Санкт-Петербургский государственный университет

***Дулатов Ильфат Тагирович***

**Выпускная квалификационная работа**

***Разработка вычислительных моделей для анализа технологии дистанционного перехвата видеосигнала***

Уровень образования: магистратура

Направление 03.04.01 «Прикладные математика и физика»

Основная образовательная программа ВМ.5521.2019 «Математические и информационные технологии»

Научный руководитель: профессор кафедры ТСУЭФА, д.ф.-м.н., Сычевский С.Е.

Рецензент: ведущий научный сотрудник АО «НИИЭФА»   
им. Д.В. Ефремова, Амосков В.М.

Санкт-Петербург

2021

**Содержание**

[Введение 3](#_Toc70942631)

[Постановка задачи 4](#_Toc70942632)

[Обзор литературы 5](#_Toc70942633)

[Глава 1. Научные исследования дистанционного перехвата видеосигнала ранних лет 6](#_Toc70942634)

[1.1. Исследования Wim van Eck 6](#_Toc70942635)

[1.2. Исследования Markus Kuhn 8](#_Toc70942636)

[Глава 2. Теоретические основы технологии перехвата видеосигнала 10](#_Toc70942637)

[2.1. Видеосигнал 10](#_Toc70942638)

[2.2. Образование радиоволн. Уравнение аналогового и цифрового видеосигнала 13](#_Toc70942639)

[Глава 3. Практические исследования 16](#_Toc70942640)

[3.1. Обзор оборудования 16](#_Toc70942641)

[3.2. Решение задачи дистанционного перехвата видеосигнала. 19](#_Toc70942642)

[Выводы 22](#_Toc70942643)

[Заключение 22](#_Toc70942644)

[Список литературы 24](#_Toc70942645)

# **Введение**

Информационные технологии в настоящее время используются в нашей жизни повсеместно, и многие уже не могут представить свою жизнь без них: стационарные компьютеры, ноутбуки, планшеты, смартфоны и так далее. Все эти средства хранят в себе большие объемы данных и многие аспекты нашей жизни в значительной мере зависят от их бесперебойной работы, целостности и конфиденциальности, обрабатываемой в них информации.

Из курса физики известно, что наши устройства получают и излучают энергию в различных формах, таких как: электрический ток, тепло, свет, электромагнитные излучения, звук и вибрация. Большая часть потребляемой энергии расходуется для формирования информационных сигналов и выделяются в виде тепла. В то же время часть энергии, имеющая информационные признаки обрабатываемых данных, может сформировать непреднамеренные каналы утечки информации такие как: побочные электрические, электромагнитные, оптические, акустические, ультразвуковые, механические, и т.п. Если информационные сигналы излучаются в форме, которая может быть на практике выделена из помех и декодирована на определенном расстоянии, используя компактное и доступное оборудование, то такие излучения могут стать потенциальной угрозой безопасности сохранности данных. Побочные излучения в этом случае могут быть использованы для обхода физических, криптографических, и программных средства защиты информации, обычно используемые в операционной системе, сети, или в программном обеспечении.

Как уже было сказано ранее каждое электронное устройство является источником непреднамеренных электромагнитных излучений. Эти излучения часто обладают такими же характеристиками, что и обрабатываемая информация. Для таких устройств как персональные компьютеры (мобильные или стационарные), наиболее опасными для безопасности обрабатываемых данных являются информационные цепи дисплеев. Эти цепи состоят из графических адаптеров, сигнальных кабелей и дисплейных мониторов. Наибольшая опасность заключается в том, что информация отображается на дисплее в явной форме и беглого взгляда на экран или копию экрана достаточно для перехвата информации. Такая копия экрана может быть воссоздана из электромагнитных излучений от работающих видео цепей. Достаточно лишь вспомнить, что в соответствии с уравнениями Максвелла, изменение электрического тока в любой цепи является источником изменения электромагнитного поля. Если изменение параметров формы тока (амплитуда, длительности импульса) напрямую отражает обрабатываемую информацию, то восстановить эту информацию становится сравнительно простым делом и в данном случае речь уже может идти о возможности бесконтактного (дистанционного) сбора информации [1].

# **Постановка задачи**

Поэтому целью данного научного исследования является: доказательство возможности и наглядная демонстрация дистанционного перехвата видеосигнала.

Научной новизной работы является – выполнение задачи дистанционного перехвата видеосигнала с помощью наиболее доступного на сегодняшний день решения.

Задачи магистерской диссертационной работы:

1. Исследование теоретических основ технологии дистанционного перехвата видеосигнала.
2. Анализ моделей аналогового и цифрового видеосигнала.
3. Решение задачи дистанционного перехвата видеосигнала.
4. Разработка демонстрационной методики перехвата на основе полученных результатов экспериментов, включающих численные оценки.

Методы исследования: теоретические, экспериментальные.

# **Обзор литературы**

К сожалению, на сегодняшний день в нашей стране данная проблема несмотря на всю свою актуальность исследована слабо, что выражается, например, в малом количестве научных работ. В большей степени это связано с распространённым заблуждением о том, что такой перехват информации невозможен и, если даже и возможен, то представляется очень дорогостоящим.

В основном данное исследование опирается на труды иностранных учёных, подробный анализ которых приведён в первой главе диссертационной работы.

# **Глава 1. Научные исследования дистанционного перехвата видеосигнала ранних лет**

## **1.1. Исследования Wim van Eck**

В 1985 году голландский компьютерный исследователь **Wim van Eck** опубликовал статью «Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?» включавшую исследования для проверки процесса перехвата содержимого экрана монитора путем обнаружения распространяемых им электромагнитных волн. Это было первым опубликованным исследованием на тему излучений от видео мониторов [2].

Электронное оборудование образует вокруг себя [электромагнитное поле](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%BD%D0%B8%D1%82%D0%BD%D0%BE%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B5). Это поле несёт информацию о сигналах, протекающих внутри оборудования. В некоторых случаях эта информация оказывается исчерпывающей, то есть наблюдая (удалённо) за электромагнитным полем, можно восстановить состояние излучающего объекта, восстановить данные, которые он обрабатывает.

