Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Майоров Андрей Игоревич

«Анализ каналов утечки информации, обрабатываемой на СВТ за счет побочных электромагнитных излучений и наводок»

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-39 80 02 Радиотехника, в том числе системы и устройства радионавигации, радиолокации и телевидения

_____

Научный руководитель

Титович Николай Алексеевич

Кандидат технических наук, доцент

_____

Минск 2019

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Зачастую, канал утечки информации через побочные электромагнитные излучения (далее – ПЭМИ) либо игнорируется, либо неизвестен. Однако, такой канал утечки информации имеет место быть. Одними из тех, кто обосновал и продемонстрировал метод съёма информации по каналу ПЭМИН являются Робин ван Эйк и Маркус Кун. Преимуществом такого метода съёма информации является отсутствие необходимости физического подключения к источнику информации или какого-либо воздействия на источник информации. Техническую разведку можно осуществлять за пределами контролируемой зоны, факт снятия информации установить практически невозможно. Гарантированно закрыть этот канал передачи информации можно только доведя соотношение опасный сигнал (от узлов средства вычислительной техники (далее – СВТ), обрабатывающей информацию)/шум на входе разведывательного радиоприёмника до величины, которая не позволит детектировать сигнал.

Выполнить эту задачу можно несколькими способами: увеличение контролируемой зоны вокруг СВТ, экранирование СВТ, применение средств защиты (генераторы шума, помехоподавляющие фильтры и т.д.). Очевидно, чтобы оценить возможность проведения технической разведки информации, обрабатываемой на СВТ, необходимо измерить либо рассчитать отношение опасный сигнал/шум на границах контролируемой зоны.

Для правильной оценки возможности утечки информации необходимо точно знать параметры ПЭМИ, однако зачастую параметры ПЭМИ носят случайный характер. Цель работы заключается в анализе ПЭМИ от различных устройств, входящих в состав типовой современной персональной электронной вычислительной машины для последующей правильной оценки рисков утечки информации по каналу ПЭМИ.

ВВЕДЕНИЕ

Значение информации в нашем мире непрерывно растет. Во все времена сведения, имеющие важное военно-стратегическое значение для государства, тщательно скрывались и защищались. В настоящее время информация стала рыночным товаром, имеющим большой спрос как на внутреннем, так и на внешнем рынках. Информационные технологии постоянно совершенствуются, затрагивая все больше аспектов жизни современного общества.

Развитие новых информационных технологий сопровождается такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ к секретной и конфиденциальной информации. Особую остроту проблема защиты информации приобретает в связи с повсеместной и массовой «компьютеризацией» информационных процессов. Учитывая тот факт, что потеря информации может привести не только к экономическим убыткам компаний и организаций, но в некоторых случаях даже к человеческим жертвам, ее сохранение является актуальной проблемой. Поэтому защита информации в настоящее время становится одной из важнейших государственных задач в любой стране [1].

Отправной точкой в формировании системы защиты информации в Республике Беларусь выразилось в создании правовой базы. Приняты и введены в действие законы «О государственных секретах», «Об информации, информатизации и защите информации», «Об электронном документе и электронной цифровой подписи» и другие. Система защиты информации должна отвечать требованиям законов и других нормативных правовых актов, а также интересам пользователей информации. Целью данной работы является проведение анализа основных интерфейсов обработки информации персональных электронных вычислительных машин (далее – ПЭВМ), оценка рисков утечки информации по каналу побочных электромагнитных излучений (далее – ПЭМИ), обзор методов защиты от утечки информации по каналу ПЭМИ, а также предложен собственный метод снижения уровня ПЭМИ от видеотракта ПЭВМ.

В современном мире все больше информации обрабатывается с помощью ПЭВМ, во многих ведомствах активно внедряется электронный документооборот. Такое положение вещей обязывает уделять особое внимание защите информации, обрабатываемой на ПЭВМ. Однако, если направление программной защиты ПЭВМ (антивирусная защита, межсетевые экраны и т.д.) обширно представлено в различного рода литературе, направление технической защиты ПЭВМ в открытых источниках освещен крайне скудно.

