Чемпионат Свердловской области
«Абилимпикс»

СОГЛАСОВАНО

Свердловское региональное
отделение Общероссийской
общественной организации инвалидов
«Всероссийское общество глухих»

Председатель _____Черемера Л.А.
«09» февраля 2023 г.

Свердловская областная
Организация Общероссийской
общественной организации инвалидов
«Всероссийское ордена Трудового Красного
Знамени общество слепых»

Председатель _____Юдина М.А.
«09» февраля 2023 г.

Центр цифрового образования IT куб
_____Федоров В.П._____/_____
«31» января 2023 г.

УТВЕРЖДАЮ

Региональный центр
развития движения «Абилимпикс»

Руководитель _____Чешко С.Л.
«09» февраля 2023г.

Конкурсное задание по компетенции «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Екатеринбург, 2023 г.

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 10.2.4 «Обеспечение информационной безопасности телекоммуникационных систем», 10.2.5 «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 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. 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 требованийпо защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; использовать типовые программные криптографические средства, в том числе электронную подпись;	*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 требованийпо 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	*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

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.	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.	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

		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.

Школьники: В ходе выполнения конкурсного задания необходимо настроить кластер горячего резервирования ViPNet Coordinator VA. Настроить инфраструктуру Windows Server и клиентской машины.

Студенты: В ходе выполнения конкурсного задания необходимо настроить кластер горячего резервирования ViPNet Coordinator VA.. Настроить инфраструктуру Windows Server и клиентской машины. Установить защищенное HTTPS взаимодействие.

Специалисты: В ходе выполнения конкурсного задания необходимо настроить кластер горячего резервирования ViPNet Coordinator VA. Настроить инфраструктуру Windows Server и клиентской машины. Установить защищенное HTTPS взаимодействие. В ходе выполнения конкурсного задания необходимо произвести установку и настройку программного обеспечения для работы с рутокен, настроить аутентификацию по рутокен в Linux.

2.2. Структура и подробное описание конкурсного задания.

	Наименование и описание	**День**	**Время**	**Результат**
Школьник	Модуль 1. Настроить кластер горячего резервирования ViPNet.	Первый день	1 час	Кластер горячего резервирования находится в рабочем состоянии.
	Модуль 2. Настроить инфраструктуру Windows Server и клиентской машины.	Первый день	1 час	Сконфигурированы машины с Windows Server и клиентская машина в доменной зоне.

Студент	Модуль 1. Настроить кластер горячего резервирования ViPNet.	Первый день	1 час	Кластер горячего резервирования находится в рабочем состоянии.
	Модуль 2. Настроить инфраструктуру Windows Server и клиентской машины.	Первый день	1 час	Сконфигурированы машины с Windows Server и клиентская машина в доменной зоне.
	Модуль 3. Установить защищенное HTTPS	Первый день	30 минут	Работает защищенное HTTPS соединение
Специалист	Модуль 1. Настроить кластер горячего резервирования ViPNet.	Первый день	1 час	Кластер горячего резервирования находится в рабочем состоянии.
	Модуль 2. Настроить инфраструктуру Windows Server и клиентской машины.	Первый день	1 час	Сконфигурированы машины с Windows Server и клиентская машина в доменной зоне.
	Модуль 3. Установить защищенное HTTPS взаимодействие.	Первый день	30 минут	Работает защищенное HTTPS соединение
	Модуль 4. Аутентификация в Linux с помощью Рутокен	Первый день	30 минут	Настроена аутентификация по Рутокену

2.3.Последовательность выполнения задания.

Школьники:

Модуль 1. Сканирование сетевого траффика.

Инициализировать ViPNet Coordinator VA, настроить кластер горячего резервирования, проверить работоспособность.

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

Модуль 2. Настроить инфраструктуру Windows Server и клиентской машины.

Настроить инфраструктуру Windows Server и клиентской машины. Завести пользователей в AD с необходимыми правами. Настроить групповые политики.

