

Профессиональный стандарт «Информационная безопасность»

1. Общие положения

1. Профессиональный стандарт «Информационная безопасность» предназначен для формирования образовательных программ, в том числе для обучения персонала на предприятиях, для сертификации работников и выпускников образовательных учреждений, для решения широкого круга задач в области управления персоналом.

На основании настоящего профессионального стандарта организации могут разрабатывать для внутреннего применения корпоративные профессиональные стандарты на работников с уточнением уровня профессионального образования, перечня трудовых функций, знаний, умений и навыков с учетом особенностей организации производства, труда и управления, их ответственности.

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

1) квалификация – степень готовности работника к качественному выполнению конкретных трудовых функций;

2) уровень квалификации – совокупность требований к уровню подготовки и компетенции работника, дифференцируемой по параметрам сложности, нестандартности трудовых действий, ответственности и самостоятельности;

3) национальная рамка квалификаций – структурированное описание квалификационных уровней, признаваемых на рынке труда;

4) национальная система квалификаций – совокупность механизмов правового и институционального регулирования спроса и предложений на квалификации специалистов со стороны рынка труда;

5) отраслевая рамка квалификаций – структурированное описание квалификационных уровней, признаваемых в отрасли;

б) профессиональная группа – совокупность профессиональных подгрупп, имеющая общую интеграционную основу (аналогичные или близкие назначение, объекты, технологии, в том числе средства труда) и предполагающая схожий набор трудовых функций и компетенций для их выполнения;

7) профессиональная подгруппа – совокупность профессий, сформированная целостным набором трудовых функций и необходимых для их выполнения компетенций;

8) профессиональный стандарт – стандарт, определяющий в конкретной области профессиональной деятельности требования к уровню квалификации и компетентности, содержанию, качеству и условиям труда;

9) профессия – основной род занятий трудовой деятельности человека, требующий определенных знаний, умений и практических навыков, приобретенных в результате специальной подготовки и подтверждаемых соответствующими документами об образовании;

10) трудовая функция – набор взаимосвязанных действий, направленных на решение одной или нескольких задач процесса труда.

3. В настоящем профессиональном стандарте используются следующие сокращения:

- 1) ИКТ – информационно-коммуникационные технологии;
- 2) ОРК – отраслевая рамка квалификации;
- 3) ПС – профессиональный стандарт;
- 4) КС – квалификационный справочник должностей руководителей, специалистов и других служащих;
- 5) ИКТ – информационно-коммуникационные технологии;
- 6) ПО – программное обеспечение;
- 7) ИБ – информационная безопасность;
- 8) ИС – информационная система;
- 9) ОС – операционная система;
- 10) НТД – нормативно-технические документы;
- 11) СКУД – система контроля и управления доступом.

2. Паспорт профессионального стандарта

4. Наименование ПС: «Информационная безопасность».

5. Цель разработки ПС: Системное и структурированное описание трудовых функций, соответствующих требованиям к знаниям, умениям, навыкам и личностным компетенциям работников.

6. Краткое описание ПС: Планирование, контроль, мониторинг и обеспечение ИБ.

7. Основная группа: ИКТ.

Профессиональная группа: Эксплуатация и сопровождение ПО.

Профессиональная подгруппа: Обеспечение ИБ.

3. Карточки профессий

8. Перечень профессий:

- 1) Специалист по информационной безопасности, 4 уровень квалификации по ОРК;
- 2) Специалист по информационной безопасности, 5 уровень квалификации по ОРК;
- 3) Специалист по информационной безопасности, 6 уровень квалификации по ОРК.

Карточки профессий приводятся в Приложении к настоящему профессиональному стандарту.

Приложение
к Профессиональному стандарту
«Информационная безопасность»

КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»	
Код профессии:	-
Наименование профессии:	«Специалист по информационной безопасности»
Квалификационный уровень по ОРК:	4. Техническое и профессиональное образование, без практического опыта
Уровень квалификации по КС:	-
Трудовые функции	<ol style="list-style-type: none"> 1) Планирование процессов управления ИБ организации. 2) Планирование процессов обеспечения ИБ организации. 3) Планирование мероприятий по обеспечению ИБ организации. 4) Контроль процессов управления и обеспечения ИБ организации. 5) Обеспечение ИБ организации.
Трудовая функция 1 Планирование процессов управления ИБ организации	Умения и навыки: 1. Выявление и описание бизнес-процессов, связанных с автоматизированной обработкой информации.
	Знания: 1. Базовые знания о принципах и применении ИКТ для автоматизации бизнес-процессов. 2. Методики описания бизнес-процессов. 3. Общие представления о принципах и этапах проектирования, создания и эксплуатации ИС.
Трудовая функция 2 Планирование процессов обеспечения ИБ организации	Умения и навыки: 1. Разработка (актуализация) шаблонов (макетов) документов, регламентирующих процессы обеспечения ИБ в организации (регистрация и учет событий ИБ, резервное копирование, антивирусная защита, контроль доступа, обеспечение ИБ при работе со съемными носителями, мобильными устройствами, почтовыми службами и Интернетом, реагирование на инциденты ИБ, использование средств криптографии и их носителей, управление лицензиями и версионностью ПО).
	Знания: 1. Основные принципы, методы и средства обеспечения ИБ. 2. Основные нормативные правовые акты Республики Казахстан в сфере информатизации, ИБ.

	<p>3. Стандарты Республики Казахстан, международные и межгосударственные по вопросам обеспечения ИБ.</p> <p>4. Порядок разработки, оформления и утверждения нормативно-технических документов.</p>
<p>Трудовая функция 3 Планирование мероприятий по обеспечению ИБ организации</p>	<p>Умения и навыки:</p> <p>1. Участие в выполнении инвентаризации активов, связанных с автоматизированной обработкой информации.</p> <p>Знания:</p> <p>1. Стандарты и методы классификации, учета и маркировки активов, связанных с обработкой информации.</p> <p>2. Порядок оформления технической и отчетной документации.</p>
<p>Трудовая функция 4 Контроль процессов управления и обеспечения ИБ организации</p>	<p>Умения и навыки:</p> <p>1. Контроль полноты, своевременности и фактов ознакомления сотрудниками с документами, регламентирующими процессы обеспечения ИБ.</p> <p>2. Проведение проверки соблюдения требований документов, регламентирующих процессы обеспечения ИБ сотрудниками, подрядчиками и третьими сторонами.</p> <p>3. Составление и оформление актов контрольных проверок выполнения требований документов, регламентирующих процессы обеспечения ИБ.</p> <p>Знания:</p> <p>1. Нормативно-техническая документация по ИБ организации.</p> <p>2. Принципы оценки результатов применения организационных и технических решений по обеспечению ИБ.</p> <p>3. Основы способов контроля выполнения планов и мероприятий по контролю процессов управления и обеспечения ИБ организации.</p> <p>4. Иметь представления о принципах и методах 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.</p>
<p>Трудовая функция 5 Обеспечение ИБ организации</p>	<p>Умения и навыки:</p> <p>1. Осуществление тестирования (апробации) аппаратно-программных средств обеспечения ИБ.</p>

	<ol style="list-style-type: none"> 2. Проверка состояния аппаратно-программных средств обеспечения ИБ, поступивших из ремонта. 3. Осуществление технического сопровождения (регламентные и профилактические работы) аппаратно-программных средств обеспечения ИБ. 4. Выполнение работ по обеспечению послеаварийного восстановления работоспособности аппаратно-программных средств обеспечения ИБ. 5. Осуществление технического сопровождения (регламентные и профилактические работы) систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации. 6. Анализ журналов СКУД и записей систем видеонаблюдения. 7. Формирование отчетной документации по результатам проведенных работ.
	<p>Знания:</p> <ol style="list-style-type: none"> 1. Базовые знания и представления об ОС и встроженных в них механизма защиты. 2. Назначения, технические характеристики, конструкции, особенности и правила эксплуатации аппаратно-программных средств обеспечения ИБ. 3. Общие представления о назначении, сферах применения и принципах построения систем мониторинга уязвимостей, мониторинга ИБ и предотвращения утечек информации. 4. Общие представления о принципах функционирования СКУД и систем видеонаблюдения. 5. Общие представления о назначении и содержании регламентных и профилактических работ по обеспечению ИБ организации. 6. Понимать принципы ведения технической и отчетной документации.
Требования к личностным компетенциям	Организованность, инициативность, внимательность, ответственность, дисциплинированность, исполнительность, ориентация на результат, работа в команде.
Связь с другими профессиями в рамках ОРК	-
КАРТОЧКА ПРОФЕССИИ «СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»	
Код профессии:	-
Наименование профессии:	«Специалист по информационной безопасности»
Квалификационный уровень по ОРК:	5. Техническое и профессиональное образование, с

