3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 621.96

СОВРЕМЕННЫЕ МЕТОДЫ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ ПУТЕМ ПРОГРАММНОГО УПРАВЛЕНИЯ ИЗЛУЧЕНИЕМ КОМПЬЮТЕРА

Сергей Чеховский
ООО ЕПОС

Аннотация: **Обобщаются результаты исследований, проводимых фирмой ЕПОС по защите информации от утечки по каналам паразитных электромагнитных излучений и наводок. Показано, что для скрытой передачи разведанной информации могут применяться методы стеганографии. Наиболее перспективным способом скрытой передачи информации является программное управление излучением компьютера.**
Summary: **This paper presents the results of research of EPOS Ltd. in information security and TEMPEST. We have shown that for latent transmission of revealed information can be used steganographic methods. The most prospective method for latent transmission of information is software-controlled computer emissions.**
Ключевые слова: **Информация, информационная безопасность, техническая защита информации.**

Методы проникновения в сеть и последующей кражи информации достаточно хорошо известны. Наиболее действенным является внедрение в систему программы-закладки. В зависимости от поставленных целей программа-закладка может, например, перехватывать пароли пользователей или по определенному критерию находить необходимую информацию на жестких дисках. В дальнейшем собранная информация отправляется по электронной почте на заранее обусловленный адрес. Соответственно, все системные администраторы принимают определенные меры по пресечению подобных попыток. Это заставляет придумывать новые методы проникновения в сеть или совершенствовать известные.

Самыми трудными действиями в процессе хищения информации являются установка программы-закладки («троянского коня») и передача разведанной информации. В эти моменты разведывательную деятельность проще всего обнаружить. Причем, чем больше объем внедряемой программы или объем передаваемых такой программой данных, тем выше вероятность того, что разведывательная деятельность будет обнаружена и пресечена. Необходимость скрывать факт передачи сообщения неминуемо приводит к внедрению злоумышленниками методов стеганографии (скрытной передачи данных).

I Компьютерная стеганография

Компьютерная стеганография – это часть стеганографии, которая занимается вопросами реализации стеганосистем с использованием компьютерной техники.

Поскольку цифровая информация обычно передается в виде файлов, то в компьютерной стеганосистеме используются понятия файл-контейнер и файл-сообщение. Для того, чтобы посторонние не заподозрили факт передачи сообщения файл-сообщение особым образом (при помощи стеганоключа) «смешивают» с файлом-контейнером. При этом, как и принято в «классической» стеганографии, файл-контейнер должен выглядеть вполне безобидно, а подмешивание секретной информации не должно изменять его основных свойств.

Компьютерная стеганография может использовать только ей присущие специфические методы, основанные, например, на использовании специальных свойств компьютерных форматов. Не очень сложные компьютерные стеганосистемы уже реально применяются злоумышленниками (в частности, создателями вирусов).

Известен, например, вирус, имеющий кодовое название «W32/Perrun». Этот вирус «прячет» свое тело объемом 18 К в файле *.jpg. Точнее говоря, он просто добавляет свой код в конец *.jpg файла. С точки зрения стеганографии (впрочем, и с точки зрения вирусологии) это весьма примитивный вирус. Но он показывает метод, как внедрить в систему программу-закладку большого объема. Нужно сделать эту программу двухкомпонентной. Стартовая часть, которая только ищет основное тело программы в других

файлах, может быть очень маленькой, что облегчает ее внедрение. Объем же основной части программы может быть очень большим, и при этом риск ее обнаружения может быть сведен к минимуму.

Более сложный механизм маскировки реализован создателем вируса Win95.CIH. Этот вирус внедряется в *.exe файл, используя особенности формата PE (Portable Executable), принятого в системе Windows начиная с Windows 95. В Windows исполнимый файл *.exe может содержать не только код, но и многочисленные дополнительные данные. Это пиктограммы, различные служебные данные и дополнительная информация, например, об экспортируемых и импортируемых функциях. Каждый вид данных, содержащихся в файле формата PE, – это отдельный объект. Для хранения всех объектов файл формата PE разбивается на ряд секций фиксированного размера. Каждый объект начинается с новой секции. Если объект не занимает всего объема секции, то эта часть секции не используется. Поэтому в файле формата PE всегда достаточно свободного места (рис. 1).

Больше всего свободного места в первой секции, в которую записывается только заголовок файла (PE header). В эти свободные места можно упрятать достаточно много информации, и при этом размер файла не изменится и работоспособность файла не нарушится.

Описанные выше примеры показывают возможность максимально скрыть процесс внедрения программы-закладки в компьютер. Результат работы внедренной программы – это найденные ею файлы. Файлы могут быть различных форматов и иногда очень большого объема. Для их скрытной передачи могут применяться и более совершенные методы компьютерной стеганографии, основанные на избыточности аудио-, фото- и видеоинформации. Действительно, младшие цифровые разряды таких файлов содержат мало полезной информации, и их изменение очень слабо влияет на качество исходного файла. Поэтому можно использовать младшие разряды для передачи скрытой информации без видимого искажения исходного файла. К тому же эти файлы сами по себе имеют большой объем, поэтому в них легче встроить большой объем скрываемой информации.

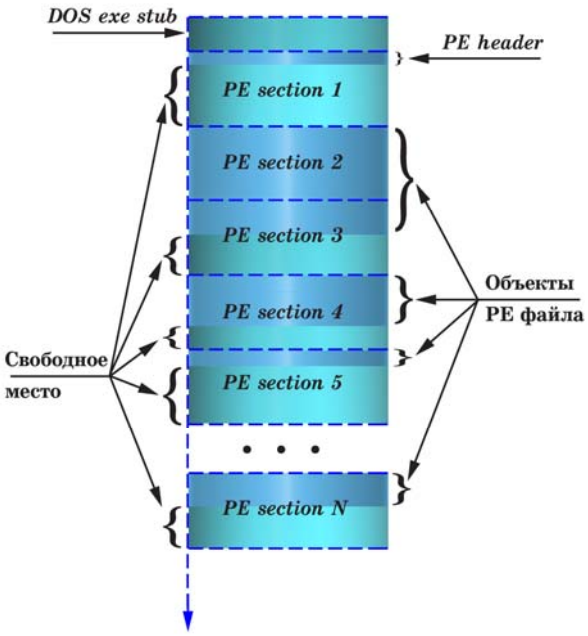

Рисунок 1 – Структура файла формата PE

Развитие методов компьютерной стеганографии не ограничилось только разработкой более совершенных способов, программ и алгоритмов встраивания сообщений, а и поиском каналов передачи информации.

Конечно, Интернет является очень удобным каналом для передачи разведанной информации, однако не всегда есть возможность воспользоваться им. Например, очень трудно скрытно передать информацию при использовании межсетевых экранов и жестком администрировании передачи информации. Тем более, что администратору системы, как правило, и не нужно просматривать каждый файл в поисках недозволенных вложений. Он анализирует адреса, в которые отправляется почта, и с каких узлов принимаются файлы. Как правило, этой информации достаточно, чтобы выявить подозрительные сообщения.

Поиск новых каналов передачи разведанной информации привел к идее побочных электромагнитных излучений и наводок (ПЭМИН).

II Soft Tempest – технология скрытой передачи данных по каналу побочных излучений компьютера

Давно известно, что утечка информации может происходить и по каналам ПЭМИН. Эти каналы неудобны только тем, что они неуправляемы. Чтобы получить нужную информацию требуется огромное время работы дорогостоящей аппаратуры. Ученым Кембриджа (Андерсону и Куну) пришла идея использовать в качестве канала передачи данных побочные излучения компьютера, но только сделать этот канал управляемым. Работа над этой идеей привела к рождению технологии Soft Tempest – технологии скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств [4].

Soft Tempest атака, предложенная Куном, позволяет с помощью специальной программы-закладки,

внедряемой с использованием стандартной техники применения «вирусов», «червей» и «троянцев», искать необходимую информацию в компьютере и передавать ее путем модуляции изображения монитора. Принимая побочные излучения монитора можно выделить полезный сигнал и таким образом получить секретную информацию, хранящуюся в компьютере – пароли, письма, документы.

Эта технология получила и второе название: ПЭМИН-вирус. Правда, название это весьма неточное. Оно только отражает тот факт, что программа-закладка, управляющая излучением компьютера (в частности, монитора) может быть внедрена в целевой компьютер, в том числе и с использованием технологии построения компьютерных вирусов.

