DOI 10.37882/2223–2966.2022.04.08

ПАССИВНЫЕ МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПЭМИ

PASSIVE METHODS AND WAYS TO PROTECT CONFIDENTIAL INFORMATION FROM LEAKAGE THROUGH THE PEM CHANNEL

A. Vasilyev
S. Ryzhikov
I. Agureev

Summary. In addition to active means, passive methods can also be successfully used to protect against information leakage through the spurious radiation channel. This article discusses approaches based on matching the monitor screen resolution mode and the length of the interface cable, choosing a color palette and special fonts, which, in combination, significantly reduce the quality of the restored original text image to the point of impossibility of character recognition.

Keywords: TEMPEST fonts, SDR.

Васильев Андрей Савельевич
Старший преподаватель, Национальный исследовательский университет «МЭИ»
VasilyevAS@mpei.ru
Рыжиков Сергей Сергеевич
Доцент, Национальный исследовательский университет «МЭИ» RyzhikovSS@mpei.ru
Агуреев Иван Александрович
Национальный исследовательский университет «МЭИ»
universe@mpei.ac.ru

Аннотация. Для защиты от утечки информации по каналу побочных излучений кроме активных средств могут успешно применяться и пассивные методы. В данной статье рассмотрены подходы, основанные на согласовании режима разрешения экрана монитора и длины интерфейсного кабеля, выборе цветовой палитры и специальных шрифтов, позволяющие в комплексе значительно снизить вплоть до невозможности распознавания символов качество восстанавливаемого исходного текстового изображения.

Ключевые слова: ПЭМИ, TEMPEST шрифты, SDR.

В современных условиях использование технических каналов утечки информации из средств вычислительной техники представляет собой значительную угрозу защищаемой информации. Наиболее информативными являются устройства отображения, поскольку они предоставляют пользователям разнообразную визуальную информацию [1, 2].

К настоящему времени сформировался общий подход к защите информации от утечки конфиденциальной информации по каналу ПЭМИ, который заключается в том, что организация эффективной защиты возможна только на основе системного применения комплекса взаимодополняющих методов и средств защиты информации. Организационные методы реализуются посредством проведения комплекса мероприятий по установлению и поддержанию временных, территориальных и пространственных ограничений на условия функционирования и режим работы объекта, где обрабатывается конфиденциальная информация. Технические методы направлены на то, чтобы за пределами контролируемой зоны объекта, напряженности электромагнитного поля не превышали бы нормируемые значения, а также на затруднение злоумышленником процесса выделения и восстановления полезной информации из полученной в результате перехвата ПЭМИ.

При организации и проведении мероприятий по защите информации от утечки по каналу ПЭМИ одной из наиболее важных задач является определение величины зоны 2 (R2), которая характеризует минимальное расстояние от ПЭВМ, за пределами которого соотношение «сигнал/шум» $\Delta = Pc/Pш$ не превышает нормированного значения, что делает процесс перехвата для злоумышленника невозможным.

С этой целью видеосистема компьютера переводится в тестовый режим. При использовании интерфейса VGA на экране монитора отображаются черные и светлые вертикальные линии шириной в 1 пиксель, что обеспечивает максимальный уровень побочных излучений интерфейсным кабелем. Для интерфейсов DVI, HDMI и DisplayPort тестовые режимы иные. В тестовом режиме уровень ПЭМИ заведомо многократно превышает уровень побочных излучений при отображении на мониторе текстовой информации. Далее осуществляется поиск частот ПЭМИ, определяемых режимом разрешения экрана монитора.

Если величина зоны 2 (R2) превышает размеры контролируемой зоны — пространства (территории, здания, части здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических

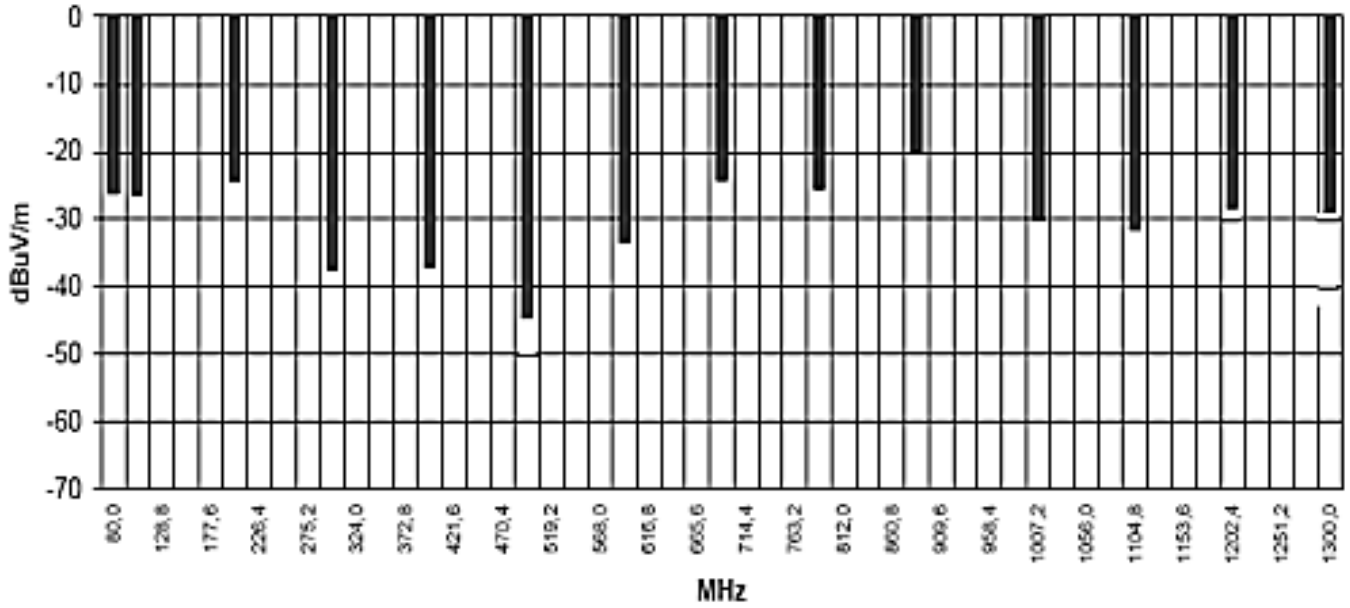


Рис. 1. Гистограмма спектральной чувствительности антенны для частот от 80 МГц до 1,3 ГГц

№ п/п	Частота излучения, МГц	Уровень ПЭМИ, дБмкВ/м
1	80,218734	71,72
2	160,437469	58,7
3	240,656203	66,91
4	320,874938	62,04
5	401,093672	59,54
6	481,312407	67,43
7	561,531141	62,56
8	641,749876	57,74
9	721,96861	52,51
10	802,187345	49,15

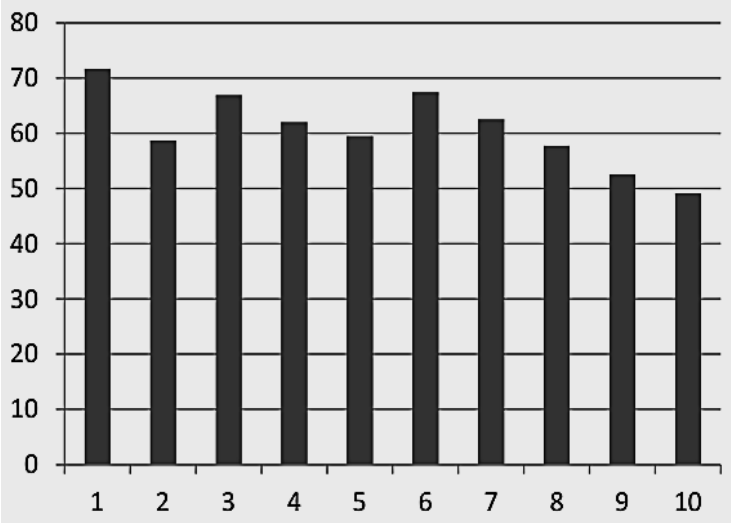


Рис. 2. Гистограмма уровня ПЭМИ для одного из режимов разрешения экрана монитора.

или иных средств [3], то необходимо принимать дополнительные меры по снижению уровня ПЭМИ и защиты конфиденциальной информации.

В [4] продемонстрирована взаимосвязь чувствительности приемной биконической измерительной антенны НБА-02 при приеме ПЭМИ в значительном диапазоне частот, что определяется соотношением между геометрическими размерами вибраторов антенны и длиной волны принимаемого излучения. Гистограммы спектральной чувствительности представлены на рис. 1.

Из представленных гистограмм видно, что максимальная чувствительность антенны зависит от кратности размеров ее вибраторов величине λ/4, где λ — длина волны принимаемого излучения. При кратности λ/2 — наблюдается снижение чувствительности.

При трансляции видеосигнала от видеокарты из системного блока на монитор интерфейсный кабель выступает в качестве передающей антенны, для которой характерна та же зависимость уровня побочного излучения от соотношения длины кабеля (совместно с длиной

Таблица 1. Значения амплитуды напряжения в зависимости от выбранного цвета

Цвет	Уровень амплитуды сигнала
Белый	~ 700.0 mV
Серый (насыщенность черным 12,5%)	~ 612.5 mV
Серый (насыщенность черным 25,0%)	~ 525.0 mV
Серый (насыщенность черным 37,5%)	~ 437.5 mV
Серый (насыщенность черным 50,0%)	~ 350.0 mV
Серый (насыщенность черным 62,5%)	~ 262.5 mV
Серый (насыщенность черным 75,0%)	~ 175.0 mV
Серый (насыщенность черным 87,5%)	~ 87.5 mV
Черный	~ 0.0 mV

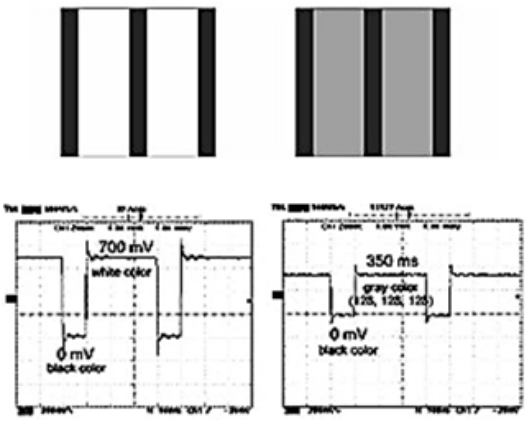


Рис. 3. Снижение амплитуды сигнала в интерфейсном кабеле

соответствующих печатных проводников видеокарты и платы монитора) и частоты (дины волны) ПЭМИ (рис. 2).

