



ЗАЩИТА ИЗОБРАЖЕНИЯ НА ДИСПЛЕЕ ПЭВМ ПО КАНАЛУ ПЭМИ

МАЙОРОВ А.И., КОЛЕСНИК Д.Ю.

Органы пограничной службы Республики Беларусь

*Научный руководитель:
Титович Н.А. – к.т.н., доцент*



Потенциальные источники ПЭМИ ПЭВМ:

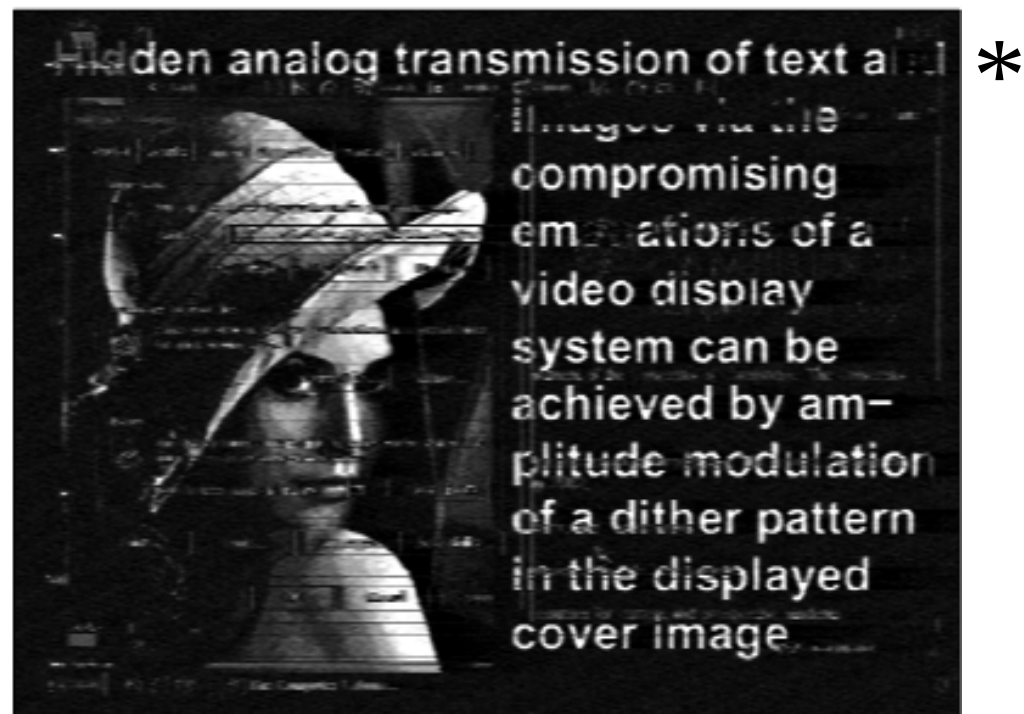
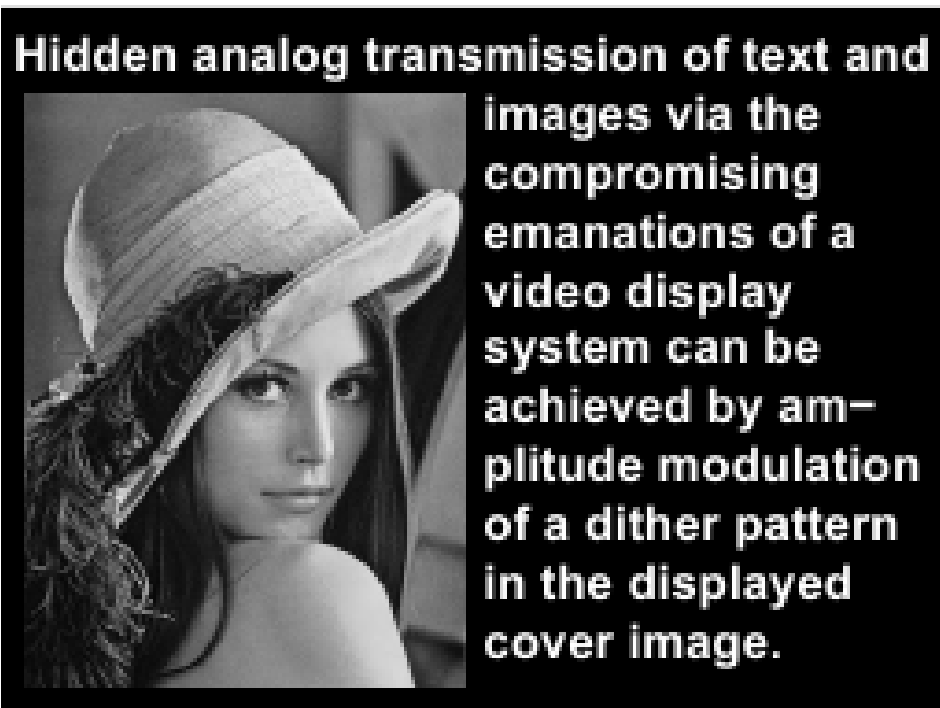
- накопители на жестком и гибком дисках, внешняя флэш-память;
- устройства *CD*, *CD-R*, *CD-RW*, *DVD*, *DVD-RW*;
- клавиатура;
- последовательный порт (*COM*, *USB*);
- принтеры;
- **видеоподсистема.**



ПЭМИ видеотракта

1985 год — Ван Эйк впервые продемонстрировал перехват изображения видеодисплея на расстоянии.

Пример перехвата:



* Markus G. Kuhn. Technical Report Compromising emanations: eavesdropping risks of computer displays



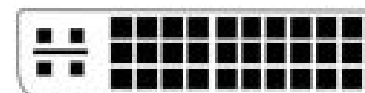
Интерфейсы видеотракта

Составные части видеотракта:

- Видеоконтроллер
- Дисплей
- Интерфейс:
 - **VGA**
 - DVI
 - HDMI
 - LVDS



VGA



DVI



HDMI

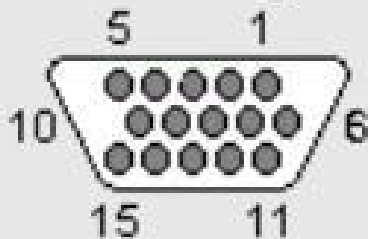


Интерфейс VGA

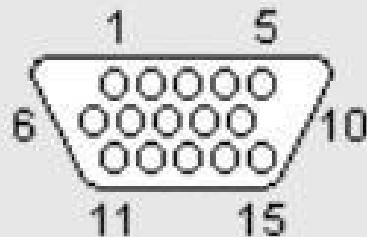


Разъём BD-15

Видеокарта:



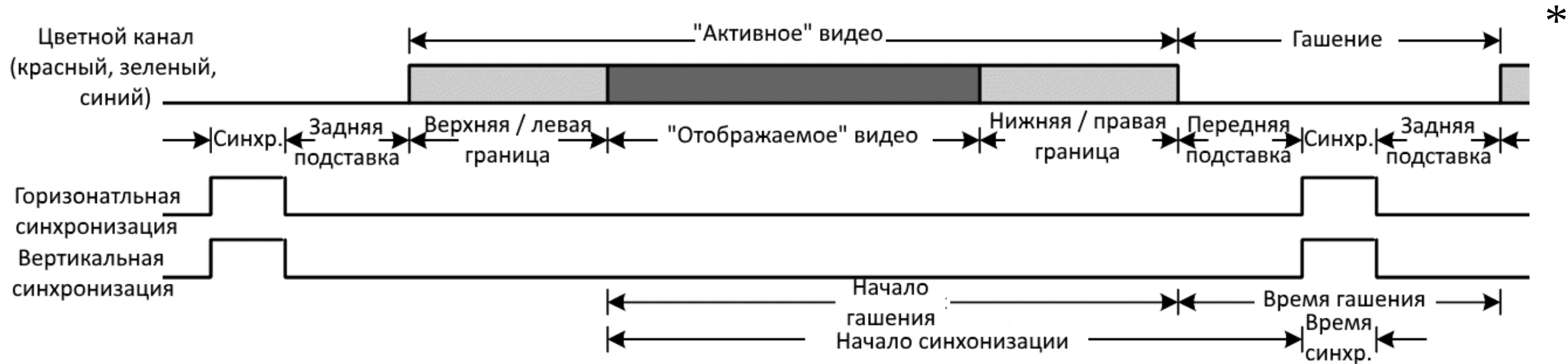
Монитор:



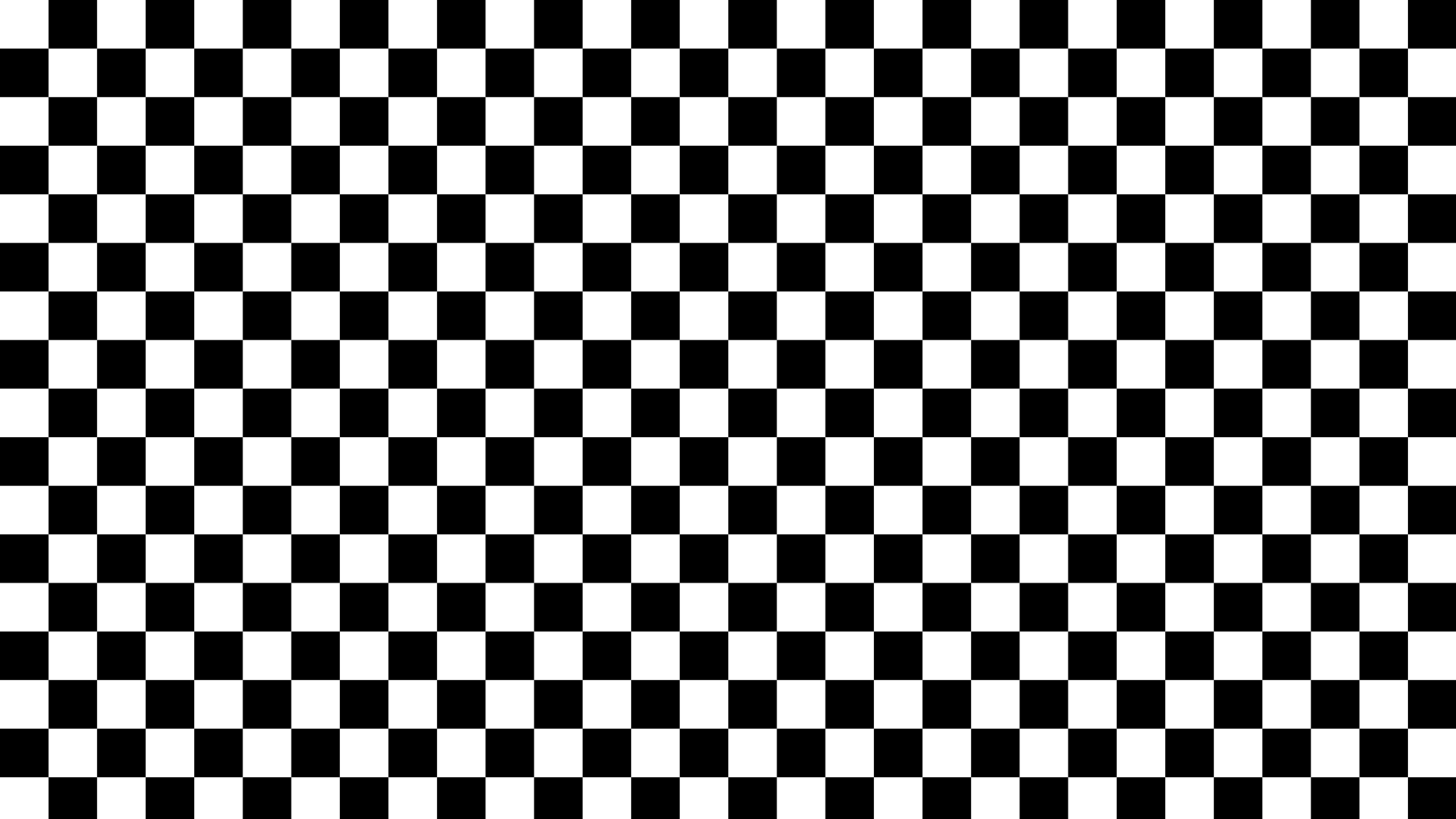
1	RED	Канал сигнала красного цвета (75 Ом, 0...0,7 В)
2	GREEN	Канал сигнала зеленого цвета (75 Ом, 0...0,7 В)
3	BLUE	Канал сигнала синего цвета (75 Ом, 0...0,7 В)
4	ID2	Второй бит идентификации
5	GND	Заземление (Корпус)
6	RGND	Заземление сигнала красного канала
7	GGND	Заземление сигнала зеленого канала
8	BGND	Заземление сигнала синего канала
9	KEY	Ключ
10	SGND	Заземление синхросигнала
11	ID0	Нулевой бит идентификации
12	ID1	Первый бит идентификации
13	HSYNC	Синхросигнал горизонтальной развертки
14	VSYNC	Синхросигнал вертикальной развертки
15	ID3	Третий бит идентификации



