РЕГИОНАЛЬНЫЙ ЧЕМПИОНАТ «АБИЛИМПИКС» 2026

Утверждено
советом по компетенции:
«Информационная безопасность»

Протокол от 19.12.2025 № 5

Председатель совета:

С. Л. Грибаков

Главный эксперт Московской области:

В. В. Королева

КОНКУРСНОЕ ЗАДАНИЕ

по компетенции

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Москва
2026

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. Утверждено 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: Код безопасности, ИнфоТеКС, Инфовотч, Информзащита и др. Информация конфиденциального характера нуждается в защите, следовательно - в защите нуждаются все элементы системы: ПК, автоматизированные системы, сеть, сетевое оборудование, периметр объекта и т.п. Специалист 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 получения данной компетенции:

Инженер по информационной безопасности, администратор безопасности, архитектор безопасности, техник по защите информации, аналитики информационной безопасности.

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

Школьники	Студенты	Специалисты
Федеральный государственный образовательный стандарт (далее – ФГОС)		
ФГОС СПО 10.02.04 "Обеспечение информационной безопасности телекоммуникационных систем" https://fgos.ru/fgos/fgos-10-02-04-obespechenie-informacionnoy-bezopasnosti-telekommunikacionnyh-sistem-1551/ ФГОС СПО 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" https://fgos.ru/fgos/fgos-10-02-05-obespechenie-informacionnoy-bezopasnosti-avtomatizirovannyh-sistem-1553/	ФГОС СПО 10.02.04 "Обеспечение информационной безопасности телекоммуникационных систем" https://fgos.ru/fgos/fgos-10-02-04-obespechenie-informacionnoy-bezopasnosti-telekommunikacionnyh-sistem-1551/ ФГОС СПО 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" https://fgos.ru/fgos/fgos-10-02-05-obespechenie-informacionnoy-bezopasnosti-avtomatizirovannyh-sistem-1553/ ФГОС ВО 10.03.01 Информационная безопасность https://fgos.ru/fgos/fgos-10-03-01-informacionnaya-bezopasnost-1427/	ПС «Специалист по защите информации в автоматизированных системах» https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=116917

Профессиональный стандарта (далее – ПС)		
		ПС «Специалист по защите информации в автоматизированных системах» https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=116917

1.4. Требования к квалификации:

Школьники	Студенты	Специалисты
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	**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	**Знать:** – типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; – базовые конфигурации 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
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	**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	**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;

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.	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.	– 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; – выявлять угрозы безопасности информации в автоматизированных системах; – устранять недостатки 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

2. Конкурсное задание

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

2.1. Краткое описание задания

2.1.1. Категория участников «ШКОЛЬНИКИ»:

В ходе выполнения конкурсного задания участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- настройка VPN-сети на существующей и вычислительной инфраструктуре, администрирование узлов и пользователей;
- развертывание ViPNet Client для Windows, Linux, ViPNet Coordinator, ViPNet xFirewall;
- выполнение компрометации узлов, ключей, пользователей. Восстановление связи;
- проверка работоспособности VPN-сети.

2.1.2. Категория участников «СТУДЕНТЫ»:

В ходе выполнения конкурсного задания участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- настройка VPN-сети на существующей и вычислительной инфраструктуре, администрирование узлов и пользователей;
- развертывание ViPNet Client для Windows, Linux, ViPNet Coordinator, ViPNet xFirewall;
- выполнение компрометации узлов, ключей, пользователей. Восстановление связи;
- организацию межсетевого взаимодействия и туннелирования;
- проверка работоспособности VPN-сети.

2.1.3. Категория участников «СПЕЦИАЛИСТЫ»:

В ходе выполнения конкурсного задания участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- настройка VPN-сети на существующей и вычислительной инфраструктуре, администрирование узлов и пользователей;
- развертывание ViPNet Client для Windows, Linux, ViPNet Coordinator, ViPNet xFirewall;
- выполнение компрометации узлов, ключей, пользователей. Восстановление связи;
- организацию межсетевого взаимодействия и туннелирования;
- проверка работоспособности VPN-сети.
- внедрение централизованных политик безопасности. Обеспечение защиты рабочих мест.

2.2. Структура и подробное описание конкурсного задания

Категория участников	Наименование и описание модуля	Время	Результат
Школьники	**Модуль А.** Настройка защищенной VPN сети.	45 минут	Создана защищенная сеть ViPNet.
	Модуль Б. Развертывание узлов сети.	45 минут	Узлы сети развернуты и настроены.
	Модуль В. Компрометация узла.	45 минут	Произведена компрометация ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.
	Модуль Г. Работоспособность сети.	45 минут	Сделаны скриншоты работоспособной сети ViPNet.
Время выполнение всех модулей: **3 часа**			
Студенты	**Модуль А.** Настройка защищенной VPN сети.	40 минут	Создана защищенная сеть ViPNet.
	Модуль Б. Развертывание узлов сети.	1,5 часа	Узлы сети развернуты и настроены.
	Модуль В. Компрометация узла.	20 минут	Произведена компрометация ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.
	Модуль Г. Работоспособность сети.	1,5 часа	Сделаны скриншоты работоспособной сети ViPNet Проверено взаимодействие узлов. Настроено туннелирование.

			Установлены клиенты для Linux.
Время выполнение всех модулей: **4 часа**			
Специалисты	**Модуль А.** Настройка защищенной VPN сети.	40 минут	Создана защищенная сеть ViPNet.
	Модуль Б. Развертывание узлов сети.	1,5 часа	Узлы сети развернуты и настроены.
	Модуль В. Компрометация узла.	20 минут	Произведена компрометация ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.
	Модуль Г. Работоспособность сети.	1,5 часа	Сделаны скриншоты работоспособной сети ViPNet Проверено взаимодействие узлов, Настроено туннелирование. Установлены клиенты для Linux. Настроены централизованные политики безопасности.
Время выполнение всех модулей: **4 часа**			

2.3 Последовательность выполнения задания.

2.3.1. Категория участников «ШКОЛЬНИКИ»:

Модуль А. Настройка защищенной VPN сети.

С помощью системы виртуализации необходимо установить компоненты для администрирования защищенной сети VPN, настроить узлы сети ViPNet.

Модуль Б. Развертывание узлов сети.

Развернуть в системе виртуализации узлы защищенной сети, настроить сетевые интерфейсы, настроить необходимые фильтры.

Модуль В. Компрометация узла.

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя. Сделать скриншоты экрана «защищенная сеть» на двух координаторах. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.

Модуль Г. Работоспособность сети.

Проверить работоспособность сети VPN, сделать соответствующие скриншоты.

2.3.2. Категория участников «СТУДЕНТЫ»:

Модуль А. Модуль А. Настройка защищенной VPN сети.

С помощью системы виртуализации необходимо установить компоненты для администрирования защищенной сети VPN, настроить узлы сети ViPNet.

Модуль Б. Развертывание узлов сети.

Развернуть в системе виртуализации узлы защищенной сети, настроить сетевые интерфейсы, настроить необходимые фильтры.

Модуль В. Компрометация узла.

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя. Сделать скриншоты экрана «защищенная сеть» на двух координаторах. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.

Модуль Г. Работоспособность сети.

Проверить работоспособность сети VPN, сделать соответствующие скриншоты. Настроить туннелирование между открытыми узлами. Установит Linux клиенты.

2.3.3. Категория участников «СПЕЦИАЛИСТЫ»:

Модуль А. Модуль А. Настройка защищенной VPN сети.

С помощью системы виртуализации необходимо установить компоненты для

администрирования защищенной сети VPN, настроить узлы сети ViPNet.

Модуль Б. Развертывание узлов сети.

Развернуть в системе виртуализации узлы защищенной сети, настроить сетевые интерфейсы, настроить необходимые фильтры.

Модуль В. Компрометация узла.

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя. Сделать скриншоты экрана «защищенная сеть» на двух координаторах. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.

Модуль Г. Работоспособность сети.

Проверить работоспособность сети VPN, сделать соответствующие скриншоты. Настроить туннелирование между открытыми узлами. Установит Linux клиенты. Настроить политики безопасности для защищенных узлов с помощью ViPNet Policy Manager. Настроено межсетевое взаимодействие.

Особые указания по компетенции:

Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от участия в конкурсе.

Перед началом соревнований участникам будет предоставлена возможность проверить работоспособность системы виртуализации, наличие необходимого программного обеспечения, проверить работоспособность виртуальных машин.

При выполнении задания доступ в сеть Интернет для участников разрешен. Разрешается использовать только открытые источники сети Интернет, включая официальные сайты производителей программного обеспечения и организаций. Запрещено обращаться к форумам, личным страницам, ресурсам, требующим аутентификации и/или авторизации, нейросетям.

2.4. Региональный (вариативный):

Модуль Г. Работоспособность сети.

Задание

- настройка политик безопасности ViPNet Policy Manager;
- настройка туннелирования на координаторах или с помощью ЦУС;
- настройка политик безопасности с помощью командного интерпретатора;
- настройка межсетевого взаимодействия;
- сменить мастер ключи своей сети, восстановить работоспособность;
- установить ViPNet Client 4U под Linux;
- установить ViPNet EPP сервер и клиент на машину администратора;
- установить ViPNet EPP агент на машину клиента филиала, проверить работоспособность.

2.5. Критерии оценки выполнения задания

Категория участников	Наименование и описание модуля	Тип критерия (оценочный/ измеримый)	Макс. балл
Школьники	**Модуль А. Настройка защищенной VPN сети.**	**И или О**	**28**
	Настроена виртуальная машина администратора в системе виртуализации	И	2
	Настроены сетевые интерфейсы виртуальной машины администратора	И	2
	Установлена и работоспособна серверная часть ViPNet ЦУС	И	2
	Работоспособна серверная часть ViPNet ЦУС	И	2
	Установлена клиентская часть ViPNet ЦУС	И	2
	Работоспособна клиентская часть ViPNet ЦУС	И	2
	Установлен VIPNet УКЦ	И	2
	Работоспособен VIPNet УКЦ	И	2
	Созданы и настроен пользователь Администратор	И	2
	Созданы и настроен пользователь филиала	И	2
	Настроено взаимодействие между пользователями в сети	И	2
	Настроены пароли пользователей и администраторов в соответствии с заданием	И	2
	Созданы группы узлов и пользователей центрального офиса	И	2
	Созданы группы узлов и пользователей филиала	И	2
	Модуль Б. Развертывание узлов сети.	**И**	**46**
	Настроена виртуальная машина ViPNet Coordinator центрального офиса в системе виртуализации	И	2
	Установлен ViPNet Coordinator центрального офиса	И	2
	Настроен ViPNet Coordinator центрального офиса	И	2
	Настроена виртуальная машина ViPNet Coordinator филиала в системе виртуализации	И	2
	Установлен ViPNet Coordinator филиала	И	2
	Настроен ViPNet Coordinator филиала	И	2
	Настроен ViPNet xFirewall центрального офиса в системе виртуализации	И	2
	Установлен ViPNet xFirewall Центрального офиса	И	2
	Настроен ViPNet xFirewall Центрального офиса	И	2
	Установлена база решающих правил на ViPNet xFirewall Центрального офиса	И	2
	Настроен сетевой фильтра для работы защищенной сети на ViPNet xFirewall Центрального офиса	И	2
	Настроен ViPNet xFirewall филиала в системе виртуализации	И	2

	Установлен ViPNet xFirewall филиала	И	2
	Настроен ViPNet xFirewall филиала	И	2
	Установлена база решающих правил на ViPNet xFirewall филиала	И	2
	Настроен сетевой фильтра для работы защищенной сети на ViPNet xFirewall филиала	И	2
	Настроены сетевые интерфейсы виртуальной машины администратора	И	2
	Установлен ViPNet Client администратора	И	2
	Настроен ViPNet Client администратора	И	2
	Настроены сетевые интерфейсы виртуальной машины клиента филиала	И	2
	Установлен ViPNet Client филиала	И	2
	Настроен ViPNet Client филиала	И	2
	Проверена работоспособность защищенной сети	И	2
	Модуль В. Компрометация узла.	**И**	**4**
	Скомпрометированы ключи пользователя	И	2
	Скомпрометированный пользователь работоспособен	И	2
	Модуль Г. Работоспособность сети.	**И**	**22**
	Установлен ViPNet Policy Manager	И	2
	Создана политика безопасности запрещеющее RDP подключение	И	2
	Настроено туннелироване на координаторах или с помощью ЦУС	И	2
	Настроены политики безопасности с помощью командного интерпретатора на xFirewall	И	2
	Настроено межсетевое взаимодействие	И	2
	Заменены мастер ключи своей сети, восстановлена работоспособность	И	2
	Установлен ViPNet Client 4U под Linux	И	2
	Установлен ViPNet EPP сервер и клиент на машину администратора	И	2
	Установлен ViPNet EPP агент на машину клиента филиала, проверить работоспособность	И	2
	Установлена и активирована лицензия EPP	И	2
	Установлены базы решающих правил на EPP	И	2
		ОБЩЕЕ:	**100**

	Модуль А. Настройка защищенной VPN сети.	**И или О**	**28**
	Настроена виртуальная машина администратора в системе виртуализации	И	2
	Настроены сетевые интерфейсы виртуальной машины администратора	И	2
	Установлена и работоспособна серверная часть ViPNet ЦУС	И	2
	Работоспособна серверная часть ViPNet ЦУС	И	2
	Установлена клиентская часть ViPNet ЦУС	И	2
	Работоспособна клиентская часть ViPNet ЦУС	И	2
	Установлен VIPNet УКЦ	И	2
	Работоспособен VIPNet УКЦ	И	2
	Созданы и настроен пользователь Администратор	И	2
	Созданы и настроен пользователь филиала	И	2
	Настроено взаимодействие между пользователями в сети	И	2
	Настроены пароли пользователей и администраторов в соответствии с заданием	И	2
	Созданы группы узлов и пользователей центрального офиса	И	2
	Созданы группы узлов и пользователей филиала	И	2
Студенты	**Модуль Б. Развертывание узлов сети.**	**И**	**46**
	Настроена виртуальная машина ViPNet Coordinator центрального офиса в системе виртуализации	И	2
	Установлен ViPNet Coordinator центрального офиса	И	2
	Настроен ViPNet Coordinator центрального офиса	И	2
	Настроена виртуальная машина ViPNet Coordinator филиала в системе виртуализации	И	2
	Установлен ViPNet Coordinator филиала	И	2
	Настроен ViPNet Coordinator филиала	И	2
	Настроен ViPNet xFirewall центрального офиса в системе виртуализации	И	2
	Установлен ViPNet xFirewall Центрального офиса	И	2
	Настроен ViPNet xFirewall Центрального офиса	И	2
	Установлена база решающих правил на ViPNet xFirewall Центрального офиса	И	2
	Настроен сетевой фильтра для работы защищенной сети на ViPNet xFirewall Центрального офиса	И	2
	Настроен ViPNet xFirewall филиала в системе виртуализации	И	2
	Установлен ViPNet xFirewall филиала	И	2
	Настроен ViPNet xFirewall филиала	И	2

	Установлена база решающих правил на ViPNet xFirewall филиала	И	2
	Настроен сетевой фильтра для работы защищенной сети на ViPNet xFirewall филиала	И	2
	Настроены сетевые интерфейсы виртуальной машины администратора	И	2
	Установлен ViPNet Client администратора	И	2
	Настроен ViPNet Client администратора	И	2
	Настроены сетевые интерфейсы виртуальной машины клиента филиала	И	2
	Установлен ViPNet Client филиала	И	2
	Настроен ViPNet Client филиала	И	2
	Проверена работоспособность защищенной сети	И	2
	Модуль В. Компрометация узла.	**И**	**4**
	Скомпрометированы ключи пользователя	И	2
	Скомпрометированный пользователь работоспособен	И	2
	Модуль Г. Работоспособность сети.	**И**	**22**
	Установлен ViPNet Policy Manager	И	2
	Создана политика безопасности запрещеющее RDP подключение	И	2
	Настроено туннелироване на координаторах или с помощью ЦУС	И	2
	Настроены политики безопасности с помощью командного интерпретатора на xFirewall	И	2
	Настроено межсетевое взаимодействие	И	2
	Заменены мастер ключи своей сети, восстановлена работоспособность	И	2
	Установлен ViPNet Client 4U под Linux	И	2
	Установлен ViPNet EPP сервер и клиент на машину администратора	И	2
	Установлен ViPNet EPP агент на машину клиента филиала, проверить работоспособность	И	2
	Установлена и активирована лицензия EPP	И	2
	Установлены базы решающих правил на EPP	И	2
		ОБЩЕЕ:	**100**
	Модуль А. Настройка защищенной VPN сети.	**И или О**	**28**
	Настроена виртуальная машина администратора в системе виртуализации	И	2
	Настроены сетевые интерфейсы виртуальной машины администратора	И	2
	Установлена и работоспособна серверная часть ViPNet ЦУС	И	2

Специалисты	Работоспособна серверная часть ViPNet ЦУС	И	2
	Установлена клиентская часть ViPNet ЦУС	И	2
	Работоспособна клиентская часть ViPNet ЦУС	И	2
	Установлен VIPNet УКЦ	И	2
	Работоспособен VIPNet УКЦ	И	2
	Созданы и настроен пользователь Администратор	И	2
	Созданы и настроен пользователь филиала	И	2
	Настроено взаимодействие между пользователями в сети	И	2
	Настроены пароли пользователей и администраторов в соответствии с заданием	И	2
	Созданы группы узлов и пользователей центрального офиса	И	2
	Созданы группы узлов и пользователей филиала	И	2
	Модуль Б. Развертывание узлов сети.	**И**	**46**
	Настроена виртуальная машина ViPNet Coordinator центрального офиса в системе виртуализации	И	2
	Установлен ViPNet Coordinator центрального офиса	И	2
	Настроен ViPNet Coordinator центрального офиса	И	2
	Настроена виртуальная машина ViPNet Coordinator филиала в системе виртуализации	И	2
	Установлен ViPNet Coordinator филиала	И	2
	Настроен ViPNet Coordinator филиала	И	2
	Настроен ViPNet xFirewall центрального офиса в системе виртуализации	И	2
	Установлен ViPNet xFirewall Центрального офиса	И	2
	Настроен ViPNet xFirewall Центрального офиса	И	2
	Установлена база решающих правил на ViPNet xFirewall Центрального офиса	И	2
	Настроен сетевой фильтра для работы защищенной сети на ViPNet xFirewall Центрального офиса	И	2
	Настроен ViPNet xFirewall филиала в системе виртуализации	И	2
	Установлен ViPNet xFirewall филиала	И	2
	Настроен ViPNet xFirewall филиала	И	2
	Установлена база решающих правил на ViPNet xFirewall филиала	И	2
	Настроен сетевой фильтра для работы защищенной сети на ViPNet xFirewall филиала	И	2
	Настроены сетевые интерфейсы виртуальной машины администратора	И	2
	Установлен ViPNet Client администратора	И	2
	Настроен ViPNet Client администратора	И	2

	Настроены сетевые интерфейсы виртуальной машины клиента филиала	И	2
	Установлен ViPNet Client филиала	И	2
	Настроен ViPNet Client филиала	И	2
	Проверена работоспособность защищенной сети	И	2
	Модуль В. Компрометация узла.	**И**	**4**
	Скомпрометированы ключи пользователя	И	2
	Скомпрометированный пользователь работоспособен	И	2
	Модуль Г. Работоспособность сети.	**И**	**22**
	Установлен ViPNet Policy Manager	И	2
	Создана политика безопасности запрещеющее RDP подключение	И	2
	Настроено туннелироване на координаторах или с помощью ЦУС	И	2
	Настроены политики безопасности с помощью командного интерпретатора на xFirewall	И	2
	Настроено межсетевое взаимодействие	И	2
	Заменены мастер ключи своей сети, восстановлена работоспособность	И	2
	Установлен ViPNet Client 4U под Linux	И	2
	Установлен ViPNet EPP сервер и клиент на машину администратора	И	2
	Установлен ViPNet EPP агент на машину клиента филиала, проверить работоспособность	И	2
	Установлена и активирована лицензия EPP	И	2
	Установлены базы решающих правил на EPP	И	2
		ОБЩЕЕ:	**100**

3. Перечень специальной одежды, оборудования, инструментов и расходных материалов, которые участник может привезти с собой на площадку проведения чемпионата.

3.1. Требуемая специальная одежда участникам по компетенции в соответствии с требованиями охраны труда и техники безопасности: школьники/студенты/специалисты (при необходимости оформляется отдельно по категориям):

Требуемая специальная одежда (участник обязан привезти с собой) (Школьники/Студенты/Специалисты)					
№ п/п	**Наименование**	**Технические характеристики**	**Ссылка на образец (при необходимости)**	**Ед. измерения**	**Необходимое кол-во**
1	Не требуется			шт	

3.2. Рекомендуемый перечень оборудования и инструментов для участников категорий: школьники, студенты, специалисты (при необходимости оформляется отдельно для каждой категории), которые участник может привезти с собой:

Рекомендуемый набор оборудования/инструментов (участник может привезти с собой) (Школьники/Студенты/Специалисты (при необходимости оформляется отдельно по категориям)) *на площадке могут быть аналоги с аналогичными характеристиками, предоставляемые в качестве замены					
№ п/п	**Наименование**	**Технические характеристики**	**Ссылка на образец (при необходимости)**	**Ед. измерения**	**Необходимое кол-во**
1	Не требуется			шт	

3.3. Инфраструктурный лист застройки площадки предоставляется в виде отдельного документа (приложения) в формате Excel (.xlsx)