Простейший способ Soft Tempest атаки, предложенный и опробованный Куном, использует амплитудную модуляцию экранного изображения и стандартный АМ-приемник. Поставленная цель – передать информацию путем управления излучением компьютера была достигнута. Однако, при передаче информации этим простейшим способом на экране монитора возникает характерное изображение, вид которого определяется частотой амплитудной модуляции (рис. 2).

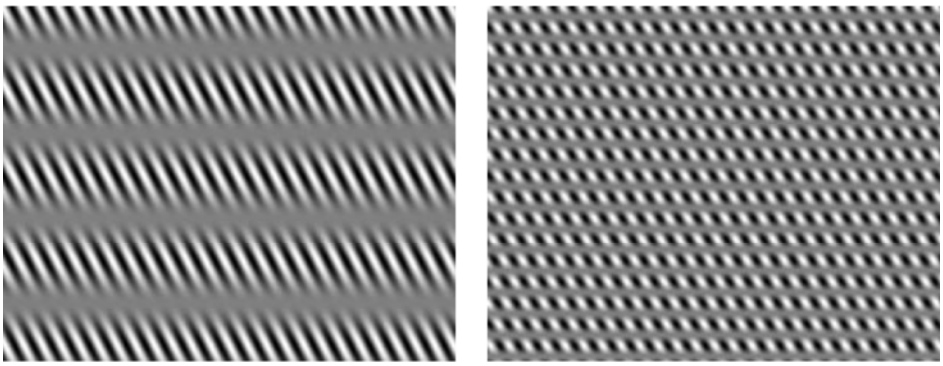

Рисунок 2 – Изображение на экране монитора при амплитудной модуляции тоном разной частоты

Подобную «рябь» на мониторе трудно не заметить. В принципе, модулировать можно не весь экран, а только его небольшую часть, но даже и в этом случае человек, увидев такую рябь на экране, может заподозрить что-то неладное. Таким образом, при передаче информации путем управления излучением монитора мы сталкиваемся с необходимостью решения задачи стеганографии в классической постановке, так называемой «проблемой заключенных» (как двум заключенным, Алисе и Бобу обменяться секретными письмами, если передавать почту они могут только через не в меру любопытного охранника Вилли).

Кун решил задачу встраивания секретного сообщения, проанализировав особенности отображения информации на экране монитора и характеристик спектра излучаемых при этом побочных колебаний. Это позволило так подобрать характеристики управляющих сигналов, чтобы информация, излучаемая в эфир, отличалась от отображаемой на экране монитора. Причем, оказалось что это возможно не только для текстовой информации, но и для графической. На рис. 3 приведены фотографии из работы Куна и Андерсона. Слева – изображение, отображаемое на экране монитора, справа – черно-белое изображение, принимаемое контрольным приемником.

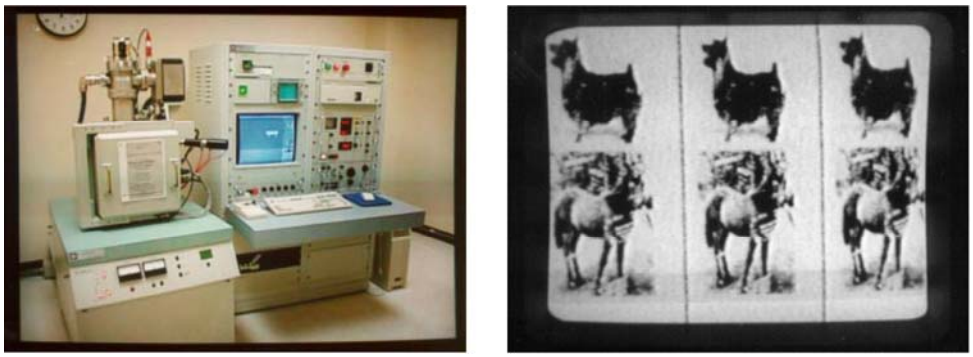

Рисунок 3 – Изображение, получаемое на экране монитора (слева) и на экране разведприемника

Если в качестве изображения, играющего роль стеганоконтейнера, выбрать «обои» рабочего стола, то такое изображение не вызывает подозрений у пользователя компьютера несмотря на то, что в это время в эфир излучается найденная программой-закладкой секретная информация. Более того, профессиональный разведчик в принципе может выбрать метод модуляции, при котором передаваемый сигнал будет оптимизирован для максимально надежного приема с помощью специального приемного и декодирующего оборудования.

