ОУД.09 Информатика

Преподаватели Уханова Е.А., Касимова М.В.

Выполненные задания присылать на почту до 19.04.2020:

uhelena@mail.ru**;**

Задание на дистанционное обучение.

ПНК-163

«Защита информации, антивирусная защита» (2 часа)

Тема: Средства информационных и коммуникационных технологий.

Цельработы: выработать практические навыки работы с антивирусными программами, навыки правильной работы с компьютером.

Оснащение рабочего места: ПК,ОСWindows,рабочая тетрадь.

Техника безопасности: Правила ТБ при работе в компьютерном классе.

Методические рекомендации:

Теоритические сведения – законспектировать в тетрадь.

Информационная безопасность

Информационная безопасность государства –состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.

Информационная безопасность -это процесс обеспечения конфиденциальности, целостности и доступности информации.

- Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.
- Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.
- Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) – состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Вирусы. Антивирусное программное обеспечение

Компьютерный вирус -программа способная самопроизвольно внедряться ивнедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере.

Признаки заражения:

- прекращение работы или неправильная работа ранее функционировавших программ
- медленная работа компьютера
- невозможность загрузки ОС
- исчезновение файлов и каталогов или искажение их содержимого
- изменение размеров файлов и их времени модификации
- уменьшение размера оперативной памяти
- непредусмотренные сообщения, изображения и звуковые сигналы
- частые сбои и зависания компьютера и др.

Классификация компьютерных вирусов

По среде обитания:

- *Сетевые* –распространяются по различным компьютерным сетям
- *Файловые* –внедряются в исполняемые модули(COM, EXE)
- *Загрузочные* –внедряются в загрузочные сектора диска или сектора,содержащие программу загрузки диска
- *Файлово-загрузочные* –внедряются и в загрузочные сектора и в исполняемыемодули

По способу заражения:

- *Резидентные* –при заражении оставляет в оперативной памяти компьютерасвою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения

- *Нерезидентные* –не заражают оперативную память и активны ограниченное время

По воздействию:

- *Неопасные* –не мешают работе компьютера,но уменьшают объем свободнойоперативной памяти и памяти на дисках
- Опасные – приводят к различным нарушениям в работе компьютера

- Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

- *Паразиты* –изменяют содержимое файлов и секторов,легкообнаруживаются
- *Черви* –вычисляют адреса сетевых компьютеров и отправляют по ним своикопии
- *Стелсы* –перехватывают обращение ОС к пораженным файлам и секторам иподставляют вместо них чистые области
- *Мутанты* –содержат алгоритм шифровки-дешифровки,ни одна из копий непохожа на другую
- *Трояны* –не способны к самораспространению,но маскируясь под полезную,разрушают загрузочный сектор и файловую систему

Основные меры по защите от вирусов

- оснастите свой компьютер одной из современных антивирусных программ: Doctor Web, Norton Antivirus, AVP

- постоянно обновляйте антивирусные базы
- делайте архивные копии ценной для Вас информации (гибкие диски, CD)

Классификация антивирусного программного обеспечения

- Сканеры (детекторы). Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.
- Мониторы. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии.
- Ревизоры. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.

Задание 1. Тест (30 баллов). Решить тест,ответы отправить на электронную почту.

Тест по теме «Защита информации, антивирусная защита»

1. Информационная безопасность – это …

1) отсутствие зараженных файлов на компьютере
2) процесс работы антивирусных программ
3) процесс обеспечения конфиденциальности, целостности и доступности информации
4) состояние защищённости информации, при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

2. Основные угрозы доступности информации:

1) непреднамеренные ошибки пользователей
2) злонамеренное изменение данных
3) перехват данных
4) хакерская атака.

3. Один из методов защиты информации на компьютере

1) тключение жесткого диска
2) защита паролем
3) копирование информации.

4. К биометрической системе защиты относятся:

1) антивирусная защита
2) защита паролем
3) идентификация по отпечаткам пальцев
4) физическая защита данных

5. Брандмауэр (firewall) – это программа, …

1) которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил
2) которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности
3) на основе которой строится система кэширования загружаемых веб-страниц
4) реализующая простейший антивирус для скриптов и прочих использующихся в Интернет активных элементов.

6. Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности

1) уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer
2) уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer
3) возможность установить отличную от www.msn.com стартовую страницу возможность одновременно работать в нескольких окнах.

7. Что такое "компьютерный вирус"?

1) самостоятельная компьютерная программа или компонент программного комплекса, предназначенная для создания и изменения текстовых файлов.
2) это совокупность программ, находящиеся на устройствах долговременной памяти;
3) это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы;
4) это сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состояни

8. **Назовите основные типы компьютерных вирусов:**
   1) почтовые, файловые, программные
   2) аппаратные, программные, загрузочные
   3) программные, макровирусы, загрузочные.
9. **Свойство вируса, позволяющее называться ему загрузочным – способность …**
   1) заражать загрузочные сектора жестких дисков
   2) заражать загрузочные дискеты и компакт-диски
   3) вызывать перезагрузку компьютера-жертвы
   4) подсвечивать кнопку Пуск на системном блоке.
10. **Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию это:**
    1) Макровирус
    2) Сетевой червь
    3) Троян
    4) Загрузочный вирус
11. **Заражение компьютерными вирусами может произойти в процессе ...**
    1) работы с файлами
    2) форматирования дискеты
    3) выключения компьютера
    4) печати на принтере
12. **Какие файлы заражают макро-вирусы?**
    1) исполнительные;
    2) файлы документов Word и элект. таблиц Excel;
    3) графические и звуковые;
    4) html документы.
13. **К каким вирусам относится "троянский конь"?**
    1) макро-вирусы
    2) скрипт-вирусы
    3) интернет-черви
    4) загрузочные вирусы.
14. **Неопасные компьютерные вирусы могут привести**
    1) к сбоям и зависаниям при работе компьютера;
    2) к потере программ и данных;
    3) к форматированию винчестера;
    4) к уменьшению свободной памяти компьютера.
15. **Опасные компьютерные вирусы могут привести…**
    1) к сбоям и зависаниям при работе компьютера;
    2) к потере программ и данных;
    3) к форматированию винчестера;
    4) к уменьшению свободной памяти компьютера.
16. **Какой вид компьютерных вирусов внедряются и поражают исполнительный файлы с расширением *.exe, *.com и активируются при их запуске?**
    1) файловые вирусы;
    2) загрузочные вирусы;
    3) макро-вирусы;
    4) сетевые вирусы
17. **Какой вид компьютерных вирусов внедряются и поражают файлы с расширением *.txt, *.doc?**
    1) файловые вирусы;

2) загрузочные вирусы;
3) макро-вирусы;
4) сетевые вирусы.

18. Как происходит заражение почтовыми вирусами?

1) При подключении к web-серверу, зараженному "почтовым" вирусом
2) При открытии зараженного файла, присланного с письмом по e-mail
3) При подключении к почтовому серверу
4) При получении с письма, присланном по e-mail, зараженного файла.

19. Сетевые черви это:

1) Вирусы, которые внедряются в документ под видом макросов
2) Вирусы, которые проникну на компьютер, блокируют работу сети
3) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей
4) Вредоносные программы, устанавливающие скрытно от пользователя другие программы.

20. Руткит – это:

1) Программа для скрытого взятия под контроль взломанной системы
2) Вредоносная программа, маскирующаяся под макрокоманду
3) Разновидность межсетевого экрана
4) Программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю.

21. Какие существуют вспомогательные средства защиты?

1) Аппаратные средства.
2) Программные средства.
3) Аппаратные средства и антивирусные программы.

22. Антивирусные программы - это программы для:

1) Обнаружения вирусов
2) Удаления вирусов
3) Размножения вирусов

23. На чем основано действие антивирусной программы?

1) На ожидании начала вирусной атаки.
2) На сравнении программных кодов с известными вирусами.
3) На удалении зараженных файлов.

24. Какие программы относятся к антивирусным?

