УДК 621.391.2 + 004.056 + 004.4.056 Вестник УрФО № 4(22) / 2016, с. 4–10

Носов Л. С., Зудин В. С.

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПО КАНАЛУ ПЭМИН ПОСРЕДСТВОМ ОПРЕДЕЛЕНИЯ СТЕПЕНИ РАСПОЗНАВАНИЯ СИГНАЛА

В работе приведена модель оценки защищенности по каналу ПЭМИН. В качестве оценки предлагается степень разборчивости сигнала ПЭМИН, методика определения которой приведена в работе. Определены параметры измерительного оборудования, при котором данная методика применима. Разработано программное обеспечение для оценки разборчивости, которое протестировано с использованием спектроанализатора Rohde & Schwarz FS300.

Ключевые слова: *ПЭМИН, аналоговый сигнал, объект информатизации, видеодисплейный монитор, электромагнитные излучения.*

Nosov L. S., Zudin V. S.

TEMPEST SECURITY ASSESSMENT MODEL BY DETERMINING THE DEGREE OF SIGNAL DETECTION

The TEMPEST security assessment model is observed in the work. As the degree of intelligibility proposed assessment TEMPEST signal, the method defined in the work. The parameters of the measuring equipment are obtained, in which the technique is applicable. Software for the determining the degree of signal has been developed, which was tested using a spectrum analyzer Rohde & Schwarz FS300.

Keywords: *TEMPEST, analog signal, informatization object, video display monitor, electromagnetic radiation.*

Одни из первых известных предположений о возможности извлечения информации из побочных излучений были сделаны в работах Герберта Ядли (Herbert Yardley) ещё в начале XX века. Военные секретные исследования ПЭМИН ведутся, по крайней мере, с начала 60-х годов[1] (некоторые источники говорят о конце 40-х - начале 50-х годов[2]). Первое упоминание побочных электромагнитных излучений, как риска компьютерной безопасности, было сделано в 1967 г. Одно из первых детальных описаний появилось в 1983 г. Широкую огласку проблема ПЭМИН получила в 1985 г. после статьи голландского инженера Вима ван Эйка (Wim van Eck) «Электромагнитное излучение видеодисплейных модулей: Риск перехвата?». Особенно сильный эффект произвела, сделанная им в этом же году на выставке Securecom-85, демонстрация перехвата излучений монитора с использованием слегка доработанного телевизионного приемника. С этого момента, перехват ПЭМИН перестал восприниматься как нечто дорогостоящее и доступное только государственным спецслужбам, и у частных организаций появился повод рассматривать этот риск как актуальный и требующий оценки[1].

Для оценки защищённости объектов информатизации от утечки информации по каналу ПЭМИН используются специальные методики. На этом этапе возникает проблема: все наиболее известные методики являются информацией ограниченного доступа. По этой причине усилия в этой работе было решено направить на разработку и программную реализацию открытой методики оценки защищенности информации от утечки по каналу ПЭМИН. Вопрос является довольно объёмным, поэтому исследование будет ограниченно излучениями монитора, использующего аналоговое подключение к компьютеру.

Все наиболее известные методики оценки защищенности информации от утечки по каналу ПЭМИН являются информацией ограниченного доступа. Это накладывает ряд ограничений на организации, желающие самостоятельно проводить оценки собственного оборудования, не прибегая к информации ограниченного доступа.

Цель настоящей работы – разработка и программная реализация открытой методики оценки защищённости информации от утечки по каналу ПЭМИН на примере излучений монитора.

Компонентный видеоинтерфейс VGA, используемый для подключения мониторов, был выпущен фирмой IBM в 1987 г. видеосигнал для такого интерфейса рассчитан на работу с ЭЛТ-мониторами, что и определяет его особенности. Во-первых, ЭЛТ-мониторы используют строчную развёртку, поэтому изображение в сигнале кодируется построчно. Во-вторых, сигнал подаётся на катод электронной пушки, поэтому он характеризуется отрицательной полярностью, т.е. белый пиксель соответствует уровню 0 В, а чёрный – уровню $-U_{\max}$[3,4,5]. Подробный анализ сигнала VGA можно найти в работах [6,7]. Помимо этого, видеосигнал обладает тремя частотными характеристиками[1]. За инструкциями по получению характеристик видеосигнала следует обратиться к документации к используемой видеокарте. Иногда информация может обнаруживаться в конфигурационных файлах системы. Кроме того, существуют стандарты VESA, определяющие продолжительности зон (их ещё называют тайминги, от англ. timings) в зависимости от разрешения и какой-нибудь частотной характеристики (некоторые из этих стандартов свободно доступны, например работа[8], по другим есть информация в косвенных источниках, например в работе[7].

Расчёт характеристик видеосигнала по разрешению и частоте обновления экрана был реализован в программе «Калькулятор таймингов VESA». Калькулятор использует формулы VESA Generalized Timing Formula (GTF)[7]. Цветные мониторы отличаются тем, что вместо одного, к ним идут сразу три канала, каждый из которых кодирует яркость одного из базовых цветов: красного, синего или зелёного. Так как эти каналы передают и излучают синхронно, отделить один цветовой канал от другого, при перехвате ПЭМИН невозможно, поэтому, с точки зрения ПЭМИН, цветной монитор не отличается от чёрно-белого[3,4,5].

Тестовый сигнал должен моделировать ситуацию, в которой оказывается злоумышленник при перехвате информации по каналу ПЭМИН. Рассмотрим некоторые особенности, возникающие при таком перехвате. Чтобы кабель излучал, в нём должен протекать переменный ток. Это значит, что злоумышленник будет наблюдать сигнал в эфире только тогда, когда в кабеле меняется уровень напряжения, т.е. когда в изображении возникает цветовой переход. В связи с этим, а также с тем,

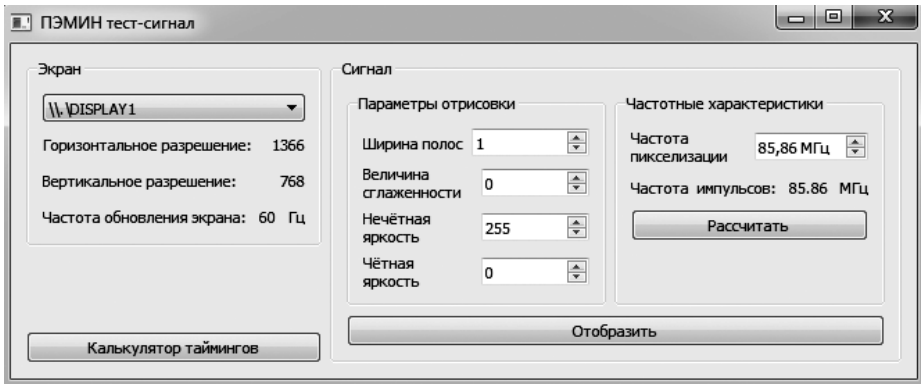

Рис. 1. Интерфейс программы «ПЭМИН тест-сигнал»

что через ПЭМИН неразличимы цветовые компоненты, перехват, в первую очередь, рассчитан на двухцветные изображения (чёрный текст на белом фоне – наиболее распространённый вид такого изображения)[1]. Перехваченное изображение, в этом случае, содержит контуры исходного.

Тогда качество распознