УДК 621.396.41

Д.А. Антипов

Анализ утечек информации на основе побочных электромагнитных излучений

Приведён систематизированный обзор исследований, посвященных каналу утечки информации через побочное электромагнитное излучение. По результатам обзора сделаны выводы об актуальности исследований в части снижения угроз утечки информации через побочное электромагнитное излучение. В частности, показано, что перспективным направлением является изучение направленности излучения. Выявлено преобладание программных способов устранения утечек над аппаратными, а также недостаток реализаций аппаратных решений.

Ключевые слова: защита информации, ПЭМИ, ОТСС, генераторы электромагнитного шума, съём информации, мягкий ПЭМИН.

doi: 10.21293/1818-0442-2018-21-2-27-32

Создание надежных систем обеспечения информационной безопасности является ключевым аспектом при проектировании комплексных систем безопасности [1, 2]. Это подтверждает необходимость общесистемного подхода при анализе рисков и оценке угроз безопасности, а также выявлении технических каналов утечки информации и обеспечения их надёжной защиты [3].

Канал утечки информации через побочное электромагнитное излучение (ПЭМИ) является одним из самых актуальных технических каналов утечки [4]. При обработке информации с помощью основных технических средств (ОТСС) неизбежно возникает ПЭМИ, несущее в себе информативный сигнал [5, 6].

Работа по защите канала утечки информации осуществляется на основе нормативных документов регуляторов, а также федеральных законов. В них описаны не только требования к информационным системам и их составляющим, но и методики оценки защищённости информации.

Основное направление исследований, посвящённых источникам ПЭМИ, излучающим информационный сигнал при использовании автоматизированных рабочих мест (АРМ), являются уязвимости экранов, жестких дисков и USB-устройств. Другие источники также изучаются, однако на практике уровень излучения от них мал, и утечка не реализуется.

Канал утечки информации традиционно делится на 3 составляющие (рис. 1):

1. Источник сигнала, под которым понимается любое радиоэлектронное устройство. Чаще рассматриваются источники, реализация угроз от которых экспериментально подтверждена.
2. Среда передачи (воздух, проводящие материалы и линии связи).
3. Устройство съёма информации, которое, как правило, включает блок обработки информации.

Области научных исследований можно условно разделить на 4 большие категории:

1. Исследования, связанные с обработкой сигнала, происходящей после съёма информации. Знания о структуре принимаемого сигнала упрощают процедуру его восстановления.

2. Исследования, связанные с источником ПЭМИ. В них речь идёт о переосмыслении характеристик и физики ПЭМИ от известных источников, а также о способах снижения уровня излучения.

3. Средства защиты информации, активные – генераторы электромагнитного шума и пассивные – экранирующие материалы. Основной темой исследования здесь выступают анализ излучения генераторов шума и решения по оптимизации их параметров.

4. Моделирование канала утечки. В этих работах показывается несостоятельность существующей классической модели канала утечки, а также предлагаются модели и способы оценки защищённости. Кроме того, рассматриваются потенциальные новые проявления канала утечки.

Рис. 1. Функциональная схема канала утечки информации

Обработка сигнала

В статье [7] говорится о том, что реализация утечки от монитора является более вероятной, чем это принято считать. Информативный сигнал восстанавливается с помощью статистической обработки на основе знаний о форме и периодичности сигнала. Проведённый эксперимент показал возможность реализации угрозы утечки на расстоянии 46 м от источника излучения.

Так как передача информации по шине USB тоже является дискретным случайным процессом с точки зрения съёма информации, а характеристики фронтов известны заранее, то можно использовать математический аппарат для восстановления информативного сигнала из смеси «сигнал+шум» [8]. В результате исследования авторы представили модель, которая позволила повысить возможность восстановления информативного сигнала на 3–6 дБ в зависимости от типа присутствующих помех.

Способ оценки защищённости предложен в работе [9]. Этот способ основан на расчёте информационной ёмкости канала, которая рассчитывается на основе проведённых измерений. Полученная ёмкость канала сравнивается с его пропускной способностью, которая рассчитывается на основе характеристик устройства. Если ёмкость канала утечки информации больше рассчитанной пропускной способности, можно говорить о риске реализации утечки.

