ТЕХНИЧЕСКОЕ ОПИСАНИЕ

«Корпоративная защита от внутренних угроз информационной безопасности»

Организация Союз «Молодые профессионалы (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 профессии (компетенции)

1.1.1 Название профессии (компетенции):

«Корпоративная защита от внутренних угроз информационной безопасности».

1.1.2. Описание профессии (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 – неправомерными действиями 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 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.

Специалист по корпоративной безопасности подготавливает и передаёт отчёты о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой) менеджменту организации, которую защищает.

1.2. Область применения

1.2.1. Все эксперты и конкурсанты должны подробно ознакомиться с данным техническим описанием.

1.2.2. В случае возникновения несоответствия между различными переводами тех. описания, русскоязычная версия будет являться приоритетной.

1.3. Сопроводительная документация

1.3.1. Техническое описание касается только профессиональных вопросов. Изучать ее следует вместе со следующими документами:

- «WorldSkills Russia», Регламент проведения конкурса;
- «WorldSkills International», «WorldSkills Russia»: онлайн-ресурсы, указанные в данном документе;
- Правила техники безопасности и санитарные нормы.

2. КВАЛИФИКАЦИЯ И ОБЪЕМ РАБОТ

Конкурс проводится для демонстрации и оценки квалификации в данной компетенции. Конкурсное задание состоит только из практической работы.

2.1. Требования к квалификации

Участники конкурса должны обладать знаниями и пониманием следующих аспектов, принимая во внимание тот факт, что конкурсное задание может включать в себя любые из приводимых ниже элементов знаний.

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**	**14%**
	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 Server и Linux Red Hat Enterprise Linux; • 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	**Обследование объекта информатизации**	**14%**
	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. •	
	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.	
4	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**25%**
	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, •	
	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. •	
5	**Технологии анализа сетевого трафика в системе корпоративной защиты информации от внутренних угроз**	**27%**
	Специалист должен знать и понимать: • 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: • Работа с категориями и терминами; • Использование регулярных выражений; • Использование морфологического поиска; • Особенности технологии «Лингвистический анализ» ; • Работа с графическими объектами;	

	• Работа с выгрузками и баз данных; • Работа с печатями; • Работа с бланками; • Работа с файловыми типами; • Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов; • 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 агентского мониторинга**	**9%**
	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. •	
	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. •	
7	**Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов**	**6%**
	Специалист должен знать и понимать: • 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: • 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 руководству, обосновывать полученные результаты анализа.	
	Всего	**100%**

2.2 Теоретические знания

2.2.1 Теоретические знания необходимы, но они не подвергаются явной проверке.

2.2.2 Знание правил и постановлений учитывается.

2.3 Практическая работа

Основное конкурсное задание.

Участники соревнований должны выполнить два задания в течение 2 дней соревнований. Практическое задание даётся в форме технического задания на защиту корпоративной среды организации от внутренних угроз. Для этого необходимо провести обследование и анализ структуры организации (как главного объекта защиты) на основании представленных материалов и стенда, её вычислительно-сетевой инфраструктуры, определить потоки данных, потенциальные угрозы и каналы утечек. Техническая часть работы включает развёртывание, настройку и поэтапную эксплуатацию системы защиты от внутренних угроз для выявления каналов утечки информации и других инцидентов безопасности.

Найденные инциденты должны быть должным образом проанализированы, подвергнуты классификации в соответствии с актуальной нормативной базой. Должна быть проведена оценка уровня угрозы информационной безопасности. Результаты работы должны быть оформлены в виде отчетов. До эксплуатации технических систем защиты должен быть подготовлен пакет документов, регламентирующий его легальное использование в организации. Техническое задание состоит из легенды организации, спецификации её вычислительно-сетевой инфраструктуры и описания используемых технических средств.

Описание организации, которую защищают участники, содержит:

- описание организационно-штатной структуры организации;
- описание вычислительно-сетевой инфраструктуры;
- пакет внутренней документации организации;

Оценка практической работы преимущественно направлена на оценку результата работ, а не процесса. При этом критерии оценки конкурсного

задания составляются таким образом, чтобы оптимальная организация процесса проектирования, планирования, установки, анализа и эксплуатации системы защиты проекта приводила к высокому результату оценки.

