СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ И СРЕДСТВ АВТОМАТИЗАЦИИ ИЗМЕРЕНИЙ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

COMPARATIVE ANALYSIS OF METHODS AND MEANS OF AUTOMATION OF MEASUREMENTS OF SPURIOUS ELECTROMAGNETIC RADIATION AND INTERFERENCE

УДК 004.054

Калита И.Ф., ассистент, Российский технологический университет МИРЭА, Россия, г. Москва

Kalita Ivan Feliksovich, tymahiii@yandex.ru

Аннотация

В данной статье рассмотрена краткая история перехвата побочных электромагнитных излучений и наводок, сравнение ручного и автоматизированного поиска информативного сигнала, а также краткий анализ средств автоматизации поиска побочных электромагнитных излучений и наводок. По мимо прочего в статье затронута «ручная» методика измерения побочных электромагнитных сигналов и наводок. Рассмотрены комплексы автоматизации поиска информативного сигнала «Навигатор», «Легенда», «Сигурд» и «Зарница».

Annotation

This article describes a brief history of the interception of spurious electromagnetic radiation and cues, a comparison of manual and automated search for an informative signal, as well as a brief analysis of automation tools for searching for spurious electromagnetic radiation and cues. Among other things, the article deals with

the "manual" method of measuring spurious electromagnetic signals and cues. The complexes of automation of search of informative signal "Navigator", "Legend", "Sigurd" and "Zarnitsa" are considered.

Ключевые слова: измерения, информативный сигнал, комплекс, сравнение, электромагнитные излучения.

Keywords: measurements, informative signal, complex, comparison, electromagnetic radiation.

Любое государство сейчас не может существовать без технической разведки. Радиоразведка появилась вместе с радиосвязью в начале XX века, а компьютерная разведка — вместе с глобальной сетью Интернет в 1980-х годах. [5]

Термин ПЭМИН (побочные электромагнитные излучения и наводки) появился в конце 60-х - начале 70-х годов при разработке методов предотвращения утечки информации через различные рода демаскирующие и побочные излучения электронного оборудования. В Европе и Канаде для обозначения данного термина используется «compromising emanation» – компрометирующее излучение. Побочные электромагнитные излучения и наводки были обнаружены еще в XVIII веке, но исследования начались во время Второй мировой войны, что было обусловлено, в первую очередь, желанием правительств стран-участниц сохранить втайне свою информацию и получить доступ к информации противников. Опасность побочных электромагнитных излучений и наводок с точки зрения защиты информации впервые наглядно была продемонстрирована голландским инженером Вим ван Эку, который в 1985 году опубликовал статью «Электромагнитное излучение видеодисплейных модулей: Риск перехвата?». Статья была посвящена возможным методам перехвата композитного сигнала видеомониторов. В марте 1985 года на выставке Securecom-85 в Каннах ван Эк продемонстрировал оборудование для перехвата излучений монитора. Опыт был достаточно прост: в автомобиле, стоящем на улице, был установлен обычный телевизионный приемник с

усовершенствованной антенной, на экране которого можно было наблюдать ту же самую картину, которую воспроизводил монитор компьютера в здании рядом с автомобилем. Эксперимент доказал, что перехват информации с монитора возможен с помощью незначительно доработанного обычного телевизионного приемника. [6]

Поиск и измерение побочных электромагнитных излучений и наводок средств электронно-вычислительной техники вручную является трудоёмким и длительным процессом. При этом значительная часть выполняемых инженером-исследователем операций – однообразные рутинные процедуры: перестройка частоты, регистрация обнаруженных информационных побочных электромагнитных излучений и наводок, запись частот и уровней этих излучений в таблицу. Поэтому автоматизация измерений побочных электромагнитных излучений и наводок является важной и актуальной задачей, как в практическом плане, так и в теоретическом аспекте. С точки зрения теории необходимо обоснованно выбрать метод автоматизации измерений, а на практике необходимо сформировать измерительный комплекс, реализующий данный метод автоматизации измерений. В настоящее время, наблюдаются значительные расхождения в результатах измерений, получаемых известными автоматизированными комплексами, так и между результатами, полученными при помощи автоматизированных систем и квалифицированным инженером-исследователем вручную. [3-4]

Согласно действующим нормативно-методическим документам, при проведении специсследований требуется измерять информативные побочные электромагнитные сигналы и наводки, то есть такие излучения и наводки, создаваемые исследуемым техническим средством, которые содержат обрабатываемую данным техническим средством информацию. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны учитываться. Для того чтобы определить информационные побочные электромагнитные излучения и наводки, на проверяемом техническом средстве предусматривают специальные тестовые