Подход [10] также заслуживает внимания. Автор [10] руководствуется формулой Шеннона–Хартли, позволяющей оценить пропускную способность канала передачи данных. Учитывая соотношение «сигнал/шум», производится её пересчёт, что выражается в максимальном разрешении изображения, которое способен перехватить злоумышленник. Уменьшение разрешения экрана при работе способно повысить защищённость, так как его будет сложнее восстановить. Однако автор [10] не учитывает особенности сигналов и шума, а также отсутствуют экспериментальные подтверждения приведённым рассуждениям, что затрудняет оценку их достоверности.

Средства защиты информации

В работе [11] описана техническая реализация режекторного фильтра, позволяющего генератору электромагнитного шума (ГЭШ) осуществлять селективное зашумление. Такое решение позволяет создать «окно» в спектре ГЭШ, в котором может работать гражданское устройство, не испытывая на себе действие генератора. Кроме того, разработанное устройство обладает возможностью подстройки частоты режекции в пределах 10–20 МГц.

В работах [12, 13] расширяется этот подход. Однако из-за технических трудностей диапазон частот, на которые может быть настроен этот режекторный фильтр, имеет ограничения по ширине и не может лежать в области высоких частот. Это делает такой подход неприменимым на практике, ведь большинство информационных сигналов лежат в полосе от 100 МГц и выше.

Работа [14] посвящена изучению эффективности применения структурных помех. Автор утверждает, что имитирующая помеха позволяет снизить общий уровень излучаемой мощности без потерь в защищённости. Также предложена модель оценки эффективности таких помех.

Работа [15] посвящена проблемам маскирования ПЭМИ. К проблемам построения адаптивных ГЭШ автор [15] подходит иначе. Суть его исследований в возможности генерирования шумоподобной помехи, используя как несущую квазигармонический сигнал, модулируя его низкочастотным сигналом. На определённой частоте имеется возможность установить помеху, которая будет обладать лучшими характеристиками зашумления по сравнению с привычным шумом от ГЭШ.

Один из основных недостатков ГЭШ, существующих в настоящее время и широко обсуждаемый сообществом, – это недостаточная полоса зашумле-

ния. В работе [16] рассматриваются современные интерфейсы передачи изображения. Видовая информация, или информация, перехватываемая с экрана АРМ, обладает наибольшей информативностью для злоумышленника. Согласно полученным результатам в работе [16], частоты первой гармоники некоторых цифровых интерфейсов передачи изображения могут выходить за 2 ГГц, что оставляет возможность для реализации уязвимости из-за технических характеристик некоторых ГЭШ.

В работе [17] автор представляет оценку эффективности маскирования сигнала подобным ему шумом. Сигнал ПЭМИ сначала записывается, а затем излучается в пространство как шумоподобная помеха. Из-за высокой схожести этих сигналов друг с другом задача по их различению и выделению информативного сигнала усложняется. Оценке возможности этого восстановления и посвящена работа [17].

В работе [18] также обращается внимание на возможность повысить защищённость, манипулируя формой шумового сигнала путём создания помехи компенсационного типа. Реализованная селекция приёма ПЭМИ в устройствах снятия информации делает ГЭШ неэффективными из-за различий между структурой информационного сигнала и шума. Предлагается реализовывать защиту в виде ретрансляторов, устанавливаемых непосредственно в близости устройства, излучающего ПЭМИ. Принимая ПЭМИ, обрабатывая его и излучая компенсационный шум, можно добиться высокого уровня защиты при минимально возможном уровне излучаемой мощности. Для развязки приёмного и передающего трактов у ретранслятора рекомендуется применять направленные антенны, которые ориентируются в сторону предполагаемого размещения устройства съёма информации.

В работе [19] авторы отмечают недостатки активных средств защиты информации, такие как вредность высокого уровня излучения для здоровья. Электромагнитный шум является демаскирующим признаком работы ГЭШ, что привлекает интерес злоумышленников к объекту. Кроме того, активный метод защиты информации (ЗИ) не обеспечивает гарантированную защиту от перехвата информации. Сам перехват, по мнению авторов [19], можно совершить с помощью доступного лабораторного оборудования, такого как анализатор спектра, антенна и средство обработки цифровых сигналов.

