IV НАЦИОНАЛЬНЫЙ ЧЕМПИОНАТ «АБИЛИМПИКС»

Утверждено

советом по компетенции

Информационная безопасность
Протокол № 1 от 07.09.2018

Председатель совета:

_____**Минин В.В.**
(подпись)

КОНКУРСНОЕ ЗАДАНИЕ

по компетенции

Информационная безопасность

Москва 2018

Содержание

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.

Имея решающую роль в повседневном функционировании, по защите информации имеет спрос в организациях различных масштабов коммерческого и государственного сектора.

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

Школьники	**Студенты**	**Специалисты**
ФГОС СПО 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" http://reestrspo.ru/node/580	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	

1.3. 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	*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	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

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.	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.	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.

2.Конкурсное задание.
2.1. Краткое описание задания.

Школьники: В ходе выполнения конкурсного задания необходимо установить и настроить Infowatch Traffic Monitor. Сгенерировать сертификат. Просканировать сетевой трафик.

Студенты: В ходе выполнения конкурсного задания необходимо установить и настроить Infowatch Traffic Monitor, настроить соответствующие политики безопасности. Сгенерировать сертификат. Просканировать сетевой трафик. Настроить подключение к заданной операционной системе по ssh.

Специалисты: В ходе выполнения конкурсного задания необходимо установить и настроить Infowatch Traffic Monitor, настроить соответствующие политики безопасности. Сгенерировать сертификат. Просканировать сетевой трафик. Настроить подключение к заданной операционной системе по ssh. Восстановить пароль к архиву.

2.2. Структура и подробное описание конкурсного задания.

	Наименование и описание модуля	**День**	**Время**	**Результат**
Школьник	Модуль 1. Установка и настройка TM.	Первый день	1 час	Установленный TM, DM, Client, настроены политики
	Модуль 2. Настройка защищенного https соединения.	Первый день	30 минут	Настроенное https соединение
	Модуль 3. Настройка защищенного соединения ssh к Linux.	Первый день	30 минут	Подключение к Linux
Студент	Модуль 1. Установка и настройка TM.	Первый день	1 час	Установленный TM, DM, Client, настроены политики
	Модуль 2. Сканирование сетевого трафика.	Первый день	20 минут	Обнаружен пароль
	Модуль 3. Настройка защищенного https соединения.	Первый день	20 минут	Настроенное https соединение
	Модуль 4. Настройка защищенного соединения ssh к Linux.	Первый день	20 минут	Подключение к Linux
Специалист	Модуль 1. Установка и настройка TM.	Первый день	1 час	Установленный TM, DM, Client, настроены политики
	Модуль 2. Сканирование сетевого трафика.	Первый день	20 минут	Обнаружен пароль
	Модуль 3. Настройка защищенного https соединения.	Первый день	20 минут	Настроенное https соединение
	Модуль 4. Настройка защищенного соединения ssh к Linux.	Первый день	20 минут	Подключение к Linux

	Модуль 5. Восстановление пароля к архиву	Первый день	20 минут	Обнаружен пароль
	Модуль 6. Восстановление удаленной информации.	Первый день	20 минут	Восстановлена информация

2.3.Последовательность выполнения задания.

Школьники:

Модуль 1. Установка и настройка ТМ.

Установить под виртуальную машину ТМ из образа. Установить DM в готовую виртуальную машину, связать ТМ и DM. Установить клиентскую часть на клиентскую виртуальную машину. Настроить политики для DM и ТМ.

Модуль 2. Настройка защищенного https соединения.

Настроить самоподписанный сертификат в Kali Linux и установить его в систему.

Модуль 3. Настройка защищенного соединения ssh к Linux.

Настроить подключение к Kali Linux по ssh протоколу посредствам rsa ключа через Putty.

Студенты:

Модуль 1. Установка и настройка ТМ.

Установить под виртуальную машину ТМ из образа. Установить DM в готовую виртуальную машину, связать ТМ и DM. Установить клиентскую часть на клиентскую виртуальную машину. Настроить политики для DM и ТМ.

Модуль 2. Сканирование сетевого трафика.

Просканировать сетевой трафик от одной виртуальной машины к другой, восстановить пароль.

Модуль 3. Настройка защищенного https соединения.

