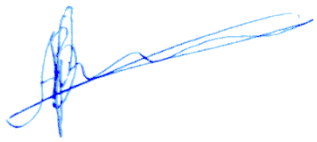
СОГЛАСОВАНО
Менеджер компетенции
«Корпоративная защита от внутренних угроз ИБ»:



ТЕХНИЧЕСКОЕ ОПИСАНИЕ КОМПЕТЕНЦИИ «Корпоративная защита от внутренних угроз информационной безопасности»

2017-2021 гг.

Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (далее WSR) в соответствии с уставом организации и правилами проведения конкурсов установила нижеизложенные необходимые требования владения этим профессиональным навыком для участия в соревнованиях по компетенции.

Техническое описание включает в себя следующие разделы:

1. ВВЕДЕНИЕ

1.1. НАЗВАНИЕ И ОПИСАНИЕ ПРОФЕССИОНАЛЬНОЙ КОМПЕТЕНЦИИ

1.1.1 Название профессиональной компетенции:

«Корпоративная защита от внутренних угроз информационной безопасности».

1.1.2 Описание профессиональной компетенции.

В наши дни одним из наиболее актуальных вопросов защиты корпоративной информации – обеспечение безопасности от внутренних утечек по техническим каналам связи. Одна из главных угроз корпоративной информационной безопасности – неправомерные действия сотрудников (т.н. инсайдеров), приводящие к потере конфиденциальных данных, совершенные как целенаправленно, так и из-за халатности, невнимательности или незнания элементарных правил безопасности предприятия. Именно «на их совести» большинство громких краж данных, зафиксированных по всему миру в последние годы. Причиной утечек также могут быть действия посторонних лиц, находящихся на территории предприятия и имеющих доступ к вычислительно-сетевой инфраструктуре (клиенты, поставщики и т.п.). Утечки информации могут породить целый ряд проблем:

1. Утечка персональных данных. Может повлечь за собой как санкции со стороны контролирующих органов, так и отток клиентов, связанный с утратой доверия к компании.

2. Утечка коммерческой тайны и ноу-хау. Утечка информации об инвестиционных планах, маркетинговых программах, инновациях, данных клиентской базы способна привести к срыву важных и прибыльных проектов.

3. Утечка служебной переписки. Служебная переписка может дать конкурентам много информации о ситуации в компании.

4. Утечки в прессу. Могут повлечь за собой разглашение коммерческой тайны организации.

5. Утечка информации о системе безопасности. Открывает широкие возможности для деятельности криминальных структур.

6. Утечка сведений, составляющих государственную тайну и т.д.

Необходимость защиты от внутренних и внешних угроз информационной безопасности не только доказана на практике, но и упомянута в ключевых международных стандартах по организации и менеджменту информационной безопасности (например, в ISO/IEC 27001).

Технологии корпоративной защиты от внутренних угроз информационной безопасности, относящиеся к классу Data Leak Prevention (DLP) позволяют выявлять и предотвращать утечки конфиденциальной информации и персональных данных, защищать компании от мошенничества, воровства и коррупции, детектировать неправомерные действия сотрудников и нецелевое использование корпоративных ресурсов. Системы корпоративной безопасности позволяют однозначно выявлять инциденты и дают весь необходимый набор инструментов для проведения внутренних расследований и дальнейшей правовой защиты корпоративных интересов.

Специалисты по корпоративной безопасности должны обладать теоретическими знаниями по обеспечению корпоративной защиты от внутренних угроз, понимать аспекты применения нормативно-правовой базы для классификации и расследования инцидентов, в совершенстве владеть системами и технологиями для достижения целей защиты.

Неотъемлемой частью работ по обеспечению корпоративной безопасности от внутренних утечек является проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его. Для этого специалисты должны уметь проводить весь цикл работ по установке, развёртыванию, настройке, использованию DLP-систем, включая разработку

политик информационной безопасности, классификацию объектов защиты, применение технологий фильтрации различных видов трафика, фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.

Важным направлением обеспечения безопасности корпоративной информации – реализация прозрачного доступа к территориально-распределенным информационным ресурсам компании через сети связи общего пользования, в том числе Интернет. Для защиты передаваемых данных используется технологии виртуальной частной сети (Virtual Private Network, VPN) и межсетевого экранирования, включая:

- защиту информации, передаваемой по каналам связи;
- защиту сети в целом, ее сегментов от несанкционированного доступа, как из внешних, так и из внутренних сетей;
- контроль трафика между узлами VPN-сети, включая фильтрацию трафика;
- использование в качестве транспортной среды передачи данных каналы сетей связи общего пользования;
- возможность модернизации, модульного наращивания VPN-сети;
- централизованное управление VPN-сетью.

Для предотвращения и минимизации последствий атак на корпоративную инфраструктуру и объекты защиты, необходимо их своевременное выявление и правильная классификация с использованием системы обнаружения атак IDS (Intrusion Detection System).

Необходимо знать и уметь применять на практике средства защиты информации и механизмы разграничения доступа операционных систем, такие как групповые политики домена Windows, цифровые сертификаты, элементы

инфраструктуры открытых ключей (PKI), файерволы, системы контроля целостности и т.п.

Помимо перечисленного, специалист по корпоративной безопасности должен уметь подготовить отчёты о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой) менеджменту организации, которую защищает, а также правильно оценить угрозы и риски информационной безопасности.

1.2. ВАЖНОСТЬ И ЗНАЧЕНИЕ НАСТОЯЩЕГО ДОКУМЕНТА

Документ содержит информацию о стандартах, которые предъявляются участникам для возможности участия в соревнованиях, а также принципы, методы и процедуры, которые регулируют соревнования. При этом WSR признаёт авторское право WorldSkills International (WSI). WSR также признаёт права интеллектуальной собственности WSI в отношении принципов, методов и процедур оценки.

Каждый эксперт и участник должен знать и понимать данное Техническое описание.