1) AVP, MS-DOS, MS Word
2) AVG, DrWeb, Norton AntiVirus
3) Norton Commander, MS Word, MS Excel.

25. Какие программы не относятся к антивирусным?

1) программы-фаги
2) программы сканирования
3) программы-ревизоры
4) программы-детекторы

26. Можно ли обновить антивирусные базы на компьютере, не подключенном к Интернет?

1) да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором
2) да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы
3) нет.

27. Основные меры по защите информации от повреждения вирусами:

1) проверка дисков на вирус
2) создавать архивные копии ценной информации
3) не пользоваться "пиратскими" сборниками программного обеспечения
4) передавать файлы только по сети.

28. Наиболее эффективное средство для защиты от сетевых атак

1) использование антивирусных программ
2) использование сетевых экранов или «firewall»
3) посещение только «надёжных» Интернет-узлов
4) использование только сертифицированных программ-браузеров при доступе к сети Интернет.

29. Основная функция межсетевого экрана

1) управление удаленным пользователем
2) фильтрация входящего и исходящего трафика
3) проверка дисков на вирусы
4) программа для просмотра файлов.

30. Создание компьютерных вирусов является

1) последствием сбоев операционной системы
2) необходимым компонентом подготовки программистов
3) побочным эффектом при разработке программного обеспечения
преступлением

Практическая работа № 19-20 (2часа)

«Эксплуатационные требования к компьютерному рабочему месту»

Тема: Эксплуатационные требования к компьютерному рабочему месту. Профилактические мероприятия для компьютерного рабочего места в соответствии с его комплектацией для профессиональной деятельности.

1. **Цель занятия:** выработать практические навыки правильной работы с компьютером.

2. Краткие теоретические сведения – законспектировать в тетрадь..

Профилактические мероприятия для компьютерного рабочего места

1. Требования к микроклимату, ионному составу и концентрации вредных химических веществ в воздухе помещений

На рабочих местах пользователей персональных компьютеров должны обеспечиваться оптимальные параметры микроклимата в соответствии с СанПин 2.2.4.548-96. Согласно этому документу для категории тяжести работ 1а температура воздуха должна быть в холодный период года не более 22-24оС, в теплый период года 20-25оС. Относительная влажность должна составлять 40-60%, скорость движения воздуха - 0,1 м/с. Для поддержания оптимальных значений микроклимата используется система отопления и кондиционирования воздуха. Для повышения влажности воздуха в помещении следует применять увлажнители воздуха или емкости с питьевой водой.

2. Требования к освещению помещений и рабочих мест

В компьютерных залах должно быть естественное и искусственное освещение. Световой поток из оконного проема должен падать на рабочее место оператора с левой стороны.

Искусственное освещение в помещениях эксплуатации компьютеров должно осуществляться системой общего равномерного освещения.

Допускается установка светильников местного освещения для подсветки документов. Местное освещение не должно создавать бликов на поверхности экрана.

Отраженная блескость на рабочих поверхностях ограничивается за счет правильного выбора светильника и расположения рабочих мест по отношению к естественному источнику света.

Для искусственного освещения помещений с персональными компьютерами следует применять светильники типа ЛПО36 с зеркализованными решетками, укомплектованные высокочастотными пускорегулирующими аппаратами. Допускается применять светильники прямого света, преимущественно отраженного света типа ЛПО13, ЛПО5, ЛСО4, ЛПО34, ЛПО31 с люминесцентными лампами типа ЛБ. Допускается применение светильников местного освещения с лампами накаливания. Светильники должны располагаться в виде сплошных или прерывистых линий сбоку от рабочих мест параллельно линии зрения пользователя при разном расположении компьютеров.

Для обеспечения нормативных значений освещенности в помещениях следует проводить чистку стекол оконных проемов и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

3. Требования к шуму и вибрации в помещениях

Уровни шума на рабочих местах пользователей персональных компьютеров не должны превышать значений, установленных СанПиН 2.2.4/2.1.8.562-96 и составляют не более 50 дБА.