Моделирование канала утечки

Авторы [20] строят модель функционирования канала утечки информации. Рассматривается структура технического канала, в которой показывается набор элементов, участвующих в нём. Такая модель позволяет оценивать защищённость системы на этапе планирования мероприятий по её защите. Кроме того, результаты работы являются базой для дальнейших исследований составных элементов канала утечки.

В работе [21] выдвинуто предложение по коррекции расчёта коэффициента затухания. Показано,

что при правильной оценке коэффициента ослабления можно получить результаты, отличающиеся от классического подхода. Для расстояния от точки излучения в 30 и 50 см – 30 и 34 дБ соответственно.

Также обсуждается и тестовый режим работы средства вычислительной техники [22]. По мнению автора [22], эта тема приобретает актуальность в связи с переходом от аналоговых сигналов к цифровым. Цифровой сигнал обладает особыми характеристиками. Это связано с кодированием информации, а также с различной структурой протоколов обмена информацией.

В работе [23] показывается возможность реализации оптического канала утечки информации от индикационных светодиодов таких устройств, как жёсткие диски, сетевые карты и др. Этот канал авторы называют «optical TEMPEST» и экспериментально доказывают возможность перехвата информативного оптического излучения. Хотя канал и не обладает электромагнитной природой распространения, он имеет право быть отнесённым к группе каналов утечки, связанной с побочным излучением. В данном случае излучение является оптическим.

Источники сигнала

Вариация программного способа защиты видовой информации предлагается в [24]. Так как цифровой сигнал монитора состоит из блоков данных, кодирующих цвет каждого пикселя по формату RGB, то авторы [24] предлагают оставить информационным только один цветовой канал, а на других двух генерировать шум. Пользователь может настроить у монитора фильтр цветových каналов, чтобы его не отвлекал их шум от работы. Рассматриваются различные способы манипуляции уровнем сигнала цветových каналов, а также делается вывод о продуктивности такого способа обеспечения информационной безопасности.

Угроза утечки информации по шине данных USB распространяется даже на линии, по которым не передаётся информативный сигнал, демонстрируется в работе [25]. Из-за близости разъёмов USB в одном USB-хабе информативный сигнал одних разъёмов может наводиться на линии других незадействованных разъёмов.

Перехват информации от жёсткого диска, согласно исследованию [26], затруднён из-за слабого уровня сигнала. Это происходит, даже если используются специальные последовательности сигналов для максимизации амплитуд сигналов. Автор утверждает, что для защиты информации от жестких дисков можно обойтись пассивными мерами: экранированием и заземлением АРМ. Хотя некоторые исследования показывают [27], что канал утечки реализуем.

Большой вклад в исследование сигналов принадлежит Markus G. Kuhn. Основная часть его работ [28–31] посвящена перехвату сигнала от мониторов. Ранние его публикации описывают перехват сигнала мониторов с электронно-лучевыми трубками (ЭЛТ), но в поздних работах возможность перехвата сигнала опытно доказана и для ЖК-мониторов. Суть его

исследований – в оценке угрозы перехвата информации, исследования частотных характеристик ПЭМИ, а также способах снизить риски реализации этого канала перехвата информации.

Оценивается угроза перехвата по распространению электромагнитных волн и по излучаемой энергии. Согласно [28], можно снизить угрозу, расширив контролируемую зону так, чтобы сигнал от монитора снизился до невозможности его восстановления. Можно влиять на уровень излучаемой энергии, управляя информацией, выводимой на экран. Специальным способом окрашивая пиксели, можно сгладить пики излучения, что затруднит восстановление цифрового сигнала.

В работе [32] отмечается, что недостаточное внимание уделено источникам ПЭМИ, находящимся внутри устройства. Большинство исследований направлено на изучение работы соединительных интерфейсов. Было получено информативное ПЭМИ от блока лазерного принтера. Это стало возможным благодаря доработке этого блока, повышающей уровень побочного излучения. Фактически ПЭМИ может быть снято, но вероятность реализации такой угрозы крайне мала ввиду сложности выполнения.