1.3. АССОЦИИРОВАННЫЕ ДОКУМЕНТЫ

Поскольку данное Техническое описание содержит лишь информацию, относящуюся к соответствующей профессиональной компетенции, его необходимо использовать совместно со следующими документами:

- WSR, регламент проведения чемпионата;
- WSR, онлайн-ресурсы, указанные в данном документе.
- WSR, политика и нормативные положения
- Инструкция по охране труда и технике безопасности по компетенции

2. СПЕЦИФИКАЦИЯ СТАНДАРТА WORLDSKILLS (WSSS)

2.1. ОБЩИЕ СВЕДЕНИЯ О СПЕЦИФИКАЦИИ СТАНДАРТОВ WORLDSKILLS (WSSS)

WSSS определяет знание, понимание и конкретные компетенции, которые лежат в основе лучших международных практик технического и профессионального уровня выполнения работы. Она должна отражать коллективное общее понимание того, что соответствующая рабочая специальность или профессия представляет для промышленности и бизнеса.

Целью соревнования по компетенции является демонстрация лучших международных практик, как описано в WSSS и в той степени, в которой они могут быть реализованы. Таким образом, WSSS является руководством по необходимому обучению и подготовке для соревнований по компетенции.

В соревнованиях по компетенции проверка знаний и понимания осуществляется посредством оценки выполнения практической работы.

WSSS разделена на четкие разделы с номерами и заголовками. Каждому разделу назначен процент относительной важности в рамках WSSS. Сумма всех процентов относительной важности составляет 100.

В схеме выставления оценок и конкурсном задании оцениваются только те компетенции, которые изложены в WSSS. Они должны отражать WSSS настолько всесторонне, насколько допускают ограничения соревнования по компетенции.

Схема выставления оценок и конкурсное задание будут отражать распределение оценок в рамках WSSS в максимально возможной степени. Допускаются колебания в пределах 5% при условии, что они не исказят весовые коэффициенты, заданные условиями WSSS.

Раздел		Важность (%)
1	**Организация работы и управление**	5%
	Специалист должен знать и понимать: • Понимание принципов работы специалиста по информационной безопасности и их применение; • Знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде; • Регламентирующие документы в области безопасности информационных систем; • Регламентирующие документы в области охраны труда и безопасности жизнедеятельности; • Важность организации труда в соответствии с методиками; • Методы и технологии исследования; • Важность управления собственным профессиональным развитием; • Скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню. • Важность умения слушать собеседника как части эффективной коммуникации; • Роли и требования коллег и наиболее эффективные методы коммуникации; • Важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими; • Способы разрешения непонимания и конфликтующих требований; • Методы управления стрессом и гневом для разрешения сложных ситуаций.	
	Специалист должен уметь: • Поддерживать безопасную, аккуратную и эффективную рабочую зону; • Использовать все оборудование и программное обеспечение безопасно и в соответствии с инструкциями производителя; • Следовать предписаниям в области охраны труда и безопасности жизнедеятельности; • Регулярно планировать свою работу и корректировать планы в соответствии с изменяющимися приоритетами; • Поддерживать рабочее место в должном состоянии и порядке. • Демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций; • Выстраивать эффективное письменное и устное общение; • Понимать изменяющиеся требования и адаптироваться к ним;	
2	**Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз**	15%

	Специалист должен знать и понимать: • Сетевое окружение; • Сетевые протоколы; • Знать методы выявления и построения путей движения информации в организации; • Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; • Типы сетевых устройств; • Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; • Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем; • Важность следования инструкциям и последствия, цену пренебрежения ими; • Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы; • Этапы установки системы корпоративной защиты от внутренних угроз; • Знать отличия различных версий систем корпоративной защиты от внутренних угроз; • Знать какие СУБД поддерживаются системой; • Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз; • Знать технологии программной и аппаратной виртуализации; • Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation; • Цель документирования процессов обновления и установки. • Важность спокойного и сфокусированного подхода к решению проблемы; • Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности; • Популярные аппаратные и программные ошибки; • Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор; • Аналитический и диагностический подходы к решению проблем; • Границы собственных знаний, навыков и полномочий; • Ситуации, требующие вмешательства службы поддержки; • Стандартное время решения наиболее популярных проблем.	
	Специалист должен уметь: • Интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований; • Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; • Настраивать сетевые устройства;	

	• Администрирование автоматизированных технические средства управления и контроля информации и информационных потоков; • Навыки системного администрирования в операционных системах Windows, Windows Server, Linux (Red Hat Enterprise Linux, CentOS и др.); • Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); • Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; • Настройка средств виртуализации под операционными системам; • Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.: • Установка серверной части системы корпоративной защиты от внутренних угроз; • Установка СУБД различного вида; • Установка агентской части системы корпоративной защиты от внутренних угроз; • Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; • Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; • Использовать дополнительные утилиты если это необходимо; • Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; • Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости; • Уметь сконфигурировать систему, чтобы она получала теневые копии; • Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; • Демонстрировать уверенность и упорство в решении проблем; • Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение; • Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей; • Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей;	
3	**Отчетность и нормативно-правовое обеспечение корпоративной безопасности**	**7%**
	Специалист должен знать и понимать: • Типовые организационно-штатные структуры организаций различных сфер деятельности и размера;	

	• Типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей; • Каналы передачи данных: определение и виды; • Подходы и методы обследования объекта информатизации для последующей защиты; • Сетевые устройства, которые могут быть использованы как источники событий для анализа; • Формирование процессов и процедур аудита ИБ. • Обследование корпоративных информационных систем. • Состояние корпоративной информации. • Инструменты и технологии обеспечения корпоративной защиты от внутренних угроз. • Критерии эффективности проекта по обеспечению корпоративной защиты от внутренних угроз. • Препятствия реализации проектов по обеспечению корпоративной защиты от внутренних угроз. • Основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах; • Инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз; • Типовой пакет нормативных документов, необходимого для развёртывания и эксплуатации системы корпоративной защиты в организации; • Виды типовых отчетных форм о выявленных угрозах и инцидентах; • Типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации; • Понимать подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз; • Системы DLP и требования по информационной безопасности. • Категорирование информации в РФ. • Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; Специальные технические средства • Меры по обеспечению юридической значимости DLP (Pre-DLP). • Практику право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).	
	Специалист должен уметь: • Проводить обследование корпоративных информационных систем. • Самостоятельно изучить структуру организации на основании полученных материалов; • Определить объекты защиты, роли пользователей, права доступа; • Выявить потоки передачи данных и возможные каналы утечки информации;	

	• Создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты; • На основании собственного анализа, уметь связать требования нормативной базы, структуру организации, выявленные угрозы, объекты, роли безопасности для построения актуальных политик безопасности; • Задокументировать и уметь представить результаты обследования (аудита), включая потоки данных, потенциальные каналы утечек, роли пользователей, объекты защиты и т.п. • Разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности; • Проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации; • Создавать отчёты о выявленных инцидентах, угрозах и т.п. • Представлять отчёты и пакеты документов руководству, обосновывать полученные результаты анализа.	
4	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**20%**
	Специалист должен знать и понимать: • Технологии работы с политиками информационной безопасности; • Создание новых политик, модификация существующих; • Общие принципы при работе интерфейсом системы защиты корпоративной информации; • Объекты защиты, персоны; • Ключевые технологии анализа трафика; • Типовые протоколы и потоки данных в корпоративной среде, такими как: • корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4) • веб-почта; • Интернет-ресурсы: сайты, блоги, форумы и т.д. (протоколы HTTP, HTTPS); • социальные сети; • интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP; • принтеры: печать файлов на локальных и сетевых принтерах; • любые съемные носители и устройства; • Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек; • Типы угроз информационной безопасности, типы инцидентов, • Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации; • Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;	

	• Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных; • Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации; • Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки; • Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе; • Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов; • Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;	
	Специалист должен уметь: • Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты; • Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; • Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; • Работа со сводками, виджетами, сводками; • Работа с персонами; • Работа с объектами защиты; • Провести имитацию процесса утечки конфиденциальной информации в системе; • Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; • Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. • Работа с категориями и терминами; • Использование регулярных выражений; • Использование морфологического поиска; • Работа с графическими объектами; • Работа с выгрузками и баз данных; • Работа с печатями и бланками; • Работа с файловыми типами; • Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;	
5	**Технологии защиты и анализа сетевого трафика**	**20%**
	Специалист должен знать и понимать: • Организационно-технические и правовые основы использования электронного документооборота в информационных системах; • Структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;	

	• Нормативно-правовые документы, требования законодательства и регулирующих органов РФ в области электронной подписи, удостоверяющих центров, СКЗИ, МЭ; • Классы защищенности и уровни доверия СЗИ; • Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений; • Ключевые компоненты VPN-сетей; • Особенности VPN-сети и механизмы их управления; • Современные криптографические алгоритмы. Криптопровайдеры, криптографические интерфейсы и библиотеки; • Архитектура, основные компоненты PKI их функции и взаимодействие; • Назначение и роль доверенного удостоверяющего центра в системе ключевой инфраструктуры организации; • Жизненный цикл ключей и сертификатов; • Электронный сертификат ключей ЭП. Формирование, подписание и использование сертификатов; • Защита видео и конференций приложений; • Назначение и основные сценарии применения IDS-технологий; • Архитектуру и особенности внедрения IDS-технологий; • Распространённые вектора атак и уязвимости современных корпоративных информационных систем.	
	Специалист должен уметь: • Осуществлять развёртывание и администрирование VPN-сетью (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.). Обновление ПО, установленного на узлах защищенной сети. • Работать и удостоверяющей и ключевой информацией. Формирование и управление ключевой структурой сети. Издание и управление сертификатами пользователей. • Настраивать защиту сегментов IP-сетей, координация работы узлов защищенной сети. Защиты трафика, передаваемого по открытым каналам связи; • Осуществлять защиту оконечных рабочих мест; Контроль пользовательских приложений; • Реализовывать межсетевое взаимодействие и туннелирование; • Компрометация рабочих мест; • Обеспечение межсетевого экранирования и криптографической защиты информации; • Производить установку, настройку, развёртывание удостоверяющих центров инфраструктуры открытых ключей включая подсистемы регистрации пользователей, создания ключей ЭП, издания сертификатов ключей проверки ЭП, поддержания инфраструктуры ключей проверки ЭП. • Конфигурировать ПО для электронного документооборота в VPN-системах; • Защита систем, обеспечивающих поддержку процессов информационного взаимодействия; • Выполнять настройку и проверку работоспособности;	

	• Проводить детектирование атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме; • Проводить правильную классификацию уровня угрозы инцидента; • Использовать базы контентной фильтрации; • Использовать дополнительные модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса;	
6	**Технологии защиты узла и агентского мониторинга**	**22%**
	Специалист должен знать и понимать: • Функции агентского мониторинга; • Общие настройки системы агентского мониторинга; • Соединение с LDAP-сервером и синхронизация с Active Directory; • Политики агентского мониторинга, особенности их настройки; • Особенности настроек событий агентского мониторинга; • Механизмы диагностики агента, подходы к защите агента. • Знать возможности и ограничения современных российских и зарубежных операционных систем в рамках решения задач защиты информации • Знать архитектуру операционных систем • Знать инструментарий по работа с современными операционными системами, команды, ПО. утилиты	
	Специалист должен уметь: • Установка и настройка агентского мониторинга; • Создание политик защиты на агентах; • Работа в консоли управления агентом; • Фильтрация событий; • Настройка совместных событий агентского и сетевого мониторинга; • Работа с носителями и устройствами; • Работа с файлами; • Контроль приложений; • Исключение из событий перехвата. • Производить настройку сервисов и компонент операционной системы для достижения целей защиты • Разделять компоненты операционной системы по уровням доверия, сокращая поверхность атаки для злоумышленника • Применять механизмы ролевого и мандатного доступа и контроля целостности • Реализовывать ограниченную программную среду для пользователя • Знать особенности безопасной работы и загрузки операционных систем на различных аппаратных платформах	
7	**Предотвращение инцидентов и управление событиями информационной безопасности**	**11%**
	Специалист должен знать и понимать:	

	• Назначение, роль, возможности систем IDS/IPS для задачи защиты организации от угроз информационной безопасности • Назначение, роль, возможности систем SIEM для задачи защиты организации от угроз информационной безопасности • Назначение, роль, возможности систем Threat Intelligence для задачи защиты организации от угроз информационной безопасности	
	Специалист должен уметь: • Устанавливать, настраивать системы IDS/IPS • Устанавливать, настраивать системы SIEM • Устанавливать, настраивать системы Threat Intelligence, генерации трафика и проверки защищенности • Применять на практике системы IDS/IPS для выявления инцидентов информационной безопасности • Применять на практике системы Threat Intelligence • Применять на практике системы Threat Intelligence и Attack Simulation (Breach and Attack Simulation) для проверки/оценки устойчивости систем и сетей к компьютерным атакам • Проводить анализ выявленных инцидентов, использовать встроенные и внешние системы подготовки отчетности	
	Всего	**100%**

3. ОЦЕНОЧНАЯ СТРАТЕГИЯ И ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ ОЦЕНКИ

3.1. ОСНОВНЫЕ ТРЕБОВАНИЯ

Стратегия устанавливает принципы и методы, которым должны соответствовать оценка и начисление баллов WSR.

