

**VI РЕГИОНАЛЬНЫЙ ЧЕМПИОНАТ ПО ПРОФЕССИОНАЛЬНОМУ МАСТЕРСТВУ СРЕДИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ «АБИЛИМПИКС»**

**БЕЛГОРОДСКОЙ ОБЛАСТИ**

**Утверждено**

**советом по компетенции**

**«Информационная безопасность»**

(название совета)

**Протокол №\_\_ от \_\_ сентября 2021 года**

**Председатель совета:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**

(подпись)

**КОНКУРСНОЕ ЗАДАНИЕ**

по компетенции

**Информационная безопасность**

(студенты)



**Белгород 2021**

1. **Описание компетенции**

**1.1. Актуальность компетенции**

Компетенция «Информационная безопасность» входит в «ТОП-50 наиболее востребованных и перспективных профессий» в соответствии с лучшими зарубежными стандартами и передовыми технологиями. Утверждена приказами Министерства образования и науки Российской федерации от 09 декабря 2016 года № 1551, №1553 в виде Федеральных образовательных стандартов среднего профессионального образования 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Имея решающую роль в повседневном функционировании, техник по защите информации имеет спрос в организациях различных масштабов коммерческого и государственного сектора, такие как: компания D-Link, Код безопасности, Инфотекс, Инфовотч, Информзащита и другие. Информация конфиденциального характера нуждается в защите, следовательно - в защите нуждаются все элементы системы: персональный компьютер, автоматизированные системы, сеть, сетевое оборудование, периметр объекта и тому подобное. Техник по защите информации несет ответственность за настройку оборудования и программного обеспечения по защите информации, надежное функционирование автоматизированных систем предприятия, поддержание информационной безопасности.

Информационная безопасность требует широкий спектр познаний и навыков в области информационных технологий. В связи с быстрым развитием этой области, требования к техникам по защите информации постоянно возрастают.

**1.2. Профессии, по которым участники смогут трудоустроиться после освоения данной компетенции**

Техник по защите информации.

**1.3. Ссылка на образовательный и/или профессиональный стандарт (конкретные стандарты)**

|  |  |  |
| --- | --- | --- |
| **Школьники** | **Студенты** | **Специалисты** |
| ФГОС СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем"  http://top-50.gapm.ru/  ФГОС СПО 10.02.05 "Обеспечение информационной безопасности автоматизированных систем"  http://reestrspo.ru/node/580 | ФГОС СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем"  http://top-50.gapm.ru/  ФГОС СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем"  http://reestrspo.ru/node/580 | ПФ «Специалист по защите информации в автоматизированных системах»  http://docs.cntd.ru/document/420377328 |
|  | ФГОС ВО «Информационная безопасность (уровень бакалавриата)»  http://fgosvo.ru/news/1/2131 |  |

**1.4. Требования к квалификации**

|  |  |  |
| --- | --- | --- |
| **Школьники** | **Студенты** | **Специалисты** |
| *Должен знать:*  особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;  типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;  типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;  основные понятия криптографии и типовых криптографических методов и средств защиты информации.  *Должен уметь:*  устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;  диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;  проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;  использовать типовые программные криптографические средства, в том числе электронную подпись;  устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;  осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.  иметь практический опыт в:  установке и настройке программных средств защиты информации;  тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;  учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности. | *Должен знать:*  особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;  типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;  типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;  основные понятия криптографии и типовых криптографических методов и средств защиты информации.  *Должен уметь:*  устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;  диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;  проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;  использовать типовые программные криптографические средства, в том числе электронную подпись;  устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;  осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.  иметь практический опыт в:  установке и настройке программных средств защиты информации;  тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;  учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности. | *Должен знать:*  Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях  Базовая конфигурация системы защиты информации автоматизированной системы  Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах  Типовые средства, методы и протоколы идентификации, аутентификации и авторизации  Нормативные правовые акты в области защиты информации  Организационные меры по защите информации  *Должен уметь:*  Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией.  Обнаруживать и устранять неисправности системы защиты информации. автоматизированной системы согласно эксплуатационной документации.  Производить монтаж и диагностику компьютерных сетей.  Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи.  Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.  Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации.  Использовать программные средства для архивирования информации.  Использовать программные и программно-аппаратные. средства для уничтожения информации и носителей информации.  Использовать типовые криптографические средства защиты информации, в том числе электронную подпись.  Определять источники и причины возникновения инцидентов.  Оценивать последствия выявленных инцидентов.  Обнаруживать нарушения правил разграничения доступа.  Устранять нарушения правил разграничения доступа.  Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах.  Использовать криптографические методы и средства защиты информации в автоматизированных системах.  Создавать, удалять и изменять учетные записи пользователей автоматизированной системы.  Планировать политику безопасности программных компонентов. автоматизированных систем  Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации.  Регистрировать события, связанные с защитой информации в автоматизированных системах.  Анализировать события, связанные с защитой информации в автоматизированных системах.  Конфигурировать параметры системы защиты информации автоматизированных систем.  Применять технические средства контроля эффективности мер защиты информации.  Применять типовые программные средства резервирования и восстановления информации в автоматизированных системах.  Применять программные средства обеспечения безопасности данных.  Документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы.  Выявление угроз безопасности информации в автоматизированных системах.  Устранение недостатков в функционировании системы защиты информации автоматизированной системы.  Применять инструментальные средства контроля защищенности информации в автоматизированных системах.  Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации.  Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации. |

1. **Конкурсное задание**

**Конкурсное задание может быть изменено на 30% в пределах существующих модулей.**

**2.1. Краткое описание задания**

**Школьники:** в ходе выполнения конкурсного задания необходимо просканировать сетевой трафик. Настроить защищенную сеть в соответствии со схемой VipNet.

**Студенты:** в ходе выполнения конкурсного задания необходимо просканировать сетевой трафик. Настроить сетевое взаимодействие между узлами операционных систем. Установить необходимое программное обеспечение VipNet и настроить защищенное соединение в соответствии со схемой.

**Специалисты:** в ходе выполнения конкурсного задания необходимо произвести установку и настройку программного обеспечения для работы с рутокен, настроить аутентификацию по рутокен в Linux. Сгенерировать сертификат для безопасного соединения в браузере. Просканировать сетевой трафик.

**2.2. Структура и подробное описание конкурсного задания.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Наименование и описание модуля** | **День** | **Время** | **Результат** |
| **Школьник** | Модуль 1. Сканирование сетевого траффика | Первый день | 30 минут | Просканирован и отфильтрован необходимый траффик, найдены ключевые параметры |
| Модуль 2. Настройка защищенной сети с помощью VipNet | Первый день | 1 час 30 минут | Сконфигурирована защищенная сеть. |
| Общее время выполнения конкурсного задания: 2 часа | | | | |
| **Студент** | Модуль 1. Сканирование сетевого траффика | Первый день | 30 минут | Просканирован и отфильтрован необходимый траффик, найдены ключевые параметры |
| Модуль 2. Установка и настройка защищенной сети с помощью VipNet | Первый день | 1 час 30 минут | Установлены все необходимые компоненты программного обеспечения VipNet.  Сконфигурирована защищенная сеть. |
| Общее время выполнения конкурсного задания: 2 часа | | | | |
| **Специалист** | Модуль 1. Аутентификация в Linux с помощью Рутокен | Первый день | 1 час | Настроена аутентификация по Рутокену |
| Модуль 2. Сканирование сетевого траффика | Первый день | 30 минут | Просканирован и отфильтрован необходимый траффик, найдены ключевые параметры |
| Модуль 3. Настройка защищенного https соединения | Второй день | 30 минут | Настроенное https соединение |
| Модуль 4. Установка и настройка защищенной сети с помощью VipNet | Первый день | 30 минут | Установлены все необходимые компоненты программного обеспечения VipNet.  Сконфигурирована защищенная сеть. |
| Общее время выполнения конкурсного задания: 2,5 часа | | | | |

2.3. Последовательность выполнения задания

Школьники:

Модуль 1. Сканирование сетевого траффика

Просканировать сетевой трафик от одной виртуальной машины к другой, определить ключевые параметры.

Модуль 2. Настройка защищенной сети VipNet

Настроить защищенную сеть с помощью программного обеспечения VipNet.

Студенты:

Модуль 1. Сканирование сетевого трафика

Просканировать сетевой трафик от одной виртуальной машины к другой, определить ключевые параметры.

