УДК 004.056.52

Д.С. Милько [1]

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

СОВРЕМЕННОЕ СОСТОЯНИЕ ИССЛЕДОВАНИЙ, СВЯЗАННЫХ С УТЕЧКОЙ ИНФОРМАЦИИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

Аннотация. В настоящей работе представлен обзор актуальной проблематики в области информационной безопасности, связанной с утечкой информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН). В работе обобщены результаты научных трудов как российских, так и зарубежных ученых, опубликованные по указанному направлению в открытых источниках за последние годы, на их основе определено направление для проведения дальнейших исследований.

Проведено обобщение задач, возникающих при исследовании каналов ПЭМИН.

Выделены основные задачи, связанные с исследованиями ПЭМИН, встречающиеся в открытых источниках: задачи, возникающие при перехвате излучений от видеоинтерфейса; перехват методом программного ПЭМИН; отложенный анализ при перехвате ПЭМИН; перехват ключей шифрования по каналам ПЭМИН; задачи, связанные с защитой от утечки по каналам ПЭМИН; пассивные способы защиты от ПЭМИН.

Выполнен обзор учебно-методических пособий для высших учебных заведений, которые готовят специалистов по направлениям, связанным с информационной безопасностью, включающих разделы о каналах ПЭМИН.

Также в работе содержится обзор авторефератов диссертаций на соискание ученой степени кандидата технических наук, затрагивающих проблематику защиты информации от утечек по каналам ПЭМИН

В заключении в качестве направления дальнейших научных исследований выбрана разработка комплексной методики оценки эффективности пассивных средств защиты информации и реализация соответствующего программно-аппаратного комплекса.

Ключевые слова: ПЭМИН, программный ПЭМИН, отложенный анализ, перехват ключей шифрования, пассивные средства защиты информации.

D.S. Milko [1]

[1] *Irkutsk State Transport University, Irkutsk, Russian Federation*

CURRENT STATE OF TRANSIENT ELECTROMAGNETIC PULSE EMANATIONS STANDARD RESEARCHES

Abstract. This paper is a review about current problems in the field of Transient Electromagnetic Pulse Emanations Standard (TEMPEST). TEMPEST research statistics of Russian and foreign investigators over recent years are summarized.

The subject of future researching are selected in light of this.

TEMPEST issue classification is available.

Main TEMPEST researching problems from non-cofidential papers are highlighted: videointerface emanations intercepting; soft-TEMPEST intercepting; delay TEMPEST signal analysis; encryption keys TEMPEST intercepting; TEMPEST information security methods; passive TEMPEST information security methods.

Textbooks for information security universities review are done.

Paper also contains review of PhD degree dissertations abstracts apply to TEMPEST information security methods.

Passive TEMPEST information security efficiency estimation method engineering and hardware and software system are selected as the subject of future researching in in the end.

Keywords: TEMPEST, soft TEMPEST, delay signal analysis, encryption key thief, passive information security facilities.

Введение. Проблема утечки конфиденциальной информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) интенсивно обсуждается в профессиональном и исследовательском сообществе с момента первой открытой наглядной демонстрации данного способа перехвата в 1985 году голландским инженером Wim Van Eck [1].

Настоящая работа обобщает результаты научных трудов по указанной тематике и представляет их в обзорном виде. В каждом разделе работы обобщены задачи в указанной проблемной области. В заключении работы выбрано направление дальнейших исследований. Выбранное направление является слабо изученным. В открытых источниках отсутствует его системное изложение.

Исследования, связанные с проблемой утечки информации по каналам ПЭМИН, можно разделить на две категории (рисунок 1):

1) исследования задач, возникающих при перехвате информативных сигналов и извлечении из них конфиденциальной информации у злоумышленника (задачи перехвата);

2) исследования задач, возникающих при защите конфиденциальной информации от утечки у собственника информации (задачи защиты).

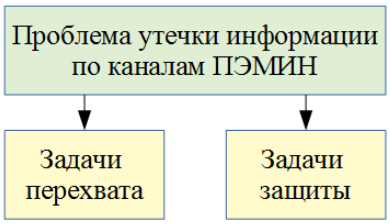

Рис. 1. — Классификация задач, связанных с проблематикой ПЭМИН

Обобщение исследований, связанных с проблематикой ПЭМИН, представлено ниже.

1. Перехват излучений от видеоинтерфейса. Наиболее часто среди исследований, связанных с ПЭМИН, встречаются исследования, касающиеся задач перехвата побочных электромагнитных излучений (ПЭМИ) от видеоинтерфейса. Исследование этого вопроса является наиболее популярным. В особенности часто ПЭМИ от видеоинтерфейса встречается в первых работах исследователей ПЭМИН (в том числе, студентов специальностей, связанных с информационной безопасностью).

Способы перехвата ПЭМИ от видеоинтерфейса являются максимально наглядными при демонстрации. При перехвате других внутренних интерфейсов передачи данных электронно-вычислительных машин нет такой наглядной возможности для демонстрации перехватываемых данных. Перехват ПЭМИ от видеоинтерфейса на сегодняшний момент достаточно просто реализовать. Именно с этим связано большое количество научных работ, в которых исследуются задачи, возникающие при перехвате излучений от видеоинтерфейса.