Снизить уровень шума в помещениях можно использованием звукопоглощающих материалов с максимальными коэффициентами звукопоглощения в области частот 63-8000 Гц для отделки стен и потолка помещений. Дополнительный звукопоглощающий эффект создают однотонные занавески из плотной ткани, повешенные в складку на расстоянии 15-20 см от ограждения. Ширина занавески должна быть в 2 раза больше ширины окна.

4. Требования к организации и оборудованию рабочих мест

Рабочие места с персональными компьютерами по отношению к световым проемам должны располагаться так, чтобы естественный свет падал сбоку, желательно слева.

Схемы размещения рабочих мест с персональными компьютерами должны учитывать расстояния между рабочими столами с мониторами: расстояние между боковыми поверхностями мониторов не менее 1,2 м, а расстояние между экраном монитора и тыльной частью другого монитора не менее 2,0 м.

Рабочий стол может быть любой конструкции, отвечающей современным требованиям эргономики и позволяющей удобно разместить на рабочей поверхности оборудование с

учетом его количества, размеров и характера выполняемой работы. Целесообразно применение столов, имеющих отдельную от основной столешницы специальную рабочую поверхность для размещения клавиатуры. Используются рабочие столы с регулируемой и нерегулируемой высотой рабочей поверхности. При отсутствии регулировки высота стола должна быть в пределах от 680 до 800 мм.

Глубина рабочей поверхности стола должна составлять 800 мм (допускаемая не менее 600 мм), ширина - соответственно 1 600 мм и 1 200 мм. Рабочая поверхность стола не должна иметь острых углов и краев, иметь матовую или полуматовую фактору.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног - не менее 650 мм.

Быстрое и точное считывание информации обеспечивается при расположении плоскости экрана ниже уровня глаз пользователя, предпочтительно перпендикулярно к нормальной линии взгляда (нормальная линия взгляда 15 градусов вниз от горизонтали).

Клавиатура должна располагаться на поверхности стола на расстоянии 100-300 мм от края, обращенного к пользователю.

Для удобства считывания информации с документов применяются подвижные подставки (пюпитры), размеры которых по длине и ширине соответствуют размерам устанавливаемых на них документов. Пюпитр размещается в одной плоскости и на одной высоте с экраном.

Для обеспечения физиологически рациональной рабочей позы, создания условий для ее изменения в течение рабочего дня применяются подъемно-поворотные рабочие стулья с сиденьем и спинкой, регулируемыми по высоте и углам наклона, а также расстоянию спинки от переднего края сидения.

Конструкция стула должна обеспечивать:

ширину и глубину поверхности сиденья не менее 400 мм;

- поверхность сиденья с закругленным передним краем;
- регулировку высоты поверхности сиденья в пределах 400-550 мм и углом наклона вперед до 15 градусов и назад до 5 градусов;
- высоту опорной поверхности спинки 300±20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости 400 мм;
- угол наклона спинки в вертикальной плоскости в пределах 0±30 градусов;
- регулировку расстояния спинки от переднего края сидения в пределах 260-400 мм;
- стационарные или съемные подлокотники длиной не менее 250 мм и шириной 50-70 мм;
- регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350-500 мм;
- поверхность сиденья, спинки и подлокотников должна быть полумягкой, с нескользящим не электризующимся, воздухонепроницаемым покрытием, легко очищаемым от загрязнения.

Рабочее место должно быть оборудовано подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона

опорной поверхности подставки до 20 град. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

5. Режим труда и отдыха при работе с компьютером

Режим труда и отдыха предусматривает соблюдение определенной длительности непрерывной работы на ПК и перерывов, регламентированных с учетом продолжительности рабочей смены, видов и категории трудовой деятельности.

Виды трудовой деятельности на ПК разделяются на 3 группы: группа А - работа по считыванию информации с экрана с предварительным запросом; группа Б - работа по вводу информации; группа В - творческая работа в режиме диалога с ПК.

Если в течение рабочей смены пользователь выполняет разные виды работ, то его деятельность относят к той группе работ, на выполнение которой тратится не менее 50% времени рабочей смены.

