Проект «Ужасно интересно»

Группа «Информатика»

Разработан
под руководством
студентки 5 курса з/о
мех.-мат. факультета
СГУ Акчуриной Е.В.

Берегите информацию

Берегите информацию

Информация сегодня стоит дорого и её необходимо охранять. Известно множество случаев, когда фирмы ведут между собой настоящие «шпионские войны», вербуя сотрудников конкурента с целью получения через них доступа к информации, составляющую коммерческую тайну. Давайте познакомимся с различными способами защиты информации и работой киберпатруля с нарушениями в сфере информационных технологий.

Защита информации

Защита - система мер по обеспечению безопасности с целью сохранения государственных и коммерческих секретов. Защита обеспечивается соблюдением режима секретности, применением охранных систем сигнализации и наблюдения, использованием шифров и паролей.

Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Безопасность: конфиденциальность, целостность, доступность.

Информационная безопасность

Информационная безопасность — это состояние защищённости информационной среды.

В вычислительной технике понятие безопасности подразумевает

- надежность работы компьютера,
- сохранность ценных данных,
- защиту информации от внесения в нее изменений неуполномоченными лицами,
- сохранение тайны переписки в электронной связи.

Во всех цивилизованных странах на безопасности граждан стоят законы, но в вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надежность работы компьютерных систем во многом опирается на меры самозащиты.

Несанкционированный доступ

Несанкционированный доступ - действия, нарушающие установленный порядок доступа или правила разграничения, доступ к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами.

Для предотвращения несанкционированного доступа осуществляется контроль доступа.

Пароли

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются ***пароли***. Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам. При этом может производиться регистрация всех попыток несанкционированного доступа.

Защита с использованием пароля используется при загрузке операционной системы. Вход по паролю может быть установлен в программе BIOS Setup, компьютер не начнет загрузку операционной системы, если не введен правильный пароль. Преодолеть такую защиту нелегко.

Пароли

От несанкционированного доступа может быть защищены

- каждый диск,
- каждая папка,
- каждый файл локального компьютера.

Для них могут быть установлены определенные права доступа

- полный доступ,
- возможность внесения изменений,
- только чтение,
- запись и др.

Права могут быть различными для различных пользователей.

Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются ***биометрические системы идентификации.***

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам защиты информации относятся системы идентификации: по отпечаткам пальцев; по характеристикам речи; по радужной оболочке глаза; по изображению лица; по геометрии ладони руки.

Идентификация по отпечаткам пальцев

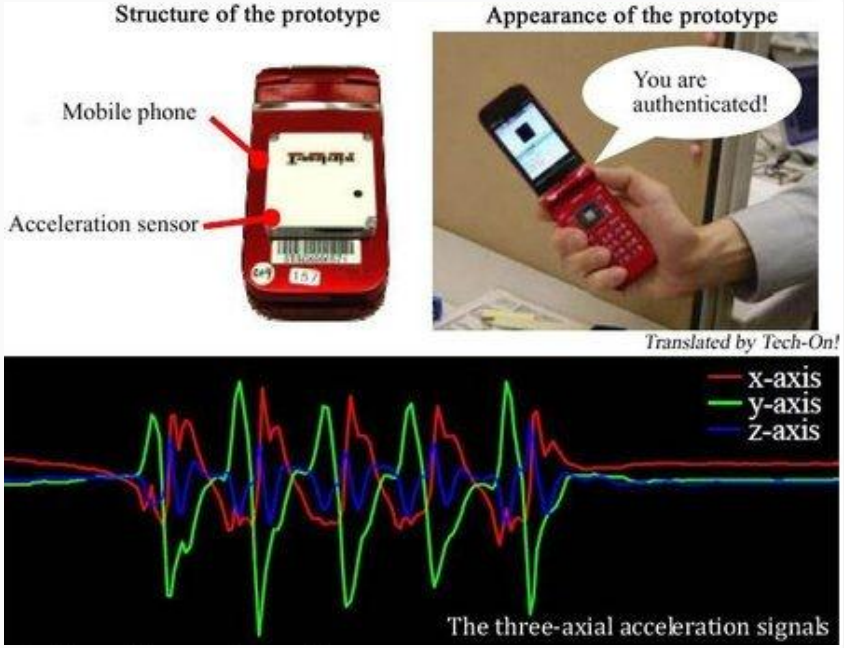
Оптический сканер отпечатка пальца, вмонтированный в ноутбук

- Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).
- Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.

Идентификация по характеристикам речи

Идентификация человека по голосу — один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



Идентификация по радужной оболочке глаза

Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру.

Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу. Распознавание человека происходит на расстоянии.

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время начинается выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.

Идентификация по ладони рук

В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях .

Физическая защита данных

Для обеспечения большей скорости чтения, записи и надежности хранения данных на жестких дисках используются RAID-массивы (Redundant Arrays of Independent Disks - избыточный массив независимых дисков). Несколько жестких дисков подключаются к RAID -контроллеру, который рассматривает их как единый логический носитель информации.

Защита от вредоносных программ

Вредоносная программа (буквальный перевод англоязычного термина **Malware**, **mal***icious* — злонамеренный и ***soft*ware** — программное обеспечение, жаргонное название — «малварь», «маловарь», «мыловарь» и даже «мыловарня») — злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями.

Вредоносные программы: вирусы, черви, троянские и хакерские программы; шпионское, рекламное программное обеспечение; потенциально опасное программное обеспечение.

Защита от вредоносных программ

Современные антивирусные программы обеспечивают ***комплексную защиту программ*** и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер: Интернет, локальная сеть, электронная почта, съемные носители информации.

Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты.

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Киберпатруль

Управление «К» действительно существует в системе МВД, и не просто существует, но и эффективно работает. Его сектор деятельности — преступления в сфере информационных технологий: Интернета, мобильной связи, пластиковых карт. Сегодня подразделения Управления «К» работают в 80 субъектах РФ, и ни одно преступление в данной области не раскрывается без их участия.

Сфера деятельности

1. Преступления в сфере компьютерной информации: всевозможные мошенничества с использованием Интернета, хакерские атаки, распространение программ-вредителей.
2. Преступления в сфере телекоммуникаций, например, участившиеся телефонные мошенничества.
3. Преступления, связанные с незаконным распространением радиоэлектронных и специальных технических средств для негласного получения приватной информации.
4. Нарушения авторских и смежных прав в информационной сфере. Наиболее яркий пример — пиратская продукция: CD и нелегальное программное обеспечение.
5. Борьба с распространением порнографических материалов с участием несовершеннолетних.

СПАСИБО ЗА ВНИМАНИЕ!