Студенты:

Модуль 1. Сканирование сетевого трафика.

Инициализировать ViPNet Coordinator VA, настроить кластер горячего резервирования, проверить работоспособность.

Модуль 2. Настроить инфраструктуру Windows Server и клиентской машины.

Настроить инфраструктуру Windows Server и клиентской машины. Завести пользователей в AD с необходимыми правами. Настроить групповые политики.

Модуль 3. Установить защищенное HTTPS взаимодействие.

Создать цепочку сертификатов для защищенного HTTPS соединения.

Специалисты:

Модуль 1. Сканирование сетевого трафика.

Инициализировать ViPNet Coordinator VA, настроить кластер горячего резервирования, проверить работоспособность.

Модуль 2. Настроить инфраструктуру Windows Server и клиентской машины.

Настроить инфраструктуру Windows Server и клиентской машины. Завести пользователей в AD с необходимыми правами. Настроить групповые политики.

Модуль 3. Установить защищенное HTTPS взаимодействие.

Создать цепочку сертификатов для защищенного HTTPS соединения.

Модуль 4. Аутентификация в Linux с помощью Рутокен.

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

2.4. 30% изменение конкурсного задания.

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

2.5. Критерии оценки выполнения задания Школьники:

№	Описание критерия	Ба
	Модуль 1.	
1.	Инициализирован координатор (загружен DST)	5
2.	Правильно настроены сетевые интерфейсы	5
3.	Сконфигурирован файл для кластера горячего резервирования	5
4.	Проверена работа с помощью параметра testip	5
	Модуль 2.	
5.	Созданы группы	10
6.	Заведены пользователи в систему в группу	10
7.	Правильно сконфигурированы права пользователей	20
8.	Правильно сконфигурированы порты для брандмауэра	20
9.	Установлено программное обеспечение через групповые	20
	Всего	100

Студенты:

№ п/п	Критерии	Наивысший балл
	Модуль 1.	
1.	Инициализирован координатор (загружен DST)	5
2.	Правильно настроены сетевые интерфейсы	5
3.	Сконфигурирован файл для кластера горячего резервирования	5
4.	Проверена работа с помощью параметра testip	5
	Модуль 2.	
5.	Созданы группы	5
6.	Заведены пользователи в систему в группу	5
7.	Правильно сконфигурированы права пользователей	10
8.	Правильно сконфигурированы порты для брандмауэра	20
9.	Установлено программное обеспечение через групповые политики	20
10.	**Модуль 3.**	
11.	Созданы необходимые сертификаты	10
12.	Работает защищенное соединение с сервером	10
	Всего	100

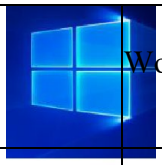
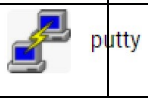
Специалисты:

№ п/п	Критерии	Наивысший балл
	Модуль 1.	
1.	Инициализирован координатор (загружен DST)	5
2.	Правильно настроены сетевые интерфейсы	5
3.	Сконфигурирован файл для кластера горячего резервирования	5
4.	Проверена работа с помощью параметра testip	5
	Модуль 2.	
5.	Созданы группы	5
6.	Заведены пользователи в систему в группу	5
7.	Правильно сконфигурированы права пользователей	5
8.	Правильно сконфигурированы порты для брандмауэра	5
9.	Установлено программное обеспечение через групповые политики	5
	Модуль 3.	
10.	Созданы необходимые сертификаты	10
11.	Работает защищенное соединение с сервером	5
	Модуль 4.	
12.	Настройка pam p11	6
13.	Создание ключей на рутокене	6
14.	Проверка сгенерированного ключ	7
15.	Создание сертификата и импорт	7
16.	Занесение сертификата в список доверенных	7
17.	Аутентификация в системе	7
	Всего	100

3 Перечень используемого оборудования, инструментов и расходных материалов.

