ЗАЩИТА

ИНФОРМАЦИИ

Общие принципы обеспечения зашиты информации

1. Надо ли защищать данные на своем компьютере?
2. Информация – стратегический ресурс государства.
3. Целенаправленное воздействие на информационные ресурсы с целью:

- разрушения или искажения существующей информации;
- навязывания ложной информации;
- навязывания ложных решений.

Основные каналы утечки информации, составляющей коммерческую тайну:

- работа с документами при посторонних лицах;
- получение несанкционированных копий документов;
- утрата и хищение документов;
- попадание сведений, составляющих коммерческую тайну, в негрифованные документы;
- наличие излишней информации в документах.

Область обращения информации:

- люди;
- документы всех видов, включая машинные носители;
- материальные элементы (выпускаемые изделия, сырье, полуфабрикаты и т.п.);
- технические средства обработки и передачи информации;
- инфраструктура предприятия.

Канал утечки информации -

путь прохождения информации, составляющей коммерческую тайну, за пределы области ее обращения.

Комплексная система защиты информации –

совокупность законодательных, организационных, технических и других способов и средств, обеспечивающие защиту информации, составляющей коммерческую тайну предприятия, по всем выявленным возможным каналам утечки.

Требованиям к комплексной системе защиты информации:

1. Базироваться на лучших алгоритмах закрытия информации, гарантирующих надежную криптографическую защиту;
2. Использование идентификации пользователей и контроль подлинности передаваемой и хранимой информации;
3. Защита от несанкционированного доступа к информации в базах данных, файлах, на носителях информации, а также при передаче ее по линиям связи в локальных и глобальных сетях;
4. Использование различных уровней доступа пользователей к защищаемой информации.

Понятие информационной безопасности

Под *информационной безопасностью* понимается защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*

Классификация угроз безопасности

Все множество потенциальных угроз по природе их возникновения разделяется на два класса:

1. Естественные (объективные - физические процессы или стихийных природные явления, независящих от человека)
2. Искусственные (субъективные - ошибками в проектировании ИС, в программном обеспечении, в корыстных действиях персонала)

Методы обеспечения информационной безопасности Российской Федерации делятся на:

- правовые,
- организационно-технические,
- экономические.

К правовым методам относится:

- разработка нормативных правовых актов, регламентирующих отношения в информационной сфере,
- нормативных методических документов по вопросам обеспечения информационной безопасности.

Организационно-технические методы :

- создание систем предотвращения несанкционированного доступа
- выявление технических устройств и программ, представляющих опасность для нормального функционирования телекоммуникационных систем,
- предотвращение перехвата информации по техническим каналам,
- применение криптографических средств защиты информации,
- контроль за действиями персонала в защищенных информационных системах

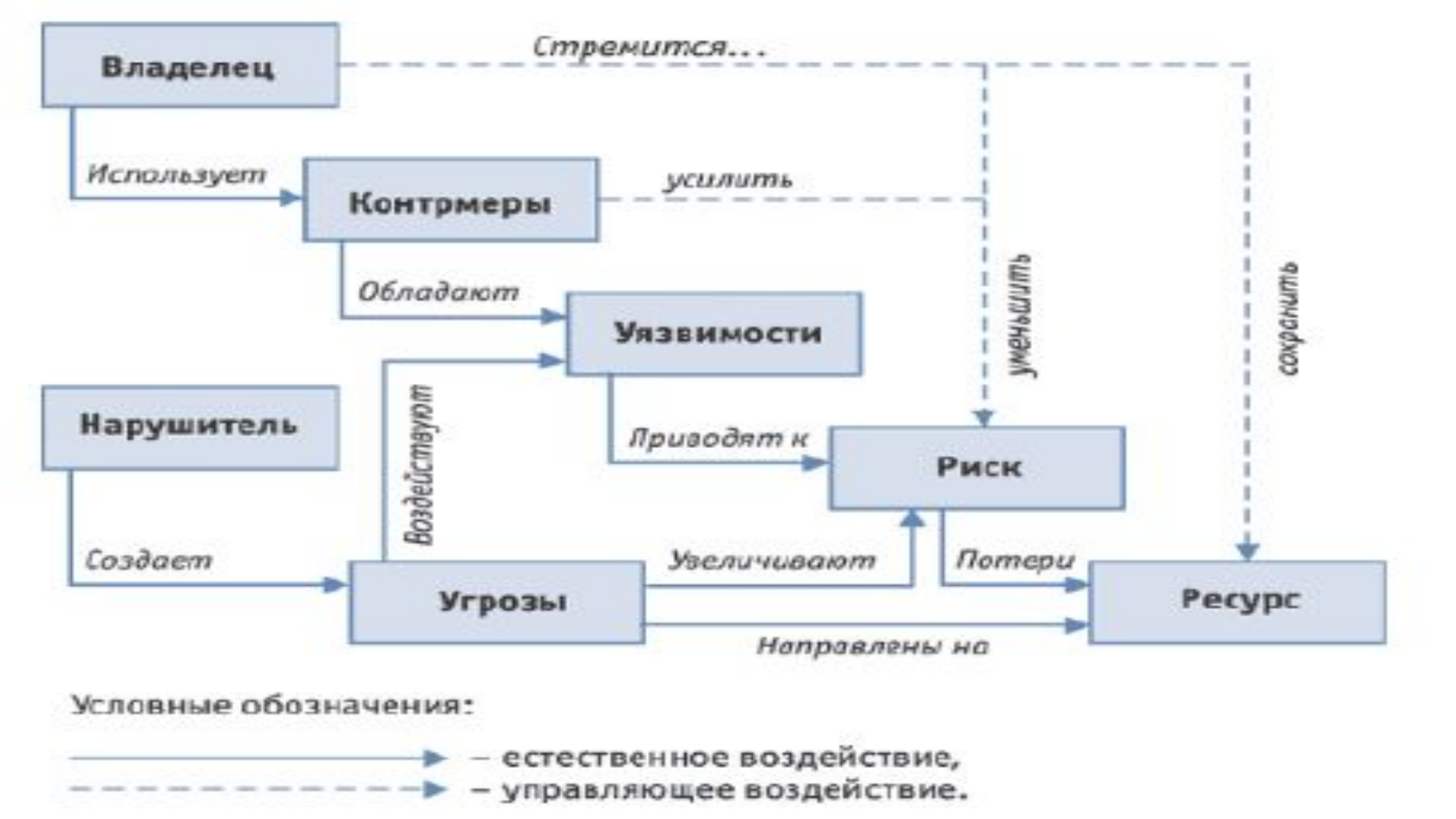
Экономические методы обеспечения информационной безопасности:

- разработка программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации,
- создание системы страхования информационных рисков физических и юридических лиц.

Аппаратные и программные средства информационной защиты

- Идентификация (опознавание);
- Аутентификация (подтверждение подлинности);
- Авторизация субъектов (присвоение полномочий);
- Контроль (разграничение) доступа к ресурсам системы;
- Регистрация и анализ событий, происходящих в системе;
- Контроль целостности ресурсов системы.

Модели безопасности информационных систем



Политика безопасности

“Политика безопасности" (security policy) – это стратегия организации в области информационной безопасности.

Стратегия определяется набором законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Пример:

Оранжевая книга (стандарт 1983 г.) Министерства обороны США "Критерии оценки *доверенных* компьютерных *систем*" определяет четыре *уровня безопасности* - D, C, B и A.

Уровень D предназначен для систем, признанных неудовлетворительными.

По мере перехода от уровня C к A к надежности систем предъявляются более жесткие требования.

Особенности применения криптографических методов

Проблемой защиты информации путем ее преобразования занимается *криптология*).

Криптология разделяется на два направления - *криптографию* и *криптоанализ*.

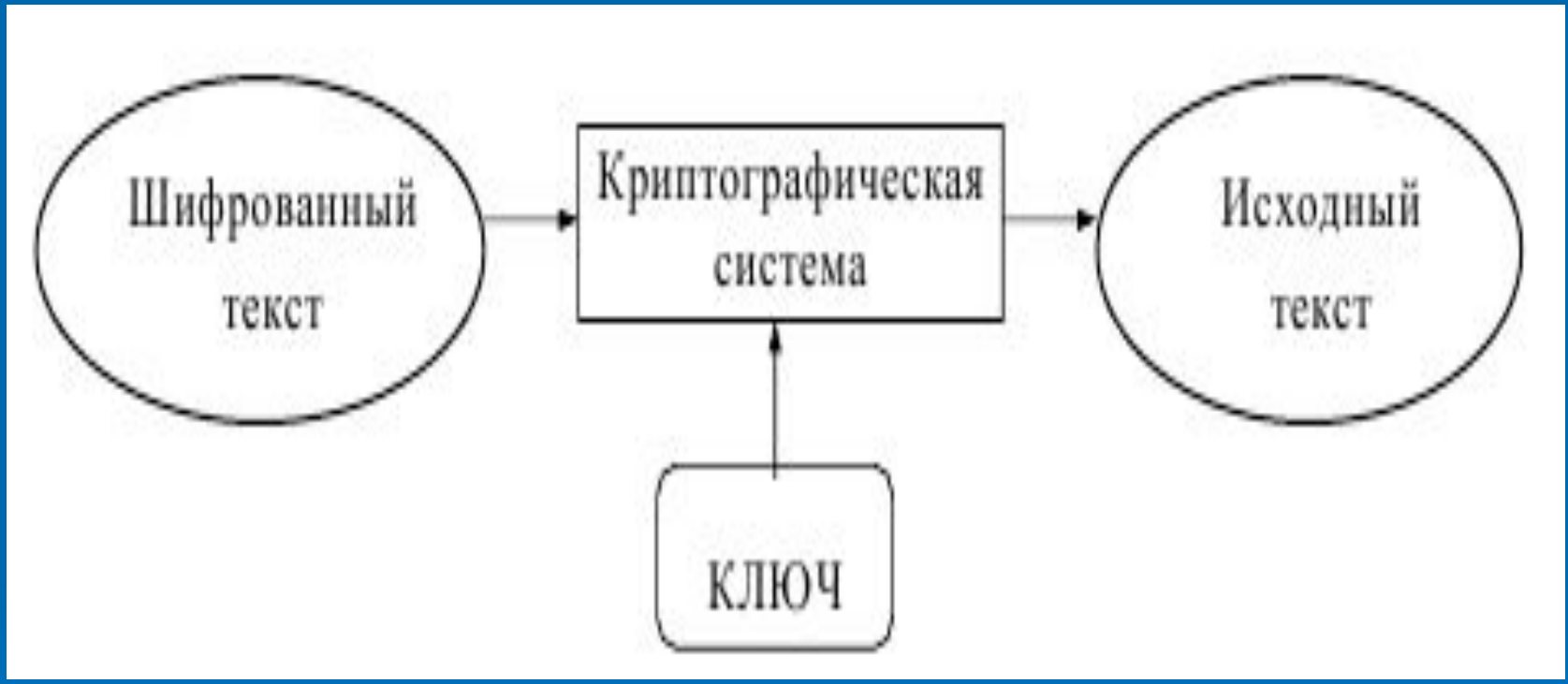
Цели этих направлений прямо противоположны.