Автор [33] рассматривает применимость пассивных средств защиты, анализируя возможность применения специальных экранирующих тканей. Обладающие высокими показателями экранирования, они могут использоваться вместе с ГЭШ. При этом предполагается, что ГЭШ будут работать на частотах до 1 ГГц, а распространение сигналов более высоких частот будут останавливаться тканями. Как показывают опыты [33], на частотах ниже 1 ГГц ткани не обеспечивают требуемую величину экранирования из-за своих физических свойств.

В работе [34] предложен схожий пассивный метод защиты. Он заключается во внедрении в резиновые материалы односторонних углеродных (карбоновых) нанотрубок. Такой материал обеспечивает поглощение 90% мощности сигнала в СВЧ-частотах.

Правильный выбор материалов для изготовления кабелей может значительно снизить излучаемый уровень шума в диапазоне 2–150 кГц. В работе [35] исследуются характеристики нанокристаллического феррита и его способность повышать электромагнитную совместимость с другими источниками сигналов этого диапазона частот.

Исследования [36] посвящены видовому каналу утечки информации. В работе [36] рассмотрена возможность восстановления изображения монитора по отражению от прочих поверхностей – зрачка глаза, бытовых предметов.

Выделяется также Soft TEMPEST, или «мягкое» ПЭМИ. Основная особенность данной вариации канала утечки в том, что на АРМ устанавливается специальное ПО для усиления ПЭМИ путём обращения к диску, при этом обращение производится именно к той информации, которая представляет ценность для злоумышленника. Soft TEMPEST также включает в себя и ПО, которое осложняет либо предотвращает

утечку. Изменяя отображаемые шрифты на экране, можно сделать ПЭМИ более стойкими к перехвату.

Заключение

Проведенный анализ исследований позволяет сделать следующие выводы:

1. Некоторые проблемы обеспечения защиты информации, возникающие из-за высокого уровня ПЭМИ от устройств в составе ОТСС, могут быть решены программным способом. Такой подход предпочтителен использованию активных средств защиты, так как является пассивным и не требует дополнительного оборудования. Пассивная защита от утечки через ПЭМИ разгружает радиодиапазон по сравнению с активными средствами постановки помехи.

2. Подходы к оптимизации работы активных средств защиты показывают свою эффективность в модели, но зачастую не имеют подтвержденной технической реализации.

3. Модель канала утечки, изложенная в нормативных документах регуляторов, обладает рядом недостатков, влияющих на точность оценки защищенности информации от утечки. Рассматривая источники излучения как систему радиоэлектронных устройств, можно точнее оценивать степень воздействия каждого элемента на защищенность информации.

4. Из-за перехода от аналоговой техники к цифровой происходит переоценка распространения сигналов. Ей подвергаются все характеристики сигнала, влияющие на возможность перехвата и восстановления информации. Однако недостаточно внимания уделяется направленности излучения информации. Работа [12] показывает, что использование информации о направленности расширяет возможности обеспечения защиты информации.

Учитывая внедряемость и практическую значимость результатов, можно выделить перспективные направления исследования:

- Программное изменение функционирования устройств, в том числе протоколов обмена информацией, что позволяет снизить уровень ПЭМИ.
- Разработка материалов, снижающих излучаемый уровень ПЭМИ.
- Глубокий анализ канала утечки, где каждый элемент рассматривается в системе с другими, а именно влияние элементов друг на друга. Благодаря системному подходу открываются новые аспекты канала утечки, представляющие угрозу защищенности информации.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУРа на 2017–2019 гг. (проект № 2.8172.2017/8.9).

Литература

1. Шелупанов А.А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия / А.А. Шелупанов, С.А. Лопарев // Вопросы защиты информации. – 2003. – С. 2–5.

2. Шелупанов А.А., Системный анализ в защите информации / А.А. Шелупанов, А.А. Шумский. – М: Гелиос, 2005. – 224 с.

3. Лось В.П. Основы информационной безопасности / В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов, Е.Б. Белов. – М.: Горячая линия – Телеком, 2006. – 544 с.

4. Мещеряков Р.В. Технические средства и методы защиты информации. – 7-е. изд. – М.: Горячая линия – Телеком, 2012. – 442 с.

5. Шелупанов А.А. Технические средства и методы защиты информации / А.А. Шелупанов, Р.В. Мещеряков, С.В. Скрыль, А.П. Зайцев. – М.: ООО «Изд-во Машиностроение», 2009. – 508 с.