Большой объем научных работ, связанных с исследованиями ПЭМИ от видеоинтерфейса, способен негативно повлиять на представление о состоянии современных исследований ПЭМИ в целом. Так, например, в обзорной работе В.Я. Сизова [2] автор делает выводы о существующих недостатках в подходах современных исследователей каналов ПЭМИ. Основой обзора автора являются результаты исследований исключительно ПЭМИ от видеоинтерфейса. Автор обращается к трудам таких зарубежных исследователей как Wim Van Eck [1], Markus G Kuhn [3], Furkan Elibol, Ugur Sarac, Isin Erer [4]. Хотя в названии работы заявлено «обобщение истории и ранних исследований ПЭМИ», автором не исследованы научные труды, связанные с другими внутренними интерфейсами передачи данных электронно-вычислительных машин. Таким образом формируется ошибочное представление о том, что под ПЭМИ понимается исключительно ПЭМИ от видеоинтерфейса.

Однако, стоит отметить, что именно исследования ПЭМИ от видеоинтерфейса лежат в основе современных исследований ПЭМИ в целом. В обзорной работе В.Я. Сизова [2] можно выделить задачи, связанные с перехватом ПЭМИ в целом, на решение которых следует обратить внимание:

– автоматическая синхронизация частоты перехвата (относится к проблемам перехвата);

– совершенствование методов, связанное с постоянным появлением новых видов протоколов обмена информацией (относится к проблемам как перехвата, так и защиты).

Синхронизация частоты перехвата требует знания характеристик электронно-вычислительной машины, на которую совершается атака. Markus G Kuhn в работах [5-7] доказал, что частота перехвата видеодисплея зависит от размеров изображения, частоты обновления экрана и протоколов передачи видеокарты. Все указанные характеристики стандартизированы, что позволяет злоумышленнику использовать автоматизированное средство перехвата. Примером такого программно-аппаратного комплекса может быть цифровой приемник (SDR, software-denied radio) Hack RF One (рисунок 2), подключаемый к персональному компьютеру, и свободно распространяемое программное обеспечение Tempest for Eliza.

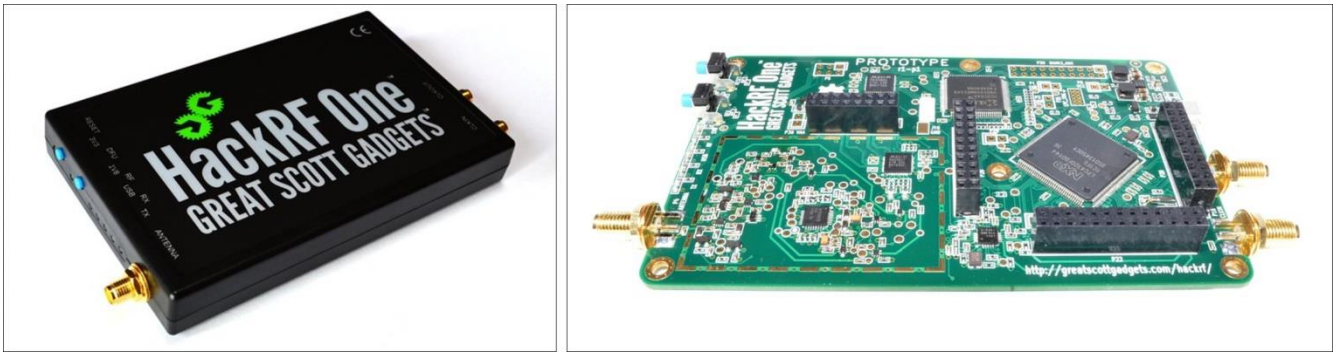

Рис. 2. Внешний вид (слева) и внутренние компоненты (справа) цифрового приемника Hack RF One

В работе Furkan Elibol, Ugur Sarac, Isin Erer [4] используется технически более сложное оборудование. Ввиду этого исследователям удалось перехватить сигнал от жидкокристаллического видеодисплея из соседнего здания с расстояния 46 метров (рисунок 3).

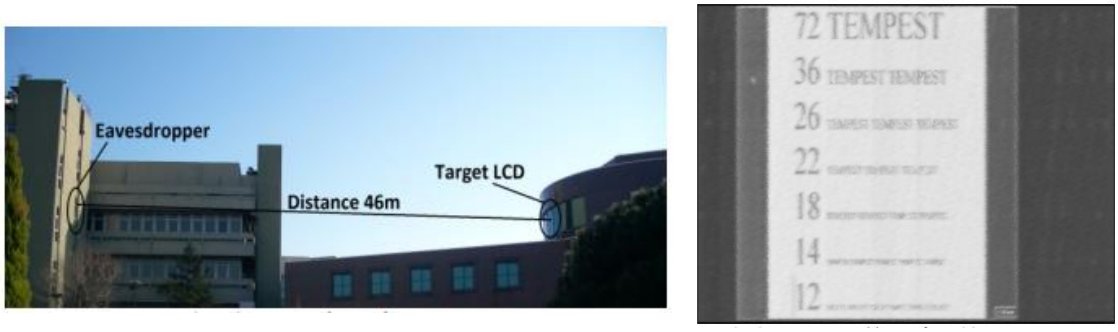

Рис. 3. Схема размещения аппаратуры (слева) и результат перехвата с расстояния 46 метров (справа)

По результатам исследований в области перехвата ПЭМИ от видеоинтерфейса опубликовано большое количество работ [8-16]. Над исследованиями в этой области работает большое количество ученых из разных стран, в частности из России, Голландии, Великобритании, Турции, Китая. Новые задачи, касающиеся проблематики перехвата, решаются достаточно оперативно путем применения современных вычислительных средств.