Физические процессы, проходящие в технических устройствах ПЭВМ при обработке информации, создают в окружающем пространстве побочные электромагнитные, акустические и другие излучения. Подобные излучения

могут обнаруживаться на довольно значительных расстояниях и, следовательно, использоваться злоумышленниками, пытающимися получить доступ к конфиденциальной информации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первая открытая публикация об угрозе ПЭМИ принадлежит Кристиану Бекману, однако внимание научного сообщества к проблеме утечки информации по этому каналу привлек голландский ученый Вим ван Эйк, который на практике показал процесс перехвата изображения на мониторе с электронной лучевой трубкой (далее – ЭЛТ) на расстоянии. Идеи Ван Эйка продолжил в своих работах его соотечественник, Маркус Кун. Он доказал, что угрозе утечки информации через ПЭМИ подвержены не только мониторы с ЭЛТ но и жидкокристаллические (далее – ЖК) дисплеи. Развитие тактики применения перехвата ПЭМИ позволило целенаправленно управлять излучением компьютера с помощью программных закладок.

Русскоязычные открытые публикации на тему технической защиты информации в целом и об угрозе утечки информации по каналам ПЭМИ в частности стали появляться с середины 90-х годов 20-го века. Основные работы по данной тематике принадлежат Кондратьеву А.В., Каторину Ю.Ф., Хореву А.А. Торокину А.А. Авторы рассматривают различные методики оценки возможности обнаружения побочных излучений технических средств. Также рассматриваются способы технической защиты информации. Активные методы защиты подразумевают использование различных генераторов шума в непосредственной близости от защищаемых технических средств. Пассивные методы используют экранирование и фильтрацию.

В последнее время вопросами утечки информации через побочные каналы активно занимаются израильские ученые. В конце 2013 года группа ученых опубликовала исследовательскую работу, в которой показали, что по звукам работы компьютера возможно восстановить секретный криптографический ключ, с помощью которого данный компьютер шифрует информацию. В 2014 году эта же группа продемонстрировала сравнительно дешевую электромагнитную атаку, которая позволила извлечь секретные ключи шифрования с персонального компьютера, замеряя электромагнитное излучение с расстояния до метра. Также они, усовершенствовали технологию *Soft TEMPEST* и продемонстрировали перехват с расстояния около 7 метров, используя в качестве приемника мобильный телефон со специальным программным обеспечением. В 2016 году была опубликована работа, посвященная оптическому каналу утечки информации.

Многие описанные выше исследования имеют относительно большой срок давности. Все эти годы работал закон Мура, значительно нарастивший возможности потенциальных злоумышленников. В частности, специализированное и весьма дорогостоящее широкополосное оборудование

для обработки сигналов, 15-20 лет назад доступное лишь государственным спецслужбам или очень богатым корпорациям, сейчас может быть эффективно заменено платой с программируемой логической интегральной схемой, общая цена которой не превышает сотни долларов. Вместе с тем стали появляться недорогие и в то же время очень мощные сигнально-процессорные системы, настраиваемые под произвольную конкретную задачу, так называемые программно-определяемые радиосистемы. Параллельно достигнут очень существенный прогресс в области общедоступных ультраширокополосных систем связи, электронные компоненты которых, все чаще встречаются в недорогой потребительской электронике.

Перечисленные выше факты свидетельствуют о том, что направление технической защиты информации не теряет своей актуальности, а также делают насущно необходимой новую переоценку рисков и угроз перехвата информации через ПЭМИ. В перечень потенциальных целей теперь попадают не только средства вычислительной техники, обрабатывающие информацию, содержащую государственную тайну государств, коммерческую тайну банков и других финансовых организаций либо промышленные секреты предприятий, но и ПЭВМ частных лиц.

В главе 2 приведены физические основы возникновения ПЭМИ и приведены рекомендации для увеличения отношения сигнал/шум при измерении ПЭМИ.

Наиболее реальной моделью сигнала в цепях ПЭВМ будет последовательность таких пакетов, в которых длина пакета существенно больше длительности одного импульса.

Спектр такого сигнала можно описать выражением (1).

$$S(f) = |S_0(f)||S_\varepsilon(f)| = t_u \left|\frac{sin(\pi f t_и)}{\pi f t_и}\right| \left|\frac{sin(\pi n f T_n)}{\pi f T_n}\right| \qquad (1)$$

где:

$S_0(f)$ – спектр одиночного прямоугольного импульса;

$S_\varepsilon(f)$ – спектр огибающей последовательности прямоугольных импульсов;

f – частота;

$T_n \approx \frac{k}{f_p}$ – период следования импульсов;

k – скважность импульсов, принимающая значения только из множества натуральных чисел;

$t_и \approx \frac{1}{f_p}$ – длительность импульса;

n – число импульсов в последовательности.