6. Тимченко С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Тимченко, А.А. Шелупанов, С.В. Прищеп // Безопасность информационных технологий. – 2007. – С. 15–21.

7. Ugur Sarac Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system / Ugur Sarac, Isin Ezer Furkan Elibil // EUSIPCO 2012. – Buharest, august 2012. – PP. 1767–1771.

8. Соколов Р.И. Исследование системы синхронизации при восстановлении сигналов ПЭМИ USB-клавиатуры в условиях индустриального шума / Р.И. Соколов, Д.В. Астрецов // Изв. Самар. нНауч. центра Российской академии наук. – 2016. – № 18, вып. 2-3. – С. 881–885.

9. Tanaka H. Evaluation of information leakage via electromagnetic emanation and effectiveness of Tempest // Ieice Trans. Inf. & Syst. – № E91-D, Is. 5. – May 2008. – PP. 1439–1447.

10. Жалковский И.В. Определение энергетического критерия оценки защищенности информации от утечки по каналу побочных электромагнитных излучений // Докл. Белорус. гос. ун-та информатики и радиоэлектроники. – 2015, вып. 3 (89). – С. 107–111.

11. Урбанович П.В. Средство формирования шумовой электромагнитной помехи / П.В. Урбанович, Н.Т. Югов, А.А. Шелупанов // Научный вестник Новосиб. гос. техн. ун-та. – 2012. – С. 121–126.

12. Шелупанов А.А. Определение режимов для формирования полос частот средств активной защиты / А.А. Шелупанов, Н.Т. Югов, П.В. Урбанович // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 78–81.

13. Урбанович П.В. Генератор шума с подстройкой диапазонов // Доклады ТУСУРа. – 2008. – № 2 (18), ч. 1. – С. 9–11.

14. Егин А.В. Применение структурных и шумовых помех для защиты информации от утечки по каналу побочных электромагнитных излучений / А.В. Егин, С.А. Святкин, А.В. Паршуткин // Вопросы оборонной техники. Сер. 16: Технические средства противодействия терроризму. – 2016. – С. 27–34.

15. Землянухин П.А. Многоканальный адаптивный генератор шума для маскирования ПЭМИН // Изв. ЮФУ. Технические науки. – 2016. – Сент. – С. 82–93.

16. Слободчиков А.А. Побочные электромагнитные излучения интерфейсов LVDS, DVI, HDMI // Безопасность информационного пространства / Сб. матер. XV Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых. – Курган – 2016. – Дек. – С. 239–242.

17. Петров И.С. оценка энергетической эффективности метода формирования маскирующих помех путём записи/воспроизведения сигналов ПЭМИ от СВТ // Технологический ин-т ФГОУ ВПО «Южный федеральный университет». – Таганрог, 2010. – Вып. 14. – С. 171–175.

18. Богаченков К.Н. Особенности создания помех компенсационного типа для решения задач защиты

информации от утечки по техническим каналам / К.Н. Богаченков, П.А. Маслаков, В.В. Вознюк // Труды военно-космической академии им. А.Ф. Можайского. – 2015. – Вып. 646. – С. 83–92.

19. Семенов А.В. Утечка информации по каналам ПЭМИ и способы их защиты / А.В. Семенов, Н.В. Киреева // Международный журнал прикладных и фундаментальных исследований. – 2016. – Вып. 8-4. – С. 499–504.

20. Авсентьев А.О. Исследование условий возникновения технических каналов утечки информации по побочным электромагнитным излучениям на объектах информатизации / А.О. Авсентьев, А.Г. Вальде, О.С. Авсентьев // Вестник Воронеж. ин-та МВД России. – 2017. – С. 22–31.

21. Катруша А.Н. Оценка уровней побочных электромагнитных излучений на основе измерений в ближней зоне технического средства // Новая наука: от идеи к результату. – 2016. – С. 100–102.

22. Рыженко С.В. К вопросу о побочных электромагнитных излучениях современных интерфейсов средств вычислительной техники // Актуальные проблемы обеспечения информационной безопасности. – 2017. – С. 170–176.

23. David A. Umphress, Joe Loughry Information leakage from optical emanations // ACM Transactions on Information and System security. – August 2002. – № 5, Is. 3. – PP. 262–289.