Модуль 2. Установка и настройка защищенной сети с помощью VipNet

Установить и настроить необходимое программное обеспечение VipNet для организации защищенной сети в соответствии со схемой. Настроить виртуальные машины для работы с сетью.

Специалисты:

Модуль 1. Аутентификация в Linux с помощью Рутокен

Настроить PAM модуль в Linux, создать необходимые ключи на токене, создание сертификата. Проверка работоспособности аутентификации.

Модуль 2. Сканирование сетевого трафика

Просканировать сетевой трафик от одной виртуальной машины к другой, определить ключевые параметры.

Модуль 3. Настройка защищенного https соединения

Сгенерировать и установить сертификат для работы веб сервера по защищенному соединению.

Модуль 4. Установка и настройка защищенной сети с помощью VipNet.

Установить и настроить необходимое программное обеспечение VipNet для организации защищенной сети в соответствии со схемой. Настроить виртуальные машины для работы с сетью.

2.4. 30% изменение конкурсного задания

Главный эксперт в праве изменить параметры настройки виртуальных машин для работы с сетью, а также изменить схему конфигурирования VipNet.

2.5. Критерии оценки выполнения задания

Школьники:

|  |  |  |
| --- | --- | --- |
| **Наименование модуля** | **Задание** | **Максимальный балл** |
| Модуль 1. Сканирование сетевого траффика | Просканировать сетевой трафик от одной виртуальной машины к другой, определить ключевые параметры | 30 |
| Модуль 2. Настройка защищенной сети VipNet | Настроить защищенную сеть с помощью программного обеспечения VipNet | 70 |
| **ИТОГО** | | **100** |

Модуль 1. Сканирование сетевого траффика

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)\*** |
|  |  | Обнаружение ключевого параметра | 15 | 15 |  |
|  | Расшифровка ключевого параметра | 15 | 15 |  |
| **ИТОГО: 30** | | | | | |

Модуль 2. Настройка защищенной сети VipNet

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)** |
|  |  | Установка УКЦ | 10 | 10 |  |
|  | Установка ЦУС | 10 | 10 |  |
|  | Установка Координатор | 10 | 10 |  |
|  | Установка 1 Клиента | 10 | 10 |  |
|  | Установка 2 Клиента | 10 | 10 |  |
|  | Генерация ключей | 10 | 10 |  |
|  | Передача сообщения от одного клиента другому | 10 | 10 |  |
| **ИТОГО: 70** | | | | | |

Студенты:

|  |  |  |
| --- | --- | --- |
| **Наименование модуля** | **Задание** | **Максимальный балл** |
| Модуль 1. Сканирование сетевого траффика. | Просканировать сетевой трафик от одной виртуальной машины к другой, определить ключевые параметры | 20 |
| Модуль 2. Установка и настройка защищенной сети с помощью VipNet. | Установить и настроить необходимое программное обеспечение VipNet для организации защищенной сети в соответствии со схемой. Настроить виртуальные машины для работы с сетью | 80 |
| **ИТОГО** | | **100** |

Модуль 1. Сканирование сетевого траффика

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)** |
|  |  | Обнаружение ключевого параметра | 10 | 10 |  |
|  | Расшифровка ключевого параметра | 10 | 10 |  |
| **ИТОГО: 20** | | | | | |

Модуль 2. Установка и настройка защищенной сети с помощью VipNet.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)** |
|  |  | Настройка виртуальных машин для работы с сетью | 10 | 10 |  |
|  | Установка УКЦ | 10 | 10 |  |
|  | Установка ЦУС | 10 | 10 |  |
|  | Установка Координаторов | 10 | 10 |  |
|  | Установка 1 Клиента | 10 | 10 |  |
|  | Установка 2 Клиента | 10 | 10 |  |
|  |  | Генерация ключей | 10 | 10 |  |
|  |  | Передача сообщения от одного клиента другому | 10 | 10 |  |
| **ИТОГО: 80** | | | | | |

Специалисты:

|  |  |  |
| --- | --- | --- |
| **Наименование модуля** | **Задание** | **Максимальный балл** |
| Модуль 1. Аутентификация в Linux с помощью Рутокен | Настроить PAM модуль в Linux, создать необходимые ключи на токене, создание сертификата. Проверка работоспособности аутентификации. | 55 |
| Модуль 2. Сканирование сетевого трафика | Просканировать сетевой трафик от одной виртуальной машины к другой, определить ключевые параметры. | 10 |
| Модуль 3. Настройка защищенного https соединения | Сгенерировать и установить сертификат для работы веб сервера по защищенному соединению. | 20 |
| Модуль 4. Установка и настройка защищенной сети с помощью VipNet | Установить и настроить необходимое программное обеспечение VipNet для организации защищенной сети в соответствии со схемой. Настроить виртуальные машины для работы с сетью. | 15 |
| **ИТОГО** | | **100** |

