# 7 Безопасность и экологичность

## 7.1 Характерные вредные и опасные производственные факторы

При проведении работ, связанных с вычислительной техникой и автоматизированными системами, существуют ряд вредных и опасных производственных факторов, которые могут негативно сказываться на здоровье и работоспособности людей.[1] Так СанПиН 2.2.2/2.4.1340-03 "Гигиенические требования к организации и условиям труда при работе с персональными электронновычислительными машинами" устанавливает ряд требований и рекомендаций в отношении организации и условий работы с ПЭВМ. Вот характерные вредные и опасные производственные факторы:

1. Электромагнитные излучения: Повышенный уровень электромагнитных излучений от компьютеров, мониторов, принтеров и другой вычислительной техники может вызывать физический дискомфорт, головные боли, раздражение глаз, сухость и покраснение кожи. Длительное воздействие высоких уровней электромагнитных излучений может привести к более серьезным заболеваниям.
2. Статическое электричество: При работе с компьютерами и электронными устройствами может возникать статическое электричество. Оно может вызывать дискомфорт, а также приводить к повреждению электронных компонентов и систем.
3. Ионизация воздуха: Пониженная ионизация воздуха в помещениях с большим количеством электронной техники может привести к сухости слизистых оболочек, раздражению глаз, ухудшению качества сна и общему ухудшению самочувствия.
4. Статические физические перегрузки: Длительное сидение в неправильной позе, неправильная организация рабочего места и эргономика могут привести к развитию мышечно-скелетных заболеваний, таких как боли в спине, шее, запястьях и других частях тела.
5. Перенапряжение зрительных анализаторов: Проведение длительной работы за компьютером может вызывать усталость глаз, сухость, раздражение и другие проблемы со зрением.
6. Недостаточная освещенность рабочего места: Отсутствие достаточного освещения на рабочем месте может привести к ухудшению зрения, напряжению глаз и проблемам с концентрацией.

## 7.2 Требования к помещениям для работы с ПЭВМ

В соответствии с требованиями СанПиН 2.2.2/2.4.1340-03, помещения, предназначенные для работы с ПЭВМ, должны обеспечивать оптимальные условия микроклимата, воздухообмена, освещения, а также защиту от электромагнитных полей, шума и вибрации.[2]

Для поддержания комфортных условий работы, температура воздуха должна находиться в диапазоне 22-24°C, относительная влажность должна составлять 40-60%, а скорость движения воздуха не должна превышать 0,1 м/с. Концентрация пыли должна быть не выше 0,15 , а содержание вредных химических веществ должно соответствовать нормативам, установленным в ГОСТ 12.1.005 и ГОСТ 12.1.007. Кроме того, требуется поддерживать концентрацию аэроионов на уровне не менее 400 .

Уровень шума в помещении, где располагаются рабочие места с ПЭВМ, не должен превышать 50 дБ, а уровень вибрации должен соответствовать требованиям, установленным в ГОСТ 12.1.012.

Освещение на рабочих местах с ПЭВМ должно обеспечивать достаточную яркость и равномерность освещения. Естественное освещение должно быть в диапазоне от 300 до 500 лк, искусственное освещение также должно находиться в этом диапазоне. Вместе с тем следует ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 .

Также необходимо соблюдать требования к уровню электромагнитных полей на рабочих местах, оборудованных ПЭВМ, в соответствии с нормативами, указанными в СанПиН 2.2.2/2.4.1340-03. Это включает электромагнитные поля низкой частоты (50 Гц) и высокой частоты (30 кГц - 300 ГГц).

Наконец, визуальные параметры ВДТ (визуального дисплея терминала) на рабочих местах должны соответствовать требованиям ГОСТ Р ИСО 9241-307. Это включает яркость экрана, разрешающую способность экрана, а также частоту вертикальной и горизонтальной развертки экрана. Визуальные параметры ВДТ согласно ГОСТ Р ИСО 9241-307 приведены в таблице 7.2.

Таблица 7.2 - визуальные параметры ВДТ по ГОСТ Р ИСО 9241-307

|  |  |
| --- | --- |
| Параметр | Пределы допустимых значений |
| Яркость экрана | 30-300 |
| Разрешающая способность экрана | не менее 1280x1024 пикселей |
| Частота вертикальной развертки экрана | не менее 75 Гц |
| Частота горизонтальной развертки экрана | не менее 30-85 кГц |

## 

## 7.3 Требования к персоналу

При обслуживании вычислительных машин, комплексов, систем и сетей существуют определенные требования к персоналу, чтобы гарантировать эффективную работу и обеспечить безопасность труда сотрудников проводятся мероприятия, которые включают в себя порядок приема на работу, медицинский осмотр, образование и стажировку на рабочем месте, а также проведение инструктажей по охране труда перед допуском к самостоятельной работе.