В мониторах, построенных на электронно-лучевых трубках изображение формируется лучом электронов, пробегающим экран построчно. Интенсивность свечения [пиксела](https://ru.wikipedia.org/wiki/%D0%9F%D0%B8%D0%BA%D1%81%D0%B5%D0%BB) получаемого изображения регулируется интенсивностью луча. Сам луч управляется с помощью высоковольтных высокочастотных сигналов, которые, в свою очередь, порождают значительное [электромагнитное излучение](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%BD%D0%B8%D1%82%D0%BD%D0%BE%D0%B5_%D0%B8%D0%B7%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) вокруг монитора. Это излучение, согласно работе Wim van Eck, имеет заметное сходство с радиосигналом [аналогового телевидения](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D0%B5_%D1%82%D0%B5%D0%BB%D0%B5%D0%B2%D0%B8%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5). Таким образом можно осуществить перехват информации с монитора с помощью обычной телевизионной [антенны](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B5%D0%BD%D0%BD%D0%B0). После этого остаётся только осуществить синхронизацию полученного сигнала, что можно сделать либо вручную, либо таким же образом перехватив сигнал [развёртки](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D1%80%D0%B5%D1%81%D1%81%D1%82%D1%80%D0%BE%D1%87%D0%BD%D0%B0%D1%8F_%D1%80%D0%B0%D0%B7%D0%B2%D1%91%D1%80%D1%82%D0%BA%D0%B0) монитора.

Wim van Eck показал схожесть между современными мониторами и черно-белыми телевизорами. Он показал, что эти знания могут быть использованы при создании устройства перехвата видеосигнала.

В статье описывался эксперимент с модифицированным бытовым черно-белым телевизором. Была проведена демонстрация в реальных условиях вне лаборатории. Van Eck доказал, что это является реальной угрозой безопасности. Он описал возможные источники излучения и способы защиты от этой угрозы.

Однако, по результатам его работы можно было выявить несколько проблем:

* модификация приемника, хотя не дорогая, требует углубленных специализированных знаний;
* то обстоятельство, что устройству требуется постоянная регулировка, чтобы синхронизировать генераторы в приемнике и передатчике, делает трудным использование его на практике;
* технологии быстро изменились с момента публикации статьи. Подобный перехват больше не работает для современных мониторов, вследствие различных видео моделей, которые значительно отличаются от телевиденья;
* отсутствие условий для автоматизированной обработки сигналов.

Можно только предполагать, почему в течение десятилетий больше не появлялось исследований на эту тему. Возможно, основными причинами были то, что модифицированный приемник нельзя было больше применять для современных видео режимов, а коммерческие узкополосные приемники не могут быть использованы для этих целей. Как позже указал Kuhn, исследователю необходимо иметь в своих руках специализированные военные широкополосные приемники, которые дороги и имеют экспортные ограничения [3].

## **1.2. Исследования Markus Kuhn**

Немецкий специалист по информатике в своей работе «Compromising emanations: eavesdropping risks of computer displays» смог усовершенствовать результаты, достигнутые его предшественником van Eck. Kuhn проанализировал свойства излучений и их источники. Он описал оборудование, которое может понадобиться исследователю для того, чтобы принять и обработать сигнал. Он выполнил эксперименты и создал систему для перехвата в реальном времени, специализированный АМ радиоприемник и VGA видеомонитор [4].

Однако в его системе перехвата есть некоторые ограничения:

* исследователю необходимо иметь доступ к очень дорогостоящему, ограниченному к экспорту оборудованию, для того чтобы повторить его эксперименты. Это оборудования также часто недостаточно мобильно, что часто требуется в реальных условиях;
* как и система van Eck, решение Kuhn также требует ручной синхронизации;
* цифровая обработка сигнала для улучшения приема слабых сигналов (например, усреднение по времени) не выполнялось в реальном времени;
* исследователю необходимо знать точные параметры видеомонитора или необходимо угадать их [5].

В работе также упоминается возможные способы для модуляции сигнала скрытыми сообщениями. Kuhn представил способ защиты от подобного перехвата, используя технические и программные решения. Он продемонстрировал автоматическое восстановление текста. Работа включает эксперименты с оптическим перехватом изображения от ЭЛТ дисплеев. [6]

Работа Kuhn дополнила исследования van Eck описанием различных современных видео режимов. Kuhn смог доказать, что явление, возникшее сравнительно давно, все еще актуально [7]. Это зажгло новый интерес к теме, результатом чего стала еще пара работ, которые он опубликовал впоследствии. В своих работах Kuhn сфокусировался на цифровых дисплеях и показал, что те же методы можно использовать и для них. Он проанализировал высокочастотные излучения от плоских жидкокристаллических телевизионных дисплеев [8].

**Выводы по первой главе.**

В первой главе магистерской диссертации приведены итоги проведенного анализа деятельности таких известных исследователей, как Wim van Eck и Markus Kuhn, исследования которых связаны с перехватом побочных электромагнитных излучений видеосигнала. В результате проведенного анализа были выделены достоинства и недостатки подходов каждого из них. Также данные труды стали основой для последующего доказательства того, что дистанционный перехват видеосигнала с экрана персонального компьютера возможен, так же, как и его последующее восстановление.

# **Глава 2. Теоретические основы технологии перехвата видеосигнала**

## **2.1. Видеосигнал**

Факт того, что изменения токов в одном проводе индуцирует токи в другом проводе, расположенном рядом, определяется уравнениями Максвелла. Сигнал как раз и есть изменение тока и/или напряжения во временной области. Допустим у нас есть провод, который назовем провод A. Передадим сигнал по нему. Подключим к этому проводу генератор сигналов, который модулирует данные 𝐼(𝑡), так что ток в проводе во времени tможет быть записан как 𝑥(𝑡)=𝐼(𝑡)∙sin(2𝜋𝑓с𝑡), где𝑓с несущая частота. Аргумент функции sin, а именно 2𝜋𝑓с𝑡, называют фазой волны. Из уравнений Максвелла, следует, что изменение тока в проводе A, вызовет изменение в окружающем пространстве электромагнитного поля [9].

В данной работе для оценок магнитных полей были использованы комплексы вычислительных программ TORNADO [10, 11], базирующиеся на интегро-дифференциальном подходе и проекционно-сеточных методах и KLONDIKE [12, 13], использующем интегральный подход. Комплексы программ разработаны в РФ, верифицированы в ходе практических работ и специально организованных сопоставительных испытаниях (беч-марках) и зарегистрированы в РОСПАТЕНТЕ.