Так как частота ПЭМИ зависит от разрешения экрана монитора, то для кабеля определенной длины может быть подобран соответствующий режим развертки изображения (количество пикселей по горизонтали и по вертикали, частота обновления кадров в секунду), при котором уровень побочных излучений будет минимальным. Второй возможный вариант — подбор длины интерфейсного кабеля или изготовление его на заказ.

Другой подход к проблеме — это уменьшение интенсивности цветов, отображаемых на мониторе, что влияет на уменьшение разностей между пиковыми и минимальными значениями напряжения импульсов, отвечающих за отображение соответствующего графического знака.

Стандартная комбинация цветов, обычно используемая при работе с текстовыми документами, черный символы на белом фоне, отличается значительными разбросами амплитуды напряжения сигнала VGA в интерфейсном кабеле в зависимости от выбранного цвета (табл. 1).

В исследованиях [5, 6] рассматривается подход, который способствует защите текстовых данных от их перехвата по каналу ПЭМИ с последующим восстановлением символов за счет устранения значительных различий в значениях амплитуды видеосигнала стандарта VGA.

Изменение интенсивности фона позволяет значительно снизить максимальную амплитуду сигнала в интерфейсном кабеле (рис. 3), что сказывается на уменьшении уровня ПЭМИ.

Изменяя цветовую палитру фона и текста на значения меньшей разности для VGA интерфейса, можно существенно снизить уровни ПЭМИ (рис. 4) [5].

В DVI стандарте, где пиксель с примененным цветом кодируется через комбинацию 0 и 1, параметры напряжения электрического сигнала остаются без изменений и уровни ПЭМИ не зависят от изменения цветовой палитры фона и текста. В [8] приведены результаты исследований по определению факторов, влияющих на разборчивость текста на экране в зависимости от используемой цветовой палитры (рис. 5).

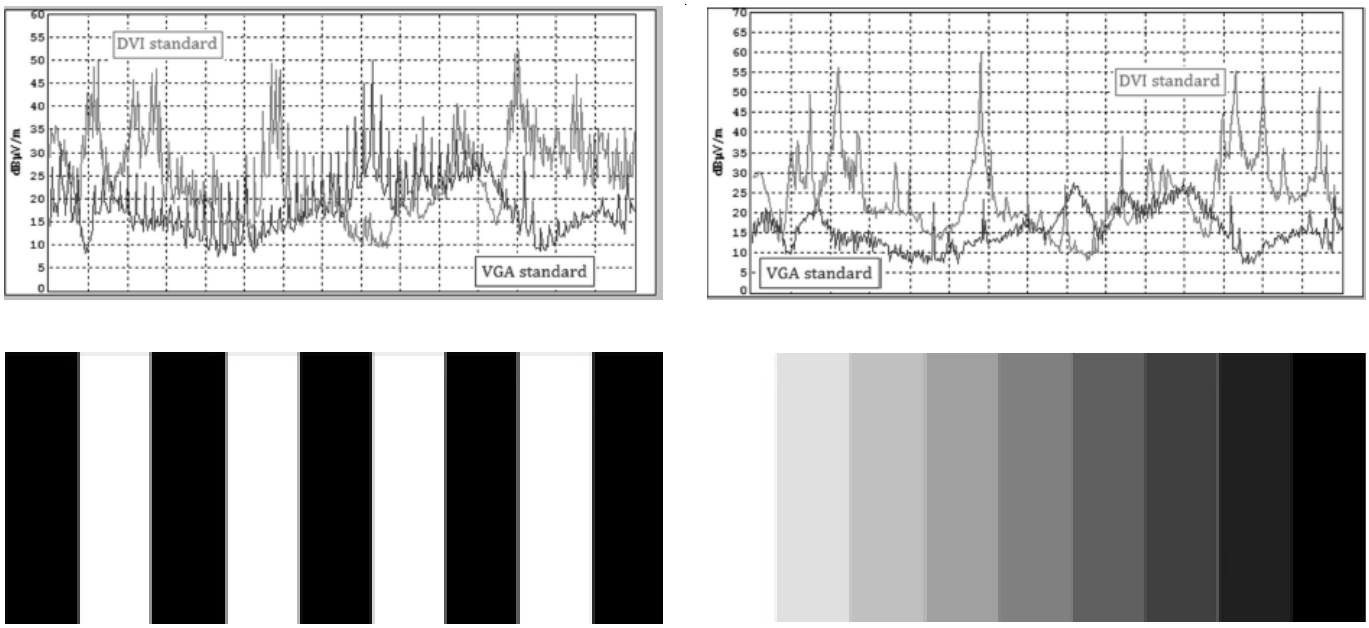


Рис. 4. Уровни электромагнитных излучений для черно-белого изображения и изображения с градациями серого