Сложности, требующие большего внимания, возникают при решении задач, которые относятся к проблемам защиты. Регулярное появление новых видов протоколов обмена данными сопровождается ростом скорости передачи информации. Увеличение роста скорости передачи информации приводит к смещению частот ПЭМИН в большую сторону. Эта тенденция требует

применения новых методов защиты информации от утечки по каналам ПЭМИН в целом, и ПЭМИ от видеоинтерфейса в частности.

2. Перехват методом программного ПЭМИН. Первой работой, в которой описан механизм перехвата методом программного ПЭМИН является работа Markus G Kuhn [5]. В работе автор описывает результаты своего эксперимента. В эксперименте каналы утечки ПЭМИН были совмещены с вредоносным программным обеспечением («вирусом»), установленным на атакуемое средство вычислительной техники.

Совместная реализация ПЭМИН и вредоносного программного обеспечения способна организовать канал передачи схожий со стеганографическими методами передачи. Markus G Kuhn дал название для нового способа получения конфиденциальной информации - «soft TEMPEST» или, переводя на русский язык, «программный ПЭМИН» (рисунок 4).

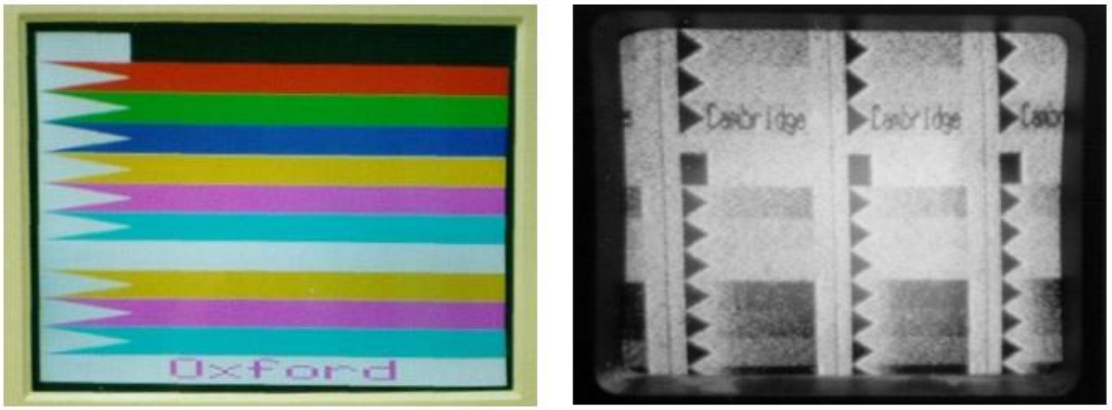

Рис. 4. Демонстрация реализации программного ПЭМИН в работе Markus G Kuhn.
Изображение, размещенное на зараженном устройстве демонстрирует слово «Oxford» (слева).
Злоумышленник тайно от оператора на экране перехватывает слово «Cambridge»,
генерируемое вредоносным программным обеспечением (справа).

Сегодня решением задач, связанных с программным ПЭМИН занимаются, в том числе, и в России. В открытых источниках опубликованы работы А.М. Рябинина, В.И. Филатова, И.В. Белкова [17,18], И.С. Антясова, А.В. Сафонова, А.Н. Соколова [19].

Особый интерес в указанных работах представляет вывод о том, что средством разведки ПЭМИН может стать современный цифровой приемник FM радиосигналов (в том числе, смартфон при наличии недекларированных программных возможностей).

Например, смартфон с приемником FM-радиосигналов и атакуемое средство вычислительной техники содержат вредоносное программное обеспечение («вирус»). «Вирус» в атакуемом средстве вычислительной техники создает режим обработки информации, при котором в радиоэфир передаются конфиденциальные данные. «Вирус» в смартфоне создает режим приема информативного сигнала из радиоэфира и его передачи по сети «Интернет». Таким образом сформирован канал утечки информации от атакуемого средства вычислительной техники в сеть «Интернет».

Одним из способов защиты от программного ПЭМИН является реализация комплекса мер антивирусной защиты и средств защиты от утечек по каналам ПЭМИН.

3. Отложенный анализ при перехвате ПЭМИН. А.М. Бонч-Бруевичу и А.А. Анженко удалось реализовать программно-аппаратный комплекс отложенного анализа информативных сигналов ПЭМИН. Идея их работы [20] состоит том, чтобы показать, что существующие методики оценки защищенности от утечки по каналам ПЭМИН не учитывают реальной

возможности отложенного анализа записанных сигналов. Способ реализации отложенного анализа записанных информативных сигналов ПЭМИН представлен в виде программно-аппаратного комплекса, позволяющего проводить такой анализ (рисунок 5).

