ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Выполнила Буторина Мариядля конкурса «Интернешка»
http://interneshka.org/

- 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.

- Число компьютерных преступлений растет - также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений

- По данным Миннесотского университета США, 93% компаний, лишившихся доступа к своим данным на срок более 10 дней, покинули свой бизнес, причем половина из них заявила о своей несостоятельности немедленно.

- 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.
- 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.

- Признаки компьютерных преступлений:
- · 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.

- 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.
- Защита информации – это деятельность по предотвращению утраты и утечки защищаемой информац

- 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.

- 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.

- Под критическими данными понимаются данные, которые требуют защиты из-за вероятности нанесения ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение, или разрушение данных. К критическим также относят данные, которые при неправильном использовании или раскрытии могут отрицательно воздействовать на способности организации решать свои задачи; персональные данные и другие данные, защита которых требуется указами Президента РФ, законами РФ и другими подзаконными документами.

- Любая система безопасности, в принципе, может быть вскрыта. Эффективной считают такую защиту, стоимость взлома которой соизмерима с ценностью добываемой при этом информации.

- Существует четыре уровня защиты компьютерных и информационных ресурсов:

- Предотвращение предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.

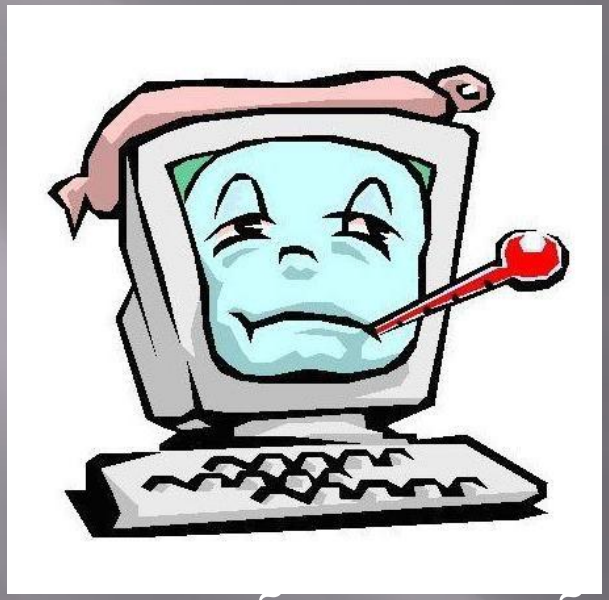
- Обнаружение предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

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

- Восстановление обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

- Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных устройств или дополнительных программ, основной целью которых является предотвращение преступлений и злоупотреблен

- Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на четыре уровня:
- - законодательный: законы, нормативные акты, стандарты и т. п.;
- - административный: действия общего характера, предпринимаемые руководством организации;
- - процедурный: конкретные меры безопасности, имеющие дело с людьми;
- - программно-технический: конкретные технические меры.



- В настоящее время наиболее подробным законодательным документом России в области информационной безопасности является Уголовный кодекс. В разделе "Преступления против общественной безопасности" имеется глава "Преступления в сфере компьютерной информации". Она содержит три статьи - "Неправомерный доступ к компьютерной информации", "Создание, использование и распространение вредоносных программ для ЭВМ" и "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети". Уголовный кодекс стоит на страже всех аспектов информационной безопасности - доступности, целостности, конфиденциальности, предусматривая наказания за "уничтожение, блокирование, модификацию и копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети".

- Аутентификация пользователей.

- Еще более надёжное решение состоит в организации контроля доступа в помещения или к конкретному компьютеру сети с помощью идентификационных пластиковых карточек с встроенной микросхемой - так называемых микропроцессорных карточек (smart - card).
- Для архивной информации, представляющей особую ценность, рекомендуется предусматривать охранное помещение. Дубликаты наиболее ценных данных, лучше хранить в другом здании или даже в другом городе. Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.

- Для архивной информации, представляющей особую ценность, рекомендуется предусматривать охранное помещение. Дубликаты наиболее ценных данных, лучше хранить в другом здании или даже в другом городе. Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.

- Помимо резервного копирования, которое производится при возникновении внештатной ситуации либо по заранее составленному расписанию, для большей сохранности данных на жестких дисках применяют специальные технологии - зеркалирование дисков и создание RAID-массивов, которые представляют собой объединение нескольких жестких дисков. При записи информация поровну распределяется между ними, так что при выходе из строя одного из дисков находящиеся на нем данные могут быть восстановлены по содержимому остальных.
- Резервирование каналов связи.

- По мере того, как компании все больше и больше обращаются к Internet, их бизнес оказывается в серьезной зависимости от функционирования Internet-провайдера. У поставщиков доступа к Сети иногда случаются достаточно серьезные аварии, поэтому важно хранить все важные приложения во внутренней сети компании и иметь договора с несколькими местными провайдерами.
- Защита данных от перехвата.

- Для защиты информации во внешнем канале связи используются следующие устройства: скремблеры для защиты речевой информации, шифраторы для широковещательной связи и криптографические средства, обеспечивающие шифрование цифровых данных

Источники

- http://www.gopwing.com/wp-content/uploads/2014/03/kaspersky-security-banner.jpg
- http://3.bp.blogspot.com/-fH7P7i_Kj6w/UhoXwQGwhMI/AAAAAAAABnU/bDjhLx49lSA/s1600/1011993_556727001051981_1364203181_n.jpg
- http://livepc-msk.ru/images/virus.png
- http://80.img.avito.st/640x480/887568880.jpg
- http://informatiki.my1.ru/265456_1.jpg
- http://comps.canstockphoto.com/can-stock-photo_csp7692493.jpg
- https://ihackers.co.in/wp-content/uploads/2013/05/Spyware.png
- http://www.rjtechsources.com/wp-content/uploads/2013/02/java-exploit.jpg
- http://it-cifra.com.ua/wp-content/uploads/2014/10/wpid-kak_mojno_udalit_vredonosnoe_po.jpg
- http://seowars.uaho.net/wp-content/uploads/2012/09/virus-artisteer.jpg
- http://flenda.ru/images/news/277/868_650x500.jpg?1362999693
- http://minsk1.net/images/uploads/2705f1a8d392fca48d01e5b747ac2bd0.jpg