**РАЙОННЫЙ ЧЕМПИОНАТ «МОЛОДЫЕ ПРОФЕССИОНАЛЫ»**

|  |  |
| --- | --- |
|  | Главный эксперт покомпетенции «Информационная безопасность» А.В. Склярова |

**КОНКУРСНОЕ ЗАДАНИЕ**

по компетенции

**Информационная безопасность**

|  |
| --- |
|  |

**Санкт-Петербург**

**2024**

**1. ВВЕДЕНИЕ**

1.1. Информационная безопасность

1.2. Описание компетенции

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

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

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

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

1.3. Количество конкурсантов

Индивидуальный конкурс

1.4. Возраст конкурсантов

В возрастной категории 14+ возраст участников 14- 16 лет включительно.

1.5. Общее время на выполнение задания.

На полное выполнение задания отводится 2 дня по 3 часа 55 минут. Общее время на выполнение задания 7 часов 50 минут.

**2. ПРИМЕРНОЕ ЗАДАНИЕ**

**КОНКУРСНОЕ ЗАДАНИЕ МОЖЕТ БЫТЬ ИЗМЕНЕНО НА 30% В ПРЕДЕЛАХ СУЩЕСТВУЮЩИХ МОДУЛЕЙ.**

Содержанием конкурсного задания являются применение на практике навыков участников в области криптографии, стеганографии, форензики и веб-безопасности.

Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Конкурс подразумевает выполнение заданий в формате CTF, с использованием специализированного программного обеспечения, применения политик информационной безопасности, контроля информационных потоков, анализа выявленных инцидентов.

Оценка производится как в отношении работы модулей, так и в отношении процесса выполнения конкурсной работы. Если участник конкурса не выполняет требования техники безопасности, конфликтен, не владеет техниками управления стрессом и разрешения конфликтных ситуаций, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри.

Конкурсное задание должно выполняться помодульно.

**2.1. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ**

Модули и время сведены в таблице 1

Таблица 1 – Модули задания и необходимое время

|  |  |  |
| --- | --- | --- |
| **№п/п** | **Наименование модуля** | **Время на задание** |
| 1 | Модуль 1: Криптография | 2 часа |
| 2 | Модуль 2: Стеганография  | 1 час 55 минут |
| 3 | Модуль 3: Форензика | 2 часа |
| 4 | Модуль 4: WEB-уязвимости | 1 час 55 минут |
| **Итого:** | **7 часов 50 минут** |

Модуль 1. Криптография

Участник должен:

- разбираться в различных методах шифрования, включая классические методы (например, шифр Цезаря) и алгоритмы (например, RSA или AES);

- уметь реализовывать скрипты для шифрования и дешифрования текстовых сообщений с использованием различных методов шифрования;

- производить анализ современных криптографических алгоритмов.

Модуль 2. Стеганография

Участник должен:

- уметь исследовать методы встраивания данных в графические файлы, аудио- и видеофайлы;

- извлекать скрытую информацию в изображениях, аудио- и видеофайлах.

Модуль 3.

Участник должен:

- знать методы анализа цифровых следов, таких как метаданные, файловые структуры, системные журналы и т.д.

- уметь восстанавливать удаленные или скрытые данные, включая файлы, текстовые сообщения и прочие цифровые следы;

- уметь производить сбор и анализ цифровых данных с использованием специализированных инструментов и программного обеспечения.

- анализировать и интерпретировать найденные данные с целью выявления инцидентов безопасности.

Модуль 4: WEB-уязвимости

Участник должен:

- производить анализ исходного кода с целью выявления потенциальных уязвимостей;

- использовать статистический анализ кода и других инструментов для поиска уязвимостей;

- осуществлять поиск уязвимостей, таких как инъекции, неправильная обработка ввода, отсутствие контроля доступа и т.д.

**2.3. КРИТЕРИИ ОЦЕНКИ**

В данном разделе определены критерии оценки и количество начисляемых баллов (объективные) таблица 2.

Общее количество баллов задания/модуля по всем критериям оценки составляет 100.

Таблица 2 — Критерии оценки

|  |  |  |
| --- | --- | --- |
| **№п/п** | **Наименование модуля** | **Оценки** |
| 1 | Модуль 1: Криптография | 25 баллов |
| 2 | Модуль 2: Стеганография  | 25 баллов |
| 3 | Модуль 3: Форензика | 25 баллов |
| 4 | Модуль 4: WEB-уязвимости | 25 баллов |
| **Итого** | **100 баллов** |

Субъективные оценки - Не применимо.