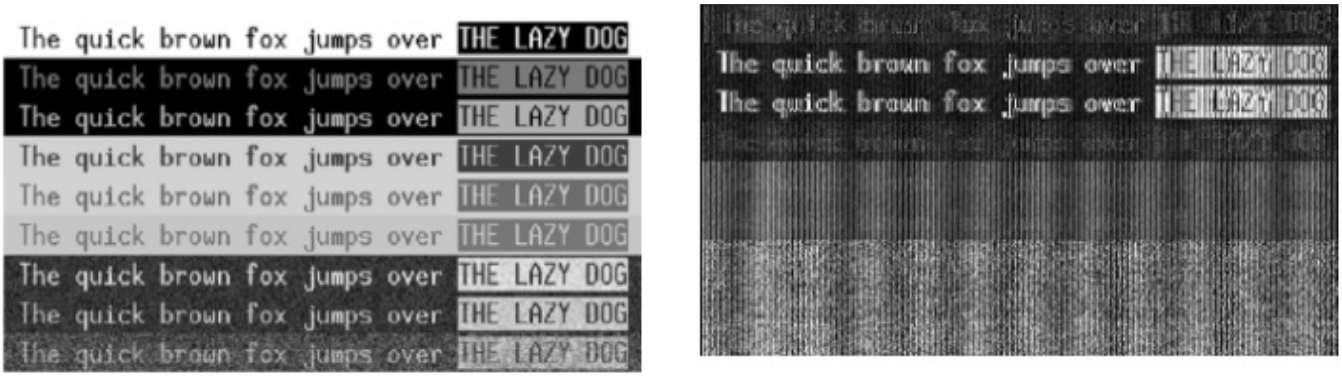


Рис. 5. Исходное (слева) и восстановленное из ПЭМИ (справа) сообщение

Следует отметить, что при работе с текстом необходимо, чтобы он сохранял свою разборчивость. Это означает, что все типографские параметры: размер и тип символа, цветовая палитра (цвет шрифта и цвет фона) должны быть выбраны таким образом, чтобы можно было воспринимать текст быстро и без проблем. Самые дружественные комбинации цветовой палитры (кроме крайних: белый фон и черный текст) имеют оттенки серого, с разницей, превышающей 50%.

В [6] приведены результаты теста на читаемость для разноцветных фонов и символов (Таблица 1), для которых комбинации, отличные от бело-черного и бело-темно-синего, снижают читаемость примерно на 20% и более и становятся очень утомительными.

Таким образом, можно утверждать, что оптимизация цветовой палитры (выбор цвета для фона и текста) способствует снижению уровня ПЭМИ, тем самым затрудняя для злоумышленника энергетическую доступность к отображаемой на мониторе информации. В случае использования стандарта VGA правильный выбор цвета может значительно уменьшить уровень электромагнитных излучений за счет снижения амплитуды напряжения электрического сигнала. Применительно к стандарту DVI из-за иного способа цветового кодирования оптимизация цветовой палитры не влияет на уровень побочных электромагнитных излучений.

Традиционные шрифты Arial и Times New Roman являются наиболее популярными при обработке текстовой инфор-

Таблица 2. Разборчивость символов для различных сочетаний цветов

Цвет текста	Цвет фона	Разборчивость символов (%)
Черный	Белый	100
Черный	Желтый	81
Желтый	Темно-синий	70
Желтый	Темно-зеленый	67
Белый	Черный	64
Желтый	Темно-красный	60
Черный	Красный	56
Желтый	Черный	56
Черный	Светло-синий	55
Черный	Светло-зеленый	53

