидчивость и внимательность Аналитический ум, Способность к самообучению, Ответственность, Математические способности		
Связь с другими профессиями в рамках ОРК	-	-	
Связь с ЕТКС или КС	КС	185. Техник-программист	
Связь с системой образования и квалификации	Уровень образования: Послевузовское (6М код по МСКО)	Направление подготовки: Информационно-коммуникационные технологии	Квалификация: Магистр в области ИКТ

3. Технические данные Профессионального стандарта	
Разработано:	Товарищество с ограниченной ответственностью «Компания системных исследований «Фактор» Руководитель проекта: Габбасов М.Б. Контактные данные руководителя:

	Mars0@mail.ru +7 701 908 25 11 Исполнители проекта и контактные данные исполнителей: Абдешов Х.У. habdeshov@rambler.ru +7 777 2505831 Увалеев Ж.Е. zh_uali@mail.ru 87015228028 Байдельдинов М.У. Make3508@gmail.com +77013918037
Экспертиза представлена:	Организация: ТОО 10Tech Эксперты и контактные данные экспертов: Заместитель Генерального директора Болдырев В.А. 87017173689
Номер версии и год выпуска:	Версия 1, 2019 год
Дата ориентировочного пересмотра:	30.12.2022