	практическим опытом Высшее образование, дополнительные профессиональные образовательные программы, без практического опыта
Уровень квалификации по КС:	-
Трудовые функции	<ol style="list-style-type: none"> 1) Планирование процессов управления ИБ организации. 2) Планирование процессов обеспечения ИБ организации. 3) Планирование мероприятий по обеспечению ИБ организации. 4) Контроль процессов управления и обеспечения ИБ организации. 5) Обеспечение ИБ организации.
Трудовая функция 1 Планирование процессов управления ИБ организации	<p>Умения и навыки:</p> <ol style="list-style-type: none"> 1. Осуществление разработки НТД процессов управления ИБ охватывающие процессы управления (оценки) рисками, активами, инцидентами, техническими уязвимостями, угрозами, техническим противодействиям угрозам, непрерывностью бизнеса. 2. Разработка шаблона (макета) политики ИБ. <p>Знания:</p> <ol style="list-style-type: none"> 1. Нормативные правовые акты Республики Казахстан в сфере информатизации, ИБ. 2. Стандарты Республики Казахстан, международные и межгосударственные по вопросам управления ИБ. 3. Принципы оценки и управления рисками ИБ. 4. Общие представления о способах анализа угроз и уязвимостей ИС.
Трудовая функция 2 Планирование процессов обеспечения ИБ организации	<p>Умения и навыки:</p> <ol style="list-style-type: none"> 1. Разработка (актуализация) документов, регламентирующих процессы обеспечения ИБ (регистрация и учет событий ИБ, резервное копирование, антивирусная защита, контроль доступа, обеспечение ИБ при работе со съемными носителями, мобильными устройствами, почтовыми службами и Интернетом, реагирование на инциденты ИБ, использование средств криптографии и их носителей, управление лицензиями и версионностью ПО). <p>Знания:</p> <ol style="list-style-type: none"> 1. Стандарты Республики Казахстан (международные и межгосударственные) по вопросам обеспечения ИБ. 2. Принципы защитных механизмов программных и аппаратных средств организации. 3. Общие представления о современном отечественном и зарубежном опыте,

	инструментарии, методах и средствах обеспечения ИБ.
Трудовая функция 3 Планирование мероприятий по обеспечению ИБ организации	Умения и навыки: <ol style="list-style-type: none"> 1. Участие в выполнении категоризации активов, связанных с автоматизированной обработкой информации. 2. Выявление рисков, угроз и каналов утечек для бизнес-процессов и активов, связанных с автоматизированной обработкой информации. 3. Анализ рынка программно-технических средств обеспечения ИБ. 4. Разработка спецификаций на подсистемы ИБ ИС. 5. Разработка профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры.
	Знания: <ol style="list-style-type: none"> 1. Стандарты и методы классификации, учета и маркировки активов, связанных с обработкой информации. 2. Подходы к формированию требований и оценке безопасности ИС. 3. Методики и средства выявления каналов утечки информации. 4. Способы применения защитных механизмов программных и аппаратных средств организации. 5. Принципы и методологии проектирования ИС.
Трудовая функция 4 Контроль процессов управления и обеспечения ИБ организации	Умения и навыки: <ol style="list-style-type: none"> 1. Осуществление контроля за соблюдением требований НТД процессов управления ИБ. 2. Составление и оформление актов контрольных проверок выполнения требований НТД процессов управления ИБ. 3. Консультирование работников организации по вопросам, связанным с обеспечением ИБ.
	Знания: <ol style="list-style-type: none"> 1. Нормативно-технические документы по ИБ организации. 2. Методики оценки результатов применения организационных и технических решений по обеспечению ИБ. 3. Основы способов контроля выполнения планов и мероприятий по обеспечению ИБ. 4. Методики оценки и управления рисками ИБ.
Трудовая функция 5 Обеспечение ИБ организации	Умения и навыки: <ol style="list-style-type: none"> 1. Установка и настройка аппаратно-программных средств обеспечения ИБ. 2. Осуществление администрирования аппаратно-программных средств обеспечения