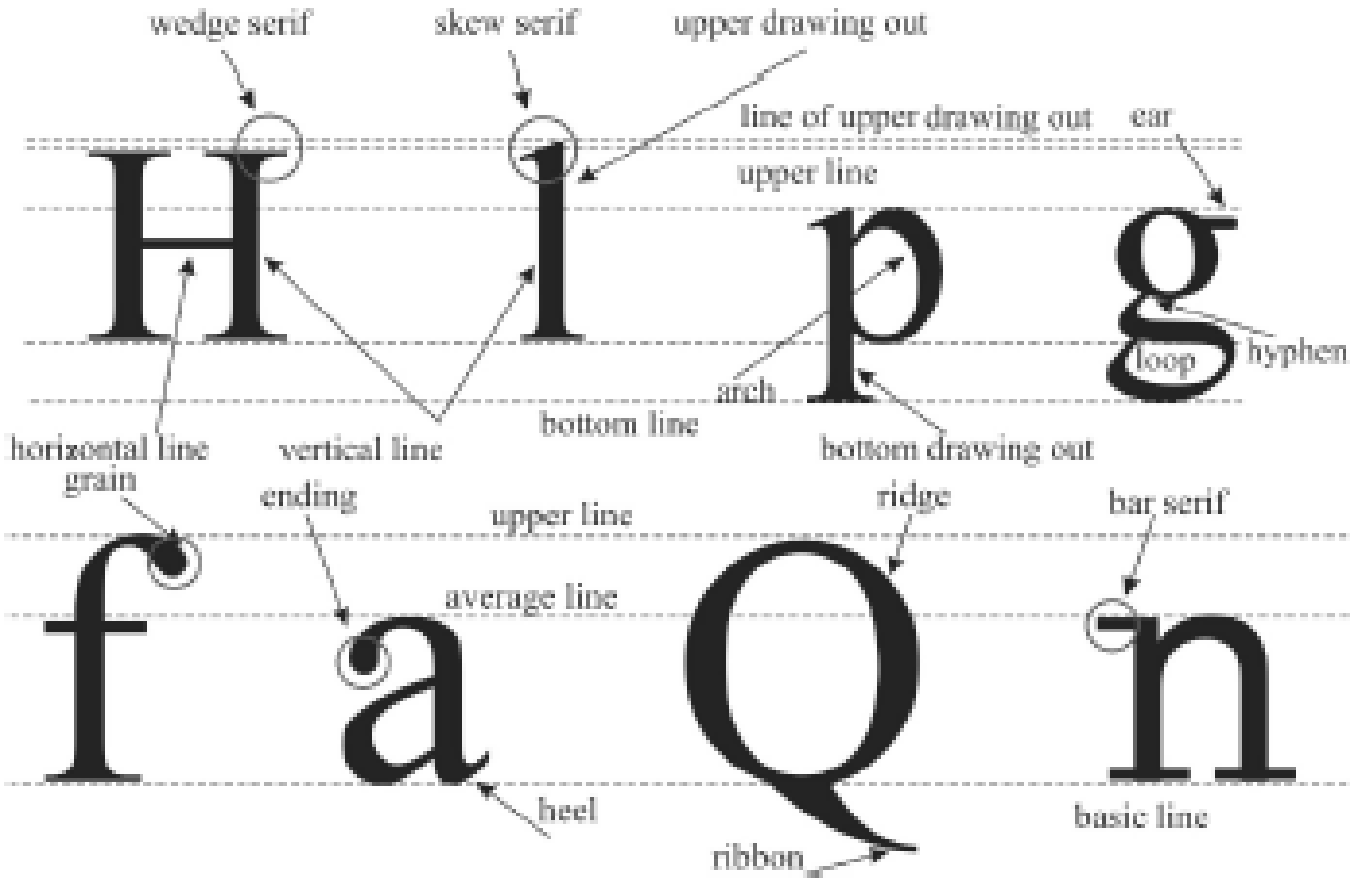


Рис. 6. Декоративные элементы шрифтов.

мации. Символы этих шрифтов имеют декоративные элементы (рис. 6), что значительно улучшает процесс распознавания перехваченных злоумышленником символов [9].

В [10] предложено универсальное решение для защиты обрабатываемой информации при ее утечке по каналу ПЭМИ на основе созданных безопасных шрифтов. Следует отметить, что эти шрифты могут применяться при использовании как VGA, так и DVI видеоинтерфейсов.

Предлагается три набора таких шрифтов: шрифт Symmetrical Safe, шрифт Asymmetrical Safe и шрифт Simply Safe (рис. 7).

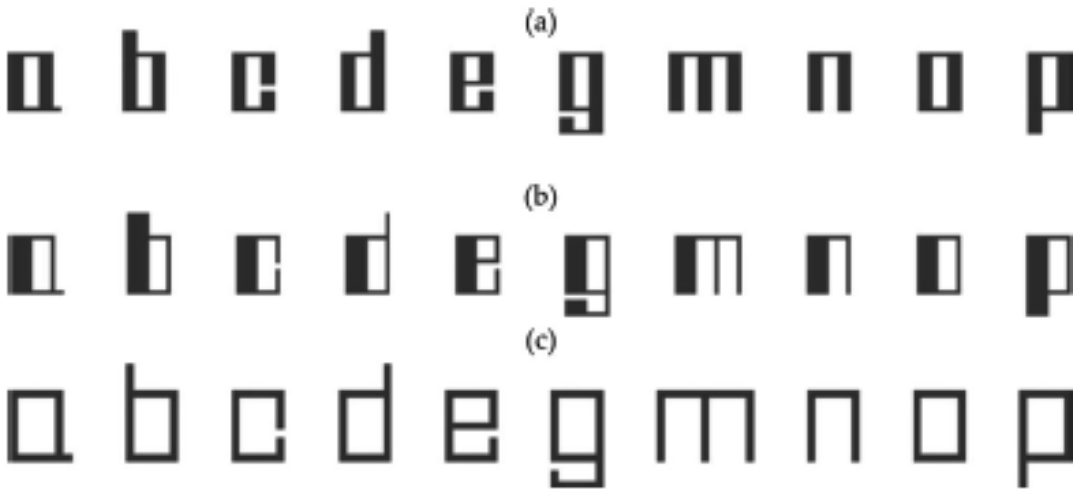


Рис. 7. Примеры символов безопасных шрифтов: (a) симметричный безопасный шрифт, (b) асимметричный безопасный шрифт и (c) просто безопасный шрифт.

Рис. 8. Отличительные особенности символа «a» Times New Roman.

Рис. 9. Конструкция символов симметричного безопасного шрифта.

Эти наборы шрифтов отличаются свойствами построения шрифтовых символов:

- Линии построения символов пересекаются под прямым углом (каждый символ строится только из вертикальных и горизонтальных линий).
- Символы шрифта лишены декоративных и диагональных элементов.
- Общий контур символов безопасного шрифта имеет форму прямоугольника.

Традиционные шрифты не соответствуют указанным требованиям. Далее несоответствие будет показано на примере печатного символа, соответствующего букве «a» (рис. 8).

Символы симметричного безопасного (Symmetrical Safe) шрифта (рис. 7a) лишены декоративных и диагональных элементов. Линии, образующие символы, пересекаются под прямым углом. Каж-

Таблица 3. Значения коэффициента ошибок применительно к отдельным выбранным символам традиционных и безопасных шрифтов.

