Введение в информационную безопасность. Компьютеры: преступления, признаки уязвимости и меры защиты

Введение

Информационная Эра привела к драматическим изменениям в способе выполнения своих обязанностей для большого числа профессий. Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Но использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Ответственность за защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание работоспособности информационных систем.

И так как автоматизация привела к тому, что теперь операции с вычислительной техникой выполняются простыми служащими организации, а не специально подготовленным техническим персоналом, нужно, чтобы конечные пользователи знали о своей ответственности за защиту информации.

Целью этого документа является дать основы компьютерной безопасности для низшего звена управления, то есть для начальников отделов, руководителей групп и т.п.

При ограблении банка потери в среднем составляют 19 тысяч долларов, а при компьютерном преступлении - 560 тысяч долларов

Число компьютерных преступлений растет - также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год и составляет около 3.5 миллиардов долларов. Одной из причин является сумма денег, получаемая в результате преступления: в то время как ущерб от среднего компьютерного преступления составляет 560 тысяч долларов, при ограблении банка - всего лишь 19 тысяч долларов.

Шансов быть пойманным у компьютерного преступника гораздо меньше, чем у грабителя банка - и даже при поимке у него меньше шансов попасть в тюрьму. Обнаруживается в среднем 1 процент компьютерных преступлений. И вероятность того, что за компьютерное мошенничество преступник попадет в тюрьму, меньше 10 процентов.

Умышленные компьютерные преступления составляют заметную часть преступлений. Но злоупотреблений компьютерами и ошибок еще больше. Как выразился один эксперт, "мы теряем из-за ошибок больше денег, чем могли бы украсть". Эти потери подчеркивают важность и серьезность убытков, связанных с компьютерами.

Основной причиной наличия потерь, связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого. Осведомленность конечного пользователя о мерах

безопасности обеспечивает четыре уровня защиты компьютерных и информационных ресурсов:

МЕРЫ ЗАЩИТЫ: ЧЕТЫРЕ УРОВНЯ ЗАЩИТЫ

Предотвращение - только авторизованный персонал имеет доступ к информации и технологии

Обнаружение - обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены

Ограничение- уменьшается размер потерь, если преступление все-таки произошло несмотря на меры по его предотвращению и обнаружению.

Восстановление - обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению

Вчера контроль за технологией работы был заботой технических администраторов. Сегодня контроль за информацией стал обязанностью каждого нетехнического конечного пользователя. Контроль за информацией требует новых знаний и навыков для группы нетехнических служащих. Хороший контроль за информацией требует понимания возможностей совершения компьютерных преступлений и злоупотреблений, чтобы можно было в дальнейшем предпринять контрмеры против них.

Когда компьютеры впервые появились, они были доступны только небольшому числу людей, которые умели их использовать. Обычно они помещались в специальных помещениях, удаленных территориально от помещений, где работали служащие. Сегодня все изменилось. Компьютерные терминалы и настольные компьютеры используются везде. Компьютерное оборудование стало дружественным к пользователю, поэтому много людей могут быстро и легко научиться тому, как его использовать.

Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет. Доступ к информации больше не ограничивается только узким кругом лиц из верхнего руководства организации. Этот процесс привел к тому, что произошла "демократизация преступления". Чем больше людей получало доступ к информационной технологии и компьютерному оборудованию, тем больше возникало возможностей для совершения компьютерных преступлений.

Трудно обобщать, но теперь компьютерным преступником может быть...

- конечный пользователь, не технический служащий и не хакер
- тот, кто не находится на руководящей должности
- тот, у кого нет судимостей
- умный, талантливый сотрудник
- тот, кто много работает
- тот, кто не разбирается в компьютерах
- тот, кого вы подозревали бы в последнюю очередь
- именно тот, кого вы взяли бы на работу

КОМПЬЮТЕРНЫМ ПРЕСТУПНИКОМ МОЖЕТ БЫТЬ ЛЮБОЙ

Типичный компьютерный преступник - это не молодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам. Типичный компьютерный преступник - это служащий, которому разрешен доступ к системе, нетехническим пользователем которой он является. В США компьютерные преступления, совершенные служащими, составляют 70-80 процентов ежегодного ущерба, связанного с компьютерами. Остальные 20 процентов дают действия нечестных и недовольных сотрудников. И совершаются они по целому ряду причин.