	<p>ИБ.</p> <ol style="list-style-type: none"> 3. Настройка политики для систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации. 4. Осуществление администрирования систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации, антивирусной защиты, обновлений антивирусных баз. 5. Проведение мониторинга событий ИБ и инцидентов ИБ. 6. Произведение оповещения о критических (аварийных) ситуациях и событиях ИБ. 7. Осуществление администрирования СКУД и систем видеонаблюдения. 8. Контроль реализации профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры. 9. Осуществление контроля за разделением сред разработки, тестирования и эксплуатации ИС. 10. Формирование отчетной документации по результатам проведенных работ.
	<p>Знания:</p> <ol style="list-style-type: none"> 1. Принципы и средства администрирования в ОС и встроенных в них механизмов защиты. 2. Принципы построения и применения аппаратно-программных средств обеспечения ИБ, систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации. 3. Методы определения, предотвращения и устранения последствий инцидентов ИБ, критических (аварийных) ситуаций. 4. Принципы работ и администрирования аппаратно-программных средств обеспечения ИБ. 5. Принципы работ и администрирования систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации. 6. Базовые принципы и способы выполнения работ по разработке, тестированию и эксплуатации программных средств.
Требования к личностным компетенциям	Организованность, инициативность, внимательность, ответственность, дисциплинированность, исполнительность, гибкость мышления, ориентация на результат, высокая обучаемость, работа в команде.
Связь с другими профессиями в рамках ОРК	-
КАРТОЧКА ПРОФЕССИИ	

«СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»	
Код профессии:	-
Наименование профессии:	«Специалист по информационной безопасности»
Квалификационный уровень по ОРК:	6. Высшее образование, практический опыт
Уровень квалификации по КС:	-
Трудовые функции	<ol style="list-style-type: none"> 1) Планирование процессов управления ИБ организации. 2) Планирование процессов обеспечения ИБ организации. 3) Планирование мероприятий по обеспечению ИБ организации. 4) Контроль процессов управления и обеспечения ИБ организации. 5) Обеспечение ИБ организации.
Трудовая функция 1 Планирование процессов управления ИБ организации	<p>Умения и навыки:</p> <ol style="list-style-type: none"> 1. Координация аналитической работы по ИБ. 2. Анализ, выбор методик и методов оценки и реализации процессов управления ИБ охватывающие процессы управления рисками, активами, инцидентами, техническими уязвимостями, угрозами, техническим противодействиям угрозам, непрерывностью бизнеса. 3. Согласование НТД процессов управления ИБ. 4. Координация деятельности по разработке (актуализации) политики ИБ, НТД процессов управления ИБ и документов, регламентирующих процессы обеспечения ИБ. 5. Публикация и доведение утвержденной (актуализированной) политики ИБ организации до сведения сотрудников. <p>Знания:</p> <ol style="list-style-type: none"> 1. Базовые принципы регламентации бизнес-процессов. 2. Нормативные правовые акты Республики Казахстан в сфере информатизации, ИБ. 3. Стандарты Республики Казахстан, международные, межгосударственные в области ИКТ, ИБ, защиты информации и криптографии. 4. Принципы и методологии проектирования и эксплуатации ИС. 5. Принципы регламентации бизнес-процессов. 6. Методы управления проектами. 7. Методики оценки и управления рисками ИБ. 8. Методика анализа угроз и уязвимостей ИС. 9. Методы классификации, учета и маркировки активов, связанных с обработкой информации.
Трудовая функция 2	Умения и навыки:

<p>Планирование процессов обеспечения ИБ организации</p>	<p>1. Координация работ по разработке (актуализации) документов, регламентирующих процессы обеспечения ИБ (регистрация и учет событий ИБ, резервное копирование, антивирусная защита, контроль доступа, обеспечение ИБ при работе со съемными носителями, мобильными устройствами, почтовыми службами и Интернетом, реагирование на инциденты ИБ, использование средств криптографии и их носителей, управление лицензиями и версионностью ПО).</p> <p>Знания:</p> <ol style="list-style-type: none"> 1. Нормативные правовые акты Республики Казахстан а области ИБ. 2. Нормативно-технические документы по ИБ. 3. Принципы, методы и средства обеспечения ИБ при определении мероприятий по непрерывности бизнеса, регистрации и учету событий ИБ, резервному копированию, антивирусной защите, контролю доступа, работе со съемными носителями, мобильными устройствами, удаленного доступа, использованием криптографии и их носителей, лицензиях и версионностью ПО. 4. Основные тенденции развития отечественного и зарубежного рынка инструментария и средств обеспечения ИБ.
<p>Трудовая функция 3 Планирование мероприятий по обеспечению ИБ организации</p>	<p>Умения и навыки:</p> <ol style="list-style-type: none"> 1. Анализ защищенности бизнес-процессов и активов, связанных с автоматизированной обработкой информации. 2. Выбор инструментария и методов обеспечения ИБ. 3. Разработка мероприятий, направленных на реализацию политики ИБ организации. 4. Составление плана по обеспечению непрерывности бизнеса и восстановления после инцидентов ИБ и форс-мажорных ситуаций. 5. Разработка технических спецификаций, тендерной документации на закупаемые средства обеспечения ИБ. 6. Разработка требований, технических заданий на подсистемы ИБ ИС. 7. Организация и координация работ по разработке профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры. <p>Знания:</p> <ol style="list-style-type: none"> 1. Углубленное понимание методики описания и