Экспертная оценка лежит в основе соревнований WSR. По этой причине она является предметом постоянного профессионального совершенствования и тщательного исследования. Накопленный опыт в оценке будет определять будущее использование и направление развития основных инструментов оценки, применяемых на соревнованиях WSR: схема выставления оценки, конкурсное задание и информационная система чемпионата (CIS).

Оценка на соревнованиях WSR попадает в одну из двух категорий: измерение и судейское решение. Для обеих категорий оценки использование

точных эталонов для сравнения, по которым оценивается каждый аспект, является существенным для гарантии качества.

Схема выставления оценки должна соответствовать процентным показателям в WSSS. Конкурсное задание является средством оценки для соревнования по компетенции, и оно также должно соответствовать WSSS. Информационная система чемпионата (CIS) обеспечивает своевременную и точную запись оценок, что способствует надлежащей организации соревнований.

Схема выставления оценки в общих чертах является определяющим фактором для процесса разработки Конкурсного задания. В процессе дальнейшей разработки Схема выставления оценки и Конкурсное задание будут разрабатываться и развиваться посредством итеративного процесса для того, чтобы совместно оптимизировать взаимосвязи в рамках WSSS и Стратегии оценки. Они представляются на утверждение Менеджеру компетенции вместе, чтобы демонстрировать их качество и соответствие WSSS.

Для повышения объективности и справедливости оценки результатов выполнения конкурсных заданий в компетенции используются преимущественно объективные критерии оценки.

4. СХЕМА ВЫСТАВЛЕНИЯ ОЦЕНКИ

4.1. ОБЩИЕ УКАЗАНИЯ

В данном разделе описывается роль и место Схемы выставления оценки, процесс выставления экспертом оценки конкурсанту за выполнение конкурсного задания, а также процедуры и требования к выставлению оценки.

Схема выставления оценки является основным инструментом соревнований WSR, определяя соответствие оценки Конкурсного задания и WSSS. Она предназначена для распределения баллов по каждому оцениваемому аспекту, который может относиться только к одному модулю WSSS.

Отражая весовые коэффициенты, указанные в WSSS Схема выставления оценок устанавливает параметры разработки Конкурсного задания. В зависимости от природы навыка и требований к его оцениванию может быть полезно изначально разработать Схему выставления оценок более детально, чтобы она послужила руководством к разработке Конкурсного задания. В другом случае разработка Конкурсного задания должна основываться на обобщённой Схеме выставления оценки. Дальнейшая разработка Конкурсного задания сопровождается разработкой аспектов оценки.

В разделе 2.1 указан максимально допустимый процент отклонения, Схемы выставления оценки Конкурсного задания от долевых соотношений, приведенных в Спецификации стандартов.

Схема выставления оценки и Конкурсное задание могут разрабатываться одним человеком, группой экспертов или сторонним разработчиком. Подробная и окончательная Схема выставления оценки и Конкурсное задание, должны быть утверждены Менеджером компетенции (МК) или его заместителем, уполномоченным на это МК.

Кроме того, всем экспертам предлагается представлять свои предложения по разработке Схем выставления оценки и Конкурсных заданий на форум экспертов для дальнейшего их рассмотрения Менеджером компетенции.

Во всех случаях полная и утвержденная Менеджером компетенции Схема выставления оценки должна быть введена в информационную систему соревнований (CIS) не менее чем за день до начала соревнований, с использованием стандартной электронной таблицы CIS или других согласованных способов. Главный эксперт является ответственным за данный процесс.

4.2. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество выставляемых баллов (объективные). Общее количество баллов по всем критериям оценки составляет 100.

В данном разделе описывается роль и место Схемы выставления оценки, процесс выставления экспертом оценки конкурсанту за выполнение конкурсного задания, а также процедуры и требования к выставлению оценки.

Критерий		Баллы		
		Судейские аспекты	Объективная оценка	Общая оценка
A	Организация работы и управление		5,00	5,00
B	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз		15,00	15,00
C	Отчетность и нормативно-правовое обеспечение корпоративной безопасности	5,00	2,00	7,00
D	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз		20,00	20,00
E	Технологии защиты и анализа сетевого трафика		25,00	25,00
F	Технологии защиты узла и агентского мониторинга		17,00	17,00
G	Предотвращение инцидентов и управление событиями информационной безопасности		11,00	11,00
Итого		5	95	100

Основные заголовки Схемы выставления оценки являются критериями оценки. В некоторых соревнованиях по компетенции критерии оценки могут совпадать с заголовками разделов в WSSS; в других они могут полностью отличаться. Как правило, бывает от пяти до девяти критериев оценки, при этом количество критериев оценки должно быть не менее трёх. Независимо от того,

совпадают ли они с заголовками, Схема выставления оценки должна отражать долевые соотношения, указанные в WSSS.

Критерии оценки создаются лицом (группой лиц), разрабатывающим Схему выставления оценки, которое может по своему усмотрению определять критерии, которые оно сочтет наиболее подходящими для оценки выполнения Конкурсного задания.

Сводная ведомость оценок, генерируемая CIS, включает перечень критериев оценки.

Количество баллов, назначаемых по каждому критерию, рассчитывается CIS. Это будет общая сумма баллов, присужденных по каждому аспекту в рамках данного критерия оценки.

4.3. СУБКРИТЕРИИ

Каждый критерий оценки разделяется на один или более субкритериев. Каждый субкритерий становится заголовком Схемы выставления оценок.

В каждой ведомости оценок (субкритериев) указан конкретный день, в который она будет заполняться.

Каждая ведомость оценок (субкритериев) содержит оцениваемые аспекты, подлежащие оценке. Для каждого вида оценки имеется специальная ведомость оценок.