Такая последовательность и ее спектр приведены на рисунке 1

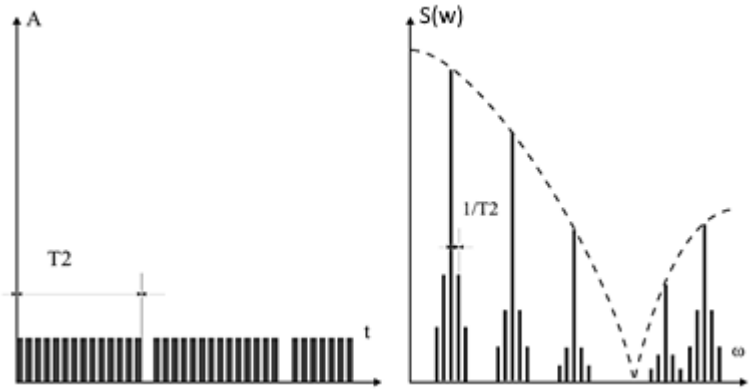

Рисунок 1 – Спектр последовательности пакетных импульсов

Исследование уровня ПЭМИ от ПЭВМ основывается на общих принципах измерений напряженностей электрических и магнитных полей. Специфика этих измерений состоит в том, что, во-первых, измеряемые сигналы являются маломощными, во-вторых заранее сложно предсказать картину электромагнитных излучений конкретного СВТ.

Реальные информативные сигналы ПЭМИ не являются периодическими и, соответственно, спектр таких сигналов может не иметь ярко выраженных пиков. Поэтому для облегчения задачи обнаружения сигналов и для измерения максимального уровня ПЭМИ исследуемое техническое средство вводится в специальный режим работы (далее – тест-режим).

Тест-режим должен обеспечить как можно большее количество изменений направления тока в проводящих линиях, что сформирует максимальный уровень ПЭМИ от технического средства. Применимо к цифровым интерфейсам – получить максимальное количество переходов из «1» в «0» и наоборот. С другой стороны, тест-режим должен создать в проводных линиях периодический сигнал для упрощения задачи обнаружения и дальнейшего измерения уровня ПЭМИ. Перечисленным выше требованиям больше всего удовлетворяет сигнал типа «меандр».

В реальных устройствах подобрать тест-режим, обеспечивающий такой сигнал, зачастую бывает затруднительно, однако необходимо создать такой режим работы, который обеспечивает максимально похожий по структуре сигнал.

В главе 3 описываются источники ПЭМИ ПЭВМ. Условно весь спектр излучений ПЭМИ можно разбить на информативные и неинформативные излучения.

Составляющие спектра ПЭМИ, порождаемые протеканием токов в цепях, по которым передаются сигналы, содержащие информацию, являются информативными ПЭМИ.

В частности, для ПЭВМ информативными ПЭМИ являются излучения, формируемые следующими цепями:

– цепью передачи сигналов от контроллера клавиатуры к порту ввода;

– цепями передачи видеосигнала от видеоадаптера до монитора;

– внутренними интерфейсами видеотракта;

– цепями шины данных системной шины компьютера;

– цепями шины данных внутри микропроцессора, и т.д.

Неинформативными ПЭМИ являются излучения, формируемые следующими цепями:

– цепями формирования и передачи сигналов синхронизации;

– цепями формирования шины управления и шины адреса системной шины;

– цепями передачи сигналов аппаратных прерываний;

– внутренними цепями блока питания ПЭВМ.

В главе 4 проводится детальный анализ основных интерфейсов современной ПЭВМ.

В состав видеотракта типичного ПЭВМ входит видеоконтроллер, монитор и интерфейс, который их объединяет. В настоящее время в большинстве интерфейсов используется один из трех стандартов: *Video Graphics Array* (далее – *VGA*) - передача изображения на монитор с помощью аналогового сигнала, *Digital Visual Interface* (далее – *DVI*) - передача видеоизображения на монитор с помощью цифрового сигнала, *High Definition Multimedia Interface* (далее – *HDMI*) по принципу передачи не отличается от *DVI* и поддерживает передачу звука. В мониторе, в свою очередь, для передачи информации к оконечным исполняющим устройствам используются внутренние интерфейсы:

– интерфейс между видеоконтроллером и модулем ЖК-дисплея в ноутбуках (длина соединения 30…50 см);

– интерфейс между платой видеоконтроллера компьютера и внешним ЖК-монитором (длина соединения 120…150 см);

– внутренний интерфейс между дисплейный контроллером и микросхемами драйверов столбцов (длина соединения 20…30 см).

