Белорусский государственный университет информатики и радиоэлектроники

Кафедра РЭС

**РЕФЕРАТ**

**На тему:**

**«Защита от несанкционированной аудиозаписи. Защита компьютерной информации. Криптографические методы защиты данных»**

МИНСК, 2008

Защита от несанкционированной аудиозаписи. Обнаружители диктофонов

Диктофон может быть использован как в качестве закладного подслушивающего устройства, так и для негласной записи доверительных бесед какой-либо из заинтересованных сторон.

**Обнаружение диктофонов**

Задача обнаружения диктофонов решается с применением: металлодетекторов; нелинейных радиолокаторов; устройств рентгеноскопии; специальных детекторов диктофонов.

Обнаружение диктофонов с помощью металлодетекторов , вследствие их ограниченной чувствительности к современным микрокассетным и цифровым диктофонам может рассматриватся только как вспомогательное средство в комплексе с другими более эффективными мероприятиями по обнаружению и подавлению средств звукозаписи.

**Нелинейные радиолокаторы** способны обнаруживать диктофоны на значительно больших расстояниях, чем металлодетекторы, и могут использоваться для контроля за проносом устройств звукозаписи на входах в помещения. Но возникают проблемы уровня безопасного излучения, идентификации отклика, наличия «мертвых» зон, совместимости с окружающими системами и электронной техникой

**Устройства рентгеноскопии** позволяют надежно выявить наличие диктофонов, но только в проносимых предметах. Очевидно, что область применения этих средств контроля крайне ограничена, так как они практически не могут использоваться для целей личного досмотра и скрытого контроля.

**Специальные устройства для определения наличия работающих диктофонов**.

Работают на эффекте:

* обнаружения акустических сигналов от аналоговых диктофонов (шум лентопротяжного механизма и щелчки при нажатии на кнопки);
* выявления побочных электромагнитных излучений (ПЭМИ от генератора стирания - подмагничивания (ГСП)). Но используемый частотный диапазон характеризуется большим количеством источников мощных магнитных полей (телевизоры, контактная сеть городского транспорта, лампы дневного света, электродвигатели бытовых приборов и т. д.), которые эффективно «глушат» излучения диктофонов. Кроме того, Многие из современных диктофонов иностранного производства вообще не имеют ГСП. Стирание обеспечивается постоянным магнитом, а подмагничивание - так называемой «постоянной составляющей».
* обнаружение побочных излучений, возникающих в результате самовозбуждения электронного устройства из-за паразитных связей в генераторных и усилительных каскадах, например, микрофонного усилителя. Однако измерения показывают, что дальность возможной регистрации ПЭМИ такого рода (в диапазоне 20 кГц... 50 Мгц) не превышает нескольких сантиметров для бытовых средств звукозаписи, а от специальных устройств с металлическим корпусом вообще не регистрируются даже высокочувствительными лабораторными приборами.
* регистрация переменного магнитного поля, возникающего при работе электродвигателей. В лаборатории они работают очень четко, но на практике главной трудностью их реализации является наличие большого числа источников низкочастотных магнитных полей, разнообразие спектральных портретов излучений диктофонов разных типов, низкие уровни сигналов. Металлические корпусадиктофонов уже не являются препятствием для обнаружения полей данного типа.

В общем виде аппаратура обнаружения диктофонов включает в себя следующие блоки:

• низкочастотную магнитную антенну, выполненную конструктивно как отдельный элемент и выносимую как можно ближе к предполагаемому месторасположению диктофона;

• детекторный блок, выполняющий операцию обнаружения ПЭМИ, с регулируемым порогом срабатывания;

• фильтры, ограничивающие полосу частот, в которых осуществляется контроль; иногда добавляют и режекторные (то есть «закрывающие» определенные диапазоны) фильтры, настроенные на частоты наиболее мощных источников местных помех (как правило, они конструктивно выполнены в детекторном блоке);

• устройства световой (шкала светодиодов, стрелочный индикатор, контрольная лампочка) и звуковой (вибрационной) индикации наличия ПЭМИ (конструктивно выполняются или в детекторном блоке, или выносятся на специальный пульт);

• блок питания.

Устройства подавления записи работающих диктофонов

Существуют следующие виды воздействия на диктофоны:

• на сам носитель информации, то есть на магнитную ленту;

• на микрофоны в акустическом диапазоне;

• на электронные цепи звукозаписывающего устройства.

Первый способ нашел применение в устройствах типа размагничивающей арки, которая устанавливается в тамбуре входной двери и создает мощное переменное магнитное поле (обычно с частотой сети или ей кратной). В результате, находящиеся в тамбуре предметы (в том числе и кассеты с записанной информацией) размагничиваются. Устройства характеризуются высоким энергопотреблением и опасны для здоровья, особенно тех лиц, которые пользуются различного рода внедренными в организм электронными стимуляторами.

