СОГЛАСОВАНО:

Главный эксперт

_____ Я.И. Веснинов

СОГЛАСОВАНО:

Индустриальный партнер

АО «Научно-исследовательский институт «Вектор»,

заместитель директора Центра защиты информации

_____ Д.В. Магницкий

М.П

ОПИСАНИЕ КОМПЕТЕНЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2023

Формат участия в соревновании: командный, в команде 2 участника

Описание компетенции.

Информационная безопасность представляет собой многодисциплинарную область знаний умений и навыков в сфере информационных технологий.

Специалисты по информационной безопасности отвечают за обеспечение конфиденциальности, целостности и доступности данных в процессе их передачи, обработки и хранения на всех этапах проектирования и эксплуатации информационных систем и/или информационной инфраструктуры предприятия в рамках своей области специализации.

Цифровая трансформация экономики характеризуется инновационными процессами внедрения информационных технологий во все сферы социально-политической и экономической жизни общества.

Инновационные решения требуют тщательного изучения. Необходимо глубокое изучение новых технических решений с целью выявления в них различного рода уязвимостей. Из-за повышенного спроса и острой конкуренции многие инновации внедряются без должного тестирования на предмет информационной безопасности. Новые технологии могут стать инструментом в руках злоумышленников для достижения ими своих противоправных целей, создавая новые, ранее не изученные вектора атак, дополнительный функционал по автоматизации процессов и увеличению масштабов и географии атак и новые механизмы обхода, существовавших ранее, средств защиты. Инновационные технологии могут послужить основой для создания принципиально новой интеллектуальной системы информационной безопасности, в том числе как ответ на новые вызовы со стороны киберпреступности.

Препятствиями для реализации целей развития цифровой экономики в

сфере информационной безопасности являются рост масштабов компьютерной преступности, в том числе международной, отставание РФ в разработке и использовании отечественного программного обеспечения, недостаточный уровень кадрового обеспечения в области информационной безопасности.

Реализация направления «Информационная безопасность» обеспечит развитие устойчивости и безопасности информационной инфраструктуры, повышение конкурентоспособности отечественных разработок и технологий информационной безопасности и выстраивание эффективной системы защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности.

Специалист должен знать и понимать:

– методы планирования своей работы;
– методы декомпозиции и приоритизации поставленных задач;
– важность проверки выполненной работы в каждом ее аспекте;
– методы эффективной работы в составе команды;
– методы демонстрации и презентации материала;
– современные тенденции в области информационных технологий и в подходах к построению ИТ-инфраструктуры;
– отраслевые стандарты и системы профессиональных сертификаций;
– стандарты профессиональной коммуникации при работе в системах поддержки пользователей;
– системы управления учетными данными пользователей;
– принципы кибербезопасности, используемые для управления рисками при использовании, обработке, хранении и передаче данных;
– принципы управления жизненным циклом информационных систем;
– цели и задачи организации в области информационных технологий;
– системы хранения ключей для поддержки шифрования данных;
– средства управления, связанные с использованием, обработкой, хранением и передачей данных;
– реализации файловых систем;

– системные файлы (например, файлы журнала, файлы реестра, файлы конфигурации) которые содержат соответствующую информацию и их местоположение;

– концепции архитектуры сетевой безопасности, включая топологию, протоколы, компоненты и принципы их взаимодействия;

– отраслевые стандартны в области анализа, методов и инструментов для выявления уязвимостей;

– категории инцидентов, методы реагирования и обработки;

– разработка контрмер для выявления угроз безопасности;

– подходы к реализации аутентификации, авторизации и учета;

– кто является объектами и субъектами угроз кибербезопасности;

– методы и приемы, используемые для обнаружения различных видов уязвимостей;

– методы и средства сбора информации и ее хранения;

– источники распространения информации об уязвимостях;

– стратегия использования инструментов для поиска уязвимостей;

– техники получения несанкционированного доступа;

– методы прогнозирования и / или эмуляции угроз;

– примеры использования системных артефактов в компьютерной криминалистике.