ПОЧЕМУ ЛЮДИ СОВЕРШАЮТ КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

- личная или финансовая выгода
- развлечение
- месть
- попытка добиться расположения кого-либо к себе
- самовыражение
- случайность

- вандализм

Но значительно больший ущерб, около 60 процентов всех потерь, наносят ошибки людей и инциденты. Предотвращение компьютерных потерь, как из-за умышленных преступлений, так и из-за неумышленных ошибок, требует знаний в области безопасности. Опросы, проводимые периодически в США, показывают, что именно служащие, имевшие знания в области компьютерной безопасности, были основной причиной выявления компьютерных преступлений.

ПРИЗНАКИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Обращайте внимание на :

- неавторизованное использование компьютерного времени
- неавторизованные попытки доступа к файлам данных
- кражи частей компьютеров
- кражи программ
- физическое разрушение оборудования
- уничтожение данных или программ
- неавторизованное владение дискетами, лентами или распечатками

И это только самые очевидные признаки, на которые следует обратить внимание при выявлении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление уже совершено, или что не выполняются меры защиты. Они также могут свидетельствовать о наличии уязвимых мест - указать, где находится дыра в защите - и помочь наметить план действий по устранению уязвимого места. В то время как признаки могут помочь выявить преступление или злоупотребление - меры защиты могут помочь предотвратить его.

Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации - административные руководящие документы(приказы, положения, инструкции), аппаратные устройства или дополнительные программы - основной целью которых является предотвратить преступления и злоупотребления, не позволив им произойти. Меры защиты могут также выполнять функцию ограничения, уменьшая размер ущерба от преступления.

Информационная безопасность

То, что в 60-е годы называлось компьютерной безопасностью, а в 70-е - безопасностью данных, сейчас более правильно именуется информационной безопасностью. Информационная безопасность подчеркивает важность информации в современном обществе - понимание того, что информация - это ценный ресурс, нечто большее, чем отдельные элементы данных.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

- конфиденциальность критической информации
- целостность информации и связанных с ней процессов(создания, ввода, обработки и вывода)
- доступность информации, когда она нужна
- учет всех процессов, связанных с информацией

Некоторые технологии по защите системы и обеспечению учета всех событий могут быть встроены в сам компьютер. Другие могут быть встроены в программы. Некоторые же выполняются людьми и являются реализацией указаний руководства, содержащихся в соответствующих руководящих документах. Принятие решения о выборе уровня сложности технологий для защите системы требует установления

критичности информации и последующего определения адекватного уровня безопасности.

Что же такое критические данные? **Под критическими данными будем понимать данные, которые требуют защиты из-за вероятности нанесения(риска) ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение, или разрушение данных.** Этот термин включает в себя данные, чье неправильное использование или раскрытие может отрицательно отразиться на способности организации решать свои задачи, персональные данные и другие данные, защита которых требуется указами Президента РФ, законами РФ и другими подзаконными документами.

ПРЕСТУПЛЕНИЯ И ЗЛОУПОТРЕБЛЕНИЯ

Анализ зарубежных и отечественных отчетов о выявленных компьютерных преступлениях позволяет описать основные технологии их совершения. Лишь немногие из них включают разрушение компьютеров или данных. Только в 3 процентах мошенничеств и 8 процентах злоупотреблений происходило специальное разрушение оборудования, уничтожение программ или данных. В большей части случаев мошенничеств и злоупотреблений использовалась информация - ею манипулировали, ее создавали, ее использовали.