Сигналы в VGA



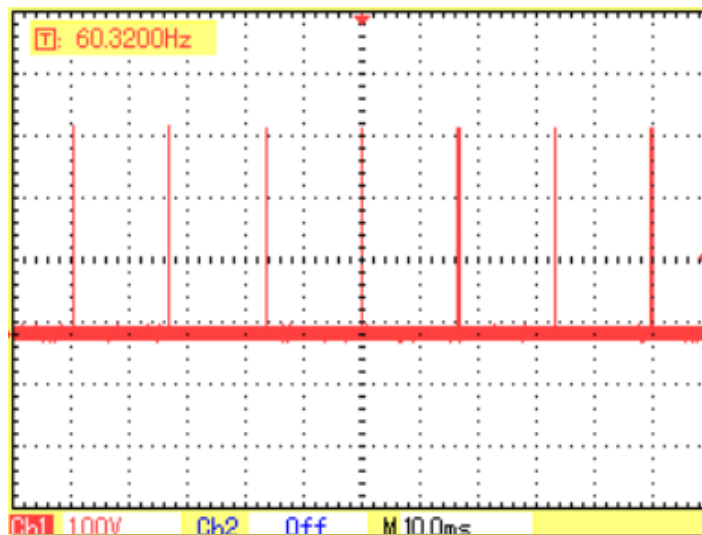
* VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Version 1.0, Revision 10 October 29, 2004



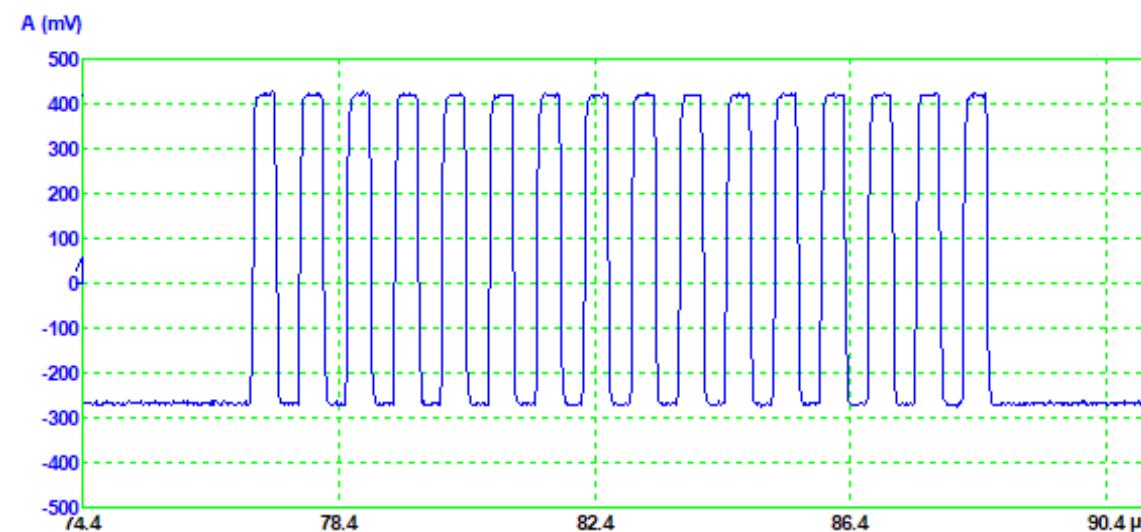
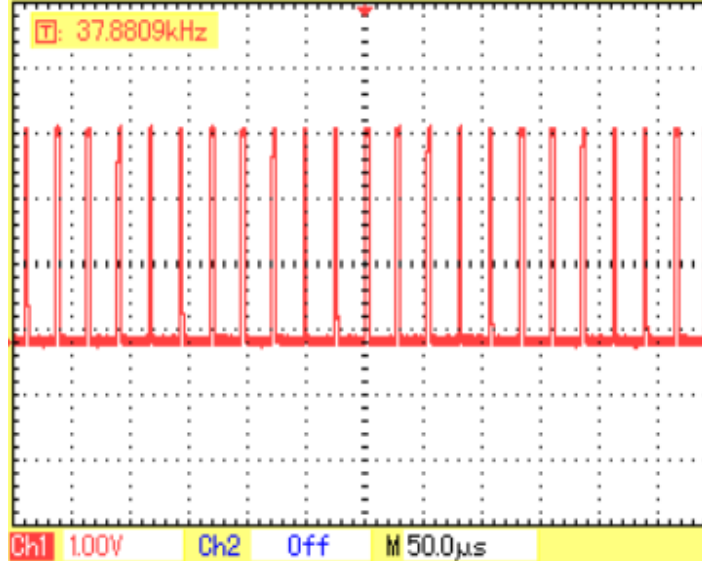


Осциллограммы VGA

Синхросигнал
вертикальной
развёртки
VSYNC (pin 14)



Синхросигнал
горизонтальной
развёртки
HSYNC (pin 13)



Сигнал одного из цветового канала
RED/GREEN/BLUE (pin 1/pin 2/pin 3)



ПЭМИ видеотракта с VGA

ПЭМИ видеотракта представляет суперпозицию трех цветковых каналов, каналов синхросигналов строки и кадра:

$$U_S = k_R U_R + k_G U_G + k_B U_B + k_{SH} U_{SH} + k_{SV} U_{SV}$$

U_S — напряжение на входе приемника;

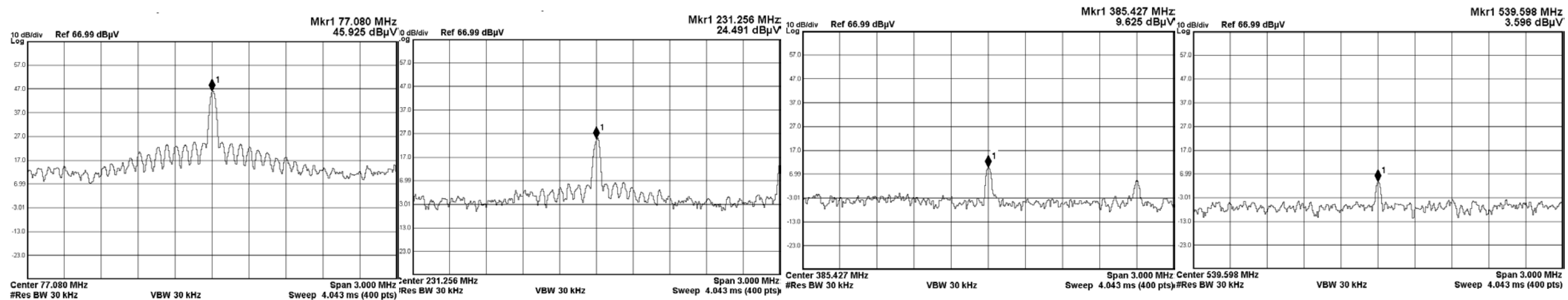
U_R, U_G, U_B — напряжение на входе приемника трех цветковых сигналов по отдельности;

U_{SH}, U_{SV} — напряжение на входе приемника каналов синхронизации строки и кадра соответственно;

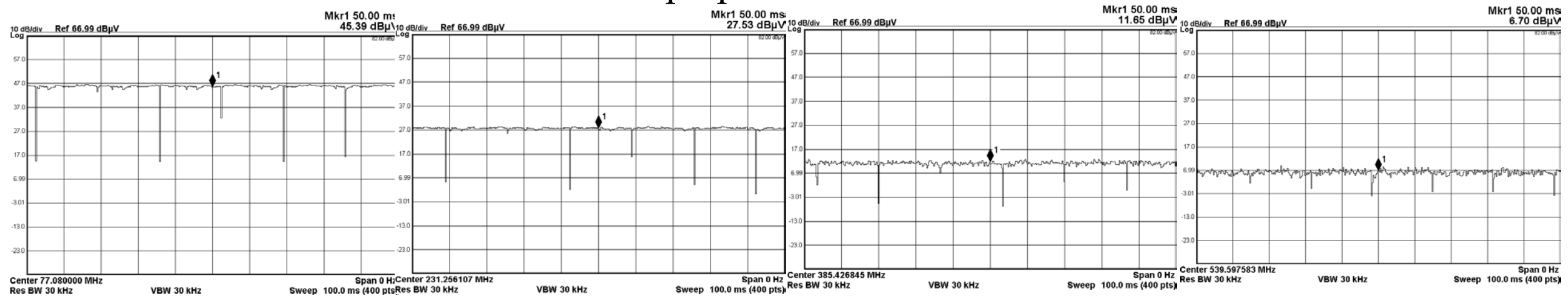
$k_R, k_G, k_B, k_{SV}, k_{SH}$ — коэффициент, зависящие от излучающего свойства случайных антенн каждого из каналов в отдельности.



Принятый сигнал ПЭМИ



Спектр принятого сигнала ПЭМИ



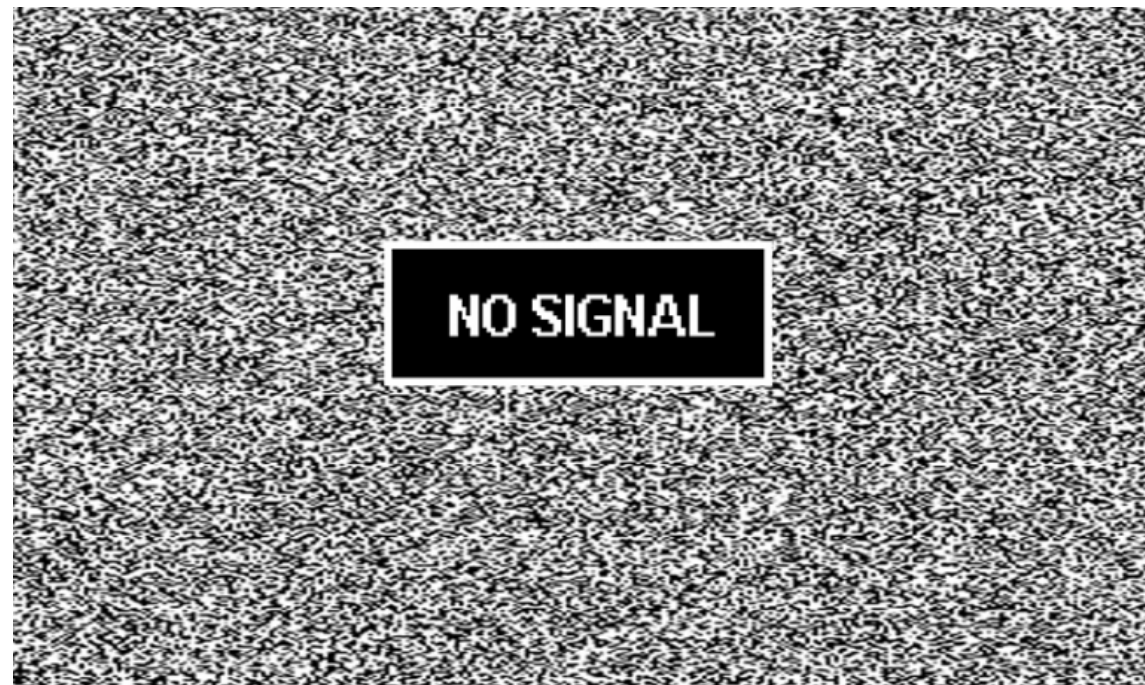
Осциллограмма принятого сигнала ПЭМИ



Уменьшение уровня ПЭМИ

Предлагаемые методы уменьшения уровня ПЭМИ

- Уменьшение напряжения в кабелях цветowych каналов;
 - Уменьшение яркости всех трех основных цветов
 - Передача цвета только по одному цветовому каналу
- Уменьшение различимости текста и фона на входе приёмника





Уменьшение яркости всех трех основных цветов

Тестовая строка	Отношение С/Ш, дБмкВ/м	Средняя оценка читаемости
Съешь ещё этих мягких французских булочек, да выпей чаю	30,96	10
Съешь ещё этих мягких французских булочек, да выпей чаю	24,38	9,6
Съешь ещё этих мягких французских булочек, да выпей чаю	22,29	8,6
Съешь ещё этих мягких французских булочек, да выпей чаю	16,37	6,8
Съешь ещё этих мягких французских булочек, да выпей чаю	9,43	4,1
Съешь ещё этих мягких французских булочек, да выпей чаю	5,07	0,9



Передача цвета только по одному цветовому каналу

Тестовая строка	Отношение С/Ш, дБмкВ/м	Средняя оценка читаемости
Съешь ещё этих мягких французских булочек, да выпей чаю	19,83	7,9
Съешь ещё этих мягких французских булочек да выпей чаю		8,3
Съешь еще этих мягких французских булочек, да выпей чаю	19,86	8,8
Съешь ещё этих мягких французских булочек, да выпей чаю		8,7
Съешь ещё этих мягких французских булочек, да выпей чаю	19,71	5,3
Съешь ещё этих мягких французских булочек, да выпей чаю		5,4