- *Криптография* занимается поиском и исследованием математических методов преобразования информации.
- *Криптоанализ* - занимается исследованием возможности расшифровывания информации без знания ключей.

Шифрование - *исходный текст*, который носит название *открытого текста*, заменяется *шифрованным текстом*.

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.


Шифрованный текст
Криптографическая система
Исходный текст
КЛЮЧ

Мера защиты информации

На *процедурном уровне* можно выделить следующие классы мер:

- *управление персоналом;*
- *физическая защита;*
- *поддержание работоспособности;*
- *реагирование на нарушения режима безопасности;*
- *планирование восстановительных работ.*

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше - с составления *описания должности*.

Существует два общих принципа, которые следует иметь в виду:

- *разделение обязанностей;*
- *минимизация привилегий.*

Например, *н*адежнее поручить одному сотруднику оформление заявок на платежи, а другому - заверять эти заявки.

Пример процедурного ограничения действий супер пользователя - искусственно "расщепить" пароль супер пользователя, сообщив первую его часть одному сотруднику, а вторую - другому.

Принцип *минимизации привилегий* предписывает выделять пользователю только те права доступа, которые необходимы ему для выполнения служебных обязанностей.

С момента присвоения сотруднику учетной записи начинается его администрирование, а также протоколирование и анализ действий пользователя.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале - одновременно с извещением о наказании или увольнении).

Направления *физической защиты*:

- физическое управление доступом

ограничение входа и выхода сотрудников,

декомпозиция контролируемой территории;

необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников.

- противопожарные меры:

установка противопожарной сигнализации и автоматических средств пожаротушения

- защита поддерживающей инфраструктуры

системы электро- водо- и теплоснабжения, кондиционеры и средства коммуникаций;

- защита от перехвата данных -

  злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок .

- защита мобильных систем.

  исключение краж портативных компьютеров, шифрование данные на жестких дисках таких компьютеров.

Безопасность локальных компьютерных сетей

Необходимость защиты информации в сетях:

1. Большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц;
2. Значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть;
3. Недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предпродажном этапе, называемом бета-тестированием, а в процессе эксплуатации.

Места и каналы возможного несанкционированного доступа к информации в компьютерной сети

Сетевые атаки через Интернет могут быть классифицированы следующим образом:

- Sniffer – пакеты – прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous mode (не делающий различия). В этом ре жиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки.
- IP-spoof – обман, мистификация. Имеет место, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя.

- Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.
- Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.
- Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.

- Атаки на уровне приложений.
- Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений.
- Злоупотребление доверием внутри сети.

Программные средства индивидуальной защиты информации

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС.

Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации.

Наиболее часто используют :

- Firewalls – брандмауэры. Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них.

  Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода – это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

- Proxy-servers (proxy – доверенное лицо).

  Весь трафик между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники.

  Этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы, код Java и JavaScript).

Методы защиты компьютерной информации от вирусов

1949 г. – основатель теории компьютеров Джон фон Нейман опубликовал статью «Теория и организация сложных автоматов», в которой рассматривал возможность создания компьютерной программы, способной к саморепликации.

1983 г. - студент Калифорнийского университета Фред Коэн написал маленькую программу, способную к саморазмножению и распространению по сетям, и назвал ее «вирусом»

Виды вирусов. Методы распространения

Вирусы можно разделить на классы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

По среде обитания вирусы можно разделить на сетевые, файловые и загрузочные:

- *сетевые вирусы* распространяются по компьютерной сети,
- *файловые* внедряются в выполняемые файлы,
- *загрузочные* - в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record).

По способу заражения вирусы делятся на резидентные и нерезидентные:

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По деструктивным возможностям вирусы можно разделить на:

- безвредные, т.е. никак не влияющие на работу компьютера
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- опасные вирусы, которые могут привести к серьезным сбоям в работе ПК
- очень опасные, которые могут привести к потере программ, уничтожению данных пользователя и системной информации ПК.

По особенностям алгоритма можно выделить следующие группы вирусов:

- компаньон-вирусы - это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM. Например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл.

- вирусы-“черви” (worm) - вирусы, которые распространяются в компьютерной сети и, так же как и компаньон-вирусы, не изменяют файлы или сектора на дисках.

  Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.

  Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

- студенческие- крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок;
- стелс - вирусы (вирусы-невидимки, stealth), представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и “подставляют” вместо себя незараженные участки информации;
- вирусы-призраки - трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. Это достигается шифрованием тела вируса и модификацией программы - дешифратора

Backdoor - утилиты скрытого администрирования позволяют, обходя системы защиты, поставить компьютер пользователя под свой контроль.

Программа, которая работает в невидимом режиме, дает хакеру неограниченные права для управления системой.