Модуль 1. Аутентификация в Linux с помощью Рутокен

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)** |
| Настроить PAM модуль в Linux, создать необходимые ключи на токене, создание сертификата. Проверка работоспособности аутентификации. |  | Настройка pam\_p11 | 10 | 10 |  |
|  | Создание ключей на рутокене | 10 | 10 |  |
|  | Проверка сгенерированного ключ | 10 | 10 |  |
|  | Создание сертификата и импорт | 10 | 10 |  |
|  | Занесение сертификата в список доверенных | 10 | 10 |  |
|  | Аутентификация в системе | 5 | 5 |  |
| **ИТОГО: 55** | | | | | |

Модуль 2. Сканирование сетевого трафика

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)** |
| Просканировать сетевой трафик от одной виртуальной машины к другой, определить ключевые параметры. |  | Обнаружен пароль | 10 | 10 |  |
| **ИТОГО: 10** | | | | | |

Модуль 3. Настройка защищенного https соединения

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)** |
| Сгенерировать и установить сертификат для работы веб сервера по защищенному соединению. |  | Создать самоподписанный сертификат. | 10 | 10 |  |
|  | Установка сертификата в систему с наличием скриншотов | 5 | 5 |  |
|  | Подключение к Linux через Putty | 5 | 5 |  |
| **ИТОГО: 20** | | | | | |

Модуль 4. Установка и настройка защищенной сети с помощью VipNet.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Задание** | **№** | **Наименование критерия** | **Максимальные баллы** | **Объективная оценка (баллы)** | **Субъективная оценка (баллы)** |
| Установить и настроить необходимое программное обеспечение VipNet для организации защищенной сети в соответствии со схемой. Настроить виртуальные машины для работы с сетью. |  | Настройка виртуальных машин для работы с сетью | 5 | 5 |  |
|  | Установка необходимого программного обеспечения | 5 | 5 |  |
|  | Правильное конфигурирование VipNet | 5 | 5 |  |
| **ИТОГО: 15** | | | | | |

**3. Перечень используемого оборудования, инструментов и расходных материалов**

**3.1. Школьники, студенты, специалисты**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ОБОРУДОВАНИЕ НА 1-ГО УЧАСТНИКА** | | | | | |
| Оборудование, инструменты, ПО, мебель | | | | | |
| **№** | **Наименование** | **Фото необходимого оборудования, средства индивидуальной защиты** | **Тех. характеристики оборудования, инструментов и ссылка на**  **сайт производителя, поставщика** | **Ед. измерения** | **Кол-во** |
| 1 | Стол |  | 1400х700 мм, https://meb-biz.ru | Шт. | 1 |
| 2 | Стул |  | Офисный, <https://beautyoffice.ru/kb-8-kreslo-burokrat> | Шт. | 1 |
| 3 | АРМ |  | Intel Core i5 или выше, 16GB RAM и более, 500GB HDD и более, ОС WINDOWS 8.1 и выше, монитор 19"-22" – 2 шт., мышь, клавиатура, доступ к точке доступа участника через wi-fi карту компьютера или сетевой кабель, <https://www.nix.ru/autocatalog/hp/hp_computers/HP-ProDesk-600-G3-Microtower-1KB31EA-ACB-i5-7500-4-500-DVD-RW-Win10Pro_323282.html> | Шт. | 1 |
| 4 | ИБП |  | Не менее 500 VA, https://www.dns-shop.ru/product/9d493cda46bd3330/ibp-dexp-cee-650va/?p=1&i=7 | Шт. | 1 |
| 5 | Удлинитель |  | 220В, 2 метра, 6 розеток, https://www.citilink.ru/catalog/computers\_and\_notebooks/powersafe/powerfilters | Шт. | 1 |
| 6 | Windows 7 или выше |  | Установленная для работы в VMware Workstation | Шт. | 1 |
| 7 | VMware Workstation |  | VMware Workstation | Шт. | 1 |
| 8 | Kali Linux |  | Установленная для работы в VMware Workstation | Шт. |  |
| 9 | Putty |  | Установщик | Шт. |  |
| **РАСХОДНЫЕ МАТЕРИАЛЫ НА 1 УЧАСТНИКА** | | | | | |
| Расходные материалы | | | | | |
| № | Наименование | Технические характеристики | | Ед. измерения | Кол-во |
| 1 | Шариковая ручка |  | | Шт. | 1 |
| 2 | Лист бумаги |  | | Шт. | 1 |
| **РАСХОДНЫЕ МАТЕРИАЛЫ, ОБОРУДОВАНИЕ И ИНСТРУМЕНТЫ, КОТОРЫЕ УЧАСТНИКИ ДОЛЖНЫ ИМЕТЬ ПРИ СЕБЕ (при необходимости)** | | | | | |
| - | - | - | | - | - |
| **РАСХОДНЫЕ МАТЕРИАЛЫ И ОБОРУДОВАНИЕ, ЗАПРЕЩЕННЫЕ НА ПЛОЩАДКЕ** | | | | | |
| 1 | Мобильные устройства |  | |  |  |
| **ДОПОЛНИТЕЛЬНОЕ ОБОРУДОВАНИЕ, ИНСТРУМЕНТЫ КОТОРОЕ МОЖЕТ ПРИВЕСТИ С СОБОЙ УЧАСТНИК (при необходимости)** | | | | | |
| **№** | **Наименование** | **Фото необходимого оборудования, средства индивидуальной защиты** | **Тех. характеристики оборудования и ссылка на сайт**  **производителя, поставщика** | **Ед. измерения** | **Кол-во** |
| 1 | Органайзер Брайля Braille Sense U2 |  | http://com-v.ru/tiflomarket/braille-sense-u2-qwerty/ | Шт. | 1 |
| 2 | Специализированное ПО для слабовидящих |  | https://www.smartaids.ru/catalog/sighting\_loss/kompyuternaya-tekhnika-i-po-dlya-slabovidyashchikh-i-slepykh/programmnoe-obespechenie/ | Шт. | 1 |
| 3 | Специальное кресло-коляска (для участников с проблемами ОДА) |  | http://www.blagomed.ru/prod/kreslo-kolyaska-invalidnaya-ly-250-a-shirina-sideniya-45sm-2798.html?utm\_source=yandex\_market&utm\_medium=cpc&utm\_campaign=ukreplennye&utm\_content=kreslo\_kolyaska\_invalidnaya\_ly\_250\_a\_shirina\_sideniya\_45sm\_2798&utm\_term=2798&ymclid=15964118568447760163500001 | Шт. | 1 |
| 4 | Слуховой аппарат для участников с проблема­ми слуха |  | https://beru.ru/product/slukhovoi-apparat-axon-d322/100864949458?offerid=69XqfvjWUk43hvlpNm1yaw&utm\_source=market&utm\_medium=cpc&utm\_term=635657.a1313&utm\_content=13120303&clid=910&ymclid=15964120902295421892300004&q=3ZRiT6a87WmQD43xbbPpDucPD4EEfkXFqPBl978r14H8q%2FXbylRz1JBexjRZigJj | Шт. | 1 |
| **ОБОРУДОВАНИЕ НА 1-ГО ЭКСПЕРТА (при необходимости)** | | | | | |
| Оборудование, мебель | | | | | |
| **№** | **Наименование** | **Фото необходимого оборудования, средства индивидуальной защиты** | **Технические характеристики и ссылка на сайт производителя, поставщика** | **Ед. измерения** | **Кол-во** |
| 1 | Стул |  | Офисный, https://beautyoffice.ru/kb-8-kreslo-burokrat | Шт. | 1/5 |
| 2 | Стол |  | 1400х700 мм, https://meb-biz.ru | Шт. | 1/5 |
| 3 | АРМ |  | Intel Core i5 или быстрее, 8GB RAM и более, 500GB HDD и более, ОС WINDOWS 8.1 и выше, Монитор 21 дюйма и более, мышь, клавиатура, доступ к точке доступа участника через wi-fi карту компьютера или сетевой кабель, https://www.nix.ru/autocatalog/hp/hp\_computers/HP-ProDesk-600-G3-Microtower-1KB31EA-ACB-i5-7500-4-500-DVD-RW-Win10Pro\_323282.html | Шт. | 1/5 |
| 4 | Принтер |  | Лазерное мфу HP LaserJet Pro MFP M132nw, https://www.ulmart.ru | Шт. | 1/5 |
| **РАСХОДНЫЕ МАТЕРИАЛЫ НА 1 Эксперта (при необходимости)** | | | | | |
| Расходные материалы | | | | | |
| № | Наименование | Технические характеристики | | Ед. измерения | Кол-во |
| 1 | Бумага | Бумага офисная | | Пч. | 1/5 |
| 2 | Ручка шариковая |  | | Шт. | 1/5 |
| **ОБЩАЯ ИНФРАСТРУКТУРА КОНКУРСНОЙ ПЛОЩАДКИ (при необходимости)** | | | | | |
| Дополнительное оборудование, средства индивидуальной защиты | | | | | |
| **№** | **Наименование** | **Фото необходимого оборудования, средства индивидуальной защиты** | **Тех. характеристики дополнительного оборудования и средств индивидуальной защиты и ссылка на сайт производителя, поставщика** | **Ед. измерения** | **Кол-во** |
| 1 | Огнетушитель | Порошковый огнетушитель ОП-4 | Огнетушитель углекислотный, http://www.magazin01.ru | Шт. | 2 |
| **КОМНАТА УЧАСТНИКОВ (при необходимости)** | | | | | |
| Оборудование, мебель, расходные материалы (при необходимости) | | | | | |
| 1 | Стол |  | |  |  |
| 2 | Вешалка | Вешало - стойка для одежды | | Шт. | 1 |
| **ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ К ПЛОЩАДКЕ/КОММЕНТАРИИ** | | | | | |
| Количество точек электропитания и их характеристики, количество точек интернета и требования к нему, количество точек воды и требования (горячая, холодная) | | | | | |
| № | Наименование | Тех. характеристики | |  |  |
| 1 | 220 В |  | | Шт. | 16 |

**4. Минимальные требования к оснащению рабочих мест с учетом основных нозологий**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Площадь, м.кв.** | **Ширина прохода между рабочими местами, м.** | **Специализированное оборудование, количество\*** |
| **Рабочее место участника с нарушением слуха** | не менее 2,5 кв. м | не менее 1 м | Звукоусиливающая аппаратура.  https://www.obrazov.org/ (Количество оборудования зависит от количества участников) |
| **Рабочее место участника с нарушением зрения** | более 3 м | не менее 1 м | Конкурсное задание может быть оформлено рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением, а также индивидуальное равномерное освещение не менее 300 люкс  https://www.obrazov.org/ (Количество оборудования зависит от количества участников)  Органайзер Брайля, специализированное программное обеспечение для слабовидящих |
| **Рабочее место участника с нарушением ОДА** | более 3 м Столы с регулировкой по высоте. Минимальный размер зоны на одно место с учетом подъезда и разворота коляски равен 1,8х1,8 м. | Размеры зоны рабочего места на одного ребенка инвалида на кресле-коляске составляют не менее 1,8х0,9 м. Проход между рабочими столами для свободного проезда и подъезда к столу должен быть не менее 0,9 м, т.е. размеры рабочей зоны вместе с проходом - 1,8х1,8 м. Ширина прохода между рядами столов для учащихся, передвигающихся в креслах колясках и на опорах - не менее 0,9 м от спинки стула до следующего стола, а у места учащегося на кресле коляске вдоль прохода не менее 1,4 м | https://www.obrazov.org/ (Количество оборудования зависит от количества участников)  Трансформируемые элементы оборудования и мебель на рабочих местах, специальные механизмы и устройства, позволяющие изменять высоту и наклон рабочей поверхности, положение сиденья рабочего стула по высоте и наклону, оборудование, обеспечивающее возможность подъезда к рабочему месту и разворота кресла-коляски |
| **Рабочее место участника с соматическими заболеваниями** | не менее 2,5 кв. м | не менее 1 м | Не допускается наличие тепловых излучений; локальной вибрации, электромагнитных излучений, ультрафиолетовой радиации.  Уровни шума на рабочих местах и освещенность должны соответствовать действующим нормативам.  https://www.istok-reatech.ru/catalog/ |
| **Рабочее место участника с ментальными нарушениями** | не менее 2,5 кв. м | рекомендуется предусматривать полузамкнутые рабочие места-кабины (с боковыми бортиками и экранами у стола, высокими спинками сидений, с бортиками ограждениями по бокам и сзади и т.п.), что создает для этих учащихся более спокойную обстановку, помогает регулировать психологическую дистанцию с окружающими. | Температура воздуха в холодный период года при легкой работе - 21 - 24 °C; при средней тяжести работ - 17 - 20 °C; влажность воздуха в холодный и теплый периоды года 40 - 60 %; отсутствие вредных веществ: аллергенов, канцерогенов, аэрозолей, металлов, оксидов металлов; электромагнитное излучение - не выше ПДУ; шум - не выше ПДУ (до 81 дБА); отсутствие локальной и общей вибрации; отсутствие микроорганизмов, продуктов и препаратов, содержащих живые клетки и споры микроорганизмов, белковые препараты.  https://inva24.ru/ |