3.1. Школьники, студенты, специалисты

ОБОРУДОВАНИЕ НА 1-ГО УЧАСТНИКА					
Оборудование, инструменты, ПО, мебель					
	Наименование	**Фото оборудования, средства индивидуальной защиты**	**Тех. характеристики оборудования, инструментов и ссылка на сайт производителя, поставщика**	**Ед. измерения**	**Кол-во**
	Стол		1400x700 мм, https://meb-biz.ru	Шт.	1
	Стул		Офисный, https://beautyoffice.ru/kb-8-kreslo-burokrat	Шт.	1
	АРМ		Intel Core i5 или быстрее, 16GB RAM и более, 500GB HDD и более,ОС WINDOWS 8.1, 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
	ИБП		Не менее 500 VA, https://www.dns-shop.ru/product/9d493cda46bd3330/ibp-dexp-cee-650va/?p=1&i=7	Шт.	1
	Удлинитель		220В, 2 метра, 6 розеток, https://www.citilink.ru/catalog/computers_and_notebooks/powersafe/powerfilters	Шт.	1

Windows 7 или выше	 Установленная для работы в VMware Workstation	Шт.	1
VMware Workstatio n	 VMware Workstation	Шт.	1
Kali Linux	 Установленная для работы в VMware Workstation	Шт.	
Putty	 Установщик	Шт.	
РАСХОДНЫЕ МАТЕРИАЛЫ НА 1 УЧАСТНИКА			
Расходные материалы			
Наименование	Технические характеристики	Ед.	Кол-во
Шариковая ручка		Шт.	1
Лист бумаги		Шт.	1
РАСХОДНЫЕ МАТЕРИАЛЫ И ОБОРУДОВАНИЕ, ЗАПРЕЩЕННЫЕ НА ПЛОЩАДКЕ			
Мобильные устройства			

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	https://www.obrazov.org/ (Количество оборудования зависит от количества участников)
Рабочее место участника с нарушением зрения	более 3 м	не менее 1 м	https://www.obrazov.org/ (Количество оборудования зависит от количества участников) Органайзер Брайля, специализированное программное обеспечение для слабовидящих
Рабочее место участника с нарушением ОДА	более 3м 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)
Рабочее место участника с соматическими заболеваниями	не менее 2,5 кв. м	не менее 1 м	https://www.istok-reatech.ru/catalog/
Рабочее место участника с ментальными нарушениями	не менее 2,5 кв. м	рекомендуется предусматривать полузамкнутые	https://inva24.ru/