С помощью таких backdoor-программ можно получить доступ к персональным и личным данным пользователя.

Нередко такие программы используются в целях заражения системы компьютерными вирусами и для скрытой установки вредоносных программ без ведома пользователя.

Bot-сеть это полноценная сеть в Интернет, которая подлежит администрированию злоумышленником и состоящая из многих инфицированных компьютеров, которые взаимодействуют между собой.

Контроль над такой сетью достигается с использованием вирусов или троянов, которые проникают в систему.

При работе ПК, вредоносные программы никак себя не проявляют, ожидая команды со стороны злоумышленника.

Подобные сети применяются для рассылки СПАМ сообщений или для организации DDoS (сокр. от англ. Distributed Denial of Service) атак на компьютерную систему с целью довести её до отказа

Пользователи зараженных компьютеров могут не догадываться о происходящем в сети.

Фарминг - это скрытая манипуляция host-файлом браузера для того, чтобы направить пользователя на фальшивый сайт.

Мошенники содержат у себя сервера больших объемов, на таких серверах хранятся большая база фальшивых интернет-страниц. При манипуляции host-файлом при помощи трояна или вируса вполне возможно манипулирование зараженной системой.

В результате этого зараженная система будет загружать только фальшивые сайты, даже в том случае, если Вы правильно введете адрес в строке браузера.

Phishing дословно переводится как "выуживание" личной информации пользователя при нахождении в сети Интернет.

Злоумышленник при своих действиях отправляет потенциальной жертве электронное письмо, где указано, что необходимо выслать личную информацию для подтверждения.

С использованием таких похищенных данных, хакер вполне может выдать себя за другое лицо и осуществить действия от его имени.

Защита экономической информации

Системы защиты информации представляют собой комплекс специальных мер законодательного и административного характера, организационных мероприятий, физических и технических средств обеспечения безопасности информации. Под безопасностью информации понимается состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

Безопасность информации - это состояние устойчивости информации к случайным или преднамеренным внешним воздействиям, исключающее недопустимый риск ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации.

Проблемы защиты информации и информационных систем определяется следующими факторами:

высокими темпами роста парка средств вычислительной техники и связи; вовлечением в процесс информационного взаимодействия большего числа людей и организаций;
повышением уровня доверия;
отношением к информации, как к товару с присущим ему стремлением к конкуренции и, как следствие промышленному шпионажу в области создания и сбыта информации услуг;
концентрацией больших объемов информации различного назначения и принадлежности в определенных местах и на электронных носителях;
наличием интенсивного обмена между участниками информационного процесса;
количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;

обострением противоречий между объективно существующими потребностями общества и расширением свободного обмена информацией и чрезмерными или недостаточными ограничениями на ее распространение и использование;
дифференциацией уровня потерь от уничтожения, фальсификации, разглашения или незаконного тиражирования информации;
многообразием видов угроз и возможных каналов несанкционированного доступа (НСД) к информации;
ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими программно-математических воздействий на систему;
развитием рыночных отношений в области разработки и обслуживания вычислительной техники и программных средств.

Компоненты системы защиты - область физической безопасности, к средствам которой можно отнести механические и электронные замки, охрану и охранную сигнализацию и т.п.;

безопасность персонала, где рассматривается защита сотрудников и защита от воздействия самих сотрудников. Это, в первую очередь, шпионаж, воздействие криминальных структур;

правовая безопасность, аккумулирующая все проблемы законодательного регулирования вопросов защиты информации и вычислительных систем;

безопасность оборудования, связанная с надежностью работы устройств, изучением возможностей несанкционированного перехвата информации и другими техническими аспектами;

безопасность программного обеспечения, исключающая воздействие различного рода программных вирусов или непредусмотренных действий разработчиков;

безопасность программного обеспечения, исключающая воздействие различного рода программных вирусов или непредусмотренных действий разработчиков;
безопасность телекоммуникационной среды, связанная с проблемами распределения вычислительных систем.
Это могут быть и физические повреждения каналов связи и просто утеря, подмена или неправомочная имитация законного пользователя.

Дестабилизирующие факторы

количественная недостаточность физическая нехватка одного или нескольких компонентов АИС для обеспечения требуемой защищенности информации по рассматриваемым показателям;
качественная недостаточность несовершенство конструкции или организации одного или нескольких компонентов АИС, в силу чего не обеспечивается требуемая защищенность информации; отказ нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им своих функций;
сбой временное нарушение работоспособности какого-либо элемента АИС, следствием чего может быть неправильное выполнение им в этот момент своих функций;

ошибка неправильное (одноразовое или систематическое) выполнение элементом системы одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния; стихийное бедствие спонтанно возникающее неконтролируемое явление, проявляющееся как разрушительная сила; злоумышленные действия действия людей, специально направленные на нарушение защищенности информации; побочное явление явление, сопутствующее выполнению элементом своих основных функций, следствием которого может быть нарушение защищенности информации.

Способы реализации угроз

Хищение носителей

Применение программных ловушек

Ошибки в программах обработки данных

Неисправность аппаратуры

Компьютерные вирусы

Электромагнитное излучение

Угрозы безопасности информации

По источнику появления

Внешние - возникают в результате деятельности недобросовестных конкурентов

Внутренние

По характеру целей

Преднамеренные, непреднамеренные

Уровни защиты информации

Аппаратно-программный
Процедурный
Административный
Законодательный

Основные законы

Закон “Об информации, информатизации и защите информации” (1995) Закон “О связи” (1995) Закон “О банках и банковской деятельности” Закон “О правовой охране программ для вычислительных машин и баз данных” Закон “Об авторском праве и смежных правах”

Формы защиты информации

Признание коммерческой тайной
Патентование
Применение норм обязательного права
К коммерческой тайне не могут быть отнесены
Учредительные документы
Документы, дающие право заниматься предпринимательской деятельностью Сведения по установленным формам отчетности о финансово – хозяйственной деятельности
Документы о платежеспособности
Сведения о численности и составе работающих, заработной плате, условиях труда
Документы об уплате налогов и других обязательных платежах

Сведения о численности и составе работающих, заработной плате, условиях труда

Документы об уплате налогов и других обязательных платежах

Сведения о загрязнении окружающей среды, нарушениях антимонопольного законодательства

Сведения об участии должностных лиц в кооперативах, малых предприятиях, товариществах, акционерных обществах и т.п.

Методы защиты

Управление доступом - метод защиты информации регулированием использования всех ресурсов системы, включающий следующие функции: идентификация ресурсов системы; установление подлинности (аутентификация) объектов или субъектов системы по идентификатору; проверка полномочий в соответствии с установленным регламентом; разрешение и создание условий работы в соответствии с регламентом; регистрация обращений к защищаемым ресурсам; реагирование при попытках несанкционированных действий.

Препятствие - метод физического преграждения пути нарушителю к защищаемым ресурсам системы.
Маскировка - метод защиты информации путем ее криптографического закрытия.
Регламентация - метод защиты информации, создающей такие условия автоматизированной обработки, хранения и передачи информации, при которых возможности несанкционированного доступа к ней минимизируются.
Принуждение - метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать регламент под угрозой ответственности.
Побуждение - метод защиты информации, который мотивирует пользователей и персонал системы соблюдать сложившиеся морально-этические нормы.

Организационные средства защиты

Организационные меры защиты определяют порядок:

ведения системы защиты от несанкционированного доступа;
ограничения доступа в помещения;
назначения полномочий по доступу;
контроля и учета событий;
сопровождения ПО;
контроля за системой защиты.

Программные средства защиты

Программные средства защиты (ПСЗ) включают в себя:

систему разграничения доступа к вычислительным и информационным ресурсам системы;

средства криптографической защиты информации, хранящейся на магнитных носителях АРМ и файл-сервера системы; с

редства регистрации и учета попыток НСД, событий в системе, документов, выводимых на печать и т. д.;

средства обеспечения и контроля целостности программных файлов, в том числе средства борьбы с программами-вирусами;

средства контроля паузы неактивности пользователя системы.

Аппаратные и криптографические средства защиты

Аппаратные средства защиты, выбор которых определяется такими техническими характеристиками как: высокая надежность - с целью исключения искажения экономической информации и преодоления рубежей защиты нарушителем;

высокая производительность шифрования информации, которая должна обеспечить время реакции системы на запрос пользователя не более 3 сек. Криптографические средства защиты информации автоматизированной системы, среди которых самым примитивным методом можно назвать обмен паролями со всеми присущими ему недостатками.

Одно из последних достижений в области криптографии - цифровая сигнатура.
Это способ обеспечения целостности с помощью дополнения сообщения специальным свойством, которое может быть проверено только тогда, когда известен открытый ключ, присвоенный автору сообщения.
Криптографические средства предназначены для эффективной защиты информации: в случае кражи, утери компьютера или магнитного носителя; при выполнении ремонтных или сервисных работ посторонними лицами или обслуживающим персоналом, не допущенным к работе с конфиденциальной информацией; при передаче информации в виде зашифрованных файлов по незащищенным каналам связи; при использовании компьютера несколькими пользователями.

Этапы создания систем защиты

инженерно-техническое обследование и описание информационных ресурсов системы;
определение наиболее критичных, уязвимых мест системы; вероятностная оценка угроз безопасности информационным ресурсам;
экономическая оценка возможного ущерба;
стоимостной анализ возможных методов и средств защиты информации;
определение рентабельности применения системы защиты информации.

Методы защиты информации

Ограничение доступа
Разграничение доступа
Разделение привилегий
Криптографическое преобразование
Контроль и учет доступа

Характеристика электробезопасности

При эксплуатации ЭВМ возникает следующий опасный фактор: опасный уровень напряжения в электрической цепи, замыкание которой может произойти через человека. Поражение электрическим током может возникнуть в результате прикосновения к оголенным проводам, находящимся под напряжением или к корпусам приборов, на которых вследствие пробоя возникло напряжение.

Электропитание ЭВМ осуществляется от сети переменного тока напряжением 220 В и частотой 50 Гц.

Перед подключением ЭВМ к сети обеспечивается либо наличие провода защитного заземления в розетке подключения ЭВМ, либо наличие заземляющего контура для внешнего заземления ЭВМ через заземляющий болт на задней крышке кожуха. Максимальное сопротивление цепи заземления 4 Ом.

Кроме того, токопроводящие части (провода, кабели) изолируются, приборы заземляются.

Обслуживающий персонал должен быть технически грамотен, а правила техники безопасности эксплуатации электроустановок должны соблюдаться неукоснительно.