Сопроводительная документация

Сопроводительная документация подготавливается участниками в процессе соревнования и содержит:

- Отчеты;
- Спецификации;
- Презентации для защиты работы.

Расчёт баллов

Регистрация и подсчёт всех баллов по основному конкурсному заданию проводится информационной системой конкурса (CIS).

3. КОНКУРСНОЕ ЗАДАНИЕ

Продолжительность конкурсного задания не может менее 15 часов 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 (КЗ не должно выходить за пределы WSSS).

Оценка знаний производится из практического выполнения конкурсного задания.

Выполнение конкурсного задание подразумевает личный зачет каждого из участников (единоличное выполнение КЗ).

3.1. Формат и структура Конкурсного задания

Задание состоит из нескольких этапов, которые оцениваются отдельно.

3.2. Требования к проекту Конкурсного задания

Задание должно соответствовать следующим требованиям:

- Модульность;
- Должно сопровождаться специальным бланком судейства, отражающем общие критерии оценки и количество набранных баллов в процессе соревнований (раздел 5);
- Соответствовать п. 3.5;
- Наличие на конкурсе всех необходимых материалов для работы экспертов;
- Наличие соответствующей документации и подробных инструкций для нового и технологически сложного оборудования и программного обеспечения;

3.3 Основные условия для предложенных модулей

Каждый предложенный модуль должен:

- соответствовать требованиям разработки конкурсного задания
- подлежать быстрому переводу на язык участника
- содержать краткое описание задания

3.4 Основные модули конкурсного задания

Модуль	Название модуля	Время выделяемое на модуль, час

1.	**Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз**	**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;	
2.	**Исследование (аудит) организации с целью защиты от внутренних угроз**	**2**
	• 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;	
3.	**Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**3**
	• 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.	
	• 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;	
4.	**Поиск и предотвращение инцидентов. Технологии анализа сетевого трафика в системе корпоративной защиты информации от внутренних угроз**	**3**
	• Разработать и применить политики, использующие регулярные выражения и морфологический поиск, для выявления соответствующих инцидентов	
	• Разработать и применить политики, использующие поиск по печатям и бланкам, для выявления соответствующих инцидентов	
	• Разработать и применить политики, использующие поиск графических объектов, для выявления соответствующих инцидентов	
	• Разработать и применить политики, использующие поиск по базам данных, для выявления соответствующих инцидентов	
	• Разработать и применить политики, использующие механизмы распознавания текста, для выявления соответствующих инцидентов	
	• Разработать и применить политики, работающие с конкретными типами файлов, для выявления соответствующих инцидентов	
	• Выявить большую часть инцидентов безопасности за ограниченное время	
5	**Технологии агентского мониторинга**	**2**
	• 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	
6	**Анализ выявленных инцидентов**	**2**
	• 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		**16 часов**

В зависимости от типа чемпионата количество модулей и время выполнения может изменяться.

3.3. Разработка конкурсного задания

Текстовые документы должны быть оформлены в формате Word, графические в PDF.

3.3.1. Кто разрабатывает конкурсные задания / модули

Главный эксперт с экспертным сообществом совместно техническими специалистами компаний индустриальных партнеров производят разработку основных модулей задания.

3.3.2. Как и когда разрабатывается конкурсное задание / модули

Специалисты индустриального партнера компетенции и эксперты разрабатывают модель организации (включая документы, описывающие организационную структуру) и собирают стенд, имитирующий корпоративный документооборот (как легальный, так и нелегальные инциденты безопасности, утечки и т.п.). Инциденты и каналы утечек данных выбираются таким образом, чтобы участники смогли продемонстрировать свои навыки по их выявлению и предотвращению.

Дополнительно подготавливается тестовые программы, которые будут использовать участники по заданию.

Экспертам, участвующим в чемпионате впервые, необходимо связаться с главным экспертом по меньшей мере за 3 месяца до даты начала чемпионата для обсуждения модулей, которые следует использовать на чемпионате.

3.3.3. Когда разрабатывается конкурсное задание

Конкурсные задания разрабатываются до конкурса и оглашаются на текущем конкурсе.

3 месяца до конкурса: оглашаются типы используемого программного обеспечения.

1 месяц до конкурса: обеспечивается доступ к документации для всех компонентов.