Для интерфейсов видеотракта на языке программирования *Processing* были разработаны программы, вводящие эти интерфейсы в тест-режим

Практически любое устройство из накопителей информации является с точки зрения ПЭМИ двумя устройствами: интерфейсом связи с собственно ПЭВМ и узлом записи на носитель. В работе рассмотрен интерфейс *Serial Advanced Technology Attachment* (далее – *SATA*) — последовательный интерфейс обмена данными с накопителями информации и интерфейсы записи

информации на магнитные и оптические носители. Также в работе рассматриваются интерфейсы связи ПЭВМ с периферийными устройствами (протоколы *USB* и *PS/2*). Даны рекомендации для увеличения отношения сигнал/шум при измерении ПЭМИ этих интерфейсов.

В главе 5 приводятся результаты экспериментальных исследований по обнаружению и измерению уровня ПЭМИ интерфейсов ПЭВМ. Измерение ПЭМИ от ПЭВМ основывается на общих принципах измерений напряженностей электрических и магнитных полей. Специфика этих измерений состоит в том, что, во-первых, измеряемые сигналы являются маломощными, во-вторых заранее сложно предсказать картину электромагнитных излучений конкретного СВТ. Поэтому, измерению уровня сигналов ПЭМИ должен предшествовать процесс подтверждения того, что обнаруженный сигнал действительно является искомым.

Поиск и измерение уровня ПЭМИ в данной работе проводился по следующей методике:

1) измерительная антенна располагается вплотную к исследуемой ПЭВМ;
2) при выключенной ПЭВМ снимается панорама фоновых шумов;
3) при включенном на исследуемой ПЭВМ тест-режиме одного из интерфейса снимается панорама смеси ПЭМИ и фонового шума.
4) сравнивая обе полученные панорамы принимается решение о наличии и локализации по частоте сигнал ПЭМИ;
5) уровень ПЭМИ переизмеряется на расстоянии 1 метр от исследуемой ПЭВМ.

На рисунке 2 изображена типовая схема измерения ПЭМИ.

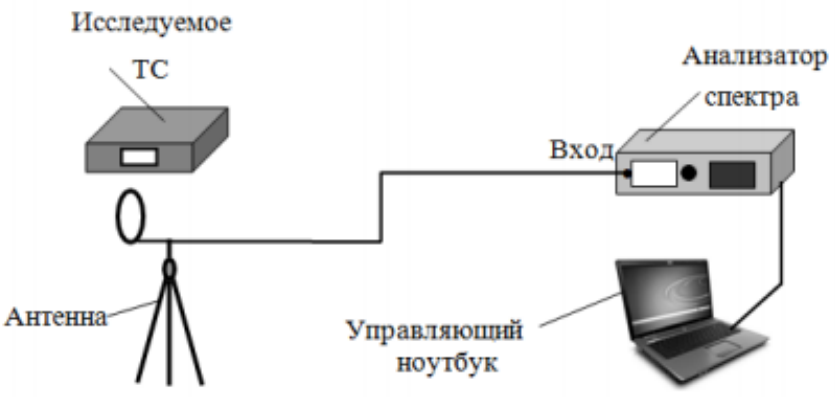

Рисунок 2 – Схема измерения ПЭМИ

В работе приведены результаты обнаружения ПЭМИ от следующих интерфейсов ПЭВМ: *VGA, DVI, LVDS, SATA* и *PS/2*. Даже не смотря на санитарные нормы, регламентирующие уровень электромагнитного излучения и нормы по электромагнитной совместимости, уровень ПЭМИ от составных

устройств ПЭВМ остается достаточно высоким, а значит есть реальный риск утечки информации по каналу ПЭМИ. Для минимизации рисков необходимо предпринимать меры защиты.

В главе 6 представлен обзор методов защиты от утечки информации по каналу ПЭМИ. Всю совокупность методов защиты информации, обрабатываемой на ПЭВМ, от утечки по каналу ПЭМИ можно разделить на организационные и технические меры.