При работе аппаратуры запрещается:

проверять на ощупь наличие напряжения токоведущих частей аппаратуры;
применять для соединения блоков и приборов провода с поврежденной изоляцией;
производить работу и монтаж в аппаратуре, находящейся под напряжением;
подключать блоки и приборы к работающей аппаратуре.
Согласно классификации правил эксплуатации электроустановок, помещение должно соответствовать первому классу: сухое, беспыльное помещение с нормальной температурой воздуха и изолированными полами.
Безопасность при работе с электроустановками регламентирует ГОСТ 12.1.038-82.

Характеристика психофизиологических и эргономических факторов при работе на ПЭВМ

Особенности характера и условий труда работников, работающих с видеотерминалом и клавиатурой - значительное умственное напряжение, постоянная статическая нагрузка, обусловленная относительно неподвижной рабочей позой и другие физические и нервно - психические нагрузки - приводят к изменению у работников функционального состояния центральной нервной системы, нервно-мышечного аппарата рук, шеи, плеч, спины, напряжению зрительного аппарата. У работников появляются боли, зрительная усталость, раздражительность, общее утомление.

Снижения влияния этих факторов и сохранения высокой работоспособности можно достичь рациональной организацией режима труда и отдыха, который предусматривает периодические перерывы и производственную гимнастику. Гимнастика должна включать специальные упражнения для глаз и для снятия утомления от статического напряжения.

Регламентированные перерывы с интервалом 5-10 минут используются на пассивный отдых и для проведения специальной гимнастики работниками индивидуально, в зависимости от усталости глаз.

В регламентированные перерывы с интервалом 15 минут необходимо проводить комплекс физических упражнений для снятия общего утомления. Гимнастику можно выполнять сидя на рабочем месте.

Большое значение при работе имеет правильная планировка рабочего места.

Предпочтительнее сидение, имеющее выемку, соответствующую форме бедер, и наклон назад. Спинка стула должна быть изогнутой формы, обнимающей поясницу.

Все необходимое для работы должно быть легко доступным.

Уровень глаз при вертикально расположенном экране должен приходится на цент или 2/3 высоты экрана. Расстояние между монитором и лицом оператора должно быть не менее, чем 40 см. клавиатура располагается в 10 см от края стола, что позволяет запястьям рук опираться на стол.

Требования по психофизическим и эргономическим параметрам регламентируются ГОСТ 12.2.032-88.

При конструировании рабочих мест учитываются следующие общие эргономические требования:

достаточное рабочее пространство, позволяющее работающему человеку осуществлять необходимые движения и перемещения при эксплуатации и техническом обслуживания оборудования;

достаточные физические, зрительные и слуховые связи между работающим человеком и оборудованием, а также между людьми в процессе выполнения общей трудовой задачи;

оптимальное размещение рабочих мест в производственных помещениях, а также безопасные и достаточные проходы для людей;

необходимое и естественное и искусственное освещение;

допустимый уровень шума и вибрации, создаваемых оборудованием рабочего места или другими источниками;

наличие необходимых средств защиты работающих от действия опасных и вредных производственных факторов (физических, химических, биологических, психофизических).

Конструкция рабочего места должна обеспечивать быстроту, безопасность, простоту и экономичность технического обслуживания в нормальных и аварийных условиях, полностью отвечать функциональным требованиям и предполагаемым условиям эксплуатации.

Характеристика шума

Повышенный уровень шума, возникающий при работе ПЭВМ и периферийных устройств, вредно воздействует на нервную систему человека, снижая производительность труда, способствуя возникновению травм.

При длительном воздействии шума на организм человека происходят нежелательные явления: снижается острота слуха, повышается кровяное давление. Кроме того, шум влияет на общее состояние человека - возникает чувство неуверенности, стесненности, плохого самочувствия.

Для снижения уровня шума в помещении, где эксплуатируется вычислительная техника, проводят:

Акустическая обработку помещения (звукоизоляция стен, окон, дверей, потолка, установка штучных звукопоглощателей);

Ослаблении шума самих источников, полностью выполнив требования по звукоизоляции оборудования, изложенные в технической документации на данное оборудование;