Процесс найма на работу представляет собой целенаправленную последовательность мероприятий, которая включает объявление о вакансиях, проведение собеседований и отбор кандидатов, удовлетворяющих требованиям и предъявляемым стандартам работодателя. В ходе этого процесса учитываются разнообразные факторы, включая квалификацию, опыт работы, образование и другие критерии, установленные для данной должности.

Таким образом, корректный подбор кадров позволяет работодателю собрать команду специалистов, способных эффективно выполнять задачи, связанные с обслуживанием вычислительной техники.

Медицинский осмотр является существенной составляющей в контексте работы с вычислительными машинами. Сотрудники, занятые обслуживанием компьютеров, подвергаются различным факторам, которые могут оказывать влияние на их здоровье, включая продолжительное пребывание в статическом положении за монитором, которое оказывает увеличенную нагрузку на зрение и мышцы спины, и другие физические и психологические аспекты, которые могут привести к возникновению профессиональных заболеваний и других негативных последствий. В связи с этим, проведение медицинского осмотра позволяет осуществить оценку общего состояния здоровья работника и определить его пригодность для выполнения конкретных видов работ.

Медицинский осмотр включает проверку различных аспектов здоровья, таких как состояние опорно-двигательной системы, функции зрения, психоэмоциональное состояние и другие важные показатели. Результаты медицинского осмотра помогают работодателю принять взвешенное решение относительно приема и дальнейшего трудоустройства работника, а также предоставить соответствующие меры поддержки и рекомендации для поддержания и улучшения здоровья работника в рабочей среде.

Требования к образованию и стажировке на рабочем месте имеют первостепенное значение в целях обеспечения эффективной и квалифицированной работы с вычислительной техникой и системами. Работники, ответственные за обслуживание и управление указанными устройствами, должны обладать соответствующим образованием, связанным с информационными технологиями, компьютерными науками или смежными областями.

Наличие специализированного образования обеспечивает работникам необходимые теоретические знания, аналитические навыки и понимание основных принципов функционирования вычислительной техники. Это включает знание программирования, сетевых технологий, операционных систем и других аспектов, существенных для обслуживания и управления компьютерными системами.

Кроме того, некоторые организации предлагают программы стажировки на рабочем месте для новых сотрудников. Эта практика позволяет работникам освоить конкретные навыки, необходимые для выполнения своих задач, и получить ценный практический опыт в реальной рабочей среде. Стажировка на рабочем месте предоставляет возможность новым сотрудникам применить свои знания на практике, разобраться во внутренних процессах организации и эффективно взаимодействовать с другими членами команды.

Таким образом, стажировка на рабочем месте в сфере связанной с вычислительной техникой направлена на обеспечение наличия необходимых знаний и навыков у прошедшего ее персонала. Это обеспечивает квалифицированную работу, что способствует эффективной деятельности и содействует достижению поставленных целей в области информационных технологий и вычислительной инфраструктуры.

Инструктаж по охране труда перед допуском к самостоятельной работе является важной составляющей безопасности при работе с вычислительной техникой. В инструктаж входят такие разделы как: общие требования охраны труда, требования охраны труда перед началом работы, требования охраны труда во время работы, требования охраны труда в аварийных ситуациях, требования охраны труда по окончании работы.

В ходе инструктажа персонал осведомляется о нормах, правилах и процедурах, связанных с обеспечением безопасности, сохранением здоровья и предотвращением возможных рисков, связанных с использованием вычислительной техники и сопутствующего оборудования.

В рамках инструктажа особое внимание уделяется информированию работников о правильной организации и эргономике рабочего места. Это включает ознакомление с оптимальным расположением монитора, клавиатуры, мыши и других устройств. Также рассматриваются методы предотвращения травм. Кроме того, работники ознакамливаются с другими мероприятиями, направленными на обеспечение их безопасности. Это может включать правила пожарной безопасности, эвакуационные планы, использование средств индивидуальной защиты, а также процедуры в случае аварийных ситуаций или возникновения чрезвычайных обстоятельств. Инструктаж также может включать информацию о профилактике и предотвращении утомления, стресса и других факторов, которые могут негативно сказываться на здоровье и благополучии работников.