Предположим, что мы проложили провод B параллельно проводу A. Изменение магнитного поля от провода A вызовет изменение тока в проводе B. Мы сможем измерить ток в проводе B как функцию от времени 𝑥̂(𝑡). И в итоге 𝑥̂(𝑡)=𝐼̂(𝑓𝑐)∙sin(2𝜋𝑓с𝑡+𝜑(𝑓𝑐)), где 𝐼̂(𝑓𝑐) ослабление амплитуды пика и 𝜑(𝑓𝑐) разность фаз сигнала в проводе B. Конкретные значения зависят от физических свойств системы, таких как емкость между проводами и их сопротивление. Измерив несущую частоту 𝑓с и имея некоторые предположения о сигнале, мы можем оценить 𝐼(𝑡). Это источник рассматриваемых нами побочных излучений – сигналы в проводах непреднамеренно наводят токи в расположенных рядом проводах, передавая некоторую информацию об исходном сигнале. На практике сигналы более сложные, чем простая синусоида, однако здесь может быть применён анализ Фурье.

Преобразование Фурье помогает увидеть, как выглядит спектр в частотной области. Функция разложится в сумму sin и cos составляющих в комплексной плоскости. Преобразование Фурье функции g(t) будет выглядеть как: 𝐺(𝑓)=F{𝑔(𝑡)}(𝑓)= , а обратное преобразование Фурье: 𝑔(𝑡)=F−1{𝐺(𝑓)}(𝑡)=

Результатом преобразования синусоидальной волны 𝑥(𝑡)=sin(2𝜋𝑓𝑐𝑡) будут пики 𝑋(𝑓)=(1/2𝑖) [𝛿(𝑓−𝑓𝑐)−𝛿(𝑓+𝑓𝑐)]sin(2𝜋𝑓𝑐𝑡) на частотах 𝑋(−𝑓𝑐) и 𝑋(𝑓𝑐), в то время как 𝑋(𝑓)=0 на всех других частотах. Поэтому видно, что преобразование Фурье в первую очередь показывает частоту исходного сигнала. Отметим, что дельта-функция Дирака определяется как: 𝛿(𝑡) =

Дельта-функция Дирака обладает свойством, которое можно характеризовать как «отсеивание» — это означает, что, умножая ее на функцию 𝑔(𝑡), удаётся выделить только одно значение функции

𝛿(𝑡−𝑇)𝑑𝑡=𝑔(𝑡).

В литературе встречается также определение «гребень Дирака», что по существу является бесконечным числом дельта-функций Дирака, повторяющихся через равные интервалы 𝑇. Можно таким образом «выбрать» значения функции 𝑥(𝑡) в моменты времени 𝑇 умножая ее на гребень Дирака. В результате получится дискретная выборка, полученная из 𝑥(𝑡) через равные интервалы 𝑇, то есть: …, 𝑥(−2𝑇), 𝑥(−𝑇), 𝑥(0), 𝑥(𝑇), 𝑥(2𝑇),…

Фильтр нижних частот ‑ это фильтр, который воздействует на сигнал, пропуская компоненты сигнала с частотами 𝑓≤𝑓𝑚𝑎𝑥, и ослабляя остальные до нулевых амплитуд. Фильтр верхних частот пропускает нетронутыми частоты 𝑓≥𝑓𝑚𝑖𝑛, ослабляя остальные до величин амплитуд. Полосовой фильтр ‑ это комбинация фильтра нижних частот и фильтра верхних частот, пропускающий частоты 𝑓𝑚𝑖𝑛≥𝑓≥𝑓𝑚𝑎𝑥, ослабляя остальные. Сигнал с ограниченной полосой ‑ это сигнал у которого отсутствуют компоненты с частотами 𝑓> 𝑓𝑚𝑎𝑥 и 𝑓<𝑓𝑚𝑖𝑛. Такой сигнал останется без изменений пройдя через полосовой фильтр с граничными частотами 𝑓𝑚𝑖𝑛 и 𝑓𝑚𝑎𝑥. Этот подход используется для отфильтровывания полезных сигналов из помех, не принадлежащих сигналу с ограниченной полосой.

Почти все современные видео мониторы имеют растровую развертку. Изображение передается из видеоконтроллера к дисплею построчно с определенной частотой. Каждая из этих строк содержит пиксели и представляет собой изменяющийся по времени сигнал. Сигнал образуется от внутреннего видеоконтроллера, генератор которого на пиксельной частоте. Уровень аналогового сигнала в каждый момент времени зависит от интенсивности пикселей.

Предположим, что сигнал начинает передаваться в момент времени *t* = 0, и каждый видео кадр содержит yt строк, каждая из которых содержит xt пикселей. Частота, с которой образуются кадры – *f*v кадров в секунду. Длительность передачи каждого отдельного пикселя

Стоит отметить, что верхний левый угол кадра имеет координаты (0,0), пиксель расположенный (x, y) начнет передаваться в момент времени 𝑇(𝑥,𝑦)=(𝑛(𝑡)𝑥𝑡𝑦𝑡+𝑦𝑥𝑡+𝑥)𝑡𝑝 и закончит передаваться в тот момент времени когда начнет передаваться следующий пиксель [14].

На практике xt и yt определяются разрешением экрана, а *f*v ‑ просто частота смены кадров. Для обычного экрана разрешение ширина × высота, в действительности ‑ xt ≥ ширины и yt ≥ высоты. Причина этого заключается в том, что видеосигналы имеют интервалы гашения. Это означает, что передается больше пикселей, чем находится в видимой области. Последнее дает возможность монитору синхронизовать свой генератор, калибровать уровни цветности, электронно-лучевой трубка предоставляет достаточное время для электронного луча вернутся к началу следующей строки или кадра. Параметры синхронизации для персональных компьютеров стандартизированы ассоциацией по стандартам в области видеоэлектроники (VESA).

## 

## **2.2. Образование радиоволн****. Уравнение аналогового и цифрового видеосигнала**

Предположим, что интенсивности отдельных пикселей аналогового видеосигнала передаются в течение времени . Предположим также, что форма пикселя *p*(*t*), причём *p*(*t*) = 0 для |𝑡|≫𝑡𝑝/2. Известно, что пиксель *i* начинает передаваться в момент времени *t*i = *it*p (если предполагать, что пиксель 0 передавался в момент времени *t* = 0). Амплитуда сигнала, передающего пиксель, линейно зависит от его интенсивности *v*i. Тогда видеосигнал во временной области будет иметь форму

𝑣̃(𝑡) = .