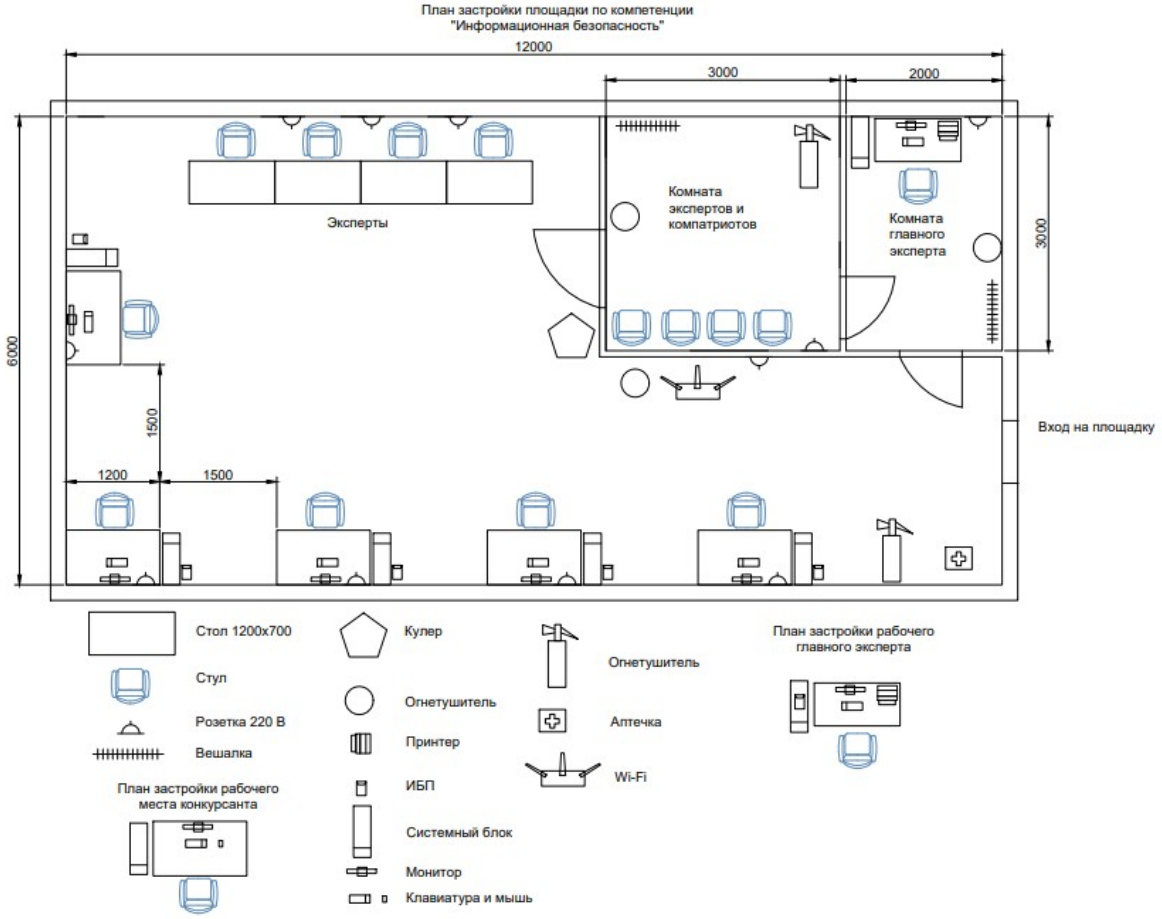
		рабочие места-кабины (с боковыми бортиками и экранами у стола, высокими спинками сидений, с бортиками ограждениями по бокам и сзади и т.п.), что создает для этих учащихся более спокойную обстановку, помогает регулировать психологическую	

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

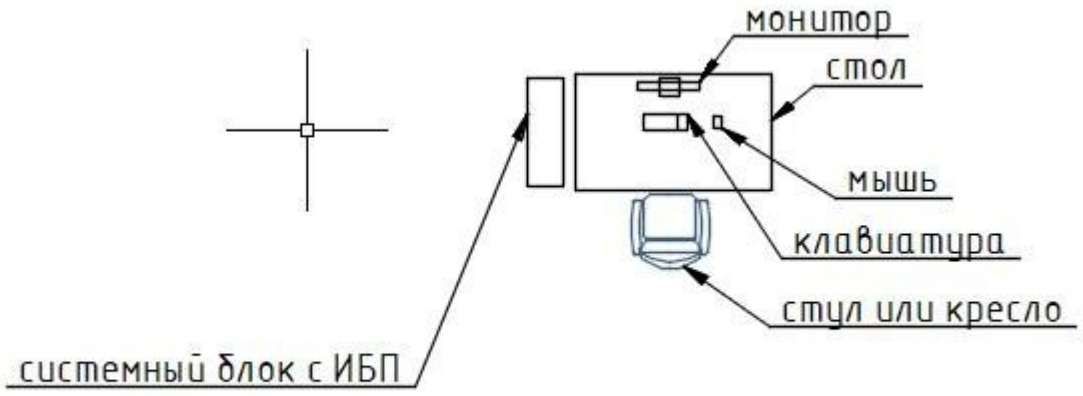
5. Схема застройки соревновательной площадки. Застройка осуществляется на группу участников

- **на 5 рабочих мест (школьники)**
- **на 5 рабочих мест (студенты)**
- **на 5 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.