24. Мищенко Д.А. Защита информации от утечки через побочные электромагнитные излучения видеосистемы компьютера / Д.А. Мищенко, Д.И. Железнов // Науч.-практ. электрон. журнал. Аллея науки. – 2017. – Вып. 10.

25. Daniel Genkin, Yuval Yarom, Damith Ranasinghe Yang Su USB Snooping Made easy: Crosstalk Leakage Attacks on USB Hubs // Матер. конф. «26th USENIX Security Symposium». – Vancouver, BC, Canada, 2017. – PP. 1145–1161.

26. Мельшиян М.А. Исследование возможности перехвата побочных электромагнитных излучений жестких дисков // Электрон. науч. журнал. – Июнь 2016. – Вып. № 5 (8). – С. 112–114.

27. Баюшкин С.С. Исследование возможности перехвата побочных электромагнитных излучений HDD ПЭВМ / С.С. Баюшкин, И.Ю. Назаров // Технологии XXI века: проблемы и перспективы развития: сб. ст. Междунар. науч.-практ. конф. – Июнь 2017. – Пенза. – Вып. 2, ч. 2. – С. 22–26.

28. Markus G. Kuhn. Compromising emanations: eavesdropping risks of computer displays / University of Cambridge. – Cambridge: Technical Report UCAM-CL-TR-577, 2003.

29. Markus G. Kuhn Electromagnetic Eavesdropping Risks of Flat-Panel Displays // 4th Workshop on Privacy Enhancing Technologies. – Toronto, Canada, 2004. – PP. 88–107.

30. Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays // Proceedings 2002 IEEE Symposium on Security and Privacy, Berkeley, California, 12–15 May 2002. IEEE Computer Society. – Berkeley, California, USA. – May 2002. – PP. 3–18.

31. Markus G. Kuhn Security Limits for Compromising Emanations // CHES 2005. – 2005, Edinburgh, UK. – P. 265–279.

32. Дириенко Е.В. Исследование возможности получения информации с печатающего блока лазерного принтера по каналу ПЭМИ / Е.В. Дириенко, А.А. Голяков // Безопасность информационных технологий. – 2015. – С. 25–32.

33. Петигин А.Ф. Применение радиоэкранирующих тканей для защиты информации от утечки за счёт побочных электромагнитных излучений // REDS: Телекоммуникационные устройства и системы. – 2015. – №5, вып. 4. – С. 428–431.

34. Masahiro Horibe, Seisuke Ata, Takeo Yamadab, Kenji Hatab Yuto Kato Stretchable electromagnetic-interference shielding materials made of a long single-walled carbon-nanotube-elastomer composite // The Royal Society of Chemistry. – Feb. 2017. – PP. 10841–10847.

35. Jorge Victoria, Antonio Alcarria Adrian Suarez Characterization of Different Cable Ferrite Materials to Reduce the Electromagnetic Noise in the 2–150 kHz Frequency Range // MDPI. – Jan. 2018. – PP. 1–20.

36. Markus Durmuth, Dominique Unruh Michael Backes. Compromising reflections or how to read LCD monitors around the corner // 2008 IEEE Symposium on Security and Privacy. – Saarbrücken, Germany, 2008. – PP. 158–169.

Антипов Денис Александрович

Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа

Ленина пр-т, 40, г. Томск, Россия, 634050

Тел.: +7-983-345-93-68

Эл. почта: antipodp@gmail.com, antipodya@yandex.ru

Antipov D.A.

Analysis of information leaks based on spurious electromagnetic emissions

This systematic review of the research devoted to the channel of information leakage through secondary electromagnetic radiation is given. Based on the results of the survey, conclusions were drawn about the relevance of research in reducing the risks of information leakage through spurious electromagnetic radiation. In particular, it has been shown that the direction of radiation is a promising direction. The predominance of software methods for eliminating leaks over hardware was identified, as well as a lack of hardware implementations.

doi: 10.21293/1818-0442-2018-21-2-27-32

References

1. Shelupanov A.A., Loparev S.A. *Analiz instrumental'nyh sredstv ocenki riskov utechki informacii v komp'yuternoj seti predpriyatiya* [Analysis of tools for assessing the risks of information leakage in an enterprise computer network]. Questions of information protection, 2003, pp. 2–5.

