СОГЛАСОВАНО:

Главный эксперт

_____ С.М. Борисов

СОГЛАСОВАНО:

Индустриальный партнер

АО «Научно-исследовательский институт «Вектор»,

заместитель директора Центра защиты информации

_____ Д.В. Магницкий

М.П

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2023 г.

Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции, в котором установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

Конкурсное задание включает в себя следующие разделы:

1. Основные требования компетенции

1.1. Общие сведения о требованиях компетенции

Требования компетенции (ТК) «Информационная безопасность» определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли.

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии.

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов / рабочих и участия их в конкурсах профессионального мастерства.

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

1.2. Перечень профессиональных задач специалиста по компетенции «Информационная безопасность»

Таблица №1

Перечень профессиональных задач специалиста

№ п/п	Раздел	Важность в %
1	ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ	20
	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;	

	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;	
2	ЭКСПЛУАТАЦИЯ, СОПРОВОЖДЕНИЕ И НАДЗОР	20
	Специалист должен знать и понимать • Системы управления учетными данными пользователей • Принципы информационной безопасности, 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	
	Специалист должен уметь • 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	
3	ЗАЩИТА ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	30
	Специалист должен знать и понимать • 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	

	Специалист должен уметь • 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 информационной безопасности в сетевой среде • Выполнять оценку конфигурации элементов информационной инфраструктуры и определять, насколько данная конфигурация отклоняется от приемлемой, определенной локальной политикой безопасности	
4	АНАЛИЗ ЗАЩИЩЕННОСТИ	30
	Специалист должен знать и понимать • Кто является объектами и субъектами угроз информационной безопасности • 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 индикаторы угроз информационной безопасности для поддержания осведомленности о состоянии информационной инфраструктуры • Собирать, обрабатывать, анализировать и распространять оценки угроз информационной безопасности • 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 информационной безопасности	

1.3. Требования к схеме оценки

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице №2.

Таблица №2

Матрица пересчета требований компетенции в критерии оценки

Критерий/Модуль						Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ
Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ		А	Б	В	Г	
	1	10	6	2	2	20
	2	8	4	2	6	20
	3	16	0	6	8	30
	4	0	14	10	6	30
Итого баллов за критерий/модуль		34	24	20	22	**100**

1.4. Спецификация оценки компетенции

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №3:

Таблица №3

Оценка конкурсного задания

Критерий		Методика проверки навыков в критерии
А	**Защита корпоративной ИТ-инфраструктуры**	Оценивается корректная интеграция и настройка средств программной защиты, созданные политики, отчет
Б	**Расследование инцидентов информационной безопасности**	Оценивается количество расследованных инцидентов и полнота описания используемых методов.
В	**Аудит информационной системы**	Оценивается умение находить и эксплуатировать имеющиеся уязвимости в сетях и системах
Г	**Проактивный анализ**	Оценивается корректность анализа полученных данных, ликвидаций результатов атаки и рекомендаций для защиты.

1.5. Конкурсное задание

Общая продолжительность Конкурсного задания: 16 часов (СПО).

Количество конкурсных дней: 3 дня

Вне зависимости от количества модулей, КЗ должно включать оценку по каждому из разделов требований компетенции.

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний / оценки квалификации.

1.5.1. Разработка/выбор конкурсного задания (ссылка на Яндекс Диск с матрицей, заполненной в Excel)

Конкурсное задание состоит из 4 модулей, включает обязательную к выполнению часть (инвариант) – 2 модулей, и вариативную часть – 2 модулей. Общее количество баллов конкурсного задания составляет 100.

Обязательная к выполнению часть (инвариант) выполняется всеми регионами без исключения на всех уровнях чемпионатов.

Количество модулей из вариативной части, выбирается регионом самостоятельно в зависимости от материальных возможностей площадки соревнований и потребностей работодателей региона в соответствующих специалистах. В случае если ни один из модулей вариативной части не подходит под запрос работодателя конкретного региона, то вариативный (е) модуль (и) формируется регионом самостоятельно под запрос работодателя. При этом, время на выполнение модуля (ей) и количество баллов в критериях оценки по аспектам не меняются.

Таблица №4

Матрица конкурсного задания

Обобщенная трудовая функция	Трудовая функция	Нормативный документ/ЗУН	Модуль	Константа/вариатив	ИЛ	КО
1	2	3	4	5	6	7

Инструкция по заполнению матрицы конкурсного задания **(Приложение № 1)**

1.5.2. Структура модулей конкурсного задания (инвариант/вариатив)

1.5.2.1. Структура модулей конкурсного задания (инвариант)

Модуль А. Защита корпоративной ИТ-инфраструктуры

Время на выполнение модуля 6 часов.

Задания: Компания ООО «ИБ» делегировала Вам права для организации защищенной инфраструктуры предприятия в условиях импортозамещения на базе программно-аппаратных комплексов компании АО «ИнфоТэКС».

Директор департамента информационной безопасности ООО «ИБ» предоставил Вам согласованную топологию сети организации и техническое задание для реализации внедрения программно-аппаратных комплексов.

Вам необходимо внедрить в использование следующие объекты:

1. Установить и настроить Центр управления сетью (далее ЦУС) и Сервер Удостоверяющий ключевой центр (далее УКЦ) на виртуальную машину.
2. Установить и настроить Клиент ЦУС и Клиент УКЦ на виртуальную машину.
3. Установить и настроить клиентов на виртуальные машину на базе ОС Windows 10 и Ubuntu Desktop.
4. Установить и настроить координатор для обеспечения защищенного VPN-соединения
5. Установить и настроить файрвол для разграничения сетевого трафика внутри корпоративной сети предприятия.
6. Установить и настроить IDS для обнаружения вторжений в корпоративную сеть предприятия.
7. Установить и настроить модуль доверенной загрузки операционной системы.
8. Установить и настроить криптографический шлюз

Для реализации технического задания Вам предоставлен максимальный уровень допуска.

Подготовить отчет о проделанной работе

Модуль Б. Расследование инцидентов информационной безопасности

Время на выполнение модуля 3 часа.

Задания: Вас пригласили в компанию ООО «ИБ» для проведения расследования инцидентов информационной безопасности.

Вам будет предоставлен набор заданий (тасков), к которым требуется найти и отправить ответ. Ответ даётся в виде флага, состоящего из набора символов или произвольной фразы. За верное выполнение каждого задания команда получает очки. Чем сложнее таск, тем больше очков даётся за правильный ответ. Задания будут выданы в формате Task-Based, по следующим возможным категориям: задачи на нахождение веб-уязвимостей (web), поиск и эксплуатацию уязвимостей в приложениях (PWN), исследование программ без исходного кода (reverse), расследование инцидентов (forensic), администрирование (admin), криптографию (crypto), стеганографию (stegano), поиск информации из открытых источников (OSINT).

Задача – решить максимальное количество инцидентов (тасков), подготовить отчет по каждому решению.

1.5.2.2. Структура модулей конкурсного задания (вариант)

Модуль В. Аудит информационной системы

Время на выполнение модуля 3 часа.

Задания: Вас пригласили в компанию ООО «ИБ» для проведения аудита компании с целью поиска возможных уязвимостей в действующем программном обеспечении и сервисах используемыми компанией. Ваша работа будет осуществляется в формате Red Team – вам разрешены попытки получить до-ступ к системе любыми способами, включающими в себя тестирование на проникновение; тестирование линий связи, беспроводных и радиочастотных систем; тестирование сотрудников посредством сценариев социальной инженерии.

Вам будет предоставлена вводная информация о компании. Необходимо провести анализ и дать описание найденной уязвимости, а также рекомендации к устранению выявленных инцидентов.

Модуль Г. Проактивный анализ

Время на выполнение модуля 4 часа.

Задания: Вас пригласили в компанию ООО «ИБ» для проведения проактивного анализа инцидентов информационной безопасности. На один из филиалов организации была совершена кибер-атака.

Вас направили для расследования инцидента и восстановления инфраструктуры и работоспособности сети и системы филиала, восстановление картины инцидента, рекомендаций, а также составления отчета о кибер-преступлении.

Задача – провести анализ произошедшей атаки, подготовить отчет о проделанной работе.

2. Специальные правила компетенции

При выполнении модуля А для каждой команды разворачиваются виртуальные стенды. Размещение стендов может быть как локальным (во внутренней локальной сети конкурсной площадки), так и на стороннем сервере с прямым доступом до стенда. При развертывании стендов на стороннем сервере необходимо обеспечить участникам доступ только до своих стендов со своих рабочих мест. Со стендов интернет разрешен только на сайт активации лицензий (при необходимости)

Оценка знаний конкурсанта проводится исключительно через практическое выполнение Конкурсного задания.

Результаты выполнения задания должны быть сохранены с соблюдением форматов и наименований файлов и папок в соответствии с заданием и предоставлены на проверку с учетом требований задания.

По истечении времени, отведенного на выполнение модуля, участник закрывает оставляет виртуальный стенд и машины на нем в рабочем состоянии и встает со своего рабочего места.

Проверка конкурсных работ выполняется на рабочих местах экспертных групп согласно типового ИЛ.

2.1. Личный инструмент конкурсанта

Нулевой - нельзя ничего привозить.

2.2. Материалы, оборудование и инструменты, запрещенные на площадке

Участникам во время выполнения конкурсного задания запрещено использовать сотовые телефоны, ноутбуки, планшеты, смарт часы и средства интернет ресурсов

3. Приложения

Приложение №1 Инструкция по заполнению матрицы конкурсного задания

Приложение №2 Матрица конкурсного задания

Приложение №3 Критерии оценки

Приложение №4 Инструкция по охране труда и технике безопасности по компетенции «Информационная безопасность».