Цель данного инструктажа заключается в том, чтобы обеспечить работникам необходимые знания и практические навыки для безопасного и эффективного использования вычислительной техники. Это помогает предотвратить возможные травмы, заболевания и профессиональные риски, а также создать комфортные и безопасные условия работы.

## 7.4 Электробезопасность

Для обеспечения безопасности работников применяются различные мероприятия, направленные на предотвращение электротравматизма.[3]

Одним из важных аспектов электробезопасности является классификация помещений по опасности поражения электрическим током. Класс помещения определяется на основе наличия или отсутствия проводящих или соприкасающихся с проводниками предметов, которые могут стать источниками опасности.

Так в соответствии с правилами устройства электроустановок (ПУЭ), производственные помещения подразделяются на четыре класса по степени опасности поражения людей электрическим током.

Класс 0: Помещения, где отсутствует опасность поражения электрическим током. В этих помещениях используются источники питания с защитным экраном или двойной изоляцией, и доступ к электрическим частям ограничен.

Класс I: Помещения, в которых возможно соприкосновение людей с напряженными частями. Для обеспечения безопасности в таких помещениях применяются защитное заземление и дополнительные защитные меры, например, изоляция или применение противоударных средств.

Класс II: Помещения, где соприкосновение людей с напряженными частями запрещено. Защита обеспечивается изоляцией и другими средствами, которые предотвращают возможность контакта с электрическими частями.

Класс III: Помещения, в которых работа допускается только при условии, что электрические устройства и оборудование отключены от источника питания. В таких помещениях требуется предоставление безопасной рабочей зоны, а персонал должен быть огражден от напряженных частей.

Мероприятия, направленные на предупреждение электротравматизма, включают:

1. применение надежной изоляции электрических проводников и элементов оборудования, чтобы предотвратить случайное соприкосновение с токоведущими деталями;
2. обеспечение недоступности деталей и элементов схем, находящихся под высоким напряжением, путем использования защитных кожухов, ограждений и блокировок;
3. применение малых напряжений, когда это возможно, для уменьшения опасности поражения электрическим током;
4. использование блокировок и средств автоматического контроля и сигнализации для предотвращения нежелательной работы оборудования во время проведения ремонтных или обслуживающих работ;
5. устройство защитного заземления, зануления, отключения и электрического разделения, чтобы минимизировать возможность поражения электрическим током.

## 7.5 Пожарная безопасность

Предотвращение пожаров в вычислительных центрах является важной задачей для обеспечения пожарной безопасности. Для этого необходимо принимать меры по предупреждению пожаров и иметь подходящие средства пожаротушения.[4] Ниже приведены подробности мероприятий по предупреждению пожаров и выбору необходимых средств пожаротушения:

1. Анализ причин возможного возникновения пожара: Перед проведением работ в вычислительных центрах необходимо провести анализ причин возможного возникновения пожара, основываясь на специфике проводимых работ. Это позволяет определить потенциальные источники пожара и принять соответствующие меры по их предотвращению. Такой анализ может включать оценку электрической безопасности, проверку электропроводки, систем охлаждения, хранения легковоспламеняющихся веществ и других возможных источников пожара.
2. Выбор необходимых средств пожаротушения: В вычислительных центрах необходимо иметь подходящие средства пожаротушения для борьбы с возможными пожарами. Этот выбор должен основываться на характеристиках помещений и потенциальных источниках пожара. Обычно используются такие средства пожаротушения, как огнетушители, системы автоматического пожаротушения, противопожарные системы дымоудаления и пожарные системы оповещения. Выбор средств пожаротушения должен быть согласован с требованиями пожарной безопасности и нормативными актами, учитывая характеристики вычислительного центра и его особенности.
3. Системы оповещения о возникновении пожара и средства связи: Важным аспектом пожарной безопасности является наличие систем оповещения о возникновении пожара и средств связи. Это включает установку пожарной сигнализации, которая предупреждает о возникновении пожара и активирует процедуры эвакуации. Кроме того, должны быть установлены средства связи, такие как телефоны, рации или другие средства передачи информации, чтобы обеспечить оперативную связь между сотрудниками и службами пожарной безопасности в случае возникновения пожара.

Мероприятия по предупреждению пожаров и выбору необходимых средств пожаротушения играют важную роль в обеспечении пожарной безопасности в вычислительных центрах. Они помогают предотвратить возникновение и распространение пожаров, а также обеспечивают эффективные средства борьбы с пожарами, оповещение персонала и своевременного реагирования на пожароопасные ситуации.