2. Shelupanov A.A., Shumsky A.A. *Sistemnyy analiz v zashchite informacii* [System analysis in the protection of information]. Moscow: Helios, 2005, 224 p.

3. Los V.P., Meshcheryakov R.V., Shelupanov A.A., Belov E.B. *Osnovy informacionnoy bezopasnosti* [Information security basics]. Moscow: Hot line – Telecom, 2006, 544 p.

4. Meshcheryakov R.V., Shelupanov A.A., Zaitsev A.P. *Tekhnicheskie sredstva i metody zashchity informacii* [Technical means and methods of information protection]. 7th edition, Moscow: Hot line – Telecom, 2012, 442 p.

5. Shelupanov A.A., Meshcheryakov R.V., Skryl S.V., Zaitsev A.P. *Tekhnicheskie sredstva i metody zashchity informacii* [Technical means and methods of information protection]. Moscow: ООО «Izdatelstvo Mashinostroenie», 2009, 508 p.

6. Timchenko S.V., Shelupanov A.A., Prishchep S.V. Approaches and criteria for assessing the risks of information security. *The safety of information technology*, 2007, pp. 15–21.

7. Ugur Sarac, Isin Erer, Furkan Elibol, Realistic eavesdropping attacks. *EUSIPCO 2012*, Buharest, august 2012, pp. 1767–1771.