Таким образом, можно скрытно передавать разведанную информацию путем программного управления излучением монитора.

Однако практическая реализация стеганосистемы с передачей информации через излучение монитора, скорее всего, окажется очень сложной. Во-первых, восстановление изображения по излучению монитора сопровождается значительными искажениями, вследствие чего встроенная информация может быть разрушена. Во-вторых, мы не можем управлять выбором изображения, используемого в качестве контейнера. И не можем управлять временем, когда выбранное в качестве контейнера изображение высвечивается на экране. Более того, модуляция изображения монитора может быть заметна оператору.

Таким образом, методы Soft Tempest атаки и компьютерной стеганографии с использованием ПЭМИН, предложенные учеными Кембриджа, имеют один существенный недостаток – для передачи полезного сигнала используется сигнал монитора, что требует выполнения определенных условий (оператор использует подходящую экранную заставку, передача возможна при перерывах в работе оператора и т. д.).

III ПЭМИН, порты и скрытая утечка информации

Описанные выше способы скрытия передаваемой развединформации основываются на методах, позволяющих обмануть контроль (оператора компьютера). Но самый лучший метод скрытой передачи информации – это передавать ее по каналу, который не охвачен контролем. В этом плане конечно лучше всего передавать разведанную информацию, используя радиоизлучения компьютера. Правда, описанный выше канал с использованием излучений монитора мало подходит на роль скрытого канала передачи, так как помимо излучения в эфир передаваемая информация всегда отображается и на мониторе. Но существуют и более простые способы управления излучением компьютера, чем вывод информации на монитор. Проведенный нами анализ показал, что обращение к любому устройству и даже к любому незадействованному порту вызывает появление побочных излучений на определенных, характерных для данного порта, частотах и с определенной мощностью. Поэтому ПЭМИН-вирусы могут существовать во множестве вариантов, в зависимости от того, какое конкретно устройство компьютера выбрано для управления излучением. При этом и программа – закладка может быть значительно проще, чем в рассмотренных выше случаях, так как и вывод в порт программно реализуется проще, чем формирование специальных кодов для модуляции луча трубки монитора, и не требуется применения стеганографических методов. Скрытность передачи обеспечивается тем, что сегодня отсутствуют штатные средства контроля излучений компьютера. Использование обычных сканирующих приемников типа AR3000 для целей контроля малоэффективно вследствие того, что компьютер излучает в широкой полосе частот, и отыскать в этой полосе частот ту, на которой осуществляется передача, очень сложно.

Нами был проведен эксперимент с программой-закладкой, имитирующей передачу данных в последовательный порт. Мы не стали создавать полноценный вирус типа «троянского коня», который ищет требуемую информацию на винчестере, дабы не выпускать джина из бутылки – нас больше интересовали особенности возникающего при этом паразитного излучения.

Интерес к последовательному порту вызван особенностью его конструктивного исполнения. Передача «1» и «0» осуществляется импульсами разной полярности с амплитудой более 5 вольт. Это позволяет предположить, что уровень излучений, вызванных передачей в порт информации, будет достаточно высоким, даже если к порту никакие устройства не подключены (соответственно, отсутствует более-менее эффективная антенна). Кроме того, последовательная передача легко перехватывается и интерпретируется. К тому же последовательный порт позволяет программно задавать скорость передачи, что важно для экспериментов.

Результаты измерения уровней излучения для случая, когда к порту не подключены никакие устройства и скорость передачи была установлена равной 9600 Кбит/с, приведены на рис. 4.

Нижняя линия, Uп, соответствует значениям уровня излучения компьютера при отсутствии передачи информации через излучение последовательного порта. Верхняя, Uс+п, - уровням излучения в моменты передачи информации.

Анализ приведенного графика показывает, что абсолютное значение уровня побочных излучений при выводе информации в незадействованный последовательный порт на отдельных частотах может быть весьма значительным. Однако, превышение этого уровня над уровнем остальных побочных излучений компьютера

во всем диапазоне частот остается небольшим. В лучшем случае можно рассчитывать на отношение сигнал/шум в 2...3 дБ.