К организационным мерам относится обеспечение вокруг функционирующего ПЭВМ контролируемой зоны (далее – КЗ) и исключение несанкционированного доступа к защищаемому ПЭВМ. КЗ – зона, в которой исключено несанкционированное пребывание сотрудников и посетителей организации, а также транспортных средств. Размер КЗ должен быть выбран таким образом, чтобы исключить возможность доступа злоумышленника к информационному сигналу с мощностью достаточной для его перехвата.

В качестве технических способов исключения возможностей перехвата информации за счет ПЭМИ ПЭВМ можно перечислить следующие:

– доработка ПЭВМ с целью минимизации уровня излучений;

– электромагнитное экранирование помещений, в которых расположена вычислительная техника;

– активная радиотехническая маскировка (зашумление);

– программные средства защиты.

Используя различные радиопоглощающие материалы и схемотехнические решения удается существенно снизить уровень излучений ПЭВМ. Стоимость подобной доработки зависит от размера имеющей в распоряжении контролируемой зоны и колеблется в пределах 20 – 200% от стоимости ПЭВМ.

Электромагнитная экранировка помещений в широком диапазоне частот является сложной технической задачей, требует значительных капитальных затрат и не всегда возможна по эстетическим и эргономическим соображениям. Защита такого рода применяется крайне редко, как правило, на ПЭВМ, обрабатывающих критически важную конфиденциальную информацию.

Активная радиотехническая маскировка предполагает формирование и излучение в непосредственной близости от ПЭВМ маскирующего сигнала. Этот метод значительно дешевле, чем предыдущие, однако возможности энергетической активной маскировки могут быть реализованы только в случае, если уровень излучений ПЭВМ существенно меньше норм на допускаемые радиопомехи от СВТ. В противном случае устройство активной энергетической маскировки будет создавать помехи различным радиоустройствам, расположенным поблизости от защищаемого ПЭВМ, и потребуется

согласование его установки с Государственной комиссией по радиочастотам при Совете Безопасности Республики Беларусь (далее – ГКРЧ).

Перспективным является неэнергетический (статистический) метод активной маскировки. Он заключается в изменении вероятностной структуры сигнала, принимаемого приемником злоумышленников, путем излучения специального маскирующего сигнала. Исходной предпосылкой в данном методе является случайный характер электромагнитных излучений ПК. Для описания этих излучений используется теория марковских случайных процессов. Сформированный с помощью оригинального алгоритма сигнал излучается в пространство компактным устройством, которое может устанавливаться как на корпусе самого ПК, так и в непосредственной близости от него. Уровень излучаемого этим устройством маскирующего сигнала не превосходит уровня информативных электромагнитных излучений ПЭВМ, поэтому согласования установки маскирующего устройства с ГКРЧ не требуется. Такие устройства эксплутируются в соседних странах, однако подобные устройства в реестре отсутсвуют.

Программные методы защиты заключаются в снижении уровня ПЭМИ за счет того, что информационные интерфейсы ПЭВМ вводятся в специальный режим с помощью специализированного программного обеспечения либо штатными средствами операционной системы. В рамках данной работы был разработан метод снижения уровня ПЭМИ видеоинтерфейса *VGA*.

Для затруднения перехвата текстовой информации с монитора атакуемой ПЭВМ необходимо уменьшить разницу напряжений каналов цветности фона и текста·ΔU. Для этого можно уменьшить яркость фона и увеличить яркость текста, тем самым уменьшить ΔU и, следовательно, затруднить распознавание текста. Однако, чем меньше·ΔU, тем сложнее будет исполнителю работать с текстом. Для различных сочетаний текста и фона были составлены программы для ввода интерфейса *VGA* исследуемой ПЭВМ, где вместо чередований черного и белого пикселя, чередовались пиксели цвета фона и цвета текста. Для каждого сочетания были измерены уровни ПЭМИ.

Чтобы оценить различимость текста более объективно, в рамках исследования был проведен опрос 100 респондентов разных возрастов и профессий. Респонденты выставляли оценки различимости текста на уровне фона по 10-ти бальной шкале, где 10 – черный текст на белом фоне. Результаты проведенного эксперимента представлены на рисунке 3.