При обеспечении пожарной безопасности одной из ключевых составляющих является наличие эффективных средств оповещения о возникновении пожара и средств связи. Это позволяет оперативно обнаруживать и реагировать на пожарные ситуации, обеспечивая безопасную эвакуацию сотрудников и вызов профессиональных пожарных служб. Далее представлены подробности о средствах оповещения о возникновении пожара и средствах связи:

1. Системы оповещения о возникновении пожара: В вычислительных центрах необходимо установить надежные и эффективные системы оповещения о возникновении пожара. Они включают в себя датчики возгорания, которые обнаруживают признаки пожара, такие как дым, повышение температуры или пламя. Когда датчики срабатывают, система оповещения активируется, предупреждая всех находящихся в помещении о возможном пожаре. Это может быть осуществлено с помощью звуковых сигналов, световых индикаторов или голосовых сообщений, которые ясно и наглядно информируют о пожарной угрозе.
2. Средства связи: Важной составляющей пожарной безопасности является наличие надежных средств связи. Это позволяет сотрудникам быстро сообщать о возникновении пожара и вызывать профессиональные пожарные службы. Возможными средствами связи могут быть телефоны, рации, пейджеры или другие системы передачи информации. Они должны быть легко доступными и функциональными, обеспечивая своевременное и эффективное информирование и координацию действий в случае пожара. Также следует обеспечить резервные источники питания для средств связи, чтобы они оставались работоспособными даже при отключении основного электропитания.

Правильное функционирование средств оповещения о возникновении пожара и средств связи является критически важным для обеспечения пожарной безопасности. Они обеспечивают быстрое обнаружение пожара и своевременное информирование персонала, что позволяет принять необходимые меры для эвакуации и борьбы с пожаром.

Руководители играют важную роль в обеспечении пожарной безопасности. Они должны быть готовы к возможности пожара и знать свои обязанности и ответственности. Правильное поведение руководителей при возникновении пожара помогает минимизировать риски для персонала и своевременно реагировать на пожарные ситуации.

Ниже приведены более подробные рекомендации для руководителей в случае пожара:

1. Быстрое начало эвакуации: Руководители должны быть ознакомлены с планами эвакуации и знать, как начать эвакуацию в случае пожара. Они должны быть в состоянии быстро оповестить персонал о возникшей пожароопасной ситуации и организовать быструю и безопасную эвакуацию. Это может включать использование сигналов оповещения, громкоговорителей или других средств связи.
2. Уведомление служб пожарной безопасности: Руководители должны немедленно уведомить службы пожарной безопасности о пожаре и предоставить им необходимую информацию о местоположении пожара, его характеристиках и возможных угрозах. Кроме того, руководители должны оказать помощь службам пожарной безопасности, предоставив доступ к необходимым системам и помогая в ограничении распространения пожара.
3. Соблюдение строгих правил безопасности: Руководители обязаны строго придерживаться норм безопасности и действовать в соответствии с ними. Это включает соблюдение запрета на самостоятельное тушение пожара без необходимого обучения и специального оборудования. Кроме того, руководители должны уделить особое внимание координации действий, эвакуации персонала и оказанию поддержки пожарным службам.
4. Пример выдержки и спокойствия: Руководители должны быть примером выдержки и спокойствия для остального персонала. Во время пожарной ситуации, они должны сохранять ясность мышления, принимать обоснованные решения и поддерживать спокойную атмосферу. Это помогает предотвратить панику среди персонала и способствует более эффективной и безопасной эвакуации.

Соблюдение данных рекомендаций позволяет руководителям эффективно реагировать на пожарные ситуации, минимизировать риски и обеспечивать безопасность персонала и инфраструктуры. Регулярное обучение и тренировки руководителей по пожарной безопасности являются важной частью подготовки к возможным чрезвычайным ситуациям.