ПЯТЬ ОСНОВНЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗОВАВШИХСЯ ПРИ СОВЕРШЕНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Мошенничества

1. Ввод неавторизованной информации
2. Манипуляции разрешенной для ввода информацией
3. Манипуляции или неправильное использование файлов с информацией
4. Создание неавторизованных файлов с информацией
5. Обход внутренних мер защиты

Злоупотребления

1. Кража компьютерного времени, программ, информации и оборудования
2. Ввод неавторизованной информации
3. Создание неавторизованных файлов с информацией
4. Разработка компьютерных программ для неслужебного использования
5. Манипулирование или неправильное использование возможностей по проведению работ на компьютерах

С другой стороны стоит рассмотреть основные методы, использовавшиеся для их совершения. Они включают:

1. **Надувательство с данными.** Наверное, самый распространенный метод при совершении компьютерных преступлений, так как он не требует технических знаний и относительно безопасен. Информация меняется в процессе ее ввода в компьютер или во время вывода. Например, при вводе документы могут быть заменены фальшивыми, вместо рабочих дискет подсунуты чужие, и данные могут быть сфальсифицированы.
2. **Сканирование.** Другой распространенный метод получения информации, который может привести к преступлению. Служащие, читающие файлы других, могут обнаружить там персональную информацию о своих коллегах. Информация, позволяющая получить доступ к компьютерным файлам или изменить их, может быть найдена после просмотра мусорных корзин. Дискеты, оставленные на столе, могут быть прочитаны, скопированы, и украдены. Очень хитрый сканирующий может даже просматривать остаточную информацию, оставшуюся на компьютере или на носителе информации после выполнения сотрудником задания и удаления своих файлов.
3. **Троянский конь.** Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы(возможности пользователя, запустившего программу, по доступу к файлам)

4. **Люк.** Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.
5. **Технология салями** Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.
6. **Суперотключение**. Названа по имени программы, использовавшейся в ряде компьютерных центров, обходившей системные меры защиты и использовавшейся при аварийных ситуациях. Владение этим "мастер-ключом" дает возможность в любое время получить доступ к компьютеру и информации, находящейся в нем.

Примеры компьютерных преступлений:

- Оператор по приему платежей узнав о смерти вкладчика, открыл счет в банке, используя имя клиента и другие его данные. Вкладчик не был удален из списка клиентов, на счета которых начислялись проценты, а в с помощью компьютерной системы был заменен его адрес и запрошен прямой перевод процентов на счет, открытый оператором
- Большой ущерб был нанесен при доставке заказа на оборудование от федерального правительства. Были приготовлены фиктивные реквизиты для счета, направленного на большой центр. Эти реквизиты приводили к отправке оборудования реальной частной фирме, выполняющей государственные заказы. Перед самой доставкой один из злоумышленников позвонил в эту фирму и предупредил об их "ошибке", а потом доставил оборудование самим злоумышленникам.
- три оператора, используя удаленный терминал, ввели фиктивный запрос в компьютер на получение 150 тысяч долларов по процентам и затем удалили записи об этих транзакциях.

Особо стоит остановиться на необычном для России виде компьютерных преступлений - краже информации. Обычно либо продается персональная информация, информация об условиях контракта, и конфиденциальная информация компании(например, технология создания продукта) посторонним лицам, либо копируются и используются программы для личной выгоды.

Признаки

Следующие признаки могут свидетельствовать о наличии уязвимых мест в информационной безопасности.

1. Не разработано положений о защите информации или они не соблюдаются. Не назначен ответственный за информационную безопасность.
2. Пароли пишутся на компьютерных терминалах, помещаются в общедоступные места, ими делятся с другими, или они появляются на компьютерном экране при их вводе
3. Удаленные терминалы и микрокомпьютеры оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра.
4. Не существует ограничений на доступ к информации, или на характер ее использования. Все пользователи имеют доступ ко всей информации и могут использовать все функции системы.
5. Не ведется системных журналов, и не хранится информация о том, кто и для чего использует компьютер.
6. Изменения в программы могут вноситься без их предварительного утверждения руководством.
7. Отсутствует документация или она не позволяет делать следующее: понимать получаемые отчеты и формулы, по которым получаются результаты, модифицировать программы, готовить данные для ввода, исправлять ошибки, производить оценку мер защиты, и понимать сами данные - их источники, формат хранения, взаимосвязи между ними.

8. Делаются многочисленные попытки войти в систему с неправильными паролями.
9. Вводимые данные не проверяются на корректность и точность, или при их проверке много данных отвергается из-за ошибок в них, требуется сделать много исправлений в данных, не делается записей в журналах об отвергнутых транзакциях.
10. Имеют место выходы из строя системы, приносящие большие убытки
11. Не производился анализ информации, обрабатываемой в компьютере, с целью определения необходимого для нее уровня безопасности
12. Мало внимания уделяется информационной безопасности. Хотя политика безопасности и существует, большинство людей считает, что на самом деле она не нужна.