Категории тяжести и напряженности работы на ПК определяются уровнем нагрузки за рабочую смену: для группы А - по суммарному числу считываемых знаков; для группы Б - по суммарному числу считываемых или вводимых знаков; для группы В - по суммарному времени непосредственной работы на ПК. В таблице приведены категории тяжести и напряженности работ в зависимости от уровня нагрузки за рабочую смену.

Виды категорий трудовой деятельности с ПК

Категория работы по тяжести и напряженности	Уровень нагрузки за рабочую смену при видах работы на ПК		
	Группа А Количество знаков	Группа Б Количество знаков	Группа В Время работы, ч
I	До 20000	До 15000	До 2,0
II	До 40000	До 30000	До 4,0
III	До 60000	До 40000	До 6,0

Количество и длительность регламентированных перерывов, их распределение в течение рабочей смены устанавливается в зависимости от категории работ на ПК и продолжительности рабочей смены.

При 8-часовой рабочей смене и работе на ПК регламентированные перерывы следует устанавливать:

для первой категории работ через 2 часа от начала смены и через 2 часа после обеденного перерыва продолжительностью 15 минут каждый;

- для второй категории работ - через 2 часа от начала рабочей смены и через 1,5-2,0 часа после обеденного перерыва продолжительностью 15 минут каждый или продолжительностью 10 минут через каждый час работы;

- для третьей категории работ - через 1,5- 2,0 часа от начала рабочей смены и через 1,5-2,0 часа после обеденного перерыва продолжительностью 20 минут каждый или продолжительностью 15 минут через каждый час работы.

При 12-часовой рабочей смене регламентированные перерывы должны устанавливаться в первые 8 часов работы аналогично перерывам при 8-часовой рабочей смене, а в течение последних 4 часов работы, независимо от категории и вида работ, каждый час продолжительностью 15 минут.

Продолжительность непрерывной работы на ПК без регламентированного перерыва не должна превышать 2 часа.

При работе на ПК в ночную смену продолжительность регламентированных перерывов увеличивается на 60 минут независимо от категории и вида трудовой деятельности.

Эффективными являются нерегламентированные перерывы (микропаузы) длительностью 1-3 минуты.

Регламентированные перерывы и микропаузы целесообразно использовать для выполнения комплекса упражнений и гимнастики для глаз, пальцев рук, а также массажа. Комплексы упражнений целесообразно менять через 2-3 недели.

Пользователям ПК, выполняющим работу с высоким уровнем напряженности, показана психологическая разгрузка во время регламентированных перерывов и в конце рабочего дня в специально оборудованных помещениях (комнатах психологической разгрузки).

6. Медико-профилактические и оздоровительные мероприятия.

Все профессиональные пользователи ПК должны проходить обязательные предварительные медицинские осмотры при поступлении на работу, периодические медицинские осмотры с обязательным участием терапевта, невропатолога и окулиста, а также проведением общего анализа крови и ЭКГ.

Не допускаются к работе на ПК женщины со времени установления беременности и в период кормления грудью.

Близорукость, дальнозоркость и другие нарушения рефракции должны быть полностью корригированы очками. Для работы должны использоваться очки, подобранные с учетом рабочего расстояния от глаз до экрана дисплея. При более серьезных нарушениях состояния зрения вопрос о возможности работы на ПК решается врачом-офтальмологом.

Для снятия усталости аккомодационных мышц и их тренировки используются компьютерные программы типа Relax.

Интенсивно работающим целесообразно использовать такие новейшие средства профилактики зрения, как очки ЛПО-тренер и офтальмологические тренажеры ДАК и «Снайпер-ультра».

Досуг рекомендуется использовать для пассивного и активного отдыха (занятия на тренажерах, плавание, езда на велосипеде, бег, игра в теннис, футбол, лыжи, аэробика,

прогулки по парку, лесу, экскурсии, прослушивание музыки и т.п.). Дважды в год (весной и поздней осенью) рекомендуется проводить курс витаминотерапии в течение месяца. Следует отказаться от курения. Категорически должно быть запрещено курение на рабочих местах и в помещениях с ПК.