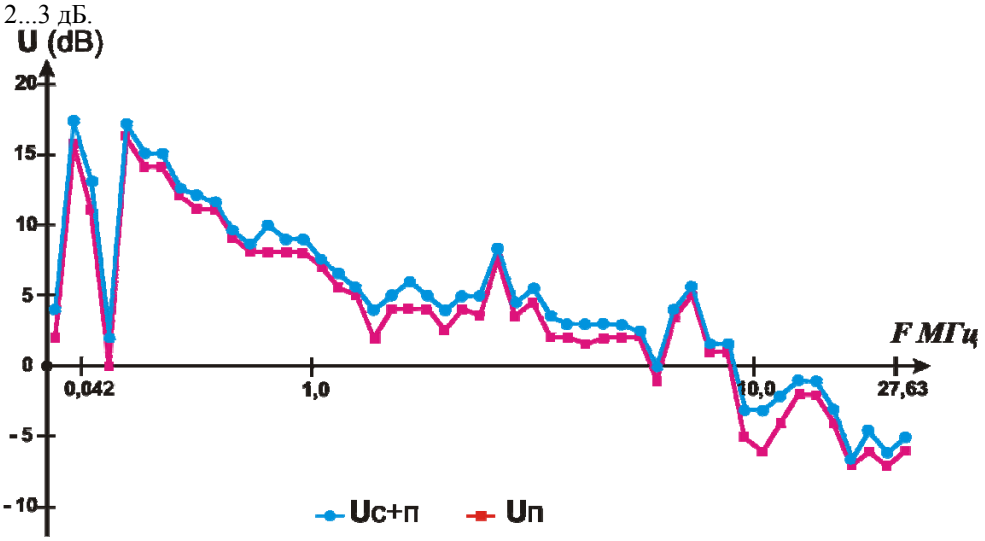

Рисунок 4 – Напряженность электрического поля, создаваемого излучением последовательного порта

Такая маленькая величина говорит о том, что обнаружить работу программной закладки, передающей информацию через побочные излучения последовательного порта, практически невозможно. А вот для разведчика, применяющего данный способ, проблема не стоит так остро. Ведь он знает, каким кодом он передает информацию. Знание вида кодирования передаваемой информации позволяет для повышения дальности разведки применять сложные технологии накопления периодического сигнала (когерентное и некогерентное накопление) или корреляционную обработку. Такие технологии очень хорошо отработаны и широко применяются в современных средствах передачи данных и радиолокационных станциях.

Эксперименты показали также, что изменяя скорость передачи данных в порт можно получить на отдельных частотах существенное превышение уровня излучения порта над уровнем излучения остальных элементов компьютера. Если к порту подключено какое либо устройство, то соединительный кабель играет роль антенны. В этом случае уровень излучения получается настолько высоким, что принимать информацию можно весьма примитивными средствами на значительном расстоянии. Этот эффект мы использовали, в частности, для демонстрации возможности управления излучением компьютера на выставке «Безпека 2002». Уверенный прием сигнала мы демонстрировали с помощью приемника AR3000A с его штатной штыревой антенной.

Рассмотренный эксперимент демонстрирует, что возможности метода передачи информации путем управления излучением портов компьютера по скрытию факта ее передачи значительно шире, чем просто использование неконтролируемого канала связи. Даже если мы установим радиомониторинг излучений каждого компьютера, мы не обнаружим работу программы – закладки, использующей для передачи разведанной информации незадействованные порты компьютера, если при передаче используются режимы, подобные рассмотренным в нашем эксперименте. Ведь это, фактически, метод радиосвязи с использованием скрытого излучения.

Методы скрытого излучения в радиосвязи основаны на том, что сложность аппаратуры приема сигналов с усложнением излучаемого сигнала растет медленнее, чем сложность аппаратуры разведки (перехвата) этих сигналов. В нашем случае можно предполагать, что сложность контрольной аппаратуры (для обнаружения факта передачи информации) имеет тот же порядок, что и приемная аппаратура нашего противника. Но для нас и эти затраты просто бессмысленны. Дешевле принять меры по подавлению всех излучений компьютера.

