БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра информатики

Факультет НиДО

Специальность ИиТП

Контрольная работа № 2

по дисциплине «Основы защиты информации»

Выполнил студент: Дегтярев А.А.

группа 393551

Зачетная книжка № 902021-26

Минск 2016

**Электромагнитная маскировка**

Электромагнитная маскировка(зашумление) применяется в случаях, когда пассивные методы не обеспечивают в достаточной степени затухание сигнала на определенной территории. Либо в случаях, когда пассивный механизм не удовлетворяет каким-либо иным требованиям. Суть метода достаточно понятна из его названия: создание активных помех, маскирующих целевой сигнал.

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий - линейное зашумление.

В обоих случаях предполагается применение генераторов шумов, различающихся принципами формирования маскирующих помех. В качестве маскирующих используются случайные помехи с нормальным законом распределения спектральной плотности мгновенных значений амплитуд (гауссовские помехи) и прицельные помехи, представляющие собой случайную последовательность сигналов помехи, идентичных побочным сигналам.

В простейшем случае **система линейного зашумления** состоит из генератора шумового сигнала подключенного в зашумляемую токопроводящую линию, формирующего маскирующее напряжение в заданном спектре, времени и другими характеристиками. Это значительно затрудняет злоумышленникам выделять наведенные сигналы.

На практике наиболее часто подобные системы используются для зашумления линий электропитания.

Системы **пространственного зашумления**, как следует из названия, применяются для создания помех в окружающем пространстве. Там также используются генераторы шумового сигнала, усилители, антенны, устройства коммутации и контроля. Цель использования таких устройств – добиться определенного снижения уровня сигнал/шум на границе контролируемой территории. Применяется *локальное пространственное зашумление* для защиты конкретного элемента системы и *объектовое пространственное зашумление* для защиты от побочных электромагнитных излучений всего объекта. При *локальном пространственном зашумлении* используются прицельные помехи. Антенна находится рядом с защищаемым элементом. *Объектовое пространственное зашумление* осуществляется, как правило, несколькими генераторами со своими антеннами, что позволяет создавать помехи во всех диапазонах побочных электромагнитных излучений всех излучающих устройств объекта.

В системах пространственного зашумления в основном используются помехи типа "белого шума" или "синфазные помехи", последние, в основном применяются для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ.

При использовании систем пространственного стоит помнить, что наряду с помехами средствам разведки создаются помехи и другим радиоэлектронным средствам (телевидения, радиосвязи и т.д.). Кроме того, уровни помех, создаваемые системой зашумления, должны соответствовать санитарно-гигиеническим нормам.

**Принципы криптографической защиты информации.**

**Криптография** – это наука о методах, алгоритмах, программных и аппаратных средствах преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования. Изначально криптография использовалась исключительно как средство обеспечения конфиденциальности сообщений, применялась в военной, дипломатической сфере. Естественно она находилась в руках спецслужб; В конце же 20ого века обстановка немного сменилась. В большей степени она была связана с развитием вычислительной техники, и огромным скачком в вопрос взлома старых алгоритмов и создания новых. В этот же момент частные компании стали интересоваться этой темой, не только для обеспечения конфиденциальности, но и для аутентификации субъектов, подтверждения истинности документов и т.д. Криптография, которая обслуживает задачи бизнеса, телекоммуникаций и управления называется **открытой**. Данные технологии становятся коммерческим продуктом и применяются в широком спектре продуктов и услуг. Существует задача анализа стойкости используемых криптопреобразований, и она решается наукой, называемой криптоанализ*.***Криптография** и **криптоанализ** вместе составляют науку - **криптологию**.

Ниже представлена схема общей криптографической системы, обеспечивающей шифрование передаваемой информации;

Отправитель генерирует открытый текст исходного сообщения(М), которое шифруется с помощью обратимого преобразования, и на выходе дает шифр текст(С), который передается получателю. Получатель расшифровывает его с помощью обратного преобразования и получает исходное сообщение М.

Преобразование - называется криптоалгоритмом. Параметр, который определяет конретное преобразование называется криптографическим ключом(К). Система зашифровывания и расшифровывания называется **криптосистемой**. Выделяют два больших класса криптосистем(симметричные и ассиметричные) огда их называют: одноключевые (с секретным ключом) и двухключевые (с открытым ключом) Во втором случае схемы выглядит так: 

В такой системе ключ К1 – откртый К2 – секретный.

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например, спецсвязью. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют в месте его генерации.  
 Любая попытка со стороны злоумышленника расшифровать шифротекст для получения открытого текста или зашифровать свой собственный текст для получения правдоподобного шифротекста в отсутствии подлинного ключа, называется **криптоатакой.** Чем лучше система противостоит такой атаке, тем более **криптостойкой** она считается. Измеряется затратами атакующего на взлом(в количестве машиновремени, затраченного на взлом).