7. Обеспечение электробезопасности и пожарной безопасности на рабочем месте

На рабочем месте пользователя размещены дисплей, клавиатура и системный блок. При включении дисплея на электронно-лучевой трубке создается высокое напряжение в несколько киловольт. Поэтому запрещается прикасаться к тыльной стороне дисплея, вытирать пыль с компьютера при его включенном состоянии, работать на компьютере во влажной одежде и влажными руками.

Перед началом работы следует убедиться в отсутствии свешивающихся со стола или висящих под столом проводов электропитания, в целостности вилки и провода электропитания, в отсутствии видимых повреждений аппаратуры и рабочей мебели.

Токи статического электричества, наведенные в процессе работы компьютера на корпусах монитора, системного блока и клавиатуры, могут приводить к разрядам при прикосновении к этим элементам. Такие разряды опасности для человека не представляют, но могут привести к выходу из строя компьютера. Для снижения величин токов статического электричества используются нейтрализаторы, местное и общее увлажнение воздуха, использование покрытия полов с антистатической пропиткой.

Пожарная безопасность - состояние объекта, при котором исключается возможность пожара, а в случае его возникновения предотвращается воздействие на людей опасных его факторов и обеспечивается защита материальных ценностей.

Противопожарная защита - это комплекс организационных и технических мероприятий, направленных на обеспечение безопасности людей, предотвращение пожара, ограничение его распространения, а также на создание условий для успешного тушения пожара.

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. Во всех служебных помещениях обязательно должен быть «План эвакуации людей при пожаре», регламентирующий действия персонала в случае возникновения очага возгорания и указывающий места расположения пожарной техники.

Пожары в вычислительных центрах (ВЦ) представляют особую опасность, так как сопряжены с большими материальнымипотерями. Характерная особенность

ВЦ - небольшие площади помещений. Как известно, пожар может возникнуть при взаимодействии горючих веществ, окислителя и источников зажигания. В помещениях ВЦ присутствуют все три основные фактора, необходимые для возникновения пожара.

Горючими компонентами на ВЦ являются: строительные материалы для акустической и эстетической отделки помещений, перегородки, двери, полы, изоляция кабелей и др.

Источниками зажигания в ВЦ могут быть электрические схемы от ЭВМ, приборы, применяемые для технического обслуживания, устройства электропитания,

кондиционирования воздуха, где в результате различных нарушений образуются перегретые элементы, электрические искры и дуги, способные вызвать загорания горючих материалов.

В современных ЭВМ очень высокая плотность размещения элементов электронных схем. В непосредственной близости друг от друга располагаются соединительные провода, кабели. При протекании по ним электрического тока выделяется значительное количество теплоты. При этом возможно оплавление изоляции. Для отвода избыточной теплоты от ЭВМ служат системы вентиляции и кондиционирования воздуха. При постоянном действии эти системы представляют собой дополнительную пожарную опасность.

Для большинства помещений ВЦ установлена категория пожарной опасности В.

Одна из наиболее важных задач пожарной защиты - защита строительных помещений от разрушений и обеспечение их достаточной прочности в условиях воздействия высоких температур при пожаре. Учитывая высокую стоимость электронного оборудования ВЦ, а также категорию его пожарной опасности, здания для ВЦ и части здания другого назначения, в которых предусмотрено размещение ЭВМ, должны быть первой и второй степени огнестойкости. Для изготовления строительных конструкций используются, как правило, кирпич, железобетон, стекло, металл и другие негорючие материалы. Применение дерева должно быть ограничено, а в случае использования необходимо пропитывать его огнезащитными составами.

3. Задание. Вы полнить задание письменно и отправить на электронную почту.

Задание 1. Укажите требования к помещениям кабинета информатики:

Задание 2. Укажите, какие действия запрещены в кабинете информатики.

Задание 3. Укажите комплекс упражнений для снятия усталости за компьютером.