Также известно, что спектр сигнала повторяется через равные интервалы в радио спектре с частотой . Интенсивность излучения на различных частотах определяются формой пикселя *p*(*t*).

Например, для разрешения 800×600 @ 75Гц с *x*t = 1056 пикселей, *y*t = 628 строк и *f*v = 75 Гц, получим частоту 1𝑡𝑝=(1056×628×75×1,36)/2≃33,74 МГц. Это означает, что можно ожидать найти такой сигнал на центральных частотах   
0, 33.74 МГц, 67.48 МГц, 135.2 МГц, и т.д. [15]

Для того чтобы получить полный видео сигнал, необходимо знать с какой минимальной частотой необходимо отцифровывать сигнал. Мы видим, что *V*(*f*) повторяется через одинаковые интервалы. Известно, что *V*(*f*) имеет ограниченную полосу, так что *V*(*f*) = 0 для всех |𝑓|≥. Поэтому необходимо иметь приемник с частотой квантования по крайней мере .

Вышеизложенное относится к аналоговым сигналам, таким как VGA. Однако, большинство современных устройств не просто модулируют интенсивность пикселя как аналоговую амплитуду. Вместо этого они передают каждый пиксель как цифровые биты используя FPD-Link (Flat Panel Display Link) для передачи (Low-voltage differential signaling). Для каждой составляющей изображения по каждому из трех путей передачи цвета, передается 7 бит, которые определяют RGB цвет. [9]

Поэтому каждый бит передается за время 𝑡𝑏=1/(xt∙yt∙fv∙nb) =𝑡𝑝/𝑛𝑏, где *n*b количество бит на пиксель, которое для FPD-Link *n*b = 7. Это представляет поток битов значений *c*k (𝑘∈ℤ). Определим k-ое значение как двоичное число (*k* mod *n*b) бит которое представляет интенсивность аналогового пикселя числом ‖‖ (интенсивность пикселя число *i* обозначается как *v*i) [16].

Поэтому можно записать результирующий аналоговый сигнал как 𝑣̃(𝑡)= 𝑏(𝑡−𝑘𝑡𝑏),

где *b*(*t*) форма цифрового бита, *b*(*t*)=0 для |𝑡|≫.

Как в предыдущем разделе, можно тоже провести анализ Фурье этого сигнала и получить F{𝑏(𝑡)∗(𝑐(𝑡)∙(𝑡))}=𝐵(𝑓)∙[𝐶(𝑓)∗(𝑓)]

Это означает, что получится также сигнал, повторяющийся в спектре, в этот раз повторения будут с частотой =𝑥𝑡∙𝑦𝑡∙𝑓𝑣∙𝑛𝑏. Это в *n*b раз выше, чем частота повторения, рассчитанная для аналогового сигнала. Например, с *n*b = 7 в видео модели 800×600 @ 75 с *x*t = 1056 *p*x, *y*t = 628 строк и *f*v = 75 Гц. Можно ожидать найти такой сигнал =1056∙628∙75∙7≃348.2 МГц.

**Выводы по второй главе.**

В данной главе был приведён минимальный математический анализ, необходимый для доказательства возможности теоретического обнаружения тактовых информативных частот как аналоговых, так и цифровых портов вывода изображения, а также базовые принципы образования электромагнитных побочных радиоволн.

# **Глава 3. Практические исследования**

## **3.1. Обзор оборудования**

Используя рассмотренные теоретические аспекты дистанционного перехвата видеосигнала, перейдем непосредственно к практическим исследованиям данного вопроса.

Для более наглядной демонстрации решения задачи, начальные исследования были проведены в экранированном помещении (рисунке 1) для обеспечения минимального уровня помех. В то же время это даёт возможность объяснить характеристики принятого сигнала и потенциал его использования.



Рисунок 1 – Экранированное помещение.

В состав оборудования входят:

1. Исследуемая цепь видеосигнала на базе персонального компьютера: встроенная видеокарта, сигнальный кабель типа (DVI, VGA, HDMI – по результатам дополнительных исследований выбран и использован наименее безопасный тип), дисплейный видеомонитор Samsung с разрешением (1920\*1080, 60Гц).
2. Анализатор спектра Rohde&Schwarz FSH4 с принимающей антенной АН-5.
3. Ноутбук Aser с установленным программным обеспечением TempestSDR.jar.
4. Портативный SDR приемник – HackRF one c подключенным всенаправленной универсальной штырьковой антенной.

Задачей данной работы является использование дешевого и доступного устройства для перехвата видеосигнала. Поэтому был выбран портативный SDR приёмник - HackRF one (Рисунок 2) – это радиопередатчик и/или радиоприёмник, использующий технологию, позволяющую с помощью программного обеспечения устанавливать или изменять рабочие радиочастотные параметры, включая, в частности, диапазон частот, тип модуляции или выходную мощность, за исключением изменения рабочих параметров, используемых в ходе обычной предварительно определённой работы с предварительными установками радиоустройства, согласно той или иной спецификации, или систем. HackRF one выполняет значительную часть цифровой обработки сигналов на обычном персональном компьютере или на программируемой логической интегральной схеме (ПЛИС). Целью формирования такой схемы является подготовка радиоприёмника или радиопередатчика произвольных радиосистем, изменяемый путём программной переконфигурации.

В качестве антенны выбрана портативная всенаправленная универсальная антенна. Она разработана для усиления сигнала беспроводной сотовой связи и интернета. Для лучшего приема на больших дистанциях подходит логопериодическая антенна с усилителем, полосовой фильтр может использоваться для предварительной обработки. Это может сделать систему менее портативной. Однако, выбранная нами антенна представляет собой недорогой вариант и позволяет выполнить необходимую работу.

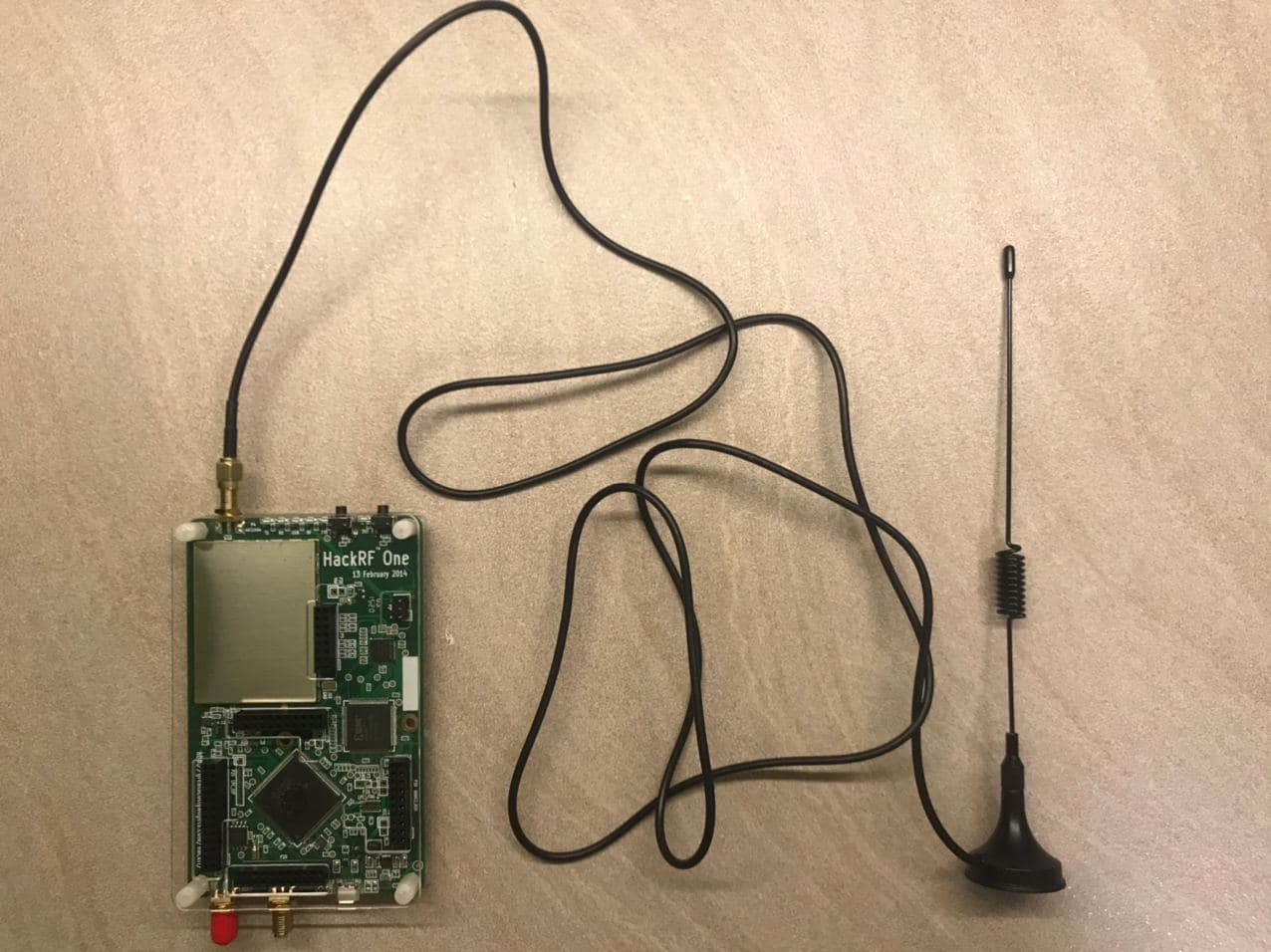
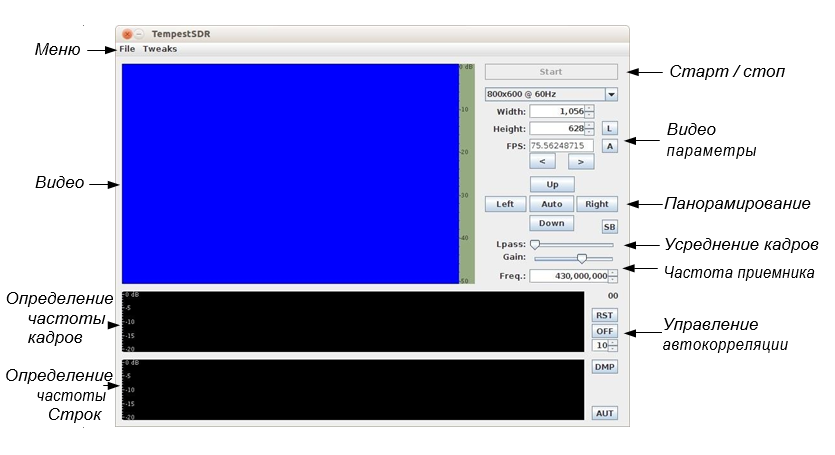


Рисунок 2 – Портативный SDR приёмник - HackRF one с подключенной всенаправленной штырьковой антенной.

TempestSDR.jar. — это программное обеспечение, которая совместно HackRF one, позволяет принимать изображение с монитора компьютера или телевизора за счет радиоволн, излучаемых экраном или кабелем между монитором и ПК. Графический интерфейс программы TempestSDR представлен на рисунке 3., кнопка «А» включает отслеживание частоты кадров. Кнопка «Auto» определяет области синхронизации. Кнопка «AUT» автоматически определяет разрешение и частоты строк. Шкала справа от видео показывает в реальном времени значения градаций серого, которые отображают интенсивность отсчетов [17, 18].

Рисунок 3 Интерфейс программы TempestSDR.jar.

## **3.2. Решение задачи дистанционного перехвата видеосигнала.**

Для максимального приближения перехвата к реальным условиям будем предполагать, что мы не имеем данных об исследуемом объекте. Поэтому сначала с помощью анализатора спектра определим частоты пика излучений монитора для этого запустим на экране режим теста (рисунок 4), затем проанализируем сигнал, чтобы определить разрешение и частоту кадров экрана. После этого зафиксируем сигнал.

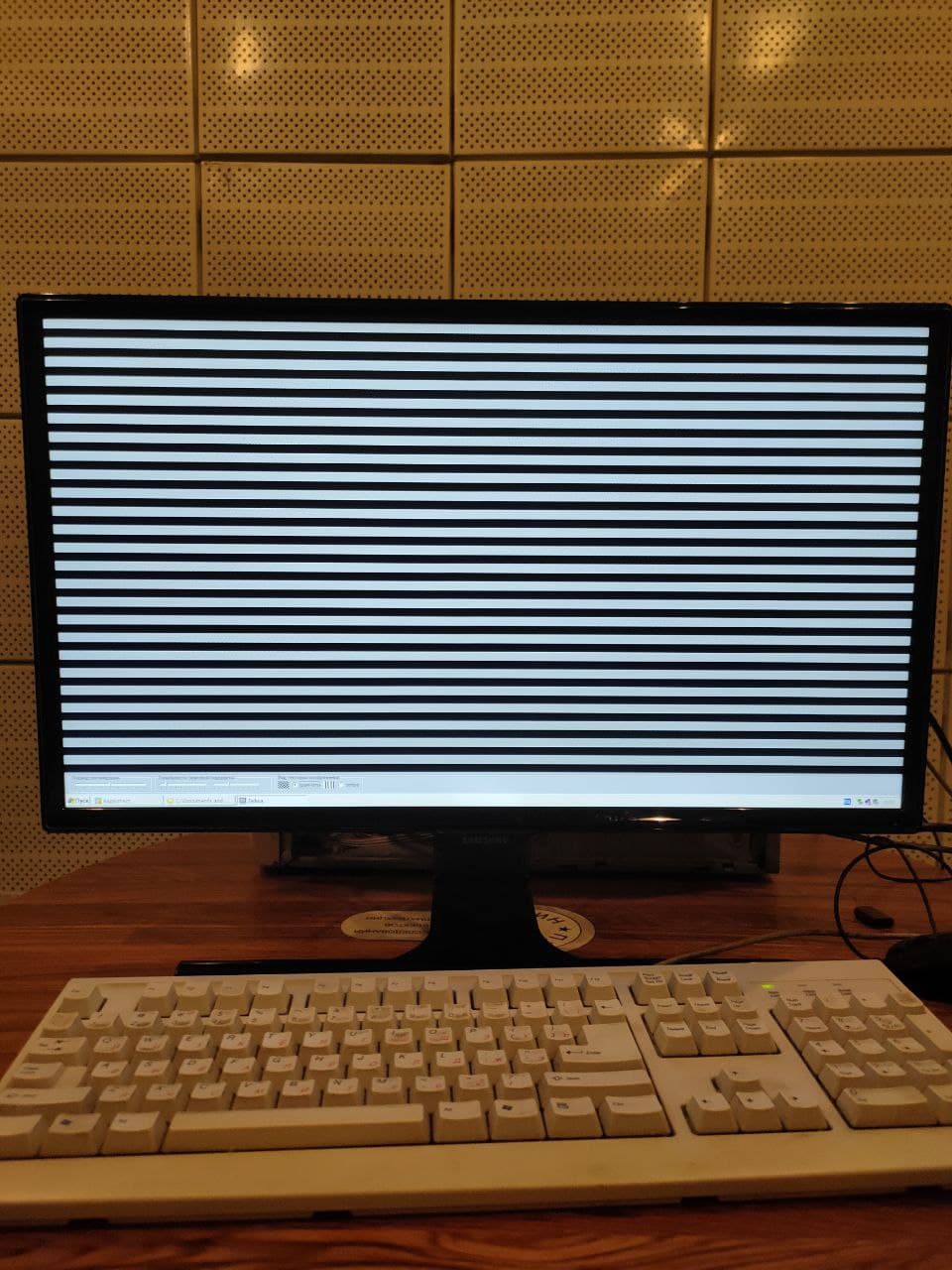


Рисунок 4 – Работа монитора в режиме теста.

Пиковый сигнал найден на частотах: 74.255, 148.500 МГц. (Рисунок 5) Согласно стандарту в области видеоэлектроники (VESA) сигнал на частоте 148.500 МГц предназначен для видеомониторов с разрешением (1920\*1080, 60Гц).

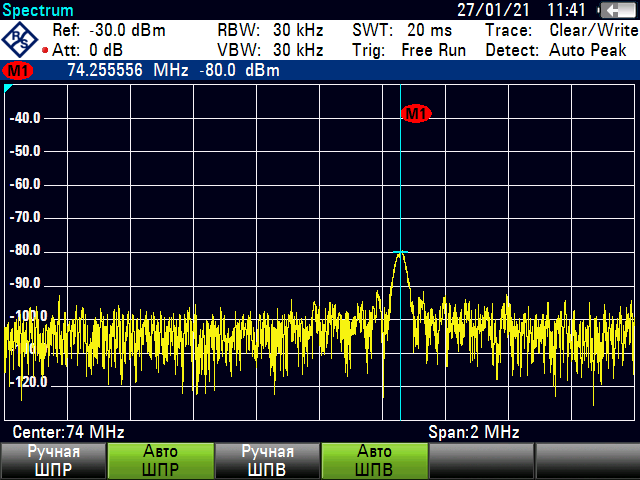
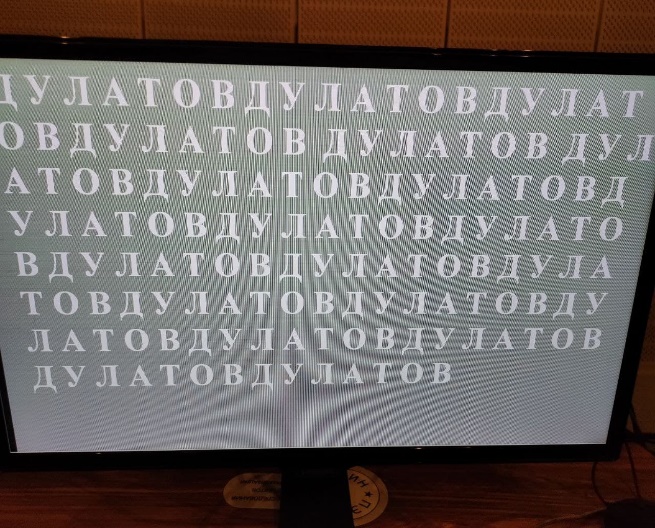
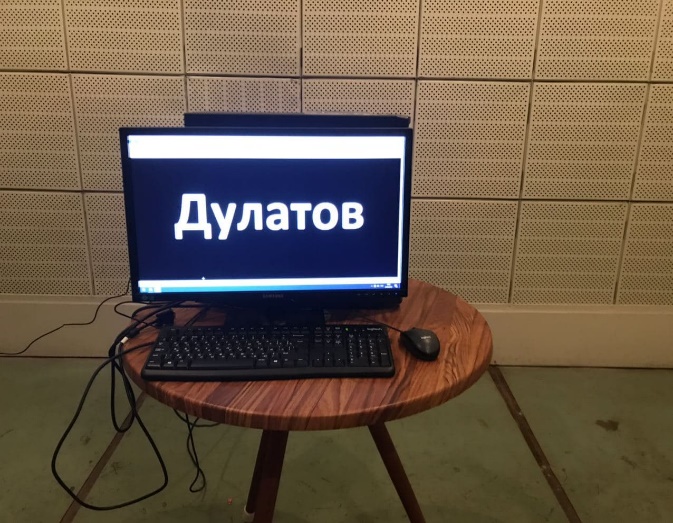
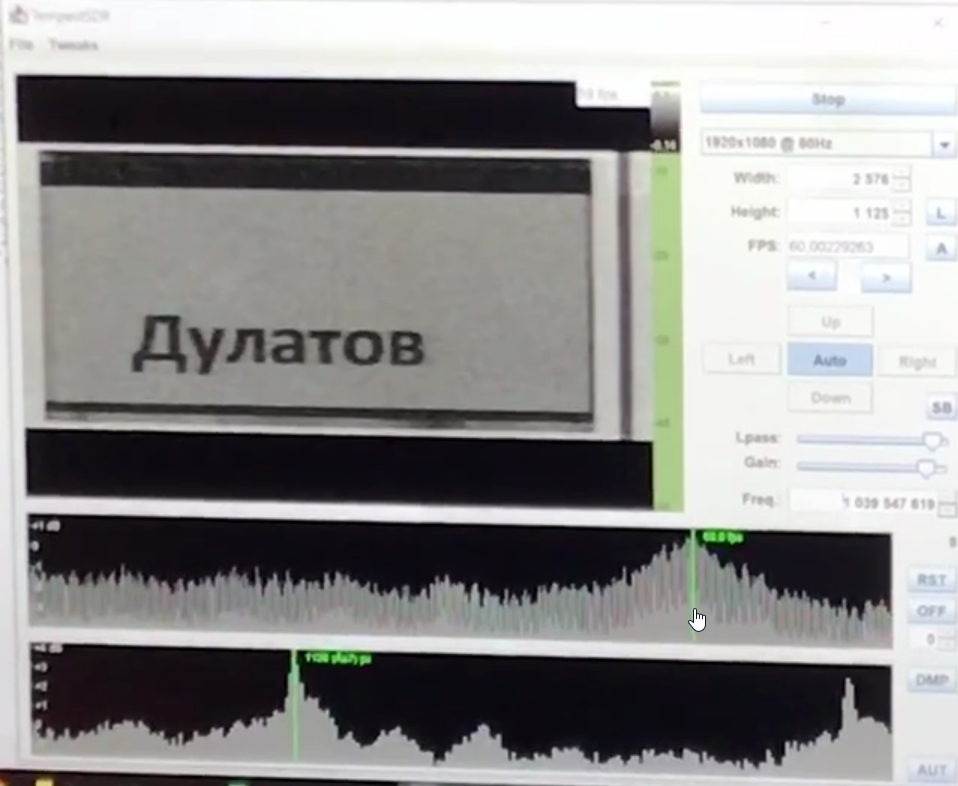