Символ	Шрифт Arial	Шрифт Times New Roman	Шрифт Symmetrical Safe	Шрифт Asymmetrical Safe	Шрифт Simply Safe
VGA стандарт					
d	0	0	0	371	1
e	1	6	122	354	48
i	43	17	1	128	115
o	3	9	399	212	174
u	1	2	369	45	107
DVI стандарт					
d	4	4	25	95	72
e	4	4	140	45	65
i	46	14	42	15	153
o	36	7	60	236	351
u	7	3	104	542	6

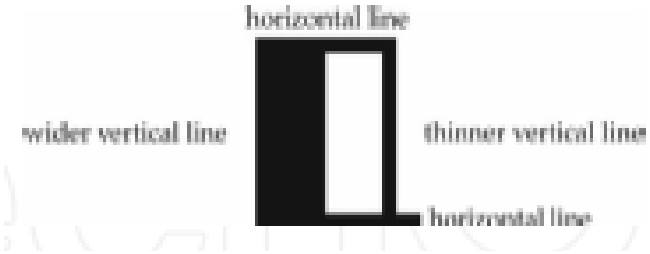


Рис. 10. Построение символов асимметричного безопасного шрифта.

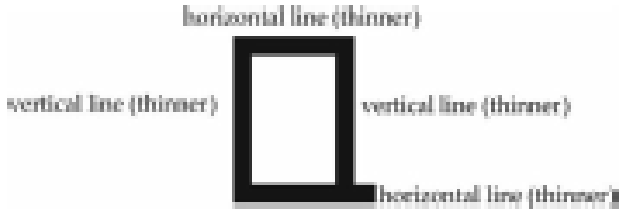


Рис. 11. Конструкция символов просто безопасного шрифта.

дый символ состоит из линий шириной около двух (рис. 9).

Более широкие линии — это вертикальные линии персонажа; более тонкие линии — это горизонтальные линии персонажа. Одновременно сохраняются правильные пропорции ширины линии и зазора каждого символа шрифта.

В символах асимметричного безопасного (Asymmetrical Safe) шрифта (рис. 7b) линии, образующие символы, пересекаются под прямым углом. Каждый символ также состоит из линий шириной около двух (рис. 10).

Однако расположение строк в символах отличается от расположения шрифта Symmetrical Safe. Более ши-

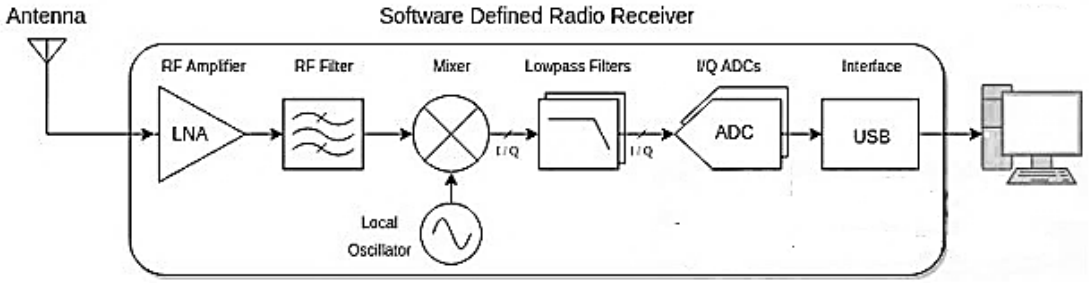


Рис. 12. Состав SDR-платформы

рокие линии — это вертикальные линии, но только как левая часть символа. Более тонкие линии отображаются как горизонтальные линии символа и как правый элемент символа. Это означает, что ширина более широкой вертикальной линии равна сумме расстояния между вертикальными линиями и ширины более тонкой вертикальной линии.

Шрифт Simply Safe — это третий набор безопасных шрифтов. Линии, образующие символы, пересекаются под прямым углом. Каждый символ состоит из линий примерно одной ширины (рис. 11).

Эффективность шрифтов Tempest в процессе защиты информации от утечки по каналу ПЭМИ может быть продемонстрирована через коэффициент ошибок символов (CER) в процессе анализа и оптического распознавания перехваченного и восстановленного изображения с экрана монитора [9]

$$\mathbf{CER}=\frac{m+k}{q}=\frac{m+(u-n)}{q},$$

где u — количество символов, которые искали в анализируемом изображении, m — количество символов, которые были распознаны неправильно, n — количество символов, которые были правильно распознаны, k — количество нераспознанных, но найденных символов в анализируемом изображении (k = u – n), а q — количество всех символов, присутствующих в анализируемом изображении, и используется для точной оценки.

Значения параметра CER приведены в таблице 3.

Таким образом, приведенные значения коэффициента ошибок CER показывают целесообразность применения указанных шрифтов для пассивной защиты отображаемой на экране монитора информации в текстовом виде, вне зависимости от типа применяемого стандарта передачи. Их использование не устраняет источник побочного излучения, который коррелирован с обрабатываемой информацией, но особая форма шрифтов напрямую влияет на качество восстанавливаемого из перехваченного изображения текста за счет ухудшения оптического распознавания символов.