4.4. АСПЕКТЫ

Каждый аспект подробно описывает один из оцениваемых показателей, а также возможные оценки или инструкции по выставлению оценок.

В ведомости оценок подробно перечисляется каждый аспект, по которому выставляется отметка, вместе с назначенным для его оценки количеством баллов.

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции в WSSS. Она будет отображаться в таблице распределения баллов CIS, в следующем формате:

Критерий									Итого баллов за раздел WSSS	БАЛЛЫ СПЕЦИФИКАЦИИ И СТАНДАРТОВ WORLDSKILLS НА КАЖДЫЙ	ВЕЛИЧИНА ОТКЛОНЕНИЯ
Разделы Спецификации стандарта WS (WSSS)		A	B	C	D	E	F	G			
	1	5							5	5	0
	2		15						15	15	0
	3			7					7	7	0
	4				17		3		20	20	0
	5					20			20	20	0
	6				3	5	14		22	22	0
	7							11	11	11	0
Итого баллов за критерий		5	15	7	20	25	17	11	100	100	0

4.5. МНЕНИЕ СУДЕЙ (СУДЕЙСКАЯ ОЦЕНКА)

В компетенции используются только объективные измеримые критерии.

При принятии решения используется шкала 0–3. Для четкого и последовательного применения шкалы судейское решение должно приниматься с учетом:

- эталонов для сравнения (критериев) для подробного руководства по каждому аспекту
- шкалы 0–3, где:
    - 0: исполнение не соответствует отраслевому стандарту;
    - 1: исполнение соответствует отраслевому стандарту;

- 2: исполнение соответствует отраслевому стандарту и в некоторых отношениях превосходит его;
- 3: исполнение полностью превосходит отраслевой стандарт и оценивается как отличное

Каждый аспект оценивают три эксперта, каждый эксперт должен произвести оценку, после чего происходит сравнение выставленных оценок. В случае расхождения оценок экспертов более чем на 1 балл, экспертам необходимо вынести оценку данного аспекта на обсуждение и устранить расхождение.

4.6. ИЗМЕРИМАЯ ОЦЕНКА

Оценка каждого аспекта осуществляется тремя экспертами. Если не указано иное, будет присуждена только максимальная оценка или ноль баллов. Если в рамках какого-либо аспекта возможно присуждение оценок ниже максимальной, это описывается в Схеме оценки с указанием измеримых параметров, перечислением допустимых отклонений от эталона и выставляемых при этом баллов.

4.7. ИСПОЛЬЗОВАНИЕ ИЗМЕРИМЫХ И СУДЕЙСКИХ ОЦЕНОК

Окончательное понимание по измеримым и судейским оценкам будет доступно, когда утверждена Схема оценки и Конкурсное задание. Приведенная таблица (в пункте 4.2) содержит приблизительную информацию и служит для разработки Оценочной схемы и Конкурсного задания.

4.8. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на следующих критериях (модулях):

А. Организация работы и управление

Методика проверки заключается в соответствии поведения участника требованиям, предъявленным конкурсным заданием.

B. Установка, конфигурирование и устранение неисправностей в системах корпоративной защиты от внутренних угроз

В ходе проверки последовательно сравнивается факт установки систем и отдельных модулей согласно конкурсному заданию, проверяется корректность их функционирования.

C. Отчетность и нормативно-правовое обеспечение корпоративной безопасности

Проверке подлежит комплект документов, разработанный участником, на соответствие заданному эталону. Допустимые отклонения от эталона указаны в задании.

D. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Процедура проверки заключается в последовательной оценке соответствия результатов выполнения сетевых политик, созданных и применённых участником, в системах защиты от внутренних угроз ИБ. Политики должны отработать корректно (с учётом требований задания в части выставления уровня угрозы, приоритета и т.п.) выявив все инциденты безопасности, без ложных срабатываний. За ошибки (ложные срабатывания, пропуски инцидентов и т.п.) балл максимальный может быть снижен. Процедура снижения должна быть описана в комментариях к аспектам.

Важно, чтобы факт выявления или пропуска инцидента в DLP-системе определялся на основе реально поступивших в систему данных или по итогу работы специального генератора трафика.

E. Технологии защиты и анализа сетевого трафика

Процедура проверки заключает в последовательной оценке факта успешного использования участником различных технологий VPN-систем для защиты сетевого трафика и/или IDS-систем для выявления факта атаки на корпоративные информационные системы, умения применить эти технологии для достижения целей защиты. Проверка заключается в последовательной

оценке результатов работы конкурсантов по развёртыванию, настройке и применения соответствующих систем.

F. Технологии защиты узла и агентского мониторинга

Процедура проверки заключается в последовательной оценке соответствия результатов выполнения агентских политик, созданных и применённых участником, в системах защиты от внутренних угроз ИБ. Политики должны отработать корректно (с учётом требований задания в части выставления уровня угрозы, приоритета и т.п.) выявив все инциденты безопасности, без ложных срабатываний.

G. Предотвращение инцидентов и управление событиями информационной безопасности

Проверке подлежит факт соответствия созданных в рамках задания отчётов и документов конкурсному заданию.

Для ускорения процедуры проверки во всех критериях (где применимо) рекомендуется обязать участников делать снимки экрана (т.н. «скриншоты») или точки остановки виртуальных машин (т.н. «снэпшоты»), в ключевых этапах выполнения работы и проводить проверку по ним.

Технически, процедура проверки по критериям D, F, G может осуществляться одновременно или последовательно.

4.9. РЕГЛАМЕНТ ОЦЕНКИ

Главный эксперт и Заместитель Главного эксперта обсуждают и распределяют Экспертов по группам (состав группы не менее трех человек) для выставления оценок. Каждая группа должна включать в себя как минимум одного опытного эксперта. Эксперт не оценивает участника из своей организации и/или региона.

На время оценки участника, его эксперт-компатриот покидает помещение и не присутствует при процессе оценки «своего» участника, чтобы исключить влияние на других экспертов. Присутствие компатриотов при оценке (из состава

группы оценки) может быть разрешено при согласии более половины экспертов и должно быть зафиксировано отдельным протоколом.

5. КОНКУРСНОЕ ЗАДАНИЕ

5.1. ОСНОВНЫЕ ТРЕБОВАНИЯ

Следующие разделы регламентируют разработку Конкурсного задания. Рекомендации данного раздела дают дополнительные разъяснения по содержанию КЗ.