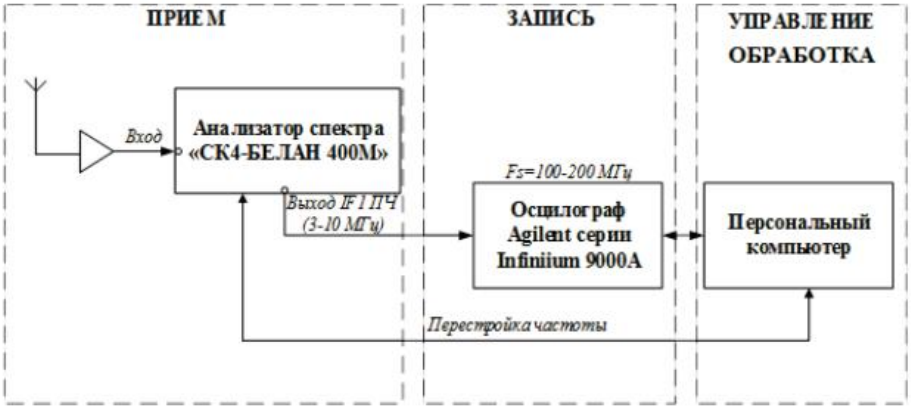

Рис. 5. Структурная схема измерительного комплекса отложенного анализа сигналов ПЭМИН

Представленный авторами метод обработки является перспективным. Данный метод может быть применен для выделения апериодических и одиночных (импульсных) информативных сигналов ПЭМИН.

4. Перехват ключей шифрования по каналам ПЭМИН. Исследователи американской компании Cryptography Research Jun и Kenworthy в своем докладе [21] наглядно продемонстрировали результаты перехвата ключей шифрования, обрабатываемых мобильными устройствам. При демонстрации перехвата процессоры смартфона и планшетного компьютера последовательно совершали операции шифрования и дешифровки. Аппаратура перехвата побочных излучений (SDR радио) находилась на расстоянии 10 футов (около 3-х метров) по прямой видимости и осуществила перехват ключей шифрования по каналам ПЭМИН.

Также перехват побочных излучений от процессора возможен из соседнего помещения. Совместная работа Genkin, Pachmanov, Pipman и Tromer [22] демонстрирует как исследователям удалось перехватить по каналу ПЭМИ закрытые ключи шифрования из ноутбука, находящегося в соседнем помещении. Для перехвата ПЭМИ использовалось SDR радио. Атакуемый ноутбук при этом был отключен от всех линий и коммуникаций, в том числе, линии электропитания, что исключало возможность наводок в них информативного сигнала.

Стоит отметить, что потенциальная возможность существования канала утечки криптографических ключей информации была представлена в 2003 году в диссертации В.М. Масловского [23].

Указанное направление исследования является одним из самых перспективных, так как средства разведки, способные осуществить перехват ключей шифрования, появились совсем недавно. Однако, исследования в указанном направлении уже ведутся

5. Защита от утечек по каналам ПЭМИН. Самая актуальная информация по решению проблем, связанных с защитой информации от утечек по каналам ПЭМИН, представлена в нормативно-методической документации по технической защите информации. Однако указанные сведения являются сведениями ограниченного доступа.

Между тем, с начала 2000-х годов в открытых источниках опубликованы учебно-методические пособия для ВУЗов, которые готовят специалистов по направлениям, связанным с информационной безопасностью. Также существует несколько авторефератов диссертаций на

соискание ученой степени кандидата технических наук, затрагивающих проблематику защиты информации от утечек по каналам ПЭМИН. Выбор актуальной темы для дальнейших исследований невозможен без обзора указанных работ, что требует их краткого обзора.

Наиболее подробное описание способов защиты информации от утечки по каналам ПЭМИН, представлено А.П. Зайцевым, Р.В. Мещеряковым и А.А. Шелупановым в учебнике для ВУЗов [24]. Каналы утечки информации в учебнике рассмотрены с точки зрения физической природы из возникновения. Также сообщается о существующих средствах выявления технических каналов утечки и средствах защиты информации.

Другое учебное пособие [25] содержит отдельную главу, посвященную побочным электромагнитным излучениям и наводкам. Автором А.А. Титовым проведена классификация видов ПЭМИН по способам возникновения. В учебном пособии подробно изложен каждый из видов ПЭМИН с инженерно-технической точки зрения. Представлены существующие на момент издания средства защиты информации от утечки по каналам ПЭМИН и технические методы устранения ПЭМИН.

Руководство [26] автора Г.А. Бузова дает описание каналов ПЭМИН как подмножества технических каналов утечки информации. Аналогичным образом каналы ПЭМИН представлены в учебном пособии А.А. Малюка [27].

В материалах [28], представленных Д.А. Скрипник, проблематике защиты от ПЭМИН посвящены два параграфа. В первом параграфе рассмотрены природа возникновения и виды ПЭМИН, подробно описаны существующие средства перехвата радиосигналов. Во втором - описаны пассивные и активные методы защиты информации от утечки по каналам ПЭМИН: экранирование, заземление, фильтрация и зашумление.