Меры защиты информационной безопасности

1. Контролируйте доступ как к информации в компьютере, так и к прикладным программам. Вы должны иметь гарантии того, что только авторизованные пользователи имеют доступ к информации и приложениям.

Идентификация пользователей

Требуйте, чтобы пользователи выполняли процедуры входа в компьютер, и используйте это как средство для идентификации в начале работы. Чтобы эффективно контролировать микрокомпьютер, может оказаться наиболее выгодным использовать его как однопользовательскую систему. Обычно у микрокомпьютера нет процедур входа в систему, право использовать систему предоставляется простым включением компьютера.

Аутентификация пользователей

Используйте уникальные пароли для каждого пользователя, которые не являются комбинациями личных данных пользователей, для аутентификации личности пользователя. Внедрите меры защиты при администрировании паролей, и ознакомьте пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению..

Другие меры защиты:

Пароли - только один из типов идентификации - что-то, что знает только пользователь. Двумя другими типами идентификации, которые тоже эффективны, являются что-то, чем владеет пользователь(например, магнитная карта), или уникальные характеристики пользователя(его голос).

Если в компьютере имеется встроенный стандартный пароль(пароль, который встроен в программы и позволяет обойти меры по управлению доступом), обязательно измените его.

Сделайте так, чтобы программы в компьютере после входа пользователя в систему сообщали ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов.

Защищайте ваш пароль

- не делитесь своим паролем ни с кем
- выбирайте пароль трудно угадываемым
- попробуйте использовать строчные и прописные буквы, цифры, или выберите знаменитое изречение и возьмите оттуда каждую четвертую букву. А еще лучше позвольте компьютеру самому сгенерировать ваш пароль.
- не используйте пароль, который является вашим адресом, псевдонимом, именем жены, телефонным номером или чем-либо очевидным.
- используйте длинные пароли, так как они более безопасны, лучше всего от 6 до 8 символов
- обеспечьте неотображаемость пароля на экране компьютера при его вводе
- обеспечьте отсутствие паролей в распечатках
- не записывайте пароли на столе, стене или терминале. Держите его в памяти

Серьезно относитесь к администрированию паролей

- периодически меняйте пароли и делайте это не по графику
- шифруйте или делайте что-нибудь еще с файлами паролей, хранящимися в компьютере, для защиты их от неавторизованного доступа.
- назначайте на должность администратора паролей только самого надежного человека
- не используйте один и тот же пароль для всех сотрудников в группе

- меняйте пароли, когда человек увольняется
- заставляйте людей расписываться за получение паролей
- установите и внедрите правила работы с паролями и обеспечьте, чтобы все знали их

Процедуры авторизации

Разработайте процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям - и используйте соответствующие меры по внедрению этих процедур в организации.

Установите порядок в организации, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Защита файлов

Помимо идентификации пользователей и процедур авторизации разработайте процедуры по ограничению доступа к файлам с данными:

- используйте внешние и внутренние метки файлов для указания типа информации, который они содержат, и требуемого уровня безопасности
- ограничьте доступ в помещения, в которых хранятся файлы данных, такие как архивы и библиотеки данных
- используйте организационные меры и программно-аппаратные средства для ограничения доступа к файлам только авторизованных пользователей

Предосторожности при работе

- отключайте неиспользуемые терминалы
- закрывайте комнаты, где находятся терминалы
- разворачивайте экраны компьютеров так, чтобы они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируются
- установите специальное оборудование, такое как устройства, ограничивающие число неудачных попыток доступа, или делающие обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру
- программируйте терминал отключаться после определенного периода неиспользования
- если это возможно, выключайте систему в нерабочие часы

2. Защищайте целостность информации. Вводимая информация должна быть авторизована, полна, точна и должна подвергаться проверкам на ошибки.

Целостность информации

Проверяйте точность информации с помощью процедур сравнения результатов обработки с предполагаемыми результатами обработки. Например, можно сравнивать суммы или проверять последовательные номера.