Существует 4 основных типа криптоаналитических атак. Предполагается, что известен применяемый алгоритм и имеются шифротексты сообщений.  
  
1) **Криптоаналитическая атака при наличии только из­вестного шифртекста.** Криптоаналитик имеет только несколько шифротекстов зашифрованных одним и тем же алгоритмом, задача вычислить ключ, использованный в шифраторе.

2) **Криптоаналитическая атака при наличии только из­вестного открытого текста.** В таком случае криптоаналитик имеет доступ еще и к нескольким открытым текстам, опять же стоит задача в нахождения ключа или алгоритма расшифровывания.  
  
3) **Криптоаналитическая атака при возможности выбора открытого текста**

В данном случае аналитик имеет возможность выбирать открытые тексты, которые затем получает в зашифрованном виде. Это позволет выбрать оптимальные блоки текста, которые дадут больше информации о ключе.

4) **Криптоаналитическая атака при с адаптивным выбором открытого текста** Это особый вариант, который дополнительно позволяет изменять выбор в зависимости от результатов предыдущего шифрования.

Также всегда существует силовая атака(brute force) которая просто заключается в переборе возможных значений ключа. Она может быть довольно эффективной при наличии словаря возможных ключей или определенными спецификациями ключа.

Применение шифрования ко всему сообщению в целом используется редко, почти все применяемые криптографические методы связаны с разбиением сообщения на большое число фраг­ментов фиксированного размера, каждый из которых шифруется отдельно.

Исходя из данного подхода можно выделить следующие признаки методов шифрования:

-Выполнения побитовых/поблочных операций

-Зависимость/независимость от результатов предыдущего шифрования

-Зависимость/независимость отдельных знаков от их положения

Отсюда и различают три основных способа шифрования

-Поточные

-Блочные

-Блочные с обратной связью

**Поточные** шифры преобразуют каждый бит открытого текста и бит ключа по определенному алгоритму. Это делает его довольно быстрым, простым в реализации. Однако для каждого сообщения необходимо использование нового ключа, иначе сообщения будет довольно легко расшифровать. Часто используют дополнительный случайный ключ, который передается в начале сообщения и применяется для модификации ключа шифрования, однако это требует передачи информаци синхронизации перед началм сообщения;  
  
**Блочные шифры** преобразуют текст по равным блокам. Каждый бит блока шифротекста зависит от значений всех битов соответствующего блока открытого текста; Никакие два блока открытого текста не могут быть представлены одним и тем же блоком шифротекста. Блочный шифр имеет серьезный недостаток, в случае использования небольшого размера блока, можно легко расшифровать сообщение «со словарем».   
  
Крипто система с открытым ключом, тоже является блочной, и оперирует блоками довольно большой длинны.  
  
**Блочное шифрование с обратной связью** аналогично блочному шифрованию, где шифрующая функция помимо ключа еще зависит от одного или более предшествующих блоков шифротекста; Достоинством этого подхода является возмодность обнаружения манипуляций сообщениями. При этом используется факт размножения ошибок. Такие системы используются не только для шифрования сообщений, но и для аутентификации. Основным недостатком данной системы явялется фактор размножения ошибок, так же разработка и реализация таких систем более трудоемки, чем системы поточного шифрования.  
  
Немного хотелось бы рассказать и о нескольких типов шифров:  
 - Перестановки

- Замены

- Гаммирования

- Основанные на аналитических преобразованиях данных

Шифры **перестановки** работают на перестановке символов шифруемого текста по определенному правилу, возможно внутри блока или всего текста. При использовании сложного неповторящегося порядка перестановку, можно добиться вполне приличных результатов стойкости шифра

Шифрование **заменой** заключается в замене символов шифруемого текста другими символами того же или иного алфавита в соответствии с заранее обусловленной схемой.

Шифрование **гаммированием** заключается в том, что сиволы исходного текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость определяется в основном длиной неповторяющейся части гаммы. Этот способ является одним из основных для шифрования информации в автоматизированных системах, так как эвм позволяют генерировать почти бесконечную гамму шифра, что делает его очень криптоустойчивым.

Шифрование **аналитическим преобразованием** заключается в том, что исходный текст преобразуется по некоторому аналитическому правилу.

Эффективными системами криптозащиты данных являются **асимметричные криптосистемы**, называемые также криптосистемами с открытым ключом. В асимметричной криптографии применяются так называемые ключевые пары из двух связанных между собой ключей. Один из них — закрытый, известен только владельцу ключа. Другой ключ — открытый, публично доступный любому желающему.