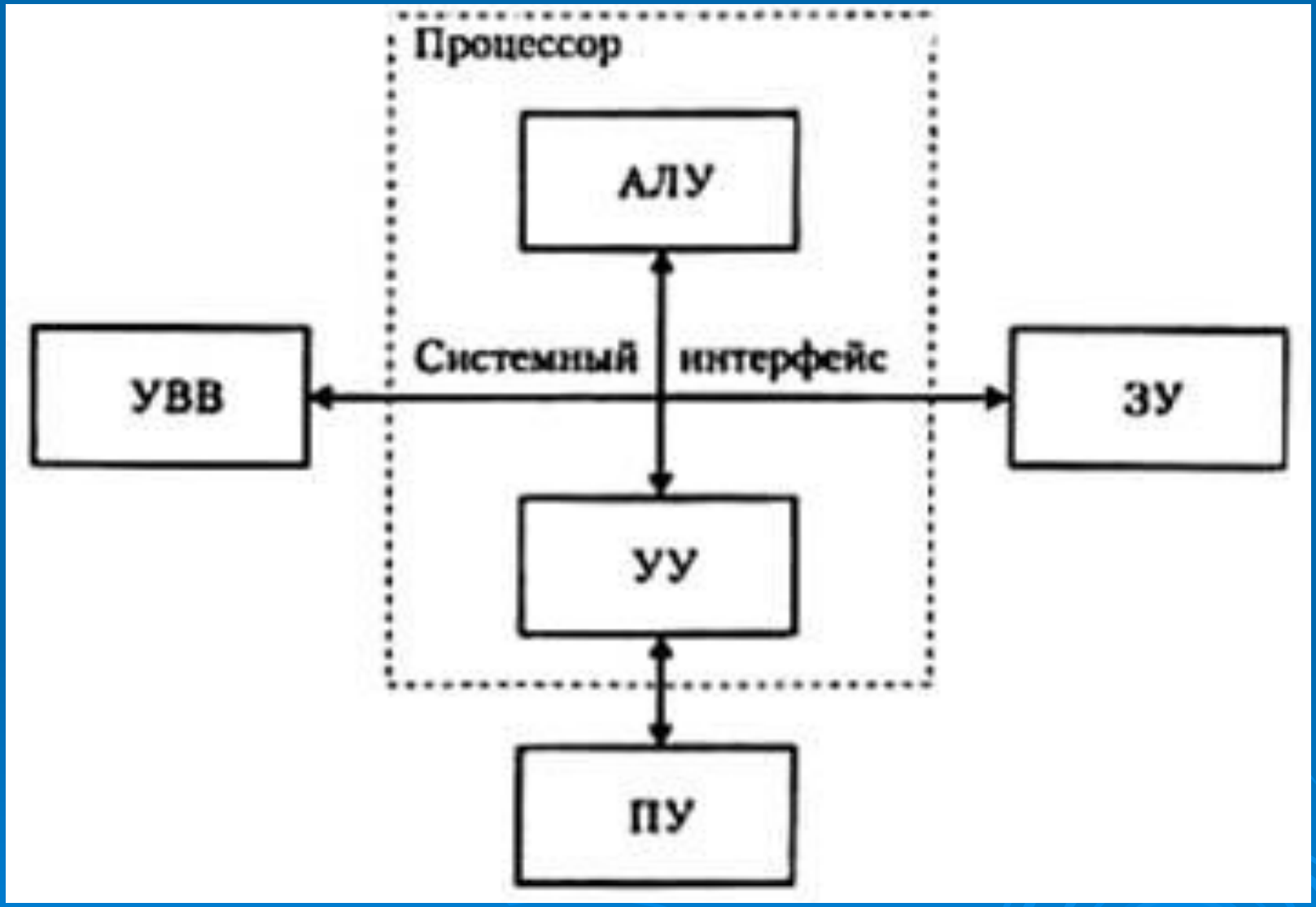
Размещение более тихих помещений вдали от шумных.

Мероприятия по борьбе с шумом на пути его распространения (звукоизолирующие ограждения, кожухи, экраны).
Уровень шума на рабочем месте должен соответствовать требованиям ГОСТ 12.1.003-83 и составлять:
для помещений, где работают программисты и операторы видеотерминалов - не более 50 дБ;
где работают инженерно-технические работники, осуществляющие лабораторный, аналитический и измерительный контроль - не более 60 дБ;
для помещений, где размещаются шумные агрегаты вычислительных машин -75 дБ.

Любая ***ЭВМ*** содержит следующие основные устройства:

- арифметико-логическое устройство (АЛУ);
- устройство управления (УУ);
- запоминающее устройство (ЗУ);
- устройства ввода-вывода (УВВ);
- пульт управления (ПУ).

В современных ЭВМ АЛУ и УУ объединены в общее устройство, называемое центральным процессором. Обобщенная логическая структура ЭВМ представлена на рисунке (ниже)



Обобщённая логическая структура ЭВМ

Нормативы эксплуатации вычислительной техники и копировально-множительной техники

Показатель	Допустимое значение
1.Расположение мониторов: от стен между собой	 1м 1,5м
2. Площадь рабочего помещения на одного работающего	6,0м2
3. Объем рабочего помещения на одного работающего	20м3
4. Расположение экрана монитора от глаз оператора	50-80см
5. Длительность перерывов при постоянной работе с монитором: каждый час каждые два часа	 5-10мин 15мин

Не допускается расположение мониторов экранами друг к другу.

Требования к видеотерминальному устройству

Видеотерминальное устройство должно отвечать следующим техническим требованиям:

яркость свечения экрана должна быть не менее 100 кдж/м2;
минимальный размер светящейся точки - не более 0,4 мм для монохромного дисплея и не более 0,6 мм - для цветного дисплея;
контрастность изображения знака - не менее 0,8;
частота регенерации изображения при работе с позитивным контрастом в режиме обработки текста - не менее 72 Гц;
количество точек на строке - не менее 640;
низкочастотное дрожание изображения в диапазоне 0,05-10Гц должно находиться в пределах 0,1 мм;
экран должен иметь антибликовое покрытие;
размер экрана должен быть не менее 31см по диагонали, а высота символов на экране - не менее 3,8мм, при этом расстояние от глаз оператора до экрана должно быть в пределах 40-80см.

Трудовую деятельность с применением ЭВМ разделяют на 3 группы:

Группа А – считывание информации (диалоговый режим работы);
Группа Б – ввод информации;
Группа В – творческая работа в режиме диалога с ПЭВМ (отладка программ, перевод и редактирование текстов и др.)
Работы с ЭВМ в зависимости от напряженности, уровень которой определяется специалистами – физиологами труда, разделяются на три категории:
в группах А и Б – по суммарному числу считываемых или вводимых за рабочую смену знаков;
в группе В – по суммарному времени работы за ЭВМ за смену.
Продолжительность непрерывной работы на ЭВМ без регламентированного перерыва не должна превышать 2ч., продолжительность обеденного перерыва определяется действующим законодательством о труде и правилами внутреннего трудового распорядка предприятия (организации, учреждения).