Диссертации на соискание ученой степени кандидата технических наук [23, 29, 30] решают конкретные практические задачи, связанные с ПЭМИН.

Целью диссертации В.М. Масловского [23] является разработка алгоритма безопасной передачи информации по каналам связи, основанного на новом принципе.

Каналы связи потенциально подвержены перехвату через ПЭМИН. Защита каналов связи от перехвата возможна физическими и криптографическими мерами. В.М. Масловский предложил новый алгоритм безопасной передачи информации по каналам связи, который не относится к физическим и криптографическим мерам. Безопасность нового алгоритма заключается в использовании кодов, которые минимизируют побочные излучения при передаче информации по каналам связи.

На момент публикации в 2003 году тема была очень актуальна. Использование криптографических алгоритмов для защиты информации требовало больших вычислительных мощностей. Однако на сегодняшний момент способы и методы шифрования информации стали доступными. Сегодня широко распространены универсальные средства вычислительной техники с высокой производительностью. Производительности современных средств вычислительной техники достаточно для применения безопасных средств криптографической защиты.

Значимость работы В.М. Масловского на сегодняшний момент состоит в анализе условий, определяющих выбор оптимального способа защиты информации. Применяя предложенный В.М. Масловским в первом разделе [24] алгоритм анализа условий эксплуатации защищаемого объекта, можно прийти к выводу о рациональности или нерациональности использования того или иного способа защиты информации от утечек по каналам ПЭМИН.

Кроме этого, идея В.М. Масловского может быть использована для разработки средств вычислительной техники в защищенном исполнении, защищенных от перехвата ключей шифрования по каналам ПЭМИН, представленного в [22].

Я.А. Жигуновой в диссертации [29] удалось разработать методику автоматизированного поиска информативных сигналов ПЭМИ от средств вычислительной техники, а также программный комплекс, реализующий указанную методику.

В целом, диссертация Я.А. Жигуновой, не утратила своей актуальности. Сегодня методы автоматизированного поиска информативных сигналов ПЭМИ все еще применяются. Для практического применения разработанной методики нужно доработать программный комплекс с учетом современных операционных сред.

В диссертации П.В. Урбановича [30] реализована методика программируемого формирования электромагнитных помех средствами активной защиты от утечек за счет ПЭМИ. Разработанная автором методика позволяет снижать уровень излучения в требуемых полосах частот таким образом, чтобы не нарушалась передача полезных радиосигналов. На основе методики разработано средство защиты, успешно реализующее её принципы.

Исследование П.В. Урбановича не утратило своей актуальности, так как основным способом защиты информации от утечки по каналам ПЭМИ сегодня является применение генераторов пространственного зашумления. Производители генераторов пространственного зашумления снижают уровни маскирующего излучения в некоторых диапазонах частот по требованиям электромагнитной совместимости и медицинским требованиям.

Однако проведенное П.В. Урбановичем исследование полезных радиосигналов требует проработки ввиду расширения диапазонов радиочастот современных генераторов пространственного зашумления.

Приоритетом учебных пособий и научных трудов, связанных с защитой информации от утечки по каналам ПЭМИН, является использование активных средств защиты информации. Вопросы, связанные с пассивными способами защиты от утечки по каналам ПЭМИН являются малоизученными.

6. Пассивные способы защиты от ПЭМИН. В открытых источниках имеются работы, посвященные применению пассивных средств защиты информации. Актуальность использования пассивных средств защиты информации крайне высока.

Актуальность объясняется смещением диапазона излучаемых частот в высокочастотную область. Данное явление объясняется увеличением скорости передачи информации. Следовательно, при применении активных средств защиты информации, требуется разработка новых генераторов пространственного зашумления с более широким частотным диапазоном.

Разработка новых средств защиты информации не потребуется при пассивных способах защиты информации. Особенностью пассивных способов защиты информации (экранирование, радиопоглощение, применение радиочастотных фильтров [31]) является высокая эффективность в сверхвысокочастотной (СВЧ) области.

Работа И.С. Петрова [31] посвящена исследованию ослабления ПЭМИ путем экранирования. В работе определены основные базовые принципы экранирования для защиты от ПЭМИН.

А.В. Любченков в работе [32] отмечает широкое распространение материалов, поглощающих сверхвысокочастотное электромагнитное излучение и рассматривает методы измерения электродинамических параметров материалов, поглощающих электромагнитное излучение в СВЧ диапазоне. В следующей работе [33] А.Г. Остапенко, А.В. Любченков и Ю.С. Науменко рассматривают методический подход к оценке эффективности применения радиопоглощающих материалов для защиты от утечки по каналам ПЭМИН.

Н.В. Колбун, С.Н. Петров и А.М. Прудник приводят в своей работе [34] результаты исследования электромагнитных характеристик экранирующих и поглощающих материалов, способных реализовать ослабление электромагнитных волн более 25 дБ.

Немногочисленные работы [31-33] являются важными для решения задач, связанных с пассивными способами защиты информации от утечки по каналам ПЭМИН. Несмотря на важность и актуальность научной области комплексные исследования, позволяющие решить практические задачи в указанной области, отсутствуют.

Заключение. Регулярное появление новых видов протоколов обмена данными сопровождается ростом скорости передачи информации. Увеличение роста скорости передачи информации приводит к смещению частот ПЭМИН в большую сторону. Эта тенденция требует применения новых методов защиты информации от утечки по каналам ПЭМИН.

Приоритетом научных работ, связанных с защитой информации от утечки по каналам ПЭМИН, является использование активных средств защиты информации. Однако, производителям генераторов пространственного зашумления приходится снижать уровни маскирующего излучения в некоторых диапазонах частот по требованиям электромагнитной совместимости и медицинским требованиям.

Вопросы, связанные с пассивными способами защиты от утечки по каналам ПЭМИН являются малоизученными. Несмотря на важность и актуальность проблематики комплексные исследования, позволяющие решить практические задачи в указанной области, отсутствуют.

Практическим решением задачи применения пассивных способов защиты от утечки по каналам ПЭМИН может быть программно-аппаратный комплекс, реализующий методику оценки эффективности пассивных средств защиты информации. По этой причине в качестве направления дальнейших научных исследований выбрана разработка комплексной методики оценки эффективности пассивных средств защиты информации и реализация соответствующего программно-аппаратного комплекса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Van Eck W. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk Text//Computers and Security. — 1985. — №4. — С. 269-286.

2. Сизов В.Я. Обобщение истории и ранних исследований ПЭМИ//Региональная информатика СПОИСУ. — 2018. — С. 280-282.

3. Kuhn M. Compromising Emanations: Eavesdropping Risks of Computer Displays//University of Cambridge Computer Laboratory. Technical Report. — 2003. — №577. 177 С.

4. Elibol F., Sarac U., Erer I. Realistic Eavedropping Attack on Computer Displays with Low-Cost and Mobile Reciever System//20th European Signal Processing Conference. — 2012 — С. 1767-1771.

5. Kuhn M. Soft Tempest Hidden Data Transmission Using Electromagnetic Emanations//Springer-Verlag Berlin Heidelberg. — 1998. — С. 124-141.

6. Kuhn M. Composing emanations of LCD TV sets// IEEE International Symposium on Electromagnetic Compability. — С. 931-936.

7. Kuhn M. Electromagnetic Eavesdropping Risks of Flat-Panel Displays//4th Workshop on Privacy Enhancing Technologies. — 2004. — С. 1-18.

8. Баталов А.С. Исследование ПЭМИ видеосистемы с интерфейсом LVDS//Радиоэлектронные устройства и системы для инфокоммуникационных технологий. Защита информации. — 2015. — С. 404-407.

9. Zhou C., Yu Q., Wang L. Investigation of the Risk of Electromagnetic Security on Computer Systems//International Journal of Computer and Electrical Engineering. — 2012. — Т.4. — №1. — С. 93-98.

10. Крылова С.Л. Исследование ПЭМИ видеосистемы ПЭВМ в учебной лаборатории информационной безопасности//Сб. науч. тр. ООО Научный мир. — 2014. — Т.18. —№2. — С. 80-85.

11. Хорев А.А. Математическая модель обнаружения ПЭМИ видеосистемы компьютера оптимальным приемником//Вопросы защиты информации, 2014. — №1(104). — С. 65-71.

12. Хорев А.А. Оценка возможности обнаружения побочных электромагнитных излучений//Доклады ТУСУРа. 2014. — №2(32). — С. 207-213.

13. Васечкин Е.А., Таранов А.Б. Модель сигналов ПЭМИ видеоинтерфейсов//Труды СПИИРАН. 2016. — №4(47). — С. 46-64.

14. Егин А.В., Левин Д.В., Паршуткин А.В. Обобщенная математическая модель воздействия активных помех на техническое средство перехвата ПЭМИ от растровых систем отображения информации//Труды военно-косм. акад. им. А.Ф. Можайского. — 2016. — №651. — С. 62-70.

15. Железнов Д.И., Мищенко Д.А. Защита информации от утечки через ПЭМИ видеосистемы компьютера//Научно-практический электронный журнал Аллея Науки. — 2017. — №10. — С. 62-70.

16. Паршуткин А.В., Егин А.В., Вознюк В.В., Левин Д.В. Применение системы активного зашумления ПЭМИ при передаче данных по стандарту DVI//Изв. вузов. Приборостроение. — 2017. — Т. 60. — №1. — С. 25-31.

17. Рябинин А.М. Передача информации по каналу ПЭМИН на основе технологии Soft Tempest//Радиоэлектронные устройства и системы для инфокоммуникационных технологий. Защита информации. — 2015. — С. 436-439.

18. Рябинин А.М., Филатов В.И., Белков И.В. Модель канала передачи информации с помощью программно-управляемого ПЭМИН//Телекоммуникации и транспорт. — 2016. — Том 10. — №1. — С. 77-80.

19. Антясов И.С., Сафонов А.В., Соколов А.Н. Программно-техническая реализация технологии мягкий ПЭМИН//Вестник УрФО. Безопасность в информационной сфере. — 2015. — №3(17). — С. 8-11.

20. Бонч-Бруевич А.М., Анженко А.А. Метод отложенного анализа сигналов ПЭМИН в задачах оценки защищенности телекоммуникационной информации//Радиоэлектронные устройства и системы для инфокоммуникационных технологий. Защита информации. —2015. — С. 402-404.

21. Jun B., Kenworthy G. Is Your Device Radiating Keys//RSA Conference. — 2012.

22. Genkin D., Pachmanov L., Pipman I., Tromer E. ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs//Proc. RSA Conference Cryptographers' Track. —2016. — С. 219-235.

23. Масловский В.М. Метод гарантированной защиты информации от утечки по каналам ПЭМИН: дис. канд. техн. наук: 05.13.19. Санкт-Петербург, 2003. — 107 с.

24. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации Учебник для вузов//М.: Горячая линия–Телеком, 2012. — С. 30-51.

25. Титов А.А. Технические средства защиты информации//Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. — С. 166-191.

26. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации//М.: Горячая линия – Телеком, 2019. — С. 28-31.

27. Малюк А.А. Защита информации в информационном обществе//М.: Горячая линия – Телеком, 2017. — С. 120-126.

28. Скрипник Д.А. Общие вопросы технической защиты информации//М.: НОУ «ИНТУИТ», 2012. — С. 120-126.

29. Жигунова Я.А. Методическое и программное обеспечение управления поиском информативных гармоник сигналов электромагнитных излучений от средств вычислительной техники: дис. канд. техн. наук: 05.13.01. Иркутск, 2009. — 123 с.

30. Урбанович П.В. Методика и средство формирования шумовой электромагнитной помехи: дис. канд. техн. наук: 05.13.19. Томск, 2010. — 143 с.

31. Петров И.С. Локализация и ослабление ПЭМИ от СВТ путем экранирования электромагнитных волн//Вестник ЮУрГУ. Серия Компьютерные технологии, управление, радиоэлектроника. — 2012 г. — Вып. 16. — №23(282). — С. 189–191.

32. Любченков А.В. Анализ методов измерения электродинамических параметров материалов, поглощающих СВЧ электромагнитное излучение//Вестник Воронежского гос. техн. ун-та. — 2009. —Т.5. — №9. — С.111-113.

33. Остапенко А.Г., Любченков А.В., Науменко Ю.С. Оценка эффективности применения радиопоглощающих материалов от утечки по каналу ПЭМИ на объектах информатизации//Информация и безопасность. — 2011. — Т.14. — №1 — С. 113-116.

34. Колбун Н.В., Петров С.Н., Прудник А.М. Электромагнитные и акустические характеристики многослойных материалов для систем интегральной защиты//Доклады БГУИР. — 2009. — №3(41). — С. 79-85.

REFERENCES

1. Van Eck W. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk Text//Computers and Security. — 1985. — №4. — P. 269-286.

2. Sizov V.Y. Early TEMPEST researches and history generalization//Regional Informatics SPOISU. — 2018. — P. 280-282.

3. Kuhn M. Compromising Emanations: Eavesdropping Risks of Computer Displays//University of Cambridge Computer Laboratory. Technical Report. — 2003. — №577. 177 P.

4. Elibol F., Sarac U., Erer I. Realistic Eavedropping Attack on Computer Displays with Low-Cost and Mobile Reciever System//20th European Signal Processing Conference. — 2012 — P. 1767-1771.

5. Kuhn M. Soft Tempest Hidden Data Transmission Using Electromagnetic Emanations//Springer-Verlag Berlin Heidelberg. — 1998. — P. 124-141.

6. Kuhn M. Composing emanations of LCD TV sets// IEEE International Symposium on Electromagnetic Compability. — P. 931-936.

7. Kuhn M. Electromagnetic Eavesdropping Risks of Flat-Panel Displays//4th Workshop on Privacy Enhancing Technologies. — 2004. — P. 1-18.

8. Batalov A.S. Investigation of videosystem TEMPEST with LVDS interface//Radioelectronic Devices and Systems for Infocommunication Technologies. Information Security. — 2015. — P. 404-407.

9. Zhou C., Yu Q., Wang L. Investigation of the Risk of Electromagnetic Security on Computer Systems//International Journal of Computer and Electrical Engineering. — 2012. — T.4. — №1. — P. 93-98.

10. Krylova S.L. Research of videosystem TEMPEST in the university information security laboratory //Collection of Scientific Papers Nauchny Mir Ltd.. — 2014. — T.18. —№2. — P. 80-85.

11. Horev A.A. Mathematical model for detecting the TEMPEST of a computer videosystem by an optimal receiver //Information Security Issues , 2014. — №1(104). — P. 65-71.

12. Horev A.A. Evaluation of the possibility of TEMPEST detection//TUSUR Reports. 2014. — №2(32). — P. 207-213.

13. Vasechkin E.A., Taranov A.B. TEMPEST signal model of videointerfaces//SPIIRAN Works. 2016. — №4(47). — P. 46-64.

14. Egin A.V., Levin D.V., Parshutkin A.V. Generalized mathematical model of the effect of active interference on the technical means of TEMPEST intercepting from raster information display systems //Proceedings of the Mozhaysky Military Space Academy. — 2016. — №651. — P. 62-70.