Тестовая строка	Отношение С/Ш, дБмкВ/м	Средняя оценка различимости
Съешь ещё этих мягких французских булочек, да выпей чаю	32,96	10
Съешь ещё этих мягких французских булочек, да выпей чаю	25,31	9,6
Съешь ещё этих мягких французских булочек, да выпей чаю	20,28	8,6
Съешь ещё этих мягких французских булочек, да выпей чаю	13,41	6,8
Съешь ещё этих мягких французских булочек, да выпей чаю	8,73	4,1
Съешь ещё этих мягких французских булочек, да выпей чаю	2,27	0,9

Рисунок 3 – Результаты эксперимента по снижению ПЭМИ за счет уменьшения яркости

Как видно из рисунка 3, чем меньше уровень ПЭМИ, тем хуже различимость текста, однако, можно понизить уровень ПЭМИ на 10 дБ с незначительной потерей различимости текста на экране монитора.

Также снизить общий уровень ПЭМИ возможно при передаче информации только по одному цветовому каналу *VGA*. Эксперимент, описанный выше был повторен для образцов, которые реализуют все возможные варианты реализации такого метода. Результаты эксперимента представлены на рисунке 4.

Тестовая строка	Отношение С/Ш, дБмкВ/м	Средняя оценка читаемости
Съешь ещё этих мягких французских булочек, да выпей чаю	14,93	7,9
Съешь ещё этих мягких французских булочек да выпей чаю		8,3
Съешь еще этих мягких французских булочек, да выпей чаю	14,28	8,8
Съешь ещё этих мягких французских булочек, да выпей чаю		8,7
Съешь ещё этих мягких французских булочек, да выпей чаю	15,11	5,3
Съешь ещё этих мягких французских булочек, да выпей чаю		5,4

Рисунок 4 – Результаты эксперимента по снижению ПЭМИ за счет использования только одного канала цвета

Как видно из рисунка 4, при передаче информации только по одному цветовому каналу *VGA*, возможно снизить уровень ПЭМИ на 15 дБ при незначительной потери в читаемости текста.

Человеческий глаз воспринимает цвет, используя для зрения комбинацию из клеток-палочек и клеток-колбочек. В каждом глазе есть три типа колбочек, каждый из которых более чувствителен к коротким, средним

или длинным световым волнам. Комбинация сигналов, возможных во всех трёх колбочках, описывает диапазон цвета, который мы можем видеть своими глазами. Рисунок 5 иллюстрирует относительную чувствительность каждого типа колбочек ко всему видимому спектру приблизительно от 400 до 700 нм.

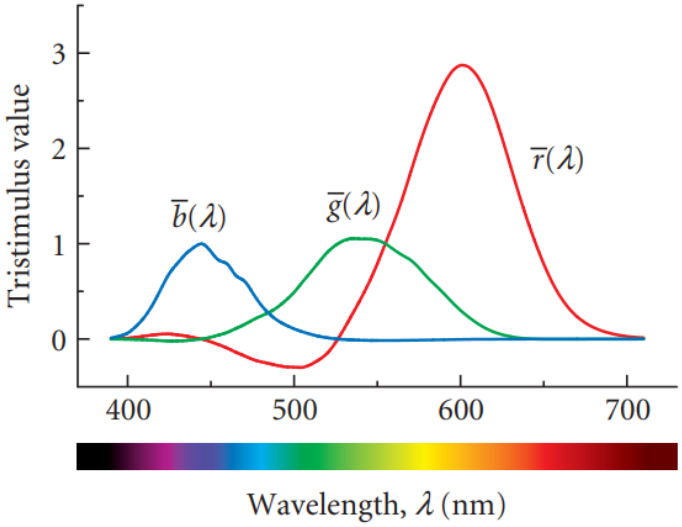

Рисунок 5 – Относительная чувствительность каждого типа колбочек к видимому спектру

Из рисунка 5 видно, что человеческое восприятие цвета максимально чувствительно к свету в жёлто-зелёном диапазоне спектра. Используя это свойство человеческого глаза, была предпринята попытка подобрать такое сочетание цветов фона и текста в желто-зелёной гамме, удовлетворяющее двум условиям: текст должен иметь хорошую различимость с фоном на дисплее исполнителя и сумма напряжений цветовых каналов фона равна сумме напряжений цветовых каналов текста. После получения приемлимых образцов – было проведено измерение уровня ПЭМИ и оценка читаемости текста. Результаты представлены на рисунке 6.