Специалист должен уметь:

– разрабатывать документацию к существующей или проектируемой информационной структуре предприятия;

– формировать корректные, отвечающие требованиям и ограничениям, рекомендации на основе запросов и потребностей заказчика;

– выстраивать эффективное письменное и устное общение на русском и английском языке;

– применять аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;

– точно описывать инцидент и документировать решение проблемы;

– осуществлять поиск информации в открытых источниках и работать с

технической документацией;

– формировать базу знаний;

– анализировать и разрабатывать процедуры интеграции, тестирования, эксплуатации, сопровождения механизмов безопасности информационных систем;

– управлять безопасностью телекоммуникационных ресурсов организации;

– работать с системами управления крипто-ключами;

– проводить оценку дизайна решений по обеспечению безопасности;

– использовать данные, собранные с помощью различных инструментов киберзащиты (например, оповещения IDS, межсетевые экраны, журналы сетевого трафика), для анализа событий, происходящих в информационной инфраструктуре, с целью уменьшения количества потенциальных инцидентов;

– тестировать, внедрять, развертывать, поддерживать и управлять аппаратным и программным обеспечением в рамках информационной инфраструктуры организации;

– расследовать, анализировать и реагировать на инциденты кибербезопасности в сетевой среде;

– разрабатывать индикаторы угроз кибербезопасности для поддержания осведомленности о состоянии информационной инфраструктуры;

– собирать, обрабатывать, анализировать и распространять оценки угроз кибербезопасности;

– выявлять уязвимости в информационных системах и/или элементах информационной инфраструктуры;

– использовать авторизованные ресурсы и аналитические методы для проникновения в целевые сети и/или системы;

– анализировать данные из одного или нескольких источников для планирования мероприятий по реагированию на инциденты кибербезопасности;

– выполнять оценку конфигурации элементов информационной

инфраструктуры и определять, насколько данная конфигурация отклоняется от приемлемой, определенной локальной политикой безопасности.

Нормативные правовые акты

Поскольку описание компетенции содержит лишь информацию, относящуюся к соответствующей компетенции, его необходимо использовать на основании следующих документов:

1. ФГОС СПО

- ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем. Приказ Министерства образования и науки РФ от 9 декабря 2016 г. № 1551;
- ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Приказ Министерства образования и науки РФ от 9 декабря 2016 г. № 1553.
- Профстандарт: 06.030 Специалист по защите информации в телекоммуникационных системах и сетях. Утвержден приказом Министерства труда и социальной защиты РФ от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции РФ 25 ноября 2016 г., регистрационный № 44449);
- Профстандарт: 06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Министерства труда и социальной защиты РФ от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции РФ 28 ноября 2016 г., регистрационный № 44464);
- Профстандарт: 06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты РФ от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции РФ 28 сентября 2016 г., регистрационный № 43857);
- Профстандарт: 06.034 Специалист по технической защите информации. Утвержден приказом Министерства труда и социальной защиты РФ от 1 ноября 2016 г. № 599н (зарегистрирован Министерством юстиции РФ 25 ноября 2016 г., регистрационный № 44443);
- Профстандарт: 06.030 Специалист по защите информации в

телекоммуникационных системах и сетях. Утвержден приказом Министерства труда и социальной защиты РФ от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции РФ 25 ноября 2016 г., регистрационный № 44449);

- Профстандарт: 06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Министерства труда и социальной защиты РФ от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции РФ 28 ноября 2016 г., регистрационный № 44464);
- Профстандарт: 06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты РФ от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции РФ 28 сентября 2016 г., регистрационный № 43857);
- Профстандарт: 06.034 Специалист по технической защите информации. Утвержден приказом Министерства труда и социальной защиты РФ от 1 ноября 2016 г. № 599н (зарегистрирован Министерством юстиции РФ 25 ноября 2016 г., регистрационный № 44443);
- Профстандарт: 12.004 Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак. Утвержден приказом Министерства труда и социальной защиты РФ от 29 декабря 2015 г. № 1179н (зарегистрирован в Минюсте России 28 января 2016 г., № 40858).
- Утвержден постановлением Министерством труда и социального развития РФ от 21 августа 1998 г. №37 «Об утверждении квалификационного справочника должностей руководителей, специалистов и других служащих».
- ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Настоящий стандарт применяется совместно с ГОСТ 34.003, ГОСТ 19781, ГОСТ Р 22.0.02, ГОСТ Р 50922, ГОСТ Р 51898, ГОСТ Р 52069.0, ГОСТ Р 51275, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 13335-1.
- ГОСТ Р52653-2006 Информационно-коммуникационные технологии в образовании. Термины и определения;
- ГОСТ Р53626-2009 Информационно-коммуникационные технологии в образовании. Технические средства обучения. Общие положения.