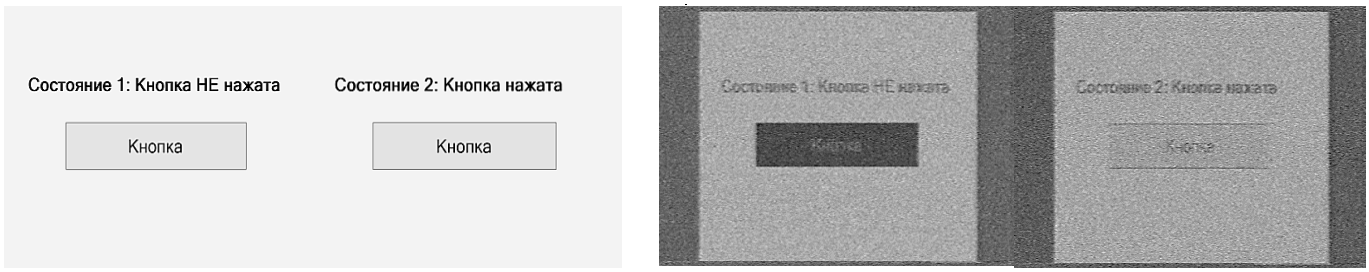
В общем случае, для восстановления информации посредством перехвата ПЭМИ злоумышленнику на своем оборудовании необходимо установить: точное значение частоты, ширину полосы, скорость выборки, период наблюдения и т.д. Однако в последние годы разрабатываются специальные интерфейсы прикладного программирования (API) и наборы инструментов для разработки ПО, что позволяет злоумышленнику использовать SDR технологию, которая подразумевает настройку рабочих радиочастотных параметров приемной части оборудования с помощью программного обеспечения, таких как GNU Radio или MATLAB.

Состав SDR-платформы (рис. 12) может быть разделен на аппаратный уровень и программный уровень.

Аппаратный уровень представляет собой ВЧ-интерфейс, состоящий из ВЧ-усилителя и быстрого аналого-цифрового преобразователя (АЦП). Обязанностью ВЧ-интерфейса является преобразование аналогового ВЧ-сигнала в оцифрованные образцы в быстрой фазе, которая может быть обработана программным уровнем. Каждая оцифрованная выборка, создаваемая ВЧ-интерфейсом, представляет собой комплексное число в формате данных I/Q, где действительное значение представляет синфазную составляющую сигнала, а мнимое значение представляет квадратурную составляющую электромагнитного сигнала.

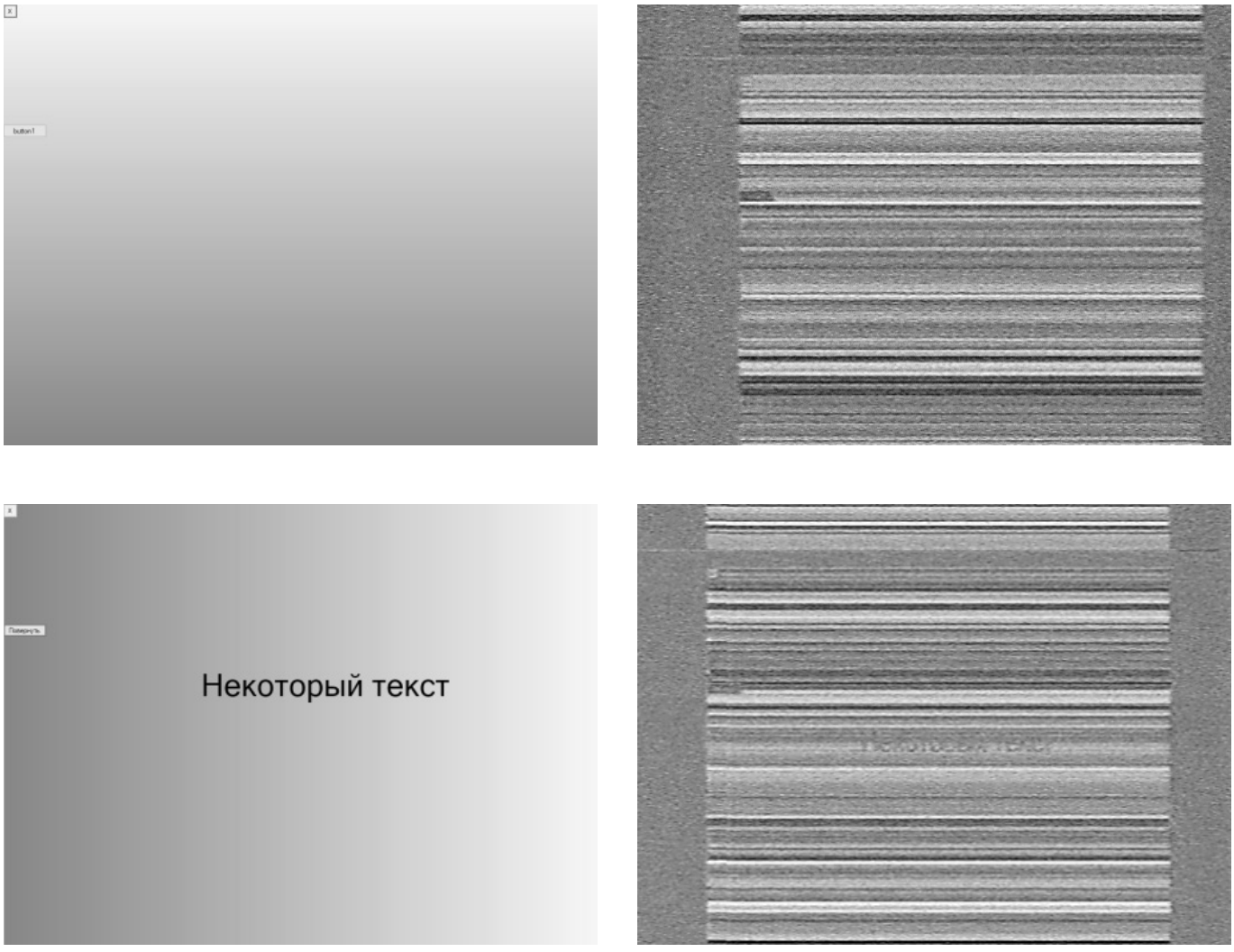
Программный уровень обработки сигнала ПЭМИ может быть реализован с помощью библиотеки TempestSDR [10]. TempestSDR — это программная библиотека с открытым исходным кодом, которая облегчает использование SDR-платформ для атак по побочным каналам EM на компьютерные мониторы.