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

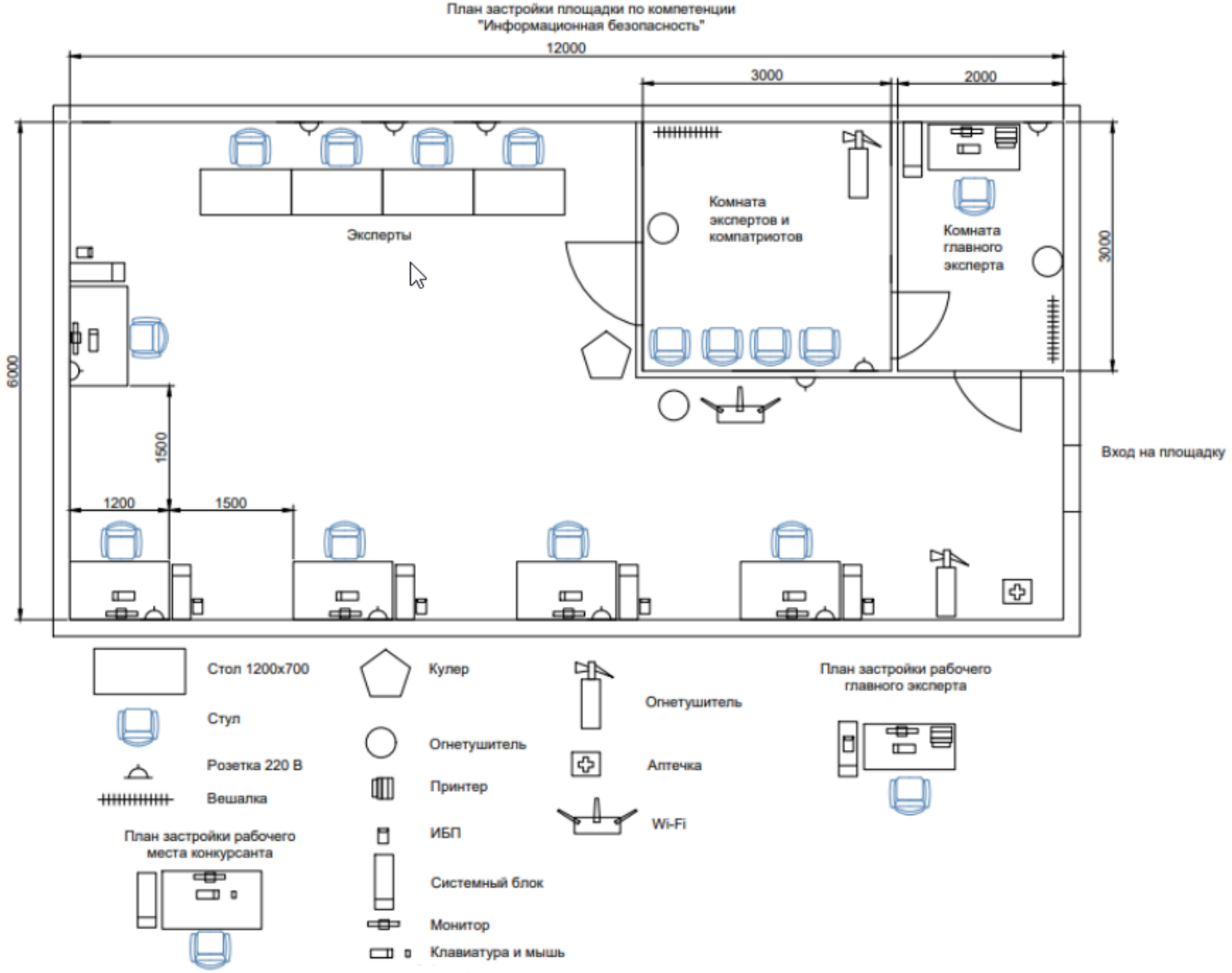
* минимальные требования к оснащению рабочих мест согласованы с общероссийскими общественными организациями инвалидов

Вид нозологии	Площадь, м.кв.	Ширина прохода между рабочими местами, м.	Специализированное оборудование, количество*
Рабочее место участника с нарушением слуха	3000х1900	1,5 м	Для участников с нарушением слуха необходимо предусмотреть: а) наличие звукоусиливающей аппаратуры, акустической системы, информационной индукционной системы, наличие индивидуальных наушников; б) наличие на площадке переводчика русского жестового языка (сурдопереводчика); в) оформление конкурсного задания в доступной текстовой информации.
Рабочее место участника с нарушением зрения	3000х1900	1,5 м	Для участников с нарушением зрения необходимо: а) текстовое описание конкурсного задания в плоскопечатном виде с крупным размером шрифта, учитывающим состояние зрительного анализатора участника с остаточным зрением (в формате Microsoft Word не менее 16-18 пт), дублированного рельефно точечным шрифтом Брайля (при необходимости); б) лупа с подсветкой для слабовидящих; электронная лупа; в) для рабочего места, предполагающего работу на компьютере - оснащение специальным компьютерным оборудованием и оргтехникой: видеоувеличитель; - программы экранного доступа NVDA и JAWS18 (при необходимости); - брайлевский дисплей (при необходимости); в) для рабочего места участника с нарушением зрения, имеющего собаку-проводника, необходимо предусмотреть место для собаки-проводника. г) оснащение (оборудование) специального рабочего места тифлотехническими ориентирами и устройствами, с возможностью использования крупного рельефно-контрастного шрифта и шрифта Брайля, акустическими навигационными средствами, обеспечивающими