Продолжительность Конкурсного задания не должна быть менее 15 и более 22 часов.

Возрастной ценз участников для выполнения Конкурсного задания регламентируется Регламентов Чемпионата (отраслевой DigitalSkills, корпоративный Hi-Tech, региональный, межвузовский).

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

Конкурсное задание не должно выходить за пределы WSSS.

Оценка знаний участника должна проводиться исключительно через практическое выполнение Конкурсного задания.

При выполнении Конкурсного задания не оценивается знание правил и норм WSR.

5.2. СТРУКТУРА КОНКУРСНОГО ЗАДАНИЯ

Конкурсное задание содержит 6 модулей:

A. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.
B. Отчетность и нормативно-правовое обеспечение корпоративной безопасности.
C. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.
D. Технологии защиты и анализа сетевого трафика.
E. Технологии агентского мониторинга.

F. Предотвращение инцидентов и управление событиями информационной безопасности.

5.3. ТРЕБОВАНИЯ К РАЗРАБОТКЕ КОНКУРСНОГО ЗАДАНИЯ

Общие требования:

- Модульность;
- Должно сопровождаться специальным бланком судейства, отражающем общие критерии оценки и количество набранных баллов в процессе соревнований;
- Наличие на конкурсе всех необходимых материалов для работы экспертов;
- Наличие соответствующей документации и подробных инструкций для нового и технологически сложного оборудования и программного обеспечения;

Конкурсное задание состоит из следующих модулей:

Модуль	Название модуля	Время выделяемое на модуль, час
A.	**Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз**	**3-4**
	• Конфигурация сетевой инфраструктуры: настройка хост-машины, сетевого окружения, виртуальных машин, и т.п.; • Установка и настройка системы корпоративной защиты от внутренних угроз; • Самостоятельный поиск и устранение неисправностей при развёртывании и настройке; • Установка и настройка агентского мониторинга;	

	• Проведена синхронизация с LDAP-сервером, раздел персоны заполнен корректно; • Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность. Провести имитацию процесса утечки конфиденциальной информации в системе; • Настройка защищенного домена Windows, групповые политики AD; • Создание и установка цифровых сертификатов; • Настройка защищенного соединения между элементами сетевой инфраструктуры: SSH, HTTPS и т.п.	
В.	**Отчетность и нормативно-правовое обеспечение корпоративной безопасности**	**3**
	• Самостоятельно изучить структуру организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем; • Определить объекты защиты; • Перечень субъектов/персон сформулирован верно, роли пользователей, права доступа; • Определить каналы передачи данных и потенциальных утечек; • Типы циркулирующих данных определены верно • Выявить потоки передачи данных и возможные каналы утечки информации; • Заполнить шаблон модели угроз; • Подготовить отчёт о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п. • Определить перечень нормативных актов РФ, задействованных в рамках модели угроз; • Разработать перечень, описание и шаблоны нормативно-правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности;	

C.	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**3-4**
	• Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания;	
	• Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п.	
	• Использовать различные технологии защиты: печатей, бланков, графических объектов, баз данных и т.п.	
	• Занести политики информационной безопасности в DLP-систему	
	• Модифицировать политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата.	
	• Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности.	
	• Работа с интерфейсом управления системы корпоративной защиты информации;	
D.	**Технологии защиты и анализа сетевого трафика**	**3-5**
	• Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре.	
	• Развёртывание, настройка и проверка работоспособности IDS-системы на существующей и вычислительной инфраструктуре.	
	• VPN. Работа с узлами и пользователями.	
	• VPN. Компрометация узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации.	
	• VPN. Межсетевое взаимодействие и туннелированные.	

	• VPN. Централизованные политики безопасности. Защита рабочих мест.	
	• IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий	
	• IDS. Разработать и применить политики, использующие различные технологии анализа траффика	
E.	**Технологии защиты узла и агентского мониторинга**	**2-3**
	• Продемонстрировать знание механизмов работы агентского мониторинга	
	• Разработать и применить политики агентского мониторинга для работы с носителями и устройствами	
	• Разработать и применить политики агентского мониторинга для работы с файлами	
	• Работа с исключениями из перехвата	
	• Защита узлов. Групповые политики AD, файерволы и т.п.	
F.	**Предотвращение инцидентов и управление событиями информационной безопасности**	**3**
	• Подготовка отчётов о нарушениях;	
	• Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов;	
	• Проведение классификацию уровня угроз инцидентов; Оценка ущерба;	
	• Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса;	
	• Разработка план по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу;	
Итого		**18-22 часов**

Требования к конкурсной площадке:

Инфраструктура компетенции подразумевает развёртывание и использование полнофункциональной DLP-системы защиты от внутренних угроз информационной безопасности на заранее развёрнутой сетевой инфраструктуре.

- На каждого участника:
    - Стол, стул на колесиках, настольная лампа, 2 UTP розетки, 4-6 розеток 220В
    - 1 рабочая станция (ПК для работы с DLP, AD, IDS, VPN и т.п.)
        - CPU не ниже Intel Core i5 (с поддержкой виртуализации) не менее 6 ядер 8 потоков (рекомендуется 6 ядер 12 потоков и более), не менее RAM 16Gb (рекомендуется 24-32Gb), HDD или SSD 500Гб (основной диск), SDD 240 Гбайт и более (для виртуальных машин);
        - ПО: VMWare Workstation, или VMWare Player, или Oracle VirtualBox;
        - Windows 10 pro (1-3 VMв зависимости от заданий),
        - Windows Server (не менее 2016, 1-2 VM в зависимости от заданий);
        - 2 проводных сетевых интерфейса на компьютере.
        - 1 доменный сервер, домен Windows (AD) не менее версии 2016. Типовая структура домена, предоставляется МК по запросу ГЭ чемпионата.
        - Виртуальные машины с развёрнутой соревновательной инфраструктурой.
    - 1 ноутбук (для имитации действий злоумышленника и проверки политик)

- CPU не ниже Intel Core2 ядра (рекомендуется 4 ядра и/или 4 потока процессора), поддержка виртуализации, не менее RAM 8 Gb (рекомендуется 16 GB), HDD 200 GB (рекомендуется SSD не менее 200 GB);
- ПО: VMWare Workstation, или VMWare Player, или Oracle VirtualBox;
- Проводной сетевой адаптер (встроенный или внешний);
- Windows 10 pro.