Для зашифрования текста применяется открытый ключ адресата, для расшифрования — закрытый. Таким образом, зашифровать сообщение может любой человек, а расшифровать — только владелец соответствующего закрытого ключа, т.е. адресат. Проблема асимметричной криптографии состоит в том, что зашифрование по асимметричным алгоритмам происходит намного медленнее, чем по симметричным. Кроме того, если зашифрованный текст предназначен для нескольких адресатов, в отправляемое сообщение приходится включать копию текста для каждого адресата, что резко увеличивает как объем сообщения, так и время, необходимое для его зашифрования.

Эта проблема решается с помощью так называемой **гибридной криптографии**. В таком случае используется одноразовый ключ шифрования на сессию. Он используется как для шифрования так и для расшифровки. Сообщение шифруется симметрично, а уже ключ сессии передается зашифрованным по ассимитричному алгоритму.

**Практическая часть**

**Контрольное задание.** Защита речевой информации от утечки по акустическому каналу пассивными методами.

***Задание 1*.** Для защиты речевой информации ограниченного доступа при проведении переговоров компания, арендующая свои производственные площади, использует специальное помещение – защищённый служебный кабинет (ЗСК). Двери и окна ЗСК надёжно защищены от прослушивания техническими средствами защиты информации. Однако кирпичная перегородка, отделяющая ЗСК от незащищённого коридора, не арендуемого компанией и допускающего возможность проникновения в него злоумышленников, имеет толщину всего в полкирпича. Размеры перегородки 10×3 м. Размеры одинарного силикатного кирпича по СТБ 1160-99 «Кирпич и камни керамические. Технические условия» составляют 250×120×65 мм.

Используя данные табл.1, определить стоимость дополнительной кирпичной кладки, усиливающей звукоизоляцию стены для обеспечения затухания *Q* информационного сигнала в стене на частоте 1000 Гц до уровня не менее:

61 дБ – для варианта 2,

при стоимости кирпича 250 $ за кубометр и при стоимости кирпичной кладки 25 $ за кубометр. Толщиной швов между кирпичами, потерями кирпича на бой и другие цели, стоимостью других работ и материалов при усилении звукоизоляции стены в первом приближении пренебречь.  
  
**Решение:** Используя табличные значения в приложении – получим текущий уровень затухания для стены с кладкой в полкирпича. Для 1000гц – это 48дб.

Цель добиться уровня затухания в 61дб для 1000гц, что обеспечивается кладкой в 1.5 кирпича, как указано в таблице. Следовательно задачей будет нарастить кладку до толщины в 1.5 кирпича.

Общий объем наращённой кладки 1 кирпич:

Стоимость дополнительной кирпичной кладки с учетом стоимости работ и материалов ($250+$25 =$275) составит:

***Задание .2.*** Используя формулу (2) и табл. 1, определить для своего варианта задания 1, во сколько раз сила звука в коридоре при использовании обсчитанного Вами варианта кирпичной кладки будет больше или меньше при установке не кирпичной перегородки, а перегородки из материала:

древесностружечная плита (ДСП), толщина 30 мм –вариант 7

Для задания 1 обсчитывалась кладка толщиной в 1.5кирпича, обеспечивающая затухание сигнала в 1000гц до 61дб

При использовании древесностружечной плиты толщиной в 30см получим затухание в 26дб на частоте в 1000гц. (используя данные табл 1)

Разница в 35дб

Из формулы (2)

Ответ: Будет больше в ~3162 раза

Таблица 1 – Звукоизоляция стен и сплошных перегородок

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Вид конструкции | Толщина конструкции | Среднее значение *Q*, дБ, для среднегеометрической частоты, Гц | | | | |
| 50 | 500 | 1000 | 2000 | 4000 |
| Кирпичная кладка, оштукатуренная с двух сторон | 0,5 кирпича  1 кирпич  1,5 кирпича  2 кирпича  2,5 кирпича | 40  44  48  52  55 | 42  51  55  59  60 | 48  58  61  65  67 | 54  64  65  70  70 | 60  65  65  70  70 |
|
| Железобетонная панель | 100мм  160 мм  300мм  400мм | 40  47  50  55 | 44  51  58  61 | 50  60  65  67 | 55  63  65  70 | 60  63  65  70 |
|
| Гипсобетонная панель | 86 мм | 33 | 39 | 47 | 54 | 60 |
| Керамзитобетонная панель | 80мм  120мм  140мм | 34  37  43 | 39  39  47 | 47  47  53 | 52  54  57 | 60  51  61 |
| Шлакоблоки, оштукатуренные с двух сторон | 220мм | 42 | 48 | 54 | 60 | 63 |
| Древесностружечная плита | 30 мм | 26 | 26 | 26 | 26 | 26 |

**Источники**  
http://www.analitika.info/  
<http://sumk.ulstu.ru/docs/mszki/Zavgorodnii/>

<http://www.cryptocom.ru/articles/crypto.html>

<http://ypn.ru/category/data-protection-technologies/principles-of-cryptographic-protection/>

http://ypn.ru/187/introducing-to-cryptographic-information-protection/