Рисунок 5 – Сигнал, принятый на анализаторе спектра.

Выведем на экран монитора случайную надпись для более наглядной демонстрации. (Рисунок 6) Запустим TempestSDR.jar и введем полученные частоты.



Полученные результат дистанционного перехвата видеосигнала можно наблюдать на Рисунке 7,



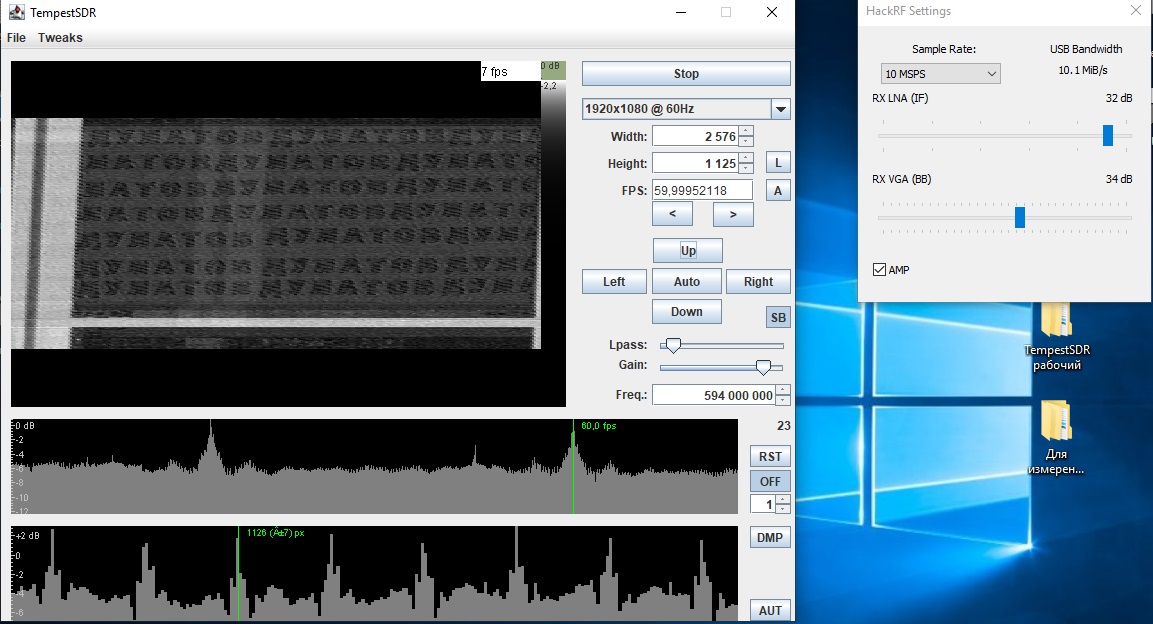


Рисунок 7 –Перехваченное изображение.

**Выводы по третьей главе.**

В данной главе были продемонстрированы результаты проведенных исследований по дистанционному перехвату видеосигнала монитора. Предложенная методика и проведённый эксперимент показывают на практике, что перехват видеосигнала возможен даже с использованием сравнительно дешевого и доступного в открытой продаже оборудования.

# **Выводы**

Доказательство возможности и наглядная демонстрация дистанционного перехвата, которая была целью данного научного исследования была достигнута.

В магистерской диссертационной работе были приведены теоретическое основы дистанционного перехвата видеосигнала. Проанализированы модели аналогового и цифрового видеосигнала. Решены задачи дистанционного перехвата видеосигнала. Разработаны демонстрационные методики перехвата на основе полученных результатов экспериментов.