- Аппаратный или программный маршрутизатор с функцией коммутации или коммутатор с поддержкой SPAN (port-mirroring), не менее 4 портов;
- ПО или программно-аппаратные комплексы:
  - IW Education Lab (в составе IWTM (виртуальная машина формата kickstart и установщик), IWDM Server (дистибутив), СУБД Postgres\СУБД Oracle (дистрибутив), файлы лицензий)
  - InfoTeCS VPN (могут быть использованы ПАК HW вместо программных координаторов);
  - InfoTeCS IDS (могут быть использованы ПАК IDS вместо программных СОВ);
  - InfoTeCS Удостоверяющий центр;
  - IW Arma Industrial Firewall;
  - ОС Astra Linux
  - Keysight Breaking Point, Threat Simulator (University Cybersecurity Bundle)

- Почтовый сервер, совместимый с IWTM и возможностью работать в режиме блокировки нежелательного трафика (например iRedMail);
- Прокси-сервер, совместимый с IWTM и возможностью работать в режиме блокировки нежелательного трафика (например Squid);
- Прокси-сервер, совместимый с ViPNet Coordinator с выходом в интернет (например Squid, WinGate);
- Системы анализа защищенности;
- Программное обеспечение для проведения тестов на безопасность на базе ОС Linux;

- На всех участников:
  - Сетевая инфраструктура, каждый участник в отдельном VLAN (для изоляции сетевых сегментов);
  - Рекомендуется использовать сервер виртуализации с доступом ко всем сегментам сети всех участников для работы генераторы трафика:
    - CPU не ниже Intel Core i5/Xeon (с поддержкой виртуализации) не менее 4 ядер 8 потоков, RAM не менее 16Gb (рекомендуется 32 GB), SSD не менее 240GB или не менее 2 HDD аналогичного объема.
  - 2 резервных рабочих станции, 2 резервных ноутбука (конфигурация эквивалента рабочим станциям участников, см. выше)
  - Рекомендуется организовать общую папку для выдачи документации и дистрибутивов; рекомендуется использовать FTP

сервер для проверки некоторых правил; рекомендуется использовать локальный почтовый сервер для проверки некоторых правил;

- Специализированное ПО для проведения соревнований (предоставляется индустриальным партнёром компетенции): Генератор вредоносного траффика. Системы автоматической оценки.
- Доступ в локальную сеть и Интернет со всех компьютеров

5.4. РАЗРАБОТКА КОНКУРСНОГО ЗАДАНИЯ

Конкурсное задание разрабатывается по образцам, представленным Менеджером компетенции на форуме WSR (http://forums.worldskills.ru). Представленные образцы Конкурсного задания должны меняться один раз в год.

5.4.1. КТО РАЗРАБАТЫВАЕТ КОНКУРСНОЕ ЗАДАНИЕ/МОДУЛИ

Общим руководством и утверждением Конкурсного задания занимается Менеджер компетенции. К участию в разработке Конкурсного задания могут привлекаться:

- Сертифицированные эксперты WSR;
- Сторонние разработчики, обладающие опытом работы в области информационной безопасности не менее 2-х лет (на позиции, связанной с разработкой и/или применением средств защиты информации). Учитывается наличие актуальных отраслевых сертификатов, свидетельств о повышении квалификации (за последние 3 года) т.п.;
- Эксперты, принимавшие участие в организации или побеждавшие (лично или в качества руководителя/эксперта-компатриота команды) в профильных соревнованиях в области кибербезопасности (например, национальных соревнованиях CTF, всероссийских олимпиадах и т. п.);
- Дипломированные специалисты (с высшим образованием) в области информационной безопасности;

Сбор предложений для Конкурсного задания

В процессе подготовки к каждому соревнованию при внесении 30% изменений к Конкурсному заданию участвуют:

- Главный эксперт;
- Сертифицированный эксперт по компетенции (в случае присутствия на соревновании);
- Эксперты, принимающие участие в оценке (при необходимости привлечения главным экспертом).

Внесенные 30 % изменения в Конкурсные задания в обязательном порядке согласуются с Менеджером компетенции.

Выше обозначенные люди при внесении 30% изменений к Конкурсному заданию должны руководствоваться принципами объективности и беспристрастности. Изменения не должны влиять на сложность задания, не должны относиться к иным профессиональным областям, не описанным в WSSS, а также исключать любые блоки WSSS. Также внесённые изменения должны быть исполнимы при помощи утверждённого для соревнований Инфраструктурного листа.

5.4.2. КАК РАЗРАБАТЫВАЕТСЯ КОНКУРСНОЕ ЗАДАНИЕ

Конкурсные задания к каждому чемпионату разрабатываются на основе единого Конкурсного задания, утверждённого Менеджером компетенции и размещённого на форуме экспертов. Задания могут разрабатываться как в целом так и по модулям. Основным инструментом разработки Конкурсного задания является форум экспертов.

5.4.3. КОГДА РАЗРАБАТЫВАЕТСЯ КОНКУРСНОЕ ЗАДАНИЕ

Конкурсное задание разрабатывается согласно представленному ниже графику, определяющему сроки подготовки документации для каждого вида чемпионатов.

Временные рамки	Локальный чемпионат	Отборочный чемпионат	Национальный чемпионат
Шаблон Конкурсного задания	Берётся в исходном виде с форума экспертов задание предыдущего Национального чемпионата	Берётся в исходном виде с форума экспертов задание предыдущего Национального чемпионата	Разрабатывается на основе предыдущего чемпионата с учётом всего опыта проведения соревнований по компетенции и отраслевых стандартов за 2 месяца до чемпионата
Утверждение Главного эксперта чемпионата, ответственного за разработку КЗ	За 1 месяца до чемпионата	За 2 месяца до чемпионата	За 4 месяца до чемпионата
Публикация КЗ (если применимо)	За 2 недели до чемпионата, без детализации заданий	За 2 недели до чемпионата, без детализации заданий	За 1 месяц до чемпионата, без детализации заданий
Внесение и согласование с Менеджером компетенции 30% изменений в КЗ	В день С-2	В день С-2	В день С-2
Внесение предложений на Форум экспертов о модернизации КЗ, КО, ИЛ, ТО, ПЗ, ОТ	В день С+1	В день С+1	В день С+1

5.5 УТВЕРЖДЕНИЕ КОНКУРСНОГО ЗАДАНИЯ

Главный эксперт и Менеджер компетенции принимают решение о выполнимости всех модулей и при необходимости должны доказать реальность его выполнения. Во внимание принимаются время и материалы.