режимы работы. Требования к тестам определяются в соответствующих ГОСТах и методиках. Информационные побочные электромагнитные сигналы и наводки от технического средства в тестовом режиме должны иметь максимально возможный уровень и легко опознаваться на слух. При поиске побочных электромагнитных излучений и наводок исследователь прослушивает через наушники сигналы на выходе демодулятора измерительного прибора, одновременно наблюдая осциллограммы этих сигналов. Если обнаружен сигнал, похожий на искомый тестовый сигнал, исследователь путём выключения и включения тестового режима исследуемого технического средства убеждается в том, что сигнал действительно генерируется именно этим средством и является информационным побочным излучением (наводкой). Получается, что, первым критерием для исследователя является информационная расцветка искомого сигнала. Другой, не менее значимый критерий, - изменение уровня на частоте показанного сигнала при включении и выключении теста на исследуемом техническом средстве. Инженер может столкнуться с трудностями при фиксации изменений уровня, если уровень побочных электромагнитных излучений и наводок в тестовом режиме незначительно отличается от уровня в штатном режиме, и в этом случае, зачастую, приходится принимать решение об отнесении данного сигнала к спектру побочных электромагнитных излучений и наводок, основываясь только на присутствии информационной окраски. [1-2]

Поиск информационных побочных электромагнитных излучений и наводок требует от исследователя непрерывной сосредоточенности. Но работать в таком режиме человек может лишь ограниченное время. При более длительной работе наблюдается эффект, в просторечии называемый «замыливанием», когда исследователь перестает узнавать сигналы среди шумов, пропускает гармонические составляющие, ошибается при измерениях. Постоянно растущий парк электронно-вычислительной техники, в том числе обрабатывающей секретную и конфиденциальную информацию, требует наращивания объемов специальных исследований. Увеличивать же пропорционально штат инженеров-исследователей, по вполне понятным причинам, не всегда возможно.

Автоматизация процесса измерения побочных электромагнитных излучений и наводок является естественным решением проблемы.

До недавнего времени на отечественном рынке средства автоматизации измерения побочных электромагнитных излучений и наводок были представлены всего лишь двумя комплексами: «Навигатор» производства ЗАО «Нелк» и «Зарница» производства ГУП «СНПО Элерон». [7]

В настоящее время в продаже появились еще два семейства комплексов для проведения специсследований: «Легенда» от ФГУП «НПП «Гамма» и «Сигурд» производства ЗАО «Маском». Все комплексы, так или иначе, решают одну и ту же задачу, поэтому, несомненно, имеют довольно много общих черт, но есть и различия, причем весьма существенные. Чтобы прояснить эти различия, рассмотрим применяемые в комплексах методы автоматизации.

Инженер-исследователь ищет гармонические составляющие «на слух», опознавая искомые компоненты по звуку и форме осциллограммы де модулированного сигнала. Инструментальная реализация такого режима обычно приводит к тому, что автоматическая система, распознающая сигналы по их форме, работает лишь ненамного быстрее квалифицированного инженера-исследователя. Поэтому в первых комплексах данный режим не был реализован, а опознавание производится по критерию изменения уровней сигналов при включении тестового режима на исследуемом техническом средстве (так называемый «энергетический критерий»). Такой способ дает неплохие результаты: вся работа по обнаружению сводится к двум проходам сканирования диапазона специсследования: при первом проходе запоминается картина шумов при выключенном тестовом режиме, при втором проходе исследуемое техническое средство переводится в тестовый режим, и измеряются уровни всех сигналов, превышающих запомненные шумы на заданное значение порога.

Ускорение работы достигается очень существенное: вместо нескольких часов (а то и рабочих дней) специсследование выполняется за считанные минуты. В результате инженер-исследователь получает таблицу частот и уровней сигналов (типичное количество обнаруженных составляющих -

несколько сотен) и может рассчитать зоны разведдоступности. К сожалению, результаты расчета могут оказаться неверными. Электромагнитная обстановка имеет свойство изменяться со временем. В диапазоне от 9 кГц до 1000 МГц работают тысячи радиостанций и источников радиопомех. [8]

Исследователю приходится вручную проверять все обнаруженные составляющие, на что, при достаточно слабых сигналах, вновь будет уходить время. По-настоящему эффективно данный способ работает в безэховых экранированных камерах, которые ввиду своей дороговизны доступны очень немногим предприятиям.

В более совершенных последних двух комплексах применено автоматическое опознавание информационных сигналов. Согласно методике инженеру-исследователю предлагается выполнить поиск какой-либо гармонической составляющей вручную или в специальном «полуавтоматическом» режиме, либо создать эталонный образ искомого сигнала при помощи редактора (генератора), либо выбрать ранее созданный образ из библиотеки, после чего комплекс автоматически обнаруживает в эфире сигналы, похожие на заданный сигнал. Для опознавания сигналов в обоих комплексах применяется взаимно корреляционная функция, в «Легенде» - в сочетании с Байесовским критерием минимального риска. Как отмечалось выше, это более затратный по времени способ, но и существенно более точный. По результатам сертификационных испытаний комплекса «Легенда» данные, полученные с его помощью, не требуют ручной верификации (сертификат Гостехкомиссии при Президенте РФ № 603). Комплекс «Сигурд» пока не прошел сертификационных испытаний, но, по-видимому, их результаты будут не хуже. Для преодоления отставания в скорости работы от комплексов, использующих «энергетический» критерий, разработчики комплексов, работающих по «информационному» критерию, используют различные приемы, такие как анализ сигнала в окрестностях частот, кратных тактовой частоте теста, измерения партий однотипных технических средств с использованием шаблонов частот. Это приводит к заметному ускорению работы без снижения точности, но, к

сожалению, не во всех режимах работы комплексов: например, режим поиска паразитной высокочастотной генерации, заявленный в комплексе «Легенда», может быть реализован только при «беспропусковом», а значит, относительно медленном контроле. Следует понимать, что, хотя комплексы «Легенда» и «Сигурд» не требуют для своей работы «тепличных» условий экранированной камеры, средний выигрыш во времени по сравнению с ручными измерениями, выполняемыми высококвалифицированными инженерами-исследователями, может оказаться ниже, чем можно было бы ожидать, прочитав рекламу.