Проверяйте точность вводимых данных, требуя от служащих выполнять проверки на корректность, такие как:

- проверки на нахождение символов в допустимом диапазоне символов(числовом или буквенном)
- проверки на нахождение числовых данных в допустимом диапазоне чисел
- проверки на корректность связей с другими данными, сравнивающими входные данные с данными в других файлах
- проверки на разумность, сравнивающие входные данные с ожидаемыми стандартными значениями
- ограничения на транзакции, сравнивающие входные данные с административно установленными ограничениями на конкретные транзакции

Трассируйте транзакции в системе

Делайте перекрестные проверки содержимого файлов с помощью сопоставления числа записей или контроля суммы значений поля записи.

3. Защищайте системные программы. Если ПО используется совместно, защищайте его от скрытой модификации при помощи политики безопасности, мер защиты при его разработке и контроле за ним в его жизненном цикле, а также обучения пользователей в области безопасности.

Меры защиты при разработке программ и соответствующие политики должны включать процедуры внесения изменений в программу, ее приемки и тестирования до ввода в эксплуатацию. Политики должны требовать разрешения ответственного лица из руководства для внесения изменений в программы, ограничения списка лиц, кому

разрешено вносить изменения и явно описывать обязанности сотрудников по ведению документации.
Должен быть разработан и поддерживаться каталог прикладных программ.
Должны быть внедрены меры защиты по предотвращению получения, изменения или добавления программ неавторизованными людьми через удаленные терминалы.
4. Сделайте меры защиты более адекватными с помощью привлечения организаций, занимающихся тестированием информационной безопасности, при разработке мер защиты в прикладных программах и консультируйтесь с ними при определении необходимости тестов и проверок при обработке критических данных. Контрольные журналы, встроенные в компьютерные программы, могут предотвратить или выявить компьютерное мошенничество и злоупотребление.
Должны иметься контрольные журналы для наблюдения за тем, кто из пользователей обновлял критические информационные файлы
Если критичность информации, хранимой в компьютерах, требует контрольных журналов, то важны как меры физической защиты, так и меры по управлению доступом.
В компьютерной сети журналы должны храниться на хосте, а не на рабочей станции.
Контрольные журналы не должны отключаться для повышения скорости работы.
Распечатки контрольных журналов должны просматриваться достаточно часто и регулярно.
5. Рассмотрите вопрос о коммуникационной безопасности. Данные, передаваемые по незащищенным линиям, могут быть перехвачены.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

Традиционная безопасность : замки, ограждение и охрана

Физическая безопасность означает лишь содержание компьютера и информации в нем в безопасности от физических опасностей с помощью замков на входах в помещение, где он находится, строительства ограждения вокруг зданий и размещения охраны вокруг помещения. Но физическая безопасность сейчас изменилась из-за современной компьютерной среды - среды, которая часто представляет собой офис с большим числом персональных ЭВМ или терминалов.
Физическая безопасность связана с внедрением мер защиты, которые защищают от стихийных бедствий(пожаров, наводнений, и землетрясений), а также всяких случайных инцидентов. Меры физической безопасности определяют, каким будет окружение компьютера, вводимые данные, и результаты обработки информации. Помимо помещений, где размещено компьютерное оборудование, окружение включает в себя библиотеки программ, журналы, магнитные носители, помещения для архивов, и помещения для ремонта техники.
Меры физической защиты должны отвечать требованиям современной действительности и сочетать эффективность с невысокой ценой. Например, установка дорогой противопожарной системы может быть необходимой для защиты большого компьютера, обрабатывающего критические данные, но оказаться неоправданно дорогой при защите одной персональной ЭВМ.

Преступления и злоупотребления

Компьютеры могут быть повреждены, украдены и специально выведены из строя с помощью короткого замыкания. Диски и ленты могут быть разрушены разлитыми напитками, а компьютеры залиты водой. Также компьютеры могут быть серьезно повреждены пожаром, скачками напряжения, стихийными бедствиями и другими инцидентами. Информация может быть перехвачена, украдена, продана и использоваться в корыстных целях отдельным человеком или целой компанией.
Персональные ЭВМ особенно привлекают воров. При пожаре диски, не хранящиеся в специальных сейфах или флоппи-диски, оставленные на терминалах, могут быть разрушены системой тушения пожара. Тысячи долларов были потрачены на восстановление информации, которую они содержали.