Конкурсное задание может быть утверждено в любой удобной для Менеджера компетенции форме.

5.6. СВОЙСТВА ОБОРУДОВАНИЯ И ИНСТРУКЦИИ ПРОИЗВОДИТЕЛЯ

Если для выполнения задания участнику конкурса необходимо ознакомиться с инструкциями по применению какого-либо оборудования или с инструкциями производителя, он получает их заранее по решению Менеджера компетенции и Главного эксперта. При необходимости, во время ознакомления Технический эксперт организует демонстрацию на месте.

6. УПРАВЛЕНИЕ КОМПЕТЕНЦИЕЙ И ОБЩЕНИЕ

6.1 ДИСКУССИОННЫЙ ФОРУМ

Все предконкурсные обсуждения проходят на особом форуме (http://forums.worldskills.ru или Телеграмм-чате «Чат компетенции WSR F7»). Решения по развитию компетенции должны приниматься только после предварительного обсуждения на форуме. Также на форуме должно происходить информирование о всех важных событиях в рамке компетенции. Модератором данного форума являются Международный эксперт и (или) Менеджер компетенции (или Эксперт, назначенный ими).

6.2. ИНФОРМАЦИЯ ДЛЯ УЧАСТНИКОВ ЧЕМПИОНАТА

Информация для конкурсантов публикуется в соответствии с регламентом проводимого чемпионата. Информация может включать:

- Техническое описание;
- Конкурсные задания;
- Обобщённая ведомость оценки;
- Инфраструктурный лист;
- Инструкция по охране труда и технике безопасности;
- Дополнительная информация.

6.3. АРХИВ КОНКУРСНЫХ ЗАДАНИЙ

Конкурсные задания доступны по адресам:

http://forums.worldskills.ru.

https://t.me/joinchat/WMSVPxWP3hrh-gzT

6.4. УПРАВЛЕНИЕ КОМПЕТЕНЦИЕЙ

Общее управление компетенцией осуществляется Международным экспертом и Менеджером компетенции с возможным привлечением экспертного сообщества.

Управление компетенцией в рамках конкретного чемпионата осуществляется Главным экспертом по компетенции в соответствии с регламентом чемпионата.

ОТЧЕТЫ

По итогам соревнований Главный эксперт чемпионата направляет Менеджеру компетенции в срок 5 рабочих дней отчет, в котором указывает:

1. Официальное название, место, время, даты проведения чемпионата
2. Перечень организаций, команды которых приняли участие в чемпионате
3. Официальные результаты, с указанием места и баллов
4. Ключевые события деловой программы, перечень представителей федеральных и региональных органов власти, а также бизнес-партнёров, посетивших мероприятие
5. Ссылки на публикации в СМИ о чемпионате, анонсы мероприятия
6. Подтверждённые отзывы участников
7. Фотографии мероприятия
8. Команда управления компетенцией: МК, ГЭ, ЗГУ, СЭ, ТАП
9. Дополнительную информацию: возникшие при проведении проблемы, выводы по чемпионату и т.п.

7. ТРЕБОВАНИЯ ОХРАНЫ ТРУДА И ТЕХНИКИ БЕЗОПАСНОСТИ

7.1 ТРЕБОВАНИЯ ОХРАНЫ ТРУДА И ТЕХНИКИ БЕЗОПАСНОСТИ НА ЧЕМПИОНАТЕ

См. документацию по технике безопасности и охране труда предоставленные оргкомитетом чемпионата.

Находясь на участке проведения работ, все участники обязаны соблюдать правила техники безопасности при работе на компьютере.

7.2 СПЕЦИФИЧНЫЕ ТРЕБОВАНИЯ ОХРАНЫ ТРУДА, ТЕХНИКИ БЕЗОПАСНОСТИ И ОКРУЖАЮЩЕЙ СРЕДЫ КОМПЕТЕНЦИИ

В компетенции отсутствуют специфичные требования.

8. МАТЕРИАЛЫ И ОБОРУДОВАНИЕ

8.1. ИНФРАСТРУКТУРНЫЙ ЛИСТ

Инфраструктурный лист включает в себя всю инфраструктуру, оборудование и расходные материалы, которые необходимы для выполнения Конкурсного задания. Инфраструктурный лист обязан содержать пример данного оборудования и его чёткие и понятные характеристики в случае возможности приобретения аналогов.

При разработке Инфраструктурного листа для конкретного чемпионата необходимо руководствоваться Инфраструктурным листом, размещённым на форуме экспертов Менеджером компетенции. Все изменения в Инфраструктурном листе должны согласовываться с Менеджером компетенции в обязательном порядке.

На каждом конкурсе технический эксперт должен проводить учет элементов инфраструктуры. Список не должен включать элементы, которые

попросили включить в него эксперты или конкурсанты, а также запрещенные элементы.

По итогам соревнования, в случае необходимости, Технический эксперт и Главный эксперт должны дать рекомендации Оргкомитету чемпионата и Менеджеру компетенции о изменениях в Инфраструктурном листе.

8.2. МАТЕРИАЛЫ, ОБОРУДОВАНИЕ И ИНСТРУМЕНТЫ В ИНСТРУМЕНТАЛЬНОМ ЯЩИКЕ (ТУЛБОКС, TOOLBOX)

В компетенции не задействовано оборудование/материалы участников. тулбокс, инструментальный ящик, отсутствует.

Участникам разрешено использовать беруши.

8.3. МАТЕРИАЛЫ И ОБОРУДОВАНИЕ, ЗАПРЕЩЕННЫЕ НА ПЛОЩАДКЕ

Разрешены материалы и оборудование, перечисленные в пункте 8.2.

Аудио-наушники к использованию запрещены.

Использование сотовых телефонов на время выполнения задания на площадке запрещено.

8.4. ПРЕДЛАГАЕМАЯ СХЕМА КОНКУРСНОЙ ПЛОЩАДКИ