3.4. Схема выставления оценок за конкурсное задание

Предложенная схема оценивания разрабатывается лицами, разрабатывающими конкурсное задание. Окончательный подробный вариант схемы оценивания разрабатывается и согласовывается всеми экспертами, принимающими участие в чемпионате.

3.5. Выбор конкурсного задания

Модель, легенду и описание производства, а также сценарии утечек данных выбирают уполномоченные лица и специалисты из компаний индустриальных партнеров.

3.6. Обнародование конкурсного задания

Конкурсное задание обнародуется на веб-сайте www.worldskills.ru за месяц до текущего конкурса.

Обнародование происходит после согласования с уполномоченными лицами и специалистами из компании индустриального партнера.

3.7. Согласование конкурсного задания (подготовка к конкурсу)

Согласованием конкурсного задания занимаются Главный эксперт и Заместитель главного эксперта.

3.8. Возможное изменение конкурсного задания

Каждое конкурсное задание подлежит 30% изменению, описанному в Меморандуме о взаимопонимании.

4. УПРАВЛЕНИЕ НАВЫКАМИ И КОММУНИКАЦИЯ

4.1. Дискуссионный форум

До начала конкурса все обсуждения, обмен сообщениями, сотрудничество и процесс принятия решений по какому-либо профессиональному вопросу происходят на дискуссионном форуме, посвященном соответствующей специальности (http://forum.worldskills.ru). Модератором форума является Главный эксперт (или Эксперт, назначенный на этот пост Главным экспертом). Временные рамки для обмена сообщениями и требования к разработке конкурса устанавливаются Правилами конкурса.

4.2. Информация для участников конкурса

Всю информацию для зарегистрированных участников конкурса можно получить на сайте http://www.worldskills.ru.

Такая информация включает в себя:

- Правила (Регламент) конкурса
- Технические описания
- Конкурсные задания
- Другую информацию, относящуюся к конкурсу.

4.3. Конкурсные задания

Обнародованные конкурсные задания можно получить на сайте forum.worldskills.ru

4.4. Текущее руководство

Текущее руководство определяется в Плане работы на площадке чемпионата, который составляет Группа управления компетенцией, возглавляемая Главным экспертом. Группа управления компетенцией

состоит из Председателя жюри, Главного эксперта и Заместителя Главного эксперта. План работы на площадке чемпионата разрабатывается за 6 месяцев до начала конкурса, а затем окончательно дорабатывается во время Конкурса совместным решением Экспертов. С Планом работы на площадке чемпионата можно ознакомиться на сайте www. worldskills.ru

5. ОЦЕНКА

В данном разделе описан процесс оценки конкурсного задания / модулей Экспертами. Здесь также указаны характеристики оценок, процедуры и требования к выставлению оценок.

5.1. 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.

Раздел	Критерий	Оценки	
		Объективная	Общая
A	Организация работы и управление	5,00	5,00
B	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	14,00	14,00

C	Исследование (аудит) организации с целью защиты от внутренних угроз	11,00	11,00
D	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	22,00	22,00
E	Поиск и предотвращение инцидентов. Технологии анализа сетевого трафика в системе корпоративной защиты информации от внутренних угроз	32,00	32,00
F	Технологии агентского мониторинга	9,00	9,00
G	Анализ выявленных инцидентов	7,00	7,00
Итого =		**100**	**100**

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.

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.

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 два дня до начала соревнований, с использованием стандартной электронной таблицы CIS или других согласованных способов. Главный эксперт является ответственным за данный процесс.

5.1.1. Выбор критериев оценки

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.

5.1.2 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.

5.1.3. 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.

5.2. Субъективные оценки и Judgment оценки

Не применяется.

5.3. Критерии оценки мастерства

Владение профессиональными навыкам оценивается по нескольким категориям с привлечением специалистов индустриального партнера компетенции.

Окончательные критерии оценки согласуются со специалистами из компании индустриального партнера.

Время выполнения задания является критерием для оценки отдельных навыков.