**\***указывается **с**сылка на сайт с тех. характеристиками, либо наименование и тех. характеристики специализированного оборудования**.**

**5. Схема застройки соревновательной площадки.**

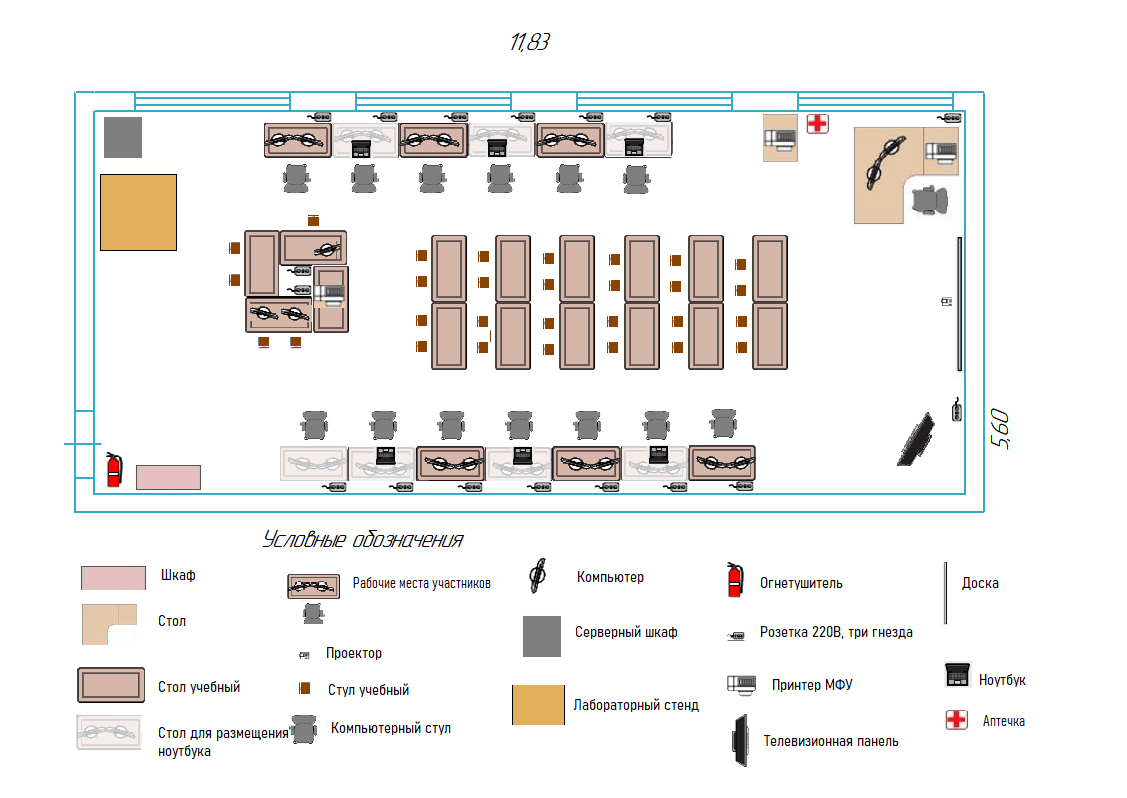
**Застройка осуществляется на группу участников**