Таким образом задачи магистерской диссертационной работы были выполнены.

# **Заключение**

Электромагнитные излучения, сопровождающие работу электрических устройств, несут в себе информацию об особенностях работы, внутреннем состоянии данных устройств.

В случае видео дисплейных устройств исследование и анализ излучения особенно важно, ведь повторяющаяся природа сигнала, в сочетании с длинными проводами, которые действуют как антенны, означает, что такие сигналы могут излучаться на большие расстояния, делая возможным, например, перехват видеосигнала из машины, припаркованного через дорогу. Практически каждая такая система излучает данные открыто, и для перехвата нет необходимости в каких-либо специализированных знаний по данной тематике. Вызывает определённое удивление малое количество исследований на тему дистанционного перехвата видеосигнала.

Работа, представленная в магистерской диссертации, имела целью решение актуальной задачи демонстрации возможности дистанционного перехвата видеосигнала, без предварительных знаний об объекте перехвата. Предложенный подход позволяет проводить данные исследования вне специализированных лабораторий. Для экспериментов требуется только, доступное имеющееся в продаже оборудование, программное обеспечение также размещено в открытом доступе для любого применения.

# **Список литературы**

1. Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров Технические методы и средства защиты информации.: ООО «Издательство Полигон», 2000.-320с
2. Вим ван Эйк: электромагнитное излучение от блоков видеодисплея: риск подслушивания? Компьютеры и безопасность, Vol. 4, pp. 269-286, 1985.
3. S. Jun, A. Yongacoglu, D. Sun, W. Dong, Computer LCD recognition based on the compromising emanations in cyclic frequency domain, IEEE International Symposium on Electromagnetic Compatibility, 2529 July 2016; Ottawa, Canada, pp.164-169.
4. Маркус Г. Кун: Компромиссные эманации: подслушивающие риски компьютерных дисплеев. Глава 3: Аналоговые видеовыходы. Технический отчет UCAM-CL-TR-577, Кембриджский университет, Компьютерная лаборатория, декабрь 2003 года.
5. Маркус Г. Кун: Электромагнитные риски подслушивания плоских дисплеев. 4-е рабочее совещание по технологиям повышения конфиденциальности, 26-28 мая 2004 года, Торонто, Канада, Труды, LNCS 3424, стр. 88-105.
6. Маркус Г. Кун: Компромиссные эманации: подслушивающие риски компьютерных дисплеев. Глава 3: Аналоговые видеовыходы. Технический отчет UCAM-CL-TR-577, Кембриджский университет, Компьютерная лаборатория, декабрь 2003 года.
7. Computer and Electrical Engineering, Dubai, United Arab Emirates, 2830 January 2009, pp. 452-456.
8. Маркус Г. Кун: Электромагнитные риски подслушивания плоских дисплеев. 4-е рабочее совещание по технологиям повышения конфиденциальности, 26-28 мая 2004 года, Торонто, Канада, Труды, LNCS 3424, стр. 88-105, Springer-Verlag. http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf
9. M.G. Kuhn, Compromising emanations: eavesdropping risks of computer displays, Technical reports published by the University of Cambridge Computer Laboratory, 2003.
10. Д.Н. Арсланова, А.В. Белов, В.А. Беляков, Т.Ф. Белякова, Е.И. Гапионок, Н.А. Крылова, В.П. Кухтин, Е.А. Ламзин, Н.А. Максименковa, И.В. Мазуль, В.О. Розов, С.Е. Сычевский “Разработка глобальных пространственных вычислительных моделей для анализа переходных электромагнитных процессов и оптимизации конструкции Международного термоядерного экспериментального реактора ИТЭР”, Вопросы атомной науки и техники, Серия “Термоядерный синтез”, научн. - техн. сборник, М., вып. 3 (31) 2011, с.3-26
11. V. Amoskov, D. Arslanova, A. Belov, V. Belyakov, T. Belyakova, E. Gapionok, N. Krylova, V. Kukhtin, E. Lamzin, N. Maximenkova, I. Mazul, S. Sytchevsky “Global computational models for analysis of electromagnetic transients to support ITER tokamak design and optimization”, Fusion Engineering and Design, 87, Issue 9, Sept. 2012, pp. 1519-1532
12. В.М.Амосков, А.В.Белов, В.А.Беляков, Т.Ф.Белякова, Е.И.Гапионок, Д.Б.Гаркуша, М.И.Глухих, В.Кухтин, Е.А.Ламзин, Н.А.Максименкова, Б.С.Мингалев,. С.Е.Сычевский, О.Г.Филатов СВИДЕТЕЛЬСТВО об официальной регистрации программы для ЭВМ №2003612487 Программный комплекс для расчета магнитных систем, содержащих магнитотвердые, магнитомягкие и токонесущие элементы конструкции сложной геометрической формы (KLONDIKE 1.0) Реестр программ для ЭВМ, Москва, 12 ноября 2003 г.
13. V.M. Amoskov, A.V. Belov, V.A. Belyakov, T.F. Belyakova, Yu.V. Gribov, V.P. Kukhtin, E.A. Lamzin, S.E. Sytchevsky, “Computation technology based on KOMPOT and KLONDIKE codes for magnetostatic simulations in tokamaks”, Plasma Devices and Operations, Vol. 16, No. 2, pp. 89 − 103 (2008)
14. L. Ho Seong, Y. Jong-Gwan, S. Kyuhong, Analysis of information leakage from display devices with LCD, URSI Asia-Pacific Radio Science Conference 2016, August 21-25, 978-1-4673-8801-6/16/$31.00 ©2016 IEEE.
15. MIL-STD-461G, Requirements for the control of electromagnetic interference characteristics of subsystems and equipment IEEE Transactions on Electromagnetic Compatibility, Vol.7, No 2, Dec. 2015.
16. N. Zhang, L. Yinghua, C. Qiang, W. Yiying, Investigation of unintentional video emanations from a VGA connector in the desktop Computers, IEEE Transactions on Electromagnetic Compatibility, Vol.59, No 6, Dec. 2017.
17. Васильев Р.А., Ротков Л. Ю.: Обнаружение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «Легенда»: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2018. – 45 с.
18. I. Kubiak, TEMPEST font counteracting a non-invasive acquisition of text data, Turkish Journal of Electrical Engineering and Computer Sciences, Vol. 26, No. 1/2018, DOI: 10.3906/elk-1704-9.