			беспрепятственное нахождение инвалидом по зрению - слепого своего рабочего места и выполнение трудовых функций; д) индивидуальное равномерное освещение не менее 300 люкс.
Рабочее место участника с нарушением ОДА	3000х1900	1,5 м	Оснащение (оборудование) специального рабочего места оборудованием, обеспечивающим реализацию эргономических принципов: а) увеличение размера зоны на одно место с учетом подъезда и разворота кресла-коляски, увеличения ширины прохода между рядами верстаков; б) для участников, передвигающихся в кресле- коляске, необходимо выделить 1 - 2 первых рабочих места в ряду у дверного проема; в) оснащение (оборудование) специального рабочего места специальными механизмами и устройствами, позволяющими изменять высоту и наклон рабочей поверхности, положение сиденья рабочего стула по высоте и наклону, угол наклона спинки рабочего стула, оснащение специальным сиденьем, обеспечивающим компенсацию усилия при вставании.
Рабочее место участника с соматически ми заболеваниям и	3000х1900	1,5 м	Специальные требования к условиям труда инвалидов вследствие заболеваний сердечно- сосудистой системы, а также инвалидов вследствие других соматических заболеваний, предусматривают отсутствие: а) вредных химических веществ, включая аллергены, канцерогены, оксиды металлов, аэрозоли преимущественно фиброгенного действия; б) тепловых излучений; локальной вибрации, электромагнитных излучений, ультрафиолетовой радиации на площадке; в) превышения уровня шума на рабочих местах; г) нарушений уровня освещенности, соответствующей действующим нормативам. Необходимо обеспечить наличие столов с регулируемыми высотой и углом наклона поверхности; стульев (кресел) с регулируемыми высотой сиденья и положением спинки (в соответствии со спецификой заболевания).

Рабочее место участника с ментальными нарушениями	3000х1900	1,5 м	Специальные требования к условиям труда инвалидов, имеющих нервно-психические заболевания: а) создание оптимальных и допустимых санитарно-гигиенических условий производственной среды, в том числе: температура воздуха в холодный период года при легкой работе - 21 - 24 °С; при средней тяжести работ - 17 - 20 °С; влажность воздуха в холодный и теплый периоды года 40 – 60 %; отсутствие вредных веществ: аллергенов, канцерогенов, аэрозолей, металлов, оксидов металлов; б) электромагнитное излучение - не выше ПДУ; шум - не выше ПДУ (до 81 дБА); отсутствие локальной и общей вибрации; отсутствие продуктов и препаратов, содержащих живые клетки и споры микроорганизмов, белковые препараты; в) оборудование (технические устройства) должны быть безопасны и комфортны в использовании (устойчивые конструкции, прочная установка и фиксация, простой способ пользования без сложных систем включения и выключения, с автоматическим выключением при неполадках; расстановка и расположение, не создающие помех для подхода, пользования и передвижения; расширенные расстояния между столами, мебелью; не должна затрудняющая доступность устройств; исключение острых выступов, углов, ранящих поверхностей, выступающих крепежных деталей)

5. Схема (план) застройки соревновательной площадки (пример)



6. Требования охраны труда и техники безопасности

6.1. Общие требования:

Настоящая инструкция распространяется на персонал, эксплуатирующий средства вычислительной техники и периферийное оборудование. Инструкция содержит общие указания по безопасному применению электрооборудования в учреждении. Требования настоящей инструкции являются обязательными, отступления от нее не допускаются. К самостоятельной эксплуатации электроаппаратуры допускается только специально обученный персонал не моложе 18 лет, пригодный по состоянию здоровья и квалификации к выполнению указанных работ.

6.2. Действия до начала работ:

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

6.3. Действия во время выполнения работ:

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 периферийном оборудовании мокрыми руками, работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию о 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 специалистам и 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.

6.4. Действия после окончания работ:

После окончания работы необходимо обесточить все средства вычислительной техники и периферийное оборудование. В случае непрерывного производственного процесса необходимо оставить включенными только необходимое оборудование.

6.5. Действия в случае аварийной ситуации:

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

При обнаружении оборвавшегося провода необходимо немедленно сообщить об этом администрации, 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 Региональный чемпионат «Абилимпикс» 2026 30 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) Зажигать 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 типа ОУ-2 или ОУБ-3.