**- на 6 рабочих мест (школьники)**

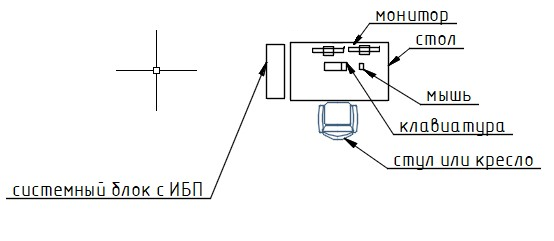
**- на 6 рабочих мест (студенты)**

**- на 6 рабочих мест (специалисты)**

**Для всех категорий**



**Рабочее место участника**

****

**6. Требования охраны труда и техники безопасности**

*Техника безопасности. Общие требования безопасности*

Настоящая инструкция распространяется на допущенных на площадку соревнований лиц, эксплуатирующих средства вычислительной техники и сетевое оборудование. Инструкция содержит общие указания по безопасному применению электрооборудования площадки соревнований. Требования настоящей инструкции являются обязательными, отступления от нее не допускаются. К самостоятельной эксплуатации электроаппаратуры допускается только лица не моложе 18 лет.

*Требования безопасности перед началом работы*

Перед началом работы следует убедиться в исправности электропроводки, выключателей, штепсельных розеток, при помощи которых оборудование включается в сеть, наличии заземления компьютера, его работоспособности.

*Требования безопасности во время работы*

Для снижения или предотвращения влияния опасных и вредных факторов необходимо соблюдать Санитарные правила и нормы, гигиенические требования к видео-дисплейным терминалам, персональным электронно-вычислительным машинам и организации работы.

Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается: вешать что-либо на провода, закрашивать и белить шнуры и провода, закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы, выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.

Для исключения поражения электрическим током запрещается: часто включать и выключать компьютер без необходимости, прикасаться к экрану и к тыльной стороне блоков компьютера, работать на средствах вычислительной техники и сетевом оборудовании мокрыми руками, а также иметь на рабочем месте тару с водой или другой жидкостью, работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками электрического напряжения на корпусе, класть на средства вычислительной техники и периферийном оборудовании посторонние предметы.

Запрещается под напряжением очищать от пыли и загрязнения электрооборудование.

Запрещается проверять работоспособность электрооборудования в неприспособленных для эксплуатации помещениях с токопроводящими полами, сырых, не позволяющих заземлить доступные металлические части.

Недопустимо под напряжением проводить ремонт средств вычислительной техники и периферийного оборудования.

Ремонт электроаппаратуры производится только специалистами техниками с соблюдением необходимых технических требований.

Во избежание поражения электрическим током, при пользовании электроприборами нельзя касаться одновременно каких-либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей.

При пользовании электроэнергией в сырых помещениях соблюдать особую осторожность.

*Требования безопасности по окончании работы.*

После окончания работы необходимо обесточить все средства вычислительной техники и сетевое оборудование. В случае необходимости оставить включенными только оборудование, указанное экспертами.

*Требования безопасности в аварийных ситуациях*

При обнаружении неисправности немедленно обесточить электрооборудование, оповестить экспертов. Продолжение работы возможно только после устранения неисправности.

При обнаружении оборвавшегося провода необходимо немедленно сообщить об этом экспертам, принять меры по исключению контакта с ним людей. Прикосновение к проводу опасно для жизни.

Во всех случаях поражения человека электрическим током немедленно вызывают врача.

До прибытия врача нужно, не теряя времени, приступить к оказанию первой помощи пострадавшему.

Необходимо немедленно начать производить искусственное дыхание, наиболее эффективным из которых является метод «рот в рот» или «рот в нос», а также наружный массаж сердца.

Искусственное дыхание пораженному электрическим током производится вплоть до прибытия врача.

На рабочем месте запрещается иметь огнеопасные вещества.

В помещениях запрещается:

а) разжигать огонь;

б) включать электрооборудование, если в помещении пахнет газом;

в) курить;

г) сушить что-либо на отопительных приборах;

д) закрывать вентиляционные отверстия в электроаппаратуре.

Источниками воспламенения являются:

а) искра при разряде статического электричества;

б) искры от электрооборудования;

в) искры от удара и трения;

г) открытое пламя.

При возникновении пожароопасной ситуации или пожара персонал должен немедленно принять необходимые меры для его ликвидации, одновременно оповестить о пожаре администрацию.

Помещения с электрооборудованием должны быть оснащены огнетушителями.