- СанПин
- СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы;
- СанПиН 2.4.2.2821-10 Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях (утверждены постановлением Главного государственного санитарного врача РФ от 29 декабря 2010 г. № 189, зарегистрированы в Минюсте России 3 марта 2011 г., регистрационный № 19993)

2. Квалификационные характеристики (профессиограмма)

- Техник по защите информации

Должностные обязанности

Участвует в работе по обеспечению информационной безопасности исследований и разработок, соблюдению государственной тайны. Осуществляет проверку технического состояния, установку, наладку и регулировку аппаратуры и приборов, их профилактические осмотры и текущий ремонт. Выполняет работы по эксплуатации средств защиты и контроля информации, следит за работой аппаратуры и другого оборудования. Ведет учет работ и объектов, подлежащих защите, установленных технических средств, журналы нарушений их работы, справочники. Готовит технические средства для проведения всех видов плановых и внеплановых контрольных проверок, аттестации оборудования, а также в случае необходимости к сдаче в ремонт. Проводит наблюдения, выполняет работу по оформлению протоколов специальных измерений и другой технической документации, в том числе отчетной, связанной с эксплуатацией средств и контроля информации. Выполняет необходимые расчеты, анализирует и обобщает результаты, составляет технические отчеты и оперативные сведения. Определяет причины отказов в работе технических средств, готовит предложения по их устранению и предупреждению, обеспечению высокого качества и надежности используемого оборудования, повышению эффективности мероприятий по контролю и защите информации. Участвует во внедрении разработанных технических решений и проектов, оказании

технической помощи при изготовлении, монтаже, наладке, испытаниях и эксплуатации проектируемой аппаратуры.

Должен знать: руководящие, нормативные и методические материалы по вопросам, связанным с обеспечением защиты информации и соблюдением государственной тайны; специализацию учреждения, организации, предприятия и особенности их деятельности; методы и технические средства, используемые в целях обеспечения защиты информации; требования, предъявляемые к выполняемой работе; терминологию, применяемую в специальной литературе по профилю работы; принципы работы и правила эксплуатации технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты и другого оборудования, используемого при проведении работ по защите информации, организацию их ремонтного обслуживания; методы измерений, контроля и технических расчетов; порядок оформления технической документации по защите информации; инструкции по соблюдению режима проведения специальных работ; отечественный и зарубежный опыт в области технической разведки и защиты информации; основы экономики, организации производства, труда и управления; основы трудового законодательства; правила и нормы охраны труда.

Требования к квалификации

Техник по защите информации I категории: среднее профессиональное образование и стаж работы в должности техника по защите информации II категории не менее 2 лет.

Техник по защите информации II категории: среднее профессиональное образование и стаж работы в должности техника по защите информации или других должностях, замещаемых специалистами со средним профессиональным образованием, не менее 2 лет.

Техник по защите информации: среднее профессиональное образование без предъявления требований к стажу работы.

3. СП (СНИП)

- СП 2.4.3648-20 Санитарно-эпидемиологические требования к

организациям воспитания и обучения, отдыха и оздоровления детей и молодежи. Утверждены постановлением Главного Государственного санитарного врача РФ от 28 сентября 2020 г. № 28.

- Перечень профессиональных задач специалиста по компетенции **о**пределяется профессиональной областью специалиста и базируется на требованиях современного рынка труда к данному специалисту.

№ п/п	Виды деятельности/трудовые функции
1.	Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД
2.	Обслуживание средств защиты информации в компьютерных системах и сетях
3.	Обслуживание систем защиты информации в автоматизированных системах
4.	Проведение работ по установке и техническому обслуживанию средств защиты информации
5.	Эксплуатация автоматизированных систем в защищенном исполнении
6.	Защита информации в автоматизированных системах в программным и программно-аппаратными средствами
7.	Защита информации техническими средствами