Настроить самоподписанный сертификат в Kali Linux и установить его в систему.

Модуль 4. Настройка защищенного соединения ssh к Linux.

Настроить подключение к Kali Linux по ssh протоколу посредствам rsa ключа через Putty.

Специалисты:

Модуль 1. Установка и настройка ТМ.

Установить под виртуальную машину ТМ из образа. Установить DM в готовую виртуальную машину, связать ТМ и DM. Установить клиентскую часть на клиентскую виртуальную машину. Настроить политики для DM и ТМ.

Модуль 2. Сканирование сетевого трафика.

Просканировать сетевой трафик от одной виртуальной машиы к другой, восстановить пароль.

Модуль 3. Настройка защищенного https соединения.

Настроить самоподписанный сертификат в Kali Linux и установить его в систему.

Модуль 4. Настройка защищенного соединения ssh к Linux.

Настроить подключение к Kali Linux по ssh протоколу посредствам rsa ключа через Putty.

Модуль 5. Восстановление пароля к архиву.

Необходимо восстановить пароль к заданному архиву.

Модуль 6. Восстановление удаленной информации.

Восстановить удаленную информацию**.**

2.4. Критерии оценки выполнения задания

Школьники:

№	Описание критерия	Баллы
	Модуль 1.	10
1.	Установка Traffic Monitor	10
2.	Установка лицензии	5
3.	Подключение к ТМ через браузер	5
4.	Установка Device Monitor	10
5.	Установка клиента	10
6.	Настройка правила для USB накопителей в DM	10
7.	Правильная работа правила на клиентской машине	10
	Модуль 2.	
8.	Создание самоподписанного сертификата с наличием скриншотов	10
9.	Установка сертификата в систему с наличием скриншотов	10
	Модуль 3.	
10.	Создание rsa ключа с наличием скриншотов	10
11.	Создание подключения через Putty	10
	Всего	100

Студенты:

№ п/п	Критерии	Наивысший балл
	Модуль 1.	
1.	Установка Traffic Monitor	10
2.	Установка лицензии	5
3.	Установка Device Monitor	
4.	Установка клиента	5
5.	Настройка правила для USB накопителей в DM	5
6.	Правильная работа правила на клиентской машине	5
7.	Работа Traffic Monitor в связке с Device Monitor	5
8.	Настройка правил для ТМ.	10
	Модуль 2.	
9.	Обнаружен пароль.	10
	Модуль 3.	
10.	Создать самоподписанный сертификат.	10
11.	Установка сертификата в систему с наличием скриншотов	10
	Модуль 4.	
12.	Генерацию ключей rsa со скриншотом	10
13.	Настройка ключа для работы с Putty	5
14.	Подключение к Linux через Putty	10
	Всего	100

Специалисты:

№ п/п	Критерии	Наивысший балл
	Модуль 1.	
1.	Установка Traffic Monitor	5
2.	Установка лицензии	5
3.	Установка Device Monitor	
4.	Установка клиента	5
5.	Настройка правила для USB накопителей в DM	5
6.	Правильная работа правила на клиентской машине	5
7.	Работа Traffic Monitor в связке с Device Monitor	5
8.	Настройка правил для TM.	10
	Модуль 2.	
9.	Обнаружен пароль.	10
	Модуль 3.	
10.	Создать самоподписанный сертификат.	10
11.	Установка сертификата в систему с наличием скриншотов	5
	Модуль 4.	
12.	Генерацию ключей rsa со скриншотом.	10
13.	Настройка ключа для работы с Putty.	5
14.	Подключение к Linux через Putty.	5
15.	**Модуль 5.**	
16.	Поучен пароль к архиву.	5
17.	**Модуль 6.**	
18.	Восстановлена информация.	10
	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	тех. характеристики оборудования, инструментов и ссылка на сайт производителя, поставщика	Ед. измерения	Кол-во
1	Стол	1400x700 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 быстрее, 8GB 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