Тестовая строка	Отношение С/Ш, дБмкВ/м	Средняя оценка читаемости
Съешь ещё этих мягких французских булочек, да выпей чаю	1,56	1,2
Съешь ещё этих мягких французских булочек, да выпей чаю		1,5
Съешь ещё этих мягких французских булочек, да выпей чаю	7,43	6,3
Съешь ещё этих мягких французских булочек, да выпей чаю		6,8
Съешь ещё этих мягких французских булочек, да выпей чаю	11,63	6,9
Съешь ещё этих мягких французских булочек, да выпей чаю		7,7
Съешь ещё этих мягких французских булочек, да выпей чаю	1,44	6,8
Съешь ещё этих мягких французских булочек, да выпей чаю		6,8

Рисунок 6 – Скриншоты экрана при различных цветовых сочетаниях фона и шрифта

Как видно из рисунка 6, образцы в желто-зеленой гаме получили гораздо более высокие оценки, кроме того, у последнего образца отношение

сигнал/шум одно из самых малых из всех исследованных образцов. Кроме того, теоретически, изображение на мониторе составленное из таких цветов не может быть получено на экране оборудования злоумышленника текст и фон будет представлен одной и той же градацией серого. Задача распознавания текста злоумышленником в перехваченном изображении становится затруднительной.

Предложенный метод защиты информации не требует аппаратной части и может быть реализован программно путем интеграции в какой-либо программный продукт как дополнительное средство защиты.

ЗАКЛЮЧЕНИЕ

В работе обоснована актуальность рисков утечки информации, обрабатываемой на ПЭВМ, через канал ПЭМИ. Обоснованы физические принципы возникновения ТКУИ. Проведен анализ самых распространенных интерфейсов современной ПЭВМ. Исходя из анализа интерфейсов и математической модели ПЭМИ были разработаны программы для ввода различных видов интерфейсов в тест-режим, обеспечивающий максимальный уровень ПЭМИ исследуемых интерфейсов. Такое программное обеспечение существует, однако распространяется на платной основе и не всегда работает корректно. С помощью тест-программ и специализированных ПАК «Навигатор» и «СОЖ» был осуществлен поиск и измерение сигналов ПЭМИ ПЭВМ. Параметры обнаруженных сигналов подтверждают теоретические утверждения, изложенные в главах 1-4.

Данные, полученные в ходе экспериментов, описанных в главе 5, подтверждают потенциальную угрозу информационной безопасности, которую несут в себе ПЭМИ ПЭВМ. Угроза утечки информации по каналу ПЭМИ диктует необходимость принимать меры по защите информации от утечки по данному каналу. В главе 6 дано краткое описание существующих методов защиты и перспективные направления в этой области. Также предложен программный метод снижения ПЭМИ интерфейса *VGA*.

Развитие современных средств радиотехники, позволяющее принимать и декодировать сигналы с все меньшим и меньшим отношением сигнал/шум, а также развитие криптографии, которое максимально затрудняет процесс дешифрования закрытой информации, способствуют тому, что актуальность защиты информации от утечки по каналу ПЭМИ будет расти. Перехват ПЭМИ уже зачастую является единственным способом перехвата информации.

Результаты данной работы могут применяться специалистами по технической защите информации как в практических, так и методических целях.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Майоров А.И. Риск утечки конфиденциальной информации через видеотракт ПЭВМ по каналу ПЭМИН / А.И. Майоров, М.А. Буневич, К.Ю. Дорох // Сборник докладов 54-й научной конференции аспирантов, магистрантов и студентов УО «БГУИР» 2018. – Минск: БГУИР, 2018. С. 135-136
2. Майоров А.И. Защита изображения на дисплее ПЭВМ по каналу ПЭМИ / А.И. Майоров, Д.Ю. Колесник // Сборник докладов 23-й научно-практической конференции «Комплексная защита информации» М.: 2018. С. 342-348
3. Титович, Н. А. Снижение уровня побочных электромагнитных излучений видеотракта персональной электронно-вычислительной машины с использованием подбора цвета текста и фона / Н. А. Титович, А. И. Майоров, Д. А. Высоцкий // Технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно – технической конференции, Минск, 5 июня 2018 г. – Минск: БГУИР, 2018. – С. 92.
4. Майоров А.И. Актуальность защиты от утечек информации по каналу побочных излучений // Сборник материалов конференции "Информационная революция и вызовы новой эпохи — стимулы формирования современных подходов к информационной безопасности". – Минск, 2018 С. 45-49