IV Выводы

Необходимо хорошо представлять опасность утечки информации по каналам побочных излучений и наводок. Современные методы разведки с использованием управления побочными излучениями компьютера позволяют разведать всю информацию, хранящуюся или обрабатываемую в компьютере и скрытно передать ее, не оставляя следов о факте передачи информации и о местонахождении разведчика.

Единственный метод защиты от утечки информации по каналам ПЭМИН – это применение компьютеров в защищенном исполнении. Причем качество защиты обязательно должно быть подтверждено лабораторией, имеющей соответствующий сертификат на право выполнения таких работ.

*Литература: **1.** Барсуков В. С. Безопасность: технологии, средства, услуги. – М.: КУДИЦ-ОБРАЗ, 2001 **2.** Генне О. В. Основные положения стеганографии // Защита информации. Конфидент, № 3, 2000 **3.** E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand. Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, In Information hiding: first international workshop, Cambridge, UK. Lecture Notes in Computer Science, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996. **4.** Markus G. Kuhn and Ross J. Anderson: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. (http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf)*

УДК 621.396

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ В ПАСИВНИХ ЕЛЕМЕНТАХ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

Михайло Прокофьєв, Андрій Тодоренко, Володимир Свірський*
НДЦ "ТЕЗІС" НТУУ "КПІ"
**НТУУ "КПІ"*

Анотація: **Розглянута проблема вибору покажчика призначення для оцінки захищеності інформації, яка циркулює в пасивних елементах локальних обчислювальних мереж, від витоку каналами побічних електромагнітних випромінювань.**
Summary: **The problem of choice the parameter of purpose for an estimation of the information security, which circulates in passive elements LAN from outflow on TEMPEST channels, is considered.**
Ключові слова: **Локальна обчислювальна мережа, побічні електромагнітні випромінювання, тестові сигнали, гармонічний сигнал, покажчик призначення.**

I Вступ

Будь-яка локальна обчислювальна мережа (ЛОМ) містить в собі три такі основні елементи: кінцеве обладнання користувачів (робочі станції, сервери), активне комутаційне обладнання (концентратори, комутатори, маршрутизатори), пасивне обладнання (інсталяційні кабелі, комутаційні шнури, з'єднувальні модулі, комутаційні панелі).

Перші два елементи є прикладом об'єктів, зосереджених в обмеженому просторі, а третій елемент – є розосередженим. Система технічного захисту інформації (ТЗІ) передбачає схожі для всіх трьох елементів методи захисту інформації від витоку за рахунок побічних електромагнітних випромінювань (ПЕМВ): екранування, активне або пасивне зашумлення. Опис витоку інформації каналами ПЕМВ та реалізація методів захисту інформації від витоку такими каналами розглянуті в [1 – 6].

В статті розглянуто питання оцінки ступеню захищеності інформації, що циркулює лише у пасивному обладнанні ЛОМ, бо для нього чинні нормативні документи в галузі технічного захисту інформації визначають покажчики призначення, їх нормативи та методи розрахунків, які не можуть бути застосовані для порівняння між собою пасивного обладнання ЛОМ різних виробників до початку виконання робіт з монтажу цього обладнання.

II Основна частина

Оцінка ступеню захищеності інформації, що циркулює в елементах ЛОМ, від витоку каналами ПЕМВ здійснюється за методикою, яка як покажчик призначення використовує величину радіуса зони II і передбачає проведення випробувань лише на конкретному об'єкті. При цьому просторова конфігурація всіх елементів, що входять до її складу, має бути відома. Будь-яка майбутня заміна встановленого пасивного обладнання ЛОМ на інше, або в іншому місці спричинить необхідність проведення повторних випробувань. Більше того, внаслідок проведення вимірювань у конкретних умовах не можливо порівняти властивості пасивного обладнання ЛОМ різних виробників з точки зору ТЗІ. Крім того, якщо результати випробувань будуть незадовільними, то перебудова ЛОМ потребує від її власника додаткових фінансових витрат. Для того, щоб проектувальник ЛОМ зміг вирішити, які компоненти і якого виробника йому слід обрати аби досягти потрібного ступеня захисту інформації, необхідно провести попередні випробування всіх елементів ЛОМ в однакових умовах.

Оцінка захищеності інформації за існуючою методикою передбачає створення тестового сигналу, що задовольняє таким вимогам: схожість структури реального інформативного сигналу та тестового;