Второй способ может осуществляться как:

• воздействие на микрофон в ультразвуковом диапазоне с целью перегрузки микрофонного усилителя;

• использование генератора активных акустических помех в речевом диапазоне.

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения -около 20 кГц), воздействующие непосредственно и на микрофоны диктофонов, и акустические закладки, что является их несомненным достоинством. Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты, стоящего сразу после акустического приемника. Перегрузка усилителя приводит к значительным искажениям записываемых (передаваемых) сигналов, часто до степени, не поддающейся дешифровке.

Например, комплекс «Завеса», при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 м3. Однако системы ультразвукового подавления имеют важный недостаток: эффективность их резко снижается, если микрофон диктофона или «закладки» прикрыть фильтром из специального материала или в усилителе с низкой частотой установить фильтр низких частот с граничной частотой 3,4...4 кГц.

Вторая группа средств подавления, использующая генераторы активных акустических помех в речевом диапазоне, применяется в ограниченных случаях из-за неудобств, создаваемых доверительному разговору между партнерами под аккомпанемент генератора шума мощностью в 75... 90 дБ.

Третий способ - воздействие на электронные цепи диктофона, получил наибольшее распространение на практике.Принцип действия таких устройств основан на генерации в дециметровом диапазоне волн электромагнитных колебаний, несущая которых модулирована шумоподобным или хаотическим импульсным сигналом. Излучаемые направленными антеннами помехи, воздействуя на элементы электронной схемы диктофона, вызывают в них шумоподобные наводки. Вследствие этого одновременно с речью осуществляется запись и шума.

## Защита компьютерной информации.

**Аппаратные средства защиты компьютерной информации** *—* это различные электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д. Основные функции аппаратных средств защиты:

• запрещение несанкционированного (неавторизованного) внешнего доступа (удаленного пользователя, злоумышленника) к работающей автоматизированной информационной системе;

• запрещение несанкционированного внутреннего доступа к отдельным файлам или базам данных информационной системы, возможного в результате случайных или умышленных действий обслуживающего персонала;

• защита активных и пассивных (архивных) файлов и баз данных, связанная с необслуживанием или отключением автоматизированной информационной системы;

• защита целостности программного обеспечения.

Эти задачи реализуются аппаратными средствами защиты информации с использованием метода управления доступом (идентификация, аутентификация и проверка полномочий субъектов системы, регистрация и реагирование). Для работы с особо ценной информацией фирмы — производители компьютеров могут изготавливать индивидуальные диски с уникальными физическими характеристиками, не позволяющими считывать информацию. При этом стоимость компьютера может возрасти в несколько раз.

**Аппаратно-программные средства защиты (А-ПСЗ) информации.**

**Аппаратно-программные средства защиты информации** *—* средства, содержащие в своем составе элементы, реализующие функции зашиты информации, в которых программные (микропрограммные) и аппаратные части полностью взаимозависимы и неразделимы.

Данные средства защиты широко используются при реализации методов аутентификации пользователей автоматизированной информационной системы.

На практике используются следующие методы аутентификации: по знаниям, no имуществу, по навыкам и по уникальным параметрам.

В аутентификации по знаниям обычно используется механизм паролей — для того, чтобы подтвердить свои права на доступ, достаточно сообщить системе секретный ответ на ее запрос. Преимущества данного метода — простота реализации и дешевизна, недостаток - невысокая надежность. Если злоумышленник каким-либо образом узнал пароль, то система не сможет отличить его от легального пользователя.

При аутентификации по имуществу для подтверждения своих прав необходимо предъявить системе некий «ключ» — предмет, уникальный для каждого пользователя и защищенный от подделки (например, магнитную или smart-карту). Преимущество данного метода — относительно невысокая стоимость реализации, недостатки — требование наличия дополнительного оборудования и трудности в управлении масштабными системами зашиты на основе этого метода.

В случае аутентификации по навыкам системе необходимо продемонстрировать какие-то умения, недоступные для других пользователей и плохо поддающиеся подделке (например, клавиатурный почерк). К преимуществам такого метода можно отнести возможность сокрытия процесса аутентификации пользователя (например, он может и не подозревать о том, что в данный момент система проверяет его манеру печатания на клавиатуре) и высокую надежность аутентификации, к недостаткам — сложность реализации и дороговизну, а также необходимость в дополнительном оборудовании и больших вычислительных ресурсах.

Аутентификация по уникальным параметрам использует сравнение каких-либо параметров человеческого тела (отпечатки пальцев, характеристики ладони, геометрия ладони руки, речь, сетчатка глаза, характеристики почерка) с их цифровыми образами, записанными в память системы, и является самым надежным методом проверки. Преимущество этого метода состоит в высокой надежности аутентификации пользователя, недостатки — в высокой цене и необходимости наличия дополнительного оборудования.