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				
-	-	-	-	-
ДОПОЛНИТЕЛЬНОЕ ОБОРУДОВАНИЕ, ИНСТРУМЕНТЫ КОТОРОЕ МОЖЕТ ПРИВЕСТИ С СОБОЙ УЧАСТНИК (при необходимости)				
№	Наименование	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/	1	1
ОБОРУДОВАНИЕ НА 1-ГО ЭКСПЕРТА (при необходимости)				
Оборудование, мебель				
№	Наименование	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, 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	тех. Характеристики дополнительного оборудования и средств индивидуальной защиты и ссылка на сайт производителя, поставщика	Ед. измерения	Кол-во
1	Огнетушитель	Огнетушитель углекислотный, http://www.magazin01.ru	Шт.	2
КОМНАТА УЧАСТНИКОВ (при необходимости)				
Оборудование, мебель, расходные материалы (при необходимости)				
1	Стол			
2	Вешал	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. Схемы оснащения рабочих мест с учетом основных нозологий.

4.1. 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			
Рабочее место участника с нарушением зрения	4	1.5	Органайзер Брайля, специализированное ПО для слабовидящих
Рабочее место участника с нарушением ОДА			
Рабочее место участника с соматическими заболеваниями			
Рабочее место участника с ментальными нарушениями			

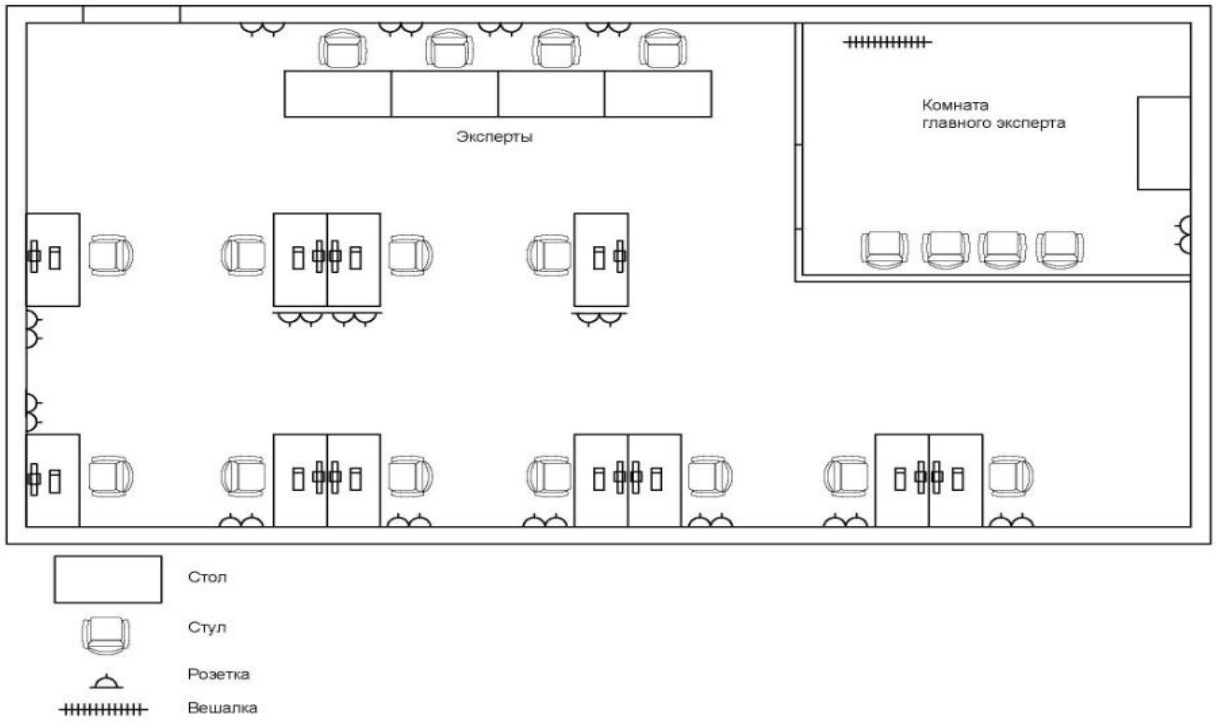
*****указывается **с**ссылка на сайт с тех. характеристиками, либо наименование и тех. характеристики специализированного оборудования**.**

4.2. Графическое изображение рабочих мест с учетом основных нозологий.

Застройка осуществляется на группу участников

4.3. Схема застройки соревновательной площадки.

Для всех категорий



5. 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.