8. Sokolov R.I., Astretsov D.V. Investigation of the synchronization system during recovery of the USB keyboard signals in the conditions of industrial noise. *Izvestiya of Samara Scientific Center*, Russian Academy of Sciences, no. 18, iss. 2-3, 2016, pp. 881–885.
9. Tanaka H. Evaluation of information leakage via electromagnetic emanation and effectiveness of Tempest. *IEICE TRANS. INF. & SYST.*, no. E91-D., iss. 5, May 2008, pp. 1439–1447.
10. Zhalkovsky I.V. Determination of the energy criterion for estimating the security of information from leakage through the channel of spurious electromagnetic radiation. *Reports of the Belarusian State University of Informatics and Radioelectronics*, vol. 3 (89), 2015, pp. 107–111.
11. Urbanovich P.V., Yugov N.T., Shelupanov A.A. Means of formation of noise electromagnetic interference. *Scientific Bulletin of Novosibirsk State Technical University*, 2012, pp. 121–126.
12. Shelupanov A.A., Yugov N.T., Urbanovich P.V. Determination of regimes for the formation of frequency bands of active protection means. *Reports of TUSUR*, No. 1 (21), part 1, June 2010, pp. 78–81.
13. Urbanovich P.V. The noise generator with tuning of ranges. *Proceedings of TUSUR University*, No. 2 (18), part 1, June 2008, pp. 9–11.
14. Egin A.V., Sviatkin S.A., Parshutkin A.V. Application of structural and noise interference to protect information from leakage through the channel of spurious electromagnetic radiation. *Questions of defensive technology*. Series 16: Technical Countermeasures to Terrorism, 2016, pp. 27–34.
15. Zemlyanukhin P.A. Multichannel adaptive noise generator for masking PEMIN. *Izvestiya SFU. Technical science*, September 2016, pp. 82–93.
16. Slobodchikov A.A. Side-by-side electromagnetic emissions of LVDS, DVI, and HDMI interfaces. *Information Space Security. Collected materials of the XV All-Russian scientific-practical conference of students, graduate students and young scientists*, Kurgan, December 2016, pp. 239–242.
17. Petrov I.S. Estimating the energy efficiency of the method of forming masking interference by recording / reproducing PEMI signals from SVT. *Technological Institute of the Federal State Educational Institution of Higher Professional Education «Southern Federal University»*. Taganrog, no. 14, 2010, pp. 171–175.
18. Bogatchnikov K.N., Maslakov P.A., Voznyuk V.V. Features of creation of jamming of the compensating type for solving problems of information protection from leakage through technical channels. *Proceedings of the Military Space Academy*, no. 466, 2015, pp. 83–92.
19. Semenov A.V. Kireeva N.V. The leakage of information through the PEMI channels and ways to protect them. *International Journal of Applied and Fundamental Research*, no. 8-4, 2016, pp. 499–504.
20. Avsentiev A.O., Valde A.G., Avsentiev O.S. Investigation of the conditions for the emergence of technical information leakage channels for secondary electromagnetic radiation at information objects. *Vestnik Voronezhskogo Institute of the Ministry of Internal Affairs of Russia*, 2017, pp. 22–31.
21. Katrusha A.N., Estimation of the levels of spurious electromagnetic radiation based on measurements in the near zone of a technical device. *New Science: From Idea to Result*, 2016, pp. 100–102.
22. Ryzhenko S.V. To the question of secondary electromagnetic radiation of modern interfaces of computer facilities. *Actual problems of information security*, 2017, pp. 170–176.
23. David A. Umphress, Joe Loughry. Information leakage from optical emanations. *ACM Transactions on Information and System security*. No 5., Iss. 3, august 2002, pp. 262–289.
24. Mishchenko D.A., Zheleznov D.I. Protection of information from leakage through secondary electromagnetic radiation of the computer's video system. *Scientific and practical electronic journal Science Alley*, no. 10, 2017.
25. Daniel Genkin, Yuval Yarom, Damith Ranasinghe Yang Su USB Snooping Easily: attacks on crosstalk leakage on USB hubs. *Proceedings of the conference «26th Symposium on USENIX Security»*. Vancouver, British Columbia, Canada, 2017, pp. 1145–1161.
26. Mel'shiyan M.A. Investigation of the possibility of interception of spurious electromagnetic radiation of hard disks. *Electronic scientific journal*, No. 5 (8), June 2016, pp. 112–114.
27. Bayushkin S.S., Nazarov I.Y. Investigation of the possibility of interception of secondary electromagnetic radiations HDD. *Technologies of the XXI century: problems and development perspectives. Collection of articles of the International Scientific and Practical Conference*, Penza, Vol 2, p. 2, June 2017, pp. 22–26.
28. Markus G. Kuhn. Compromising emanations: eavesdropping risks of computer displays. University of Cambridge, Cambridge, *Technical Report UCAM-CL-TR-577*, 2003.
29. Markus G. Kuhn. Electromagnetic Eavesdropping Risks of Flat-Panel Displays, *4th Workshop on Privacy Enhancing Technologies*, Toronto, Canada, 2004, pp. 88–107.
30. Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays. *Proceedings 2002 IEEE Symposium on Security and Privacy*, Berkeley, California, 12–15 May 2002, IEEE Computer Society, Berkeley, California, USA, May 2002, pp. 3–18.
31. Markus G. Kuhn. Security Limits for Compromising Emanations. *CHES 2005*, Edinburgh, UK, 2005, pp. 265–279.
32. Dirienko E.V., Golyakov A.A. Investigation of the possibility of obtaining information from a printing unit of a laser printer via the PEMI channel. *IT Security*, 2015, pp. 25–32.
33. Petigin A.F. The use of radio-shielding fabrics to protect information from a spike due to spurious electromagnetic radiations. *REDS: Telecommunication Devices and Systems*, no. 5, iss. 4, 2015, pp. 428–431.
34. Masahiro Horibe, Seisuke Ata, Takeo Yamadab, Kenji Hatab Yuto Kato. Stretchable electromagnetic-interference shielding materials made of a long single-walled carbon-nanotube-elastomer composite. *The Royal Society of Chemistry*, Feb. 2017, pp. 10841–10847.
35. Jorge Victoria, Antonio Alcarria, Adrian Suarez. Characterization of Different Cable Ferrite Materials to Reduce the Electromagnetic Noise in the 2–150 kHz Frequency Range. *MDPI*, Jan. 2018, pp. 1–20.
36. Markus Durmuth, Dominique Unruh Michael Backes. Compromising reflections or how to read LCD monitors around the corner. *2008 IEEE Symposium on Security and Privacy*, Saarbrücken, Germany, 2008, pp. 158–169.

Denis A. Antipov

Post-graduate student. Integrated Information Security of Electronic Computing Systems, Tomsk University of Control Systems and Radioelectronics (TUSUR) Lenina av., 40, Tomsk, Russia, 634050
Tel.: +7-983-345-93-68
Email: antipodp@gmail.com, antipodya@yandex.ru