Авторами статьи при экспериментальных исследованиях в качестве SDR-платформы использовался приемник HackRF One производства компании Great Scott



а) б)

Рис. 13. Исходное (а) и восстановленное (б) изображение на экране монитора



а) б)

Рис. 14. Оценка влияния фона отображения символов на качество восстанавливаемой информации. Исходное изображение на мониторе (а) и восстановленное (б).

Gadgets. Была создана программа, выводящая на экран монитора текстовую строку и интерактивную кнопку, меняющую свой фон и текст строки при нажатии (рис. 13). Данная кнопка имитирует нажатие клавиши на виртуальной клавиатуре.

Было подтверждено:

- влияние цветовой палитры фона и текста на снижение уровня ПЭМИ (для VGA интерфейса), существенно сказывается на качестве восстанавливаемого изображения;
- замена шрифтов Arial и Times New Roman на символы из набора TEMPEST шрифтов делает последние практически нечитаемыми при восстановлении исходного изображения.

Дальнейшие исследования были направлены на оценку влияния фона отображения символов на качество восстанавливаемой информации. Установлено, что применение градиентной заливки фона (рис. 14) создает на восстанавливаемом из ПЭМИ посредством SDR-платформы HackRF One и библиотеки TempestSDR изображении множество дополнительных повторяющихся линий.

Данный факт вероятно обусловлен наличием в SDR-платформе аналого-цифровых преобразователей (рис. 15). Учитывая, что стандартный лист формата А4 при использовании шрифта Times New Roman содержит порядка 30–50 строк в зависимости от размера шрифта (14–12 pt) при полуторном (одинарном) междустрочном интервале, возможно подобрать такую градиентную заливку фона, при которой на все строки восстанавливаемого изображения будут наложены горизонтальные линии, не позволяющие восстановить исходные символы.

Совместное применение градиентной заливки с TEMPEST шрифтами способно исключить реконструкцию перехваченного по каналу ПЭМИ изображения даже при объединении (смешивании) нескольких последовательных кадров преследующих цель повышения качества изображения методом корреляции.

Дальнейшие исследования предполагают оценку влияния градиентной заливки фона на реконструкцию перехваченного по каналу ПЭМИ изображения при применении в качестве SDR-платформ других приемников.

При невозможности реализовать гарантированную энергетическую недоступность злоумышленника к ПЭМИ от ПЭВМ, обрабатывающей конфиденциальную информацию, целесообразным является подход, основанный на выборе режима разрешения экрана монитора, который для конкретного интерфейсного кабеля обеспечивает минимальный уровень побочных излучений, а также оптимизация цветовой палитры для фона и отображаемого на мониторе текста. Применение TEMPEST шрифтов, не содержащих декоративных элементов, значительно снижает возможность реконструкции перехваченного изображения текста за счет ухудшения оптического распознавания символов. Применение градиентной заливки фона на основе предположения, злоумышленником перехват ПЭМИ может осуществляться посредством SDR-платформы, создает на восстанавливаемом изображении дополнительные помехи в виде повторяющихся линий.

ЛИТЕРАТУРА

1. H.S. Lee, D.A. Choi and J.G. Yook, “Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment”, IEEE Trans. Electromagn. Compat., vol. 61, pp. 1098–1106, Aug 2019.
2. D.H. Choi, H.S. Lee and I G. Yook, “Information leakage and recovery from multiple LCDs”, 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility, pp. 1056–1058, May 2018.
3. Методический документ. Меры защиты информации в государственных информационных системах (утвержден ФСТЭК России 11.02.2014).
4. A. Bolshakov. D. Tyulkin. Experimental Estimation of a Potential Eavesdropping Distance for Electromagnetic Emanations of Video System. FRUCT’24: Proceedings of the 24th Conference of Open Innovations Association FRUCT, April 2019, Article No.: 82, Pages 589–593.
5. Kubiak I. Video signal level (colour intensity) and effectiveness of electromagnetic infiltration. Bulletin of the Polish Academy of Sciences — Technical Sciences. 2016; 64:207–2018. DOI: 10.1515/bpasts-2016–0023.
6. A. Boitan, I. Kubiak, S. Halunga, A. Przybysz, A. Stańczak. Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process. Symmetry, 2020, № 11, p. 1908, https://doi.org/10.3390/sym12111908.
7. R. Franand. “Side Channels, Compromising Emanations and Surveillance: Current and future technologies.” (2011).
8. Kubiak I. TEMPEST font counteracting a non-invasive acquisition of text data. Turkish Journal of Electrical Engineering and Computer Sciences. 2018;26(1):582–592. DOI: 10.3906/elk-1704–9.
9. Kubiak I. Electromagnetic Eavesdropping. Recent Trends in Communication Networks, August 9th, 2019, DOI: http://dx.doi.org/10.5772/intechopen.86478.
10. Martin Marinov. TempestSDR Remote Video Eavesdropping using a Software-defned Radio Platform. https://github.com/martinmarinov/TempestSDR.

Рыжиков Сергей Сергеевич (RyzhikovSS@mpei.ru), Агуреев Иван Александрович (universe@mpei.ac.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»