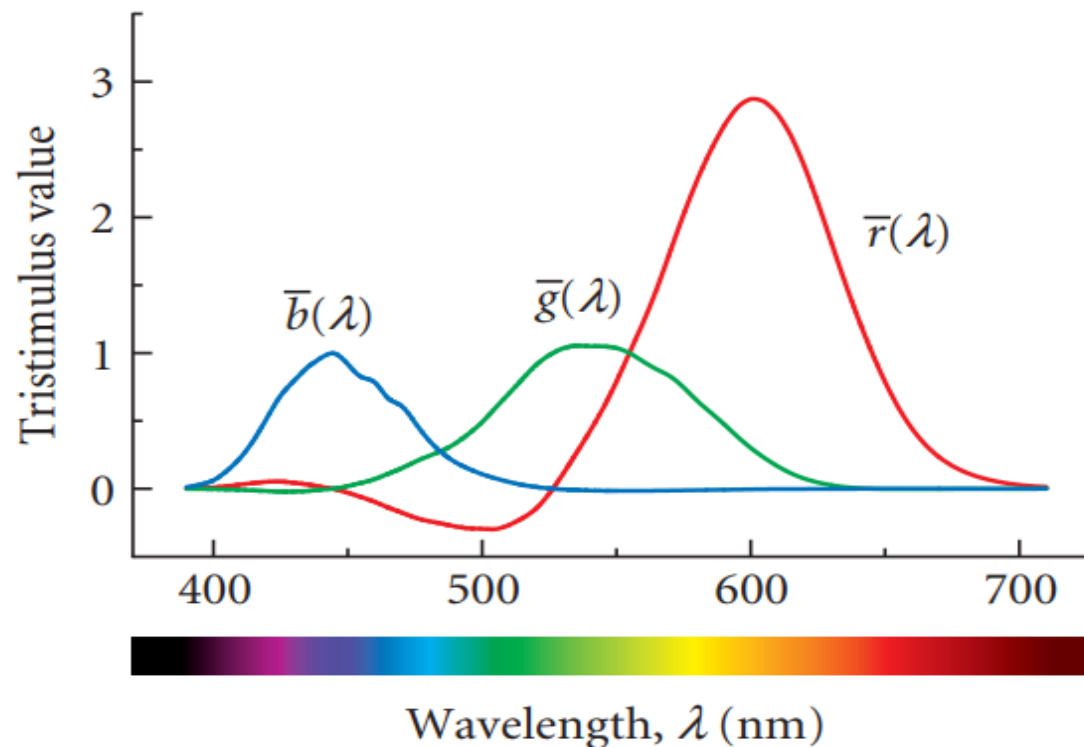


Уменьшение различимости текста и фона на входе приёмника

$$U_{RT} + U_{GT} + U_{BT} = U_{RF} + U_{GF} + U_{BF}$$

U_{RT} , U_{GT} , U_{BT} — напряжение в канале красного, зелёного и синего цветов соответственно при передаче пикселей текста;

U_{RF} , U_{GF} , U_{BF} — напряжение в канале красного, зелёного и синего цветов соответственно при передаче пикселей фона.



* Brainard D.H, Stockman A. Colorimetry



Уменьшение различимости текста и фона на входе приёмника

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



Выводы

Предложенные методы действительно уменьшают уровень ПЭМИ, а следовательно, и зону разведдоступности, в радиусе которой возможно перехватить информацию с монитора ПЭВМ.

Из предложенных вариантов цветов текста и фона возможно подобрать такие, которые значительно уменьшат уровень ПЭМИ или различимость текста и фона на стороне злоумышленника, а на читаемости текста скажутся незначительно.

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





Использованные источники

1. Kuhn M.G. Electromagnetic eavesdropping risks of flat-panel displays [Electronic resource] — Mode of access: <https://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf>. – Date of access: 01.04.2018
2. Крылова С.Л. Исследование побочных электромагнитных излучений видеосистемы ПЭВМ в учебной лаборатории информационной безопасности [Электронный ресурс] — Режим доступа: <https://www.sworld.com.ua/konfer35/597.pdf> — Дата доступа 11.04.2018
3. Филиппович А.Г. Побочные электромагнитные излучения видеотракта ПЭВМ. / А.Г. Филиппович // Управление защитой информации. — 2008 — Том №12 №1 — С.92 — 97.
4. Engdahl T. VGA analogue display connector [Electronic resource] — Mode of access: http://www.epanorama.net/documents/pc/vga_bd15.html. – Date of access: 15.04.2018
5. Васечкин Е. А., Таранов А. Б., Модель сигналов побочных электромагнитных излучений видеоинтерфейсов / Е. А. Васечкин, А. Б. Таранов // Труды СПИИРАН — 2016, № 47 — С.46–64
6. Kuhn M.G., Anderson R.J. Soft Tempest: hidden data transmission using Electromagnetic Emanations [Electronic resource] — Mode of access: <https://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>. – Date of access: 01.04.2018
7. Brainard D.H., Stockman A Colorimetry [Electronic resource] — Mode of access: <http://www.cvrl.org/people/Stockman/pubs/2010%20Colorimetry%20BS.pdf>. – Date of access: 12.04.2018
8. Kuhn M.G. Technical Report Compromising emanations: eavesdropping risks of computer displays [Electronic resource] — Mode of access: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf> – Date of access: 12.04.2018
9. VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Version 1.0, Revision 10 October 29, 2004 [Electronic resource] — Mode of access: read.pudn.com/downloads74/.../VESA-timing%20dmt10.pdf. – Date of access: 01.04.2018



Спасибо за внимание!

Докладчик: Майоров Андрей Игоревич

Органы пограничной службы Республики Беларусь

моб.: +375292323623

e-mail: 2007.maiorov@gmail.com