Но основной причиной разрушений компьютеров является, судя по всему, обычная неосторожность людей и вредное влияние окружающей среды.

Признаки

Следующие признаки могут указывать на наличие уязвимых мест в физической безопасности:

- разрешено курить, есть и пить рядом с компьютерами
- компьютерное оборудование оставляется в незапертых комнатах или является незащищенным по какой-либо другой причине
- не установлена пожарная сигнализация
- диски оставляются в ящиках столов, не делается архивных копий дисков
- посетителям не задается вопросов о причине их нахождения в помещениях, где установлены компьютеры
- реестр компьютерного оборудования и программ отсутствует, неполон, не обновляется или не проверяется после его заполнения.
- распечатки, микрофиши, диски, содержащие критические данные выбрасываются в обычное мусорное ведро
- замки на входах в помещения, где находится компьютерное оборудование, никогда не менялись
- не производилось аттестации автоматизированной системы организации, то есть анализа насколько она уязвима к доступу неавторизованных людей, пожару или наводнению.

Меры физической безопасности

1.Предотвратить злонамеренные разрушения, неавторизованное использование или кражу

ПЭВМ могут быть заперты в комнатах и доступ к ним может быть ограничен с помощью устройств блокировки клавиатуры и т.п. Удостоверьтесь, что люди соблюдают свои обязанности по использованию компьютеров и их можно проконтролировать.

Если информация обрабатывается на большом вычислительном центре, проверьте, как контролируется физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана.

Ввод критической информации требует правильного обращения с исходными документами. Правильное обращение означает соблюдение одинаковых правил работы с документами, независимо от того, используются они в автоматизированной системе или нет. Правила работы могут включать работу в безопасном помещении, учет документов в журналах, гарантии того, что только люди, имеющие соответствующий допуск, могут ознакомиться с этими документами, и использование устройств уничтожения документов(бумагорезок и т.п.).

Внимательно проанализируйте размещение компьютеров. Не слишком ли доступны они неавторизованным людям или чрезмерно уязвимы к стихийным бедствиям?

Вы должны иметь представление об основных схемах сопровождения посторонних. Например, авторизованный сотрудник должен сопровождать в компьютерной зоне посетителя с компьютерными распечатками или человека, заявляющего, что он техник по ремонту компьютеров.

Вы должны знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

Многие люди полагают, что двери, оснащенные замками и охраняемые людьми, обеспечивают физическую безопасность. Но электромагнитные излучения от компьютеров могут быть перехвачены и таким образом может быть прочитана информация с экрана. Рекомендуемые меры защиты от этого должны учитывать требуемый уровень безопасности и тот факт, что такой перехват крайне редок, но может и произойти.

Могут быть предприняты недорогие предохранительные меры , которые будут гарантировать, что телефонные и компьютерные каналы связи в состоянии выполнять свои функции и являются безопасными. В сети может потребоваться выделенный канал

связи - он не выполняет других функций. С другой стороны выделение персональной ЭВМ для работы на ней одного приложения может оказаться самым эффективным средством защиты.

Для любой из основных трех технологий для передачи автоматизированной информации существует технология перехвата : кабель(подключение к кабелю), спутник(антенна приема сигнала со спутника), радиоволны(радиоперехват).

Технологии защиты, которые могут быть использованы, включают шифрование информации, использование выделенных линий, модемы с функциям безопасности, и использование скремблирования голосовых переговоров.

2. Стихийные бедствия могут нанести большой ущерб как большим, так и маленьким компаниям.

Примите меры по предотвращению, обнаружению и минимизации ущерба от пожара, наводнения, загрязнения окружающей среды, высоких температур и скачков напряжения.

Защищайтесь от пожара с помощью регулярной проверки пожарной сигнализации и систем пожаротушения. Защищайте ПЭВМ с помощью кожухов, чтобы они не были повреждены системой пожаротушения. Не храните горючие материалы в этих помещениях.

Статическое электричество может очистить память в ПЭВМ. Антистатические коврики могут предотвратить это. Пользователям следует напоминать о снятии заряда с себя с помощью прикосновения к заземленному объекту.