При 8-часовой рабочей смене регламентированные перерывы необходимо устанавливать:

для I категории работ за ВДТ через 2ч от начала смены и через 2ч после обеденного перерыва, каждый продолжительностью 10мин;

для II категории работ за ВДТ через 2ч от начала смены продолжительностью 15мин, через 1,5 и 2,5ч после обеденного перерыва продолжительностью 15 и 10мин соответственно или продолжительностью 5-10мин через каждый час работы, в зависимости от характера технологического процесса;

для III категории работ за ВДТ через 2ч от начала смены, через 1,5 и 2,5ч после обеденного перерыва продолжительностью 20мин каждый или продолжительностью 5-15мин через каждый час работы, в зависимости от характера технологического процесса.

Нагрузка за рабочую смену при работе на ЭВМ любой продолжительности не должна превышать для группы работ А – 60 000 знаков, для группы работ Б – 45 000 знаков, для группы работ В – 6ч.

Помещение с мониторами и ЭВМ должны иметь естественное и искусственное освещение. Естественное освещение должно осуществляться через светопроемы, ориентированные преимущественно на север и северо-восток; **коэффициент естественного освещения (КЕО) должен быть не ниже 1,2 %** в **зонах с устойчивым снежным покровом и не ниже 1,5 % на остальной территории**. Указанные значения КЕО нормируются для зданий, расположенных в III световом климатическом поясе.

Для внутренней отделки интерьера помещений с мониторами и ПЭВМ должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка - 0,7 - 0,8; для стен - 0,5 - 0,6; для пола - 0,3 - 0,5.

В производственных помещениях, в которых работа с ЭВМ является основной (диспетчерские, операторские, расчетные, кабины и посты управления, залы вычислительной техники и др.), должны обеспечиваться оптимальные параметры микроклимата.

Для повышения влажности воздуха в помещениях с мониторами ПЭВМ следует применять увлажнители воздуха, заправляемые ежедневно дистиллированной или прокипяченной питьевой водой.

Защита данных в компьютерных сетях.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных "угроз" можно выделить :

1. Сбои оборудования :
- сбои кабельной системы;
- перебои электропитания;
- сбои дисковых систем;
- сбои систем архивации данных;
- сбои работы серверов, рабочих станций, сетевых карт и т.д.

2. Потери информации из-за некорректной работы ПО :
- потеря или изменение данных при ошибках ПО;
- потери при заражении системы компьютерными вирусами;

3. Потери, связанные с несанкционированным доступом :
- несанкционированное копирование, уничтожение или подделка информации;
- ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц.

4. Потери информации, связанные с неправильным хранением архивных данных.
5. Ошибки обслуживающего персонала и пользователей :
- случайное уничтожение или изменение данных;
- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных.

В зависимости от возможных видов нарушений работы сети многочисленные виды защиты информации объединяются в три основных класса :
- средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т.д.
- программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.
- административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.

Требования безопасности при выполнении работ

Оператор ПЭВМ во время работы обязан:

- в течение рабочего дня содержать в порядке и чистоте рабочее место;
- не закрывать вентиляционные отверстия ПЭВМ;
- при необходимости временного прекращения работы корректно закрыть все активные задачи;
- соблюдать правила эксплуатации оборудования;
- при работе с каждой программой выбирать наиболее оптимальное сочетание визуальных параметров (цвет и размер символов, фон экрана, яркость, контрастность и др.);
- соблюдать установленные режимом рабочего времени регламентированные перерывы в работе, выполнять рекомендованные физические упражнения.

Оператору ПЭВМ во время работы запрещается:

- прикасаться к задней панели системного блока при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- закрывать оборудование бумагами и посторонними предметами;
- допускать скапливание бумаг на рабочем месте;
- производить отключение питания во время выполнения активной задачи;
- снимать защитный фильтр с экрана монитора;
- допускать попадание влаги на поверхности устройств;
- производить самостоятельно вскрытие и ремонт оборудования;
- производить вскрытие или заправку на рабочем месте картриджей лазерных принтеров и копировальной техники;
- прикасаться к нагретым элементам принтеров и копировальной техники;
- работать со снятыми кожухами оборудования, являющегося источниками лазерного и ультрафиолетового излучения;
- располагаться при работе на расстоянии менее 50 см. от экрана монитора.

Требования безопасности в аварийных ситуациях

Обо всех неисправностях в работе оборудования и аварийных ситуациях сообщать непосредственному руководителю.

При обнаружении обрыва проводов питания или нарушения целости их изоляции, неисправности заземления и других повреждений электрооборудования, появления запаха гари, посторонних звуков в работе оборудования и тестовых сигналов, индицирующих о его неисправности, немедленно прекратить работу и отключить питание.

При поражении работника электрическим током принять меры по его освобождению от действия тока путем отключения электропитания и до прибытия врача оказать потерпевшему первую медицинскую помощь.

В случае возгорания оборудования отключить питание, сообщить в пожарную охрану и руководителю, после чего приступить к тушению пожара имеющимися средствами.