## 7.6 Меры оказания первой помощи

Меры оказания первой помощи при поражении электрическим током и других травмах имеют важное значение для обеспечения безопасности и здоровья пользователей. [5]

Ниже приведены основные меры первой медицинской помощи при поражении электрическим током:

1. Безопасность окружающей обстановки: При обнаружении случая поражения электрическим током, необходимо сразу же обеспечить безопасность окружающей обстановки. Выключите источник электропитания или отключите устройство от источника электрического тока, используя безопасные методы и инструменты, чтобы предотвратить дальнейшие риски.
2. Прекращение контакта с источником травмы: Если пострадавший все еще находится в контакте с источником травмы, например, с электрическим проводом, необходимо обеспечить его безопасное освобождение. Используйте изолирующие материалы или инструменты, чтобы избежать дополнительного поражения током при подходе к пострадавшему.
3. Оценка состояния пострадавшего: Следует немедленно оценить состояние пострадавшего и вызвать медицинскую помощь. Проверьте находится ли он в сознании, а также наличие дыхания и пульса. Если пострадавший не дышит или сердцебиение отсутствует, немедленно начните реанимационные мероприятия.
4. Контроль дыхания и кровообращения: При необходимости проведите искусственное дыхание и сердечно-легочную реанимацию (СЛР) до прибытия медицинской бригады. Следуйте рекомендациям и нормам по проведению этих процедур, чтобы обеспечить оптимальную помощь пострадавшему.

Помимо поражения электрическим током, возможны и другие травмы, связанные с работой на ПЭВМ, например, мышечные напряжения, растяжения и другие повреждения. В таких случаях применяются общепринятые меры первой помощи, такие как остановка кровотечения, наложение холодных компрессов, фиксация поврежденной области и т. д.

Важно помнить, что оказание первой помощи требует соответствующих знаний и навыков.

## 7.7 Информационная безопасность

Информационная безопасность представляет собой комплекс мер и политик, направленных на защиту информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Она имеет важное значение в современном информационном обществе, где данные и информация становятся ценными активами организаций и частных лиц.

Для обеспечения информационной безопасности применяются следующие меры:

1. Аутентификация и авторизация: Эти меры позволяют проверить легитимность пользователей и предоставить им доступ только к необходимой информации и ресурсам. Это включает использование паролей, идентификаторов, биометрических данных и других методов идентификации.
2. Шифрование: Шифрование используется для защиты конфиденциальности данных путем их преобразования в зашифрованный формат, который может быть прочитан только с помощью ключа расшифровки. Это предотвращает несанкционированный доступ к информации даже в случае ее перехвата.
3. Защита от вредоносного программного обеспечения: Для предотвращения атак со стороны вредоносного программного обеспечения, такого как вирусы, трояны и шпионское ПО, применяются антивирусные программы, брандмауэры и другие средства защиты.
4. Физическая безопасность: Важным аспектом информационной безопасности является защита физического доступа к компьютерам, серверам и другим устройствам, содержащим информацию. Это включает использование замков, систем контроля доступа и видеонаблюдения.
5. Обучение и осведомленность пользователей: Регулярное обучение и повышение осведомленности пользователей относительно информационной безопасности являются важными мерами. Это позволяет им распознавать потенциальные угрозы, следовать политикам безопасности и принимать меры предосторожности при работе с информацией.
6. Регулярное обновление программного обеспечения: Обновление операционных систем, приложений и другого программного обеспечения помогает закрывать уязвимости и исправлять ошибки, что уменьшает вероятность успешных атак на информационные системы.
7. Резервное копирование данных: Регулярное создание резервных копий информации помогает предотвратить ее потерю в результате сбоев систем или кибератак.

Все эти меры способствуют созданию безопасной информационной среды, защищают ценные данные и информацию, и минимизируют риски для организаций и частных лиц. Они должны быть применены в соответствии с установленными политиками и стандартами информационной безопасности.

## 7.8 Список использованных источников

1. Опасные и вредные производственные факторы [Электронный ресурс] URL: <https://www.protrud.com/опасные-и-вредные-производственные-факторы/> (Дата обращения: 10.05.2023)

2. Требования к помещениям для работы с ПЭВМ [Электронный ресурс] URL: <https://studfile.net/preview/6696516/page:22/> (Дата обращения: 11.05.2023)

3. Электробезопасность: мероприятия, нормы, правила, требования [Электронный ресурс] URL: <https://www.elektro-expo.ru/ru/articles/2016/elektrobezopasnost/> (Дата обращения 11.05.2023)

4. Пожарная безопасность [Электронный ресурс] URL: <https://www.fire-service.ru/informaciya/pozharnayabezopasnost> (Дата обращения 12.05.2023)

5. Меры оказания первой помощи при поражении электрическим током [Электронный ресурс] URL: <https://89.mchs.gov.ru/deyatelnost/press-centr/novosti/3922423> (Дата обращения 14.05.2023)