5.4. Регламент оценки мастерства

- Главный эксперт разделяет Экспертов на группы, так, чтобы в каждой группе присутствовали, как опытные участники мероприятий «WorldSkills», так и новички.
- Одна группа экспертов, назначенных Главным экспертом или его заместителем производят замеры объективных параметров конкурсного задания.
- Вторая группа находится на конкурсной площадке и следит за выступлением участников.
- В конце каждого дня результаты измерений подписываются индивидуально каждым экспертом, ответственным за участника и баллы заносятся в CIS.
- Какие-либо особые регламенты начисления баллов отсутствуют.

5.4. Соответствие баллов WSSS и критериев оценки Конкурсного задания

Критерий									Итого баллов за раздел WSSS	БАЛЛЫ СПЕЦИФИКАЦИИ СТАНДАРТОВ WORLDSKILLS НА КАЖДЫЙ РАЗДЕЛ	ВЕЛИЧИНА ОТКЛОНЕНИЯ
Разделы Спецификации стандарта WS (WSSS)		A	B	C	D	E	F	G			
	1	5							5	5	0
	2		14						14	14	0
	3			8	4	2			14	14	0
	4				16	3	2	1	25	25	0
	5					26		1	27	27	0
	6						7	2	9	9	0
	7				2	1		3	6	6	0
Итого баллов за критерий		5	14	11	22	32	9	7	100	100	0

6. ОТРАСЛЕВЫЕ ТРЕБОВАНИЯ ТЕХНИКИ БЕЗОПАСНОСТИ

См. документацию по технике безопасности и охране труда страны-устроительницы конкурса.

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

7. МАТЕРИАЛЫ И ОБОРУДОВАНИЕ

7.1. Инфраструктурный лист

В Инфраструктурном листе перечислено все оборудование, материалы и устройства, которые предоставляет Организатор конкурса.

С Инфраструктурным листом можно ознакомиться на веб-сайте организации: http://www.worldskills.ru

Организатор конкурса обновляет Инфраструктурный список, указывая необходимое количество, тип, марку/модель предметов.

В ходе каждого конкурса, Эксперты рассматривают и уточняют Инфраструктурный лист для подготовки к следующему конкурсу. Эксперты дают Техническому директору рекомендации по расширению площадей или изменению списка оборудования.

В ходе каждого конкурса, Технический наблюдатель проверяет Инфраструктурный лист, использовавшийся на предыдущем конкурсе.

В Инфраструктурный лист не входят предметы, которые участники и/или Эксперты должны иметь при себе, а также предметы, которые участникам запрещается иметь при себе. Эти предметы перечислены ниже.

7.2. Материалы, оборудование и инструменты, которые участники имеют при себе в своем инструментальном ящике

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

7.3. Материалы, оборудование и инструменты, предоставляемые Экспертами

Не применяются.