Существуют программно-аппаратные средства обеспечивающее блокировку доступа к файлу с секретной информацией а также уничтожение той программы, которая обеспечивает несанкционированный запрос к данному файлу

### Криптографические методы защиты данных

**Криптографические** методы защиты данных *—* это методы защиты данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием или выработкой имитовставки.

Задачи шифрования:

- Противник, перехвативший сообщение, без таких затрат времени и средств, которые сделают эту работу не целесообразной, не может восстановить сообщение;

- Получатель может прочесть то, что получил.

**Шифрованием** называется некоторое обратимое однозначное преобразование данных, делающее их непонятными для неавторизованных лиц. Специалисты считают, что шифрование является одним из самых надежных средств обеспечения безопасности данных. Метод защиты информации шифрованием подразумевает обязательное выполнение следующих требования – никто, кроме хозяина данных, и лиц, которым разрешен доступ к этим данным, не должен знать самого алгоритма преобразования данных и управляющих данных для такого алгоритма (ключей).

Основными криптографическими методами защиты информации шифрованием являются следующие:

• шифрование с помощью датчика псевдослучайных чисел;

• шифрование с помощью криптографических стандартов шифрования данных (с симметричной схемой шифрования), использующих проверенные и апробированные алгоритмы шифрования данных, например американский стандарт шифрования данных DES, отечественный стандарт — ГОСТ 28147-89;

• шифрование с помощью систем с открытым ключом (с асимметричной схемой шифрования), в которых для шифрования данных используется один ключ, а для расшифровки — другой. Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы. Второй ключ является секретным и используется получателем зашифрованной информации для ее расшифровки. Примерами могут служить методы RSA, PGP криптографической защиты информации с известным ключом.

* зашифровка информации в изображении и звуке – стенографический продукт, позволяющий прятать текстовые сообщения в файлы .bmp, .gif, .wav – маскировка криптографии;
* зашифровка с помощью архиваторов Arj, Rar, WinZip//;
* защита паролем документов МS Office – не ПОЛЬЗУЙТЕСЬ НИКОГДА!
* Защита данных с помощью программы NDEC – многоступенчатое полиморфное кодирование с использованием двух ключей. Пользователи этого метода должны при шифровании и расшифровке вводить два пароля не больше 256 символов.
* Защита данных с помощью программы «Кобра»
* Защита дискет с помощью программы DiskHide – программа делает записанную дискету «ПУСТОЙ»;
* Защита жестких дисков с помощью программы DestCrypt – шифрует диск и дискеты;

Использование криптографической техники многие эксперты по компьютерной безопасности считают основным, если не последним бастионом защиты от вирусной инфекции, во всяком случае, применение шифрования может сильно затруднить распространение вирусов. Это относится к любым вирусам, присутствие которых криптографические программы могут обнаружить по изменениям контрольных сумм файлов и других характеристик. С другой стороны, эта защита срабатывает, как правило, после того, как заражение уже состоялось, и создает определенные неудобства пользователям, а также персоналу, ответственному за обеспечение безопасности.

Так как расшифровка возможна только в том случае, когда зашифрованные данные не были искажены, криптографическую защиту можно использовать для обеспечения целостности данных. Если захватчик как-либо исказил (модифицировал) зашифрованные данные, то факт нарушения безопасности будет выявлен при первой же попытке расшифровки, поскольку в расшифрованных данных появятся искаженные участки.

Следует отметить, что при всей привлекательности и трудности преодоления защита с помощью шифрования обладает некоторыми негативными чертами, которые в нашей стране особенно существенны. Применение этого уровня защиты означает для персонала (имеется в виду персонал, ответственный за обеспечение секретности) новую жизнь, полную жестко регламентированных предопределенных действий. Необходимо обеспечить ежедневную службу резервирования информации, поскольку ошибки в чтении отдельных секторов или кластеров защищенной шифрованием области могут приводить к потере информации из всей области. Отсюда повышенные требования к качеству дисков, на которых расположена шифрованная область; абсолютные требования к качеству и регулярности службы резервирования информации; повышенный риск, по меньшей мере, дополнительные потери времени на восстановление информации в случае сбоев. Эти факторы существенны при работе с любым программным обеспечением или аппаратурой, обеспечивающей криптографический уровень защиты данных. Рекомендовать применение такой защиты можно только при наличии качественного, надежно работающего оборудования, организации надежной, автоматической службы резервирования информации и наличии действительной потребности в столь сложной защите данных.

**ЛИТЕРАТУРА**

1. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С.Барсуков. – М., 2001 – 496 с.
2. Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.
3. Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.
4. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия –Телеком, 2000. - 452 с., ил
5. Компьютерная преступность и информационная безопасность / А.П.Леонов [и др.]; под общ. Ред. А.П.Леонова. – Минск: АРИЛ, 2000. – 552 с.