Представленные на отечественном рынке комплексы для проведения специсследований позволяют в автоматическом режиме решать ряд задач измерений побочных электромагнитных излучений и наводок и способны в той или иной мере облегчить работу инженера-исследователя, повысить производительность его труда. Комплексы на основе сканирующих приемников («Зарница») пригодны для быстрого анализа спектра побочных электромагнитных излучений и наводок, излучаемых техническим средством, но не обеспечивают высокой точности измерений. При необходимости выдачи предписания на эксплуатацию технического средства, измерения, произведенные при помощи данного комплекса, подлежат обязательной ручной проверке с использованием метрологического измерительного оборудования (измерительных приемников или анализаторов спектра). Комплексы «Навигатор» пригодны для проведения достаточно точных измерений побочных электромагнитных излучений и наводок в условиях экранированных помещений (безэховых экранированных камер), однако результаты измерений могут быть корректными только при их тщательной ручной верификации с использованием средств самого «Навигатора». Комплексы «Легенда» позволяют проводить измерения, не требующие ручной верификации, что подтверждено сертификатом Гостехкомиссии. По-видимому, то же можно будет сказать и о комплексах «Сигурд» после завершения соответствующих сертификационных испытаний. Но использование комплексов «Легенда» и «Сигурд» требует от оператора достаточно высокой квалификации и четкого знания методики

проведения специсследований, так как собственно исследовательская, творческая часть методики - выявление структуры тестового сигнала, создание эталонного образа, формирование задания на проведение измерений - остается за человеком. Впрочем, стоит ли считать это обстоятельство недостатком - решать вам. Мы же убеждены, что высокая квалификация и знания всегда были и остаются основой профессионального подхода.

Библиографический список:

1. Баранова Е.К. Информационная безопасность и защита. Учебное пособие /Е.К. Баранова, А.В. Бабаш – М.: РИОР, Инфра-М, 2017. – 324 с.
2. Бирюков А.А. Информационная безопасность: защита и нападение /А.А. Бирюков – М.:ДМК Пресс, 2012. – 474 с.
3. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие /В.В. Бондарев – М.: МГТУ им. Н. Э. Баумана, 2016. – 252 с.
4. Вильдяйкин Г.Ф. Аппараты и средства перехвата информации. Для студентов технических специальностей / Г.Ф. Вильдяйкин – М.: Издательские решения, 2019. – 70 с.
5. Гребенников В. Радиоразведка России. Перехват информации /В. Гребенников – М.: Издательские решения, 2018. – 720 с.
6. Ларин Д.А. Информационная безопасность. История защиты информации в России / Д.А. Ларин, Баранова Е.К. – М.:КДУ, 2015. – 736 с.
7. Федеральная служба по техническому и экспортному контролю [Электронный ресурс]: Государственный реестр сертифицированных средств защиты информации / ФСТЭК России, 2013 г. URL: http: // www. fstec.ru (дата обращения: 01.04.21)
8. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации /А.А. Хорев – М.: МО РФ, 1998. – 224 с.

Bibliographic list:

1. Baranova E.K. Information security and protection. Study guide / E.K. Baranova, A.V. Babash - M .: RIOR, Infra-M, 2017 .-- 324 p.

2. Biryukov A.A. Information security: protection and attack / A.A. Biryukov - M.: DMK Press, 2012 .-- 474 p.
3. Bondarev V.V. Introduction to information security of automated systems. Study guide / V.V. Bondarev - M .: MGTU im. N.E.Bauman, 2016 .-- 252 p.
4. Vildyaykin G.F. Apparatus and means of intercepting information. For students of technical specialties / G.F. Vildyaykin - M .: Publishing solutions, 2019 .-- 70 p.
5. Grebennikov V. Radio intelligence of Russia. Interception of information / V. Grebennikov - M .: Publishing solutions, 2018 .-- 720 p.
6. Larin D.A. Information Security. History of information protection in Russia / D.A. Larin, Baranova E.K. - M.: KDU, 2015 .-- 736 p.
7. Federal Service for Technical and Export Control [Electronic resource]: State Register of Certified Information Security Means / FSTEC of Russia, 2013 URL: http: // www. fstec.ru (date of access: 01.04.21)
8. Khorev A.A. Methods and means of searching for electronic devices for intercepting information / A.A. Khorev - M .: Ministry of Defense of the Russian Federation, 1998 .-- 224 p.