7.4. Материалы и оборудование, запрещенные на площадке

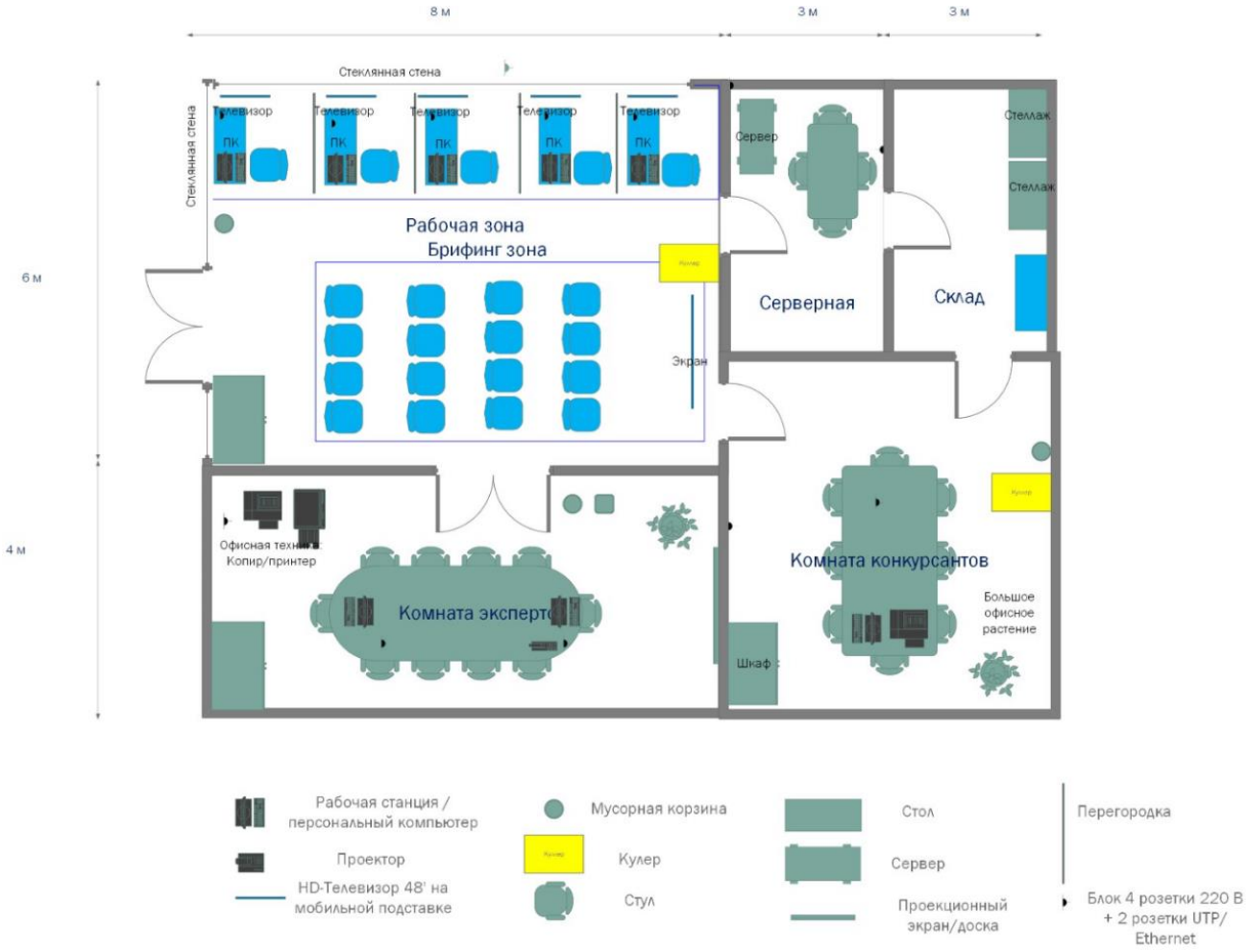
Разрешены материалы и оборудование, перечисленные в пункте 7.2.

7.5. Предлагаемая схема застройки рабочего места

С Планами застройки можно ознакомиться на веб-сайте www.worldskills.ru

Схема мастерской:

(*см. иллюстрацию*)



8. ПРЕДСТАВЛЕНИЕ МАСТЕРСТВА ПОСЕТИТЕЛЯМ И ЖУРНАЛИСТАМ

8.1. Максимальное вовлечение посетителей и журналистов

Ниже приводится список возможных способов максимизации вовлечения посетителей и журналистов в процесс кузовного ремонта.

- Экраны, транслирующие на вебсайт WorldSkills процесс соревнований
- Описание тестовых заданий (доступное зрителям)
- Интерактивные зоны
- Подробное объяснение зрителям сути деятельности конкурсантов
- Резюме конкурсантов и национальные флаги
- Мастер-классы
- Понимание того, чем занимаются участники конкурса;
- Информация об участниках («профили» участников);
- Карьерные перспективы;
- Ежедневное освещение хода конкурса.

8.2. Правила для посетителей и гостей

Посетители и гости имеют доступ на территорию площадки соревнований только с разрешения главного эксперта.

8.3 Правила для прессы

- Представители аккредитованных СМИ имеют доступ на территорию площадки соревнований только с разрешения главного эксперта,
- Фото и видеосъемка со стороны зрителей разрешена.

9. ОСОБЫЕ ПРАВИЛА ВОЗРАСТНОЙ ГРУППЫ 14-16 ЛЕТ

Время на выполнения задания не должны превышать 4 часов в день.

При разработке Конкурсного задания и Схемы оценки необходимо учитывать специфику и ограничения применяемой техники безопасности и охраны труда для данной возрастной группы. Так же необходимо учитывать антропометрические, психофизиологические и психологические особенности данной возрастной группы. Тем самым Конкурсное задание и Схема оценки может затрагивать не все блоки и поля WSSS в зависимости от специфики компетенции.