Скачки напряжения могут очистить память, изменить программы и разрушить микросхемы. Устройство бесперебойного питания(УБП) дает достаточно времени, чтобы отключить компьютер без потери данных. Предохранить компьютеры от кратковременных бросков питания могут фильтры напряжения. В грозу незащищенные ПЭВМ могут быть отключены и выключены из сети.

Температура в помещении может контролироваться кондиционерами и вентиляторами, а также хорошей вентиляцией в помещении. Проблемы с чрезмерно высокой температурой могут возникнуть в стойках периферийного оборудования или из-за закрытия вентиляционного отверстия в терминалах или ПЭВМ.

Воздушные фильтры могут очистить воздух от вредных веществ в нем, которые могут нанести вред компьютерам и дискам. Следует запретить курить возле ПЭВМ.

Размещайте компьютеры подальше от того, что может явиться источником большого количества воды, например трубопроводов, обычно затапливаемых помещений или не используйте систему пожаротушения, если есть другие способы защиты от пожара.

Держите еду и напитки подальше от компьютера.

Содержите оборудование в порядке. Следите и учитывайте в журналах ремонт техники. Это позволит проконтролировать, кто имел доступ к системе. Помните, что бригады ремонтников должны производить правильную идентификацию себя.

3. Защищайте все носители информации(исходные документы, ленты, картриджи, диски, распечатки)

- ведите, контролируйте и проверяйте реестры носителей информации
- обучайте пользователей правильным методам очищения и уничтожения носителей информации
- делайте метки на носителях информации, отражающие уровень критичности информации, которая в них содержится.
- уничтожайте носители информации в соответствии с планом организации
- удостоверьтесь, что доступ к носителям информации для их хранения, передачи, нанесения меток, и уничтожения предоставлен только авторизованным людям
- доведите все руководящие документы до сотрудников

Подумайте о возможности публикации следующих рекомендаций в общедоступном месте:

Диски уязвимы

- храните их в конвертах и коробках
- не пишите на конвертах

- не гните их
- не касайтесь самих дисков
- осторожно вставляйте их в компьютер
- не разливайте на них напитки
- держите их подальше от источников магнитного поля
- храните их в металлических сейфах
- работайте с дисками в соответствии с маркировкой критичности на них

Правильное обращение обеспечивает защиту

- убирайте диски и ленты, когда не работаете с ними
- храните их разложенными по полкам в определенном порядке
- не давайте носители информации с критической информацией неавторизованным людям
- отдавайте поврежденные диски с критической информацией только после их размагничивания или аналогичной процедуры
- уничтожайте критическую информацию на дисках с помощью их размагничивания или физического разрушения в соответствии с порядком в вашей организации
- уничтожайте распечатки и красящие ленты от принтеров с критической информацией в соответствии с порядком в вашей организации.
- обеспечьте безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру

4. Удостоверьтесь, что существуют адекватные планы действий при ЧП(планы обеспечения непрерывной работы). Помните, что целью этих планов являются гарантии того, что пользователи смогут продолжать выполнять самые главные свои обязанности в случае невозможности работы по информационной технологии. Конечные пользователи информационной технологии, а также обслуживающий персонал, должны знать, как им действовать по этим планам.

Планы обеспечения непрерывной работы и восстановления(ОНРВ) должны быть написаны, проверены и регулярно доводиться до сотрудников.

ОНРВ должны учитывать наличие операций архивации, то есть как будет обрабатываться информация, если компьютеры, на которых она обрабатывалась обычно, нельзя использовать, и необходимость восстановления потерянной или разрушенной информации.

Особенно для ПЭВМ ОНРВ должны учитывать выход из строя той или иной техники, например выход из строя сетевого принтера.

Процедуры и техника должны планироваться в расчете на пожар, затопление и т.д.

Храните архивные копии, включая план ОНРВ, в безопасном месте, удаленном от основных помещений, занимаемых компьютерами.

Процедуры плана должны быть адекватны уровню безопасности и критичности информации.

Знайте, что делать в случае ЧП, и будьте знакомы с планом ОНРВ

Помните, что план ОНРВ может применяться в условиях неразберихи и паники. Тренировки ваших сотрудников жизненно необходимы.