	<p>формализации бизнес-процессов.</p> <ol style="list-style-type: none"> 2. Принципы и методы выявления и блокирования каналов утечки информации. 3. Нормативные правовые акты Республики Казахстан в области ИБ. 4. Средства обеспечения ИБ, систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации, защитных механизмов систем. 5. Стандарты и методы классификации, учета и маркировки активов, связанных с обработкой информации. 6. Подходы к формированию требований и оценке безопасности ИС. 7. Принципы и методологии проектирования ИС. 8. Способы применения защитных механизмов программных и аппаратных средств организации.
<p>Трудовая функция 4 Контроль процессов управления и обеспечения ИБ организации</p>	<p>Умения и навыки:</p> <ol style="list-style-type: none"> 1. Осуществление контроля реализации плана мероприятий по обеспечению ИБ. 2. Анализ результатов проверок исполнения требований документов, регламентирующих процессы обеспечения ИБ и ИТД процессов управления ИБ в организации. 3. Участие в разработке соглашений о конфиденциальности или неразглашении информации с сотрудниками организации, подрядчиками и третьими сторонами. <p>Знания:</p> <ol style="list-style-type: none"> 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.
<p>Трудовая функция 5 Обеспечение ИБ организации</p>	<p>Умения и навыки:</p> <ol style="list-style-type: none"> 1. Оценка эффективности применяемых аппаратно-программных средств обеспечения ИБ. 2. Разработка политики для систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации. 3. Реагирование на инциденты ИБ организации. 4. Осуществление организации взаимодействия с полномочными организациями по вопросам ИБ. 5. Контроль выполнения планов технического противодействия угрозам информации организации.

	<ol style="list-style-type: none"> 6. Оценка эффективности применяемых систем мониторинга уязвимостей, систем мониторинга ИБ и систем предотвращения утечек информации, антивирусной защиты. 7. Анализ эффективности профилей защиты и задания по безопасности для ИС и компонентов информационно-коммуникационной инфраструктуры. 8. Анализ эффективности применения инструментария и методов обеспечения ИБ. 9. Разработка предложений по совершенствованию (развитию) и повышению эффективности применяемых средств и методов обеспечения ИБ. 				
	<p>Знания:</p> <ol style="list-style-type: none"> 1. Методики оценки эффективности применения организационных и технических средств обеспечения ИБ. 2. Принципы функционирования и администрирования ОС и встроенных в них механизмов защиты. 3. Принципы построения и применения аппаратно-программных средств обеспечения ИБ, систем мониторинга уязвимостей, систем мониторинга информационной безопасности и систем предотвращения утечек информации. 4. Принципы анализа методов определения, предотвращения и устранения последствий инцидентов ИБ, критических (аварийных) ситуаций. 5. Способы анализа процессов обеспечения ИБ организации. 6. Порядок ведения технической и отчетной документации. 7. Порядок реагирования и проведения расследования инцидента ИБ, принципов и способов регистрации событий и инцидентов ИБ. 8. Иметь представление о компетенциях полномочных организаций по вопросам ИБ. 				
Требования к личностным компетенциям	Организованность, инициативность, внимательность, ответственность, дисциплинированность, исполнительность, аналитическое мышление, планирование, принятие решения, ориентация на результат, стремление к повышению профессионального уровня, работа в команде.				
Связь с другими профессиями в рамках ОРК	<table border="1"> <tr> <td data-bbox="740 1926 874 2000">-</td> <td data-bbox="874 1926 1458 2000">Специалист по защите информации в комплексе</td> </tr> <tr> <td data-bbox="740 2000 874 2072">-</td> <td data-bbox="874 2000 1458 2072">Аудитор по информационной безопасности</td> </tr> </table>	-	Специалист по защите информации в комплексе	-	Аудитор по информационной безопасности
-	Специалист по защите информации в комплексе				
-	Аудитор по информационной безопасности				

Технические характеристики профессионального стандарта	
Разработано	АО «Национальный инфокоммуникационный Холдинг «Зерде»
Номер версии и год выпуска	Версия 1, 2015 год
Дата ориентировочного пересмотра	2018 год