15. Zheleznov D.I., Mischenko D.A. Information leakage security through TEMPEST from computer videosystems//Scientific and practical electronic journal Science Alley . — 2017. — №10. — P. 62-70.

16. Parshutkin A.V., Egin A.V., Voznuk V.V., Levin D.V. Application of active noise suppression system TEMPEST when transmitting data according to DVI standard //University Journal Priborostroenie. — 2017. — T. 60. — №1. — P. 25-31.

17. Ryabinin A.M. Information transmission via channel based by the soft TEMPEST technology //Radioelectronic Devices and Systems for Infocommunication Technologies. Information Security. — 2015. — P. 436-439.

18. Ryabinin A.M., Filatov V.I., Belkov I.V. Model of a channel for transmitting information via software-controlled TEMPEST //Telecommunication and Transport. — 2016. — Том 10. — №1. — P. 77-80.

19. Antyasov I.S., Safonov A.V., Sokolov A.N. Software and hardware implementation of soft TEMPEST technology //UrFO Messenger. Information Security . — 2015. — №3(17). — P. 8-11.

20. Bonch-Bruevich A.M., Angenko A.A. The method of delayed analysis of TEMPEST signals in the tasks of assessing the security of telecommunication information//Radioelectronic Devices and Systems for Infocommunication Technologies. Information Security. —2015. — P. 402-404.

21. Jun B., Kenworthy G. Is Your Device Radiating Keys//RSA Conference. — 2012.

22. Genkin D., Pachmanov L., Pipman I., Tromer E. ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs//Proc. RSA Conference Cryptographers' Track. —2016. — P. 219-235.

23. Maslovsky V.M. The method of guaranteed protection of information from leakage through TEMPEST channels: PhD degree dissertation: 05.13.19. Saint-Petersburg, 2003. — 107 с.

24. Zaycev A.P., Mescheryakov R.V., Shelupanov A.A. Technical means and methods of information security. Textbook for Universities//Moscow: Goryachaya linia–Telecom, 2012. — P. 30-51.

25. Titov A.A. Technical means of information security//Tomsk: TUSUR, 2010. — P. 166-191.

26. Buzov G.A. Practical guidance on identifying special technical means of unauthorized obtaining information //Moscow: Goryachaya linia–Telecom, 2019. — P. 28-31.

27. Malyuk A.A. Information Security in the Information Society//Moscow: Goryachaya linia–Telecom, 2017. — P. 120-126.

28. Skripnik D.A. General issues of technical information security //Moscow .: NOU «INTUIT», 2012. — P. 120-126.

29. Zhigunova Y.A. Methodics and software for the searching informative harmonics of electromagnetic radiation signals from computer facilities: PhD degree dissertation: 05.13.01. Irkutsk, 2009. — 123 с.

30. Urbanovich P.V. Methods and means of generating electromagnetic noise: PhD degree dissertation: 05.13.19. Tomsk, 2010. — 143 с.

31. Petrov I.S. Localization and attenuation of TEMPEST from PC by shielding electromagnetic waves //JUGU Messenger. Computer technology, control, electronics Series. — 2012 г. — Vol.16. — №23(282). — P. 189–191.

32. Lyubchenkov A.V. Analysis of methods for measuring the electrodynamic parameters of materials absorbing microwave electromagnetic radiation //Voronezh State University Messenger — 2009. —T.5. — №9. — P.111-113.

33. Ostapenko A.G., Lyubchenkov A.V., Naumenko Y.S. Evaluation of the effectiveness of the use of radar absorbing materials from leakage through the TEMPEST channel at informatization facilities//Information and Security. — 2011. — T.14. — №1 — P. 113-116.

34. Kolbun N.V., Petrov S.N., Prudnik A.M. Electromagnetic and acoustic characteristics of multilayer materials for integrated protection systems//BGUIR Reports. — 2009. — №3(41). — P. 79-85.

Информация об авторе

Дмитрий Сергеевич Милько - аспирант, кафедра «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: dmitry.s.milko@gmail.com

Author

Dmitry Sergeyevich Milko, Postgraduate Student, «Information Systems and Information Security», Irkutsk State Transport University, Irkutsk, e-mail: dmitry.s.milko@gmail.com

Для цитирования

Милько Д.С. Современное состояние исследований, связанных с утечкой информации по каналам побочных электромагнитных излучений и наводок // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №1(6). – С. 52-63. DOI: 10.26731/2658-3704.2020.1(6).52-63 – Режим доступа: http://ismm-irgups.ru/toma/16-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 20.01.2020)

For citations

Milko D.S. Sovremennoe sostoyanie issledovaniy, svyazannyh s utechkoi informacii po kanalam pobochnyh electromagnitnyh izlucheniy i navodok [Current state of trancient electromagnetic pulse emanations standard researches] // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2020. No. 1(6). P. 52-63. DOI: 10.26731/2658-3704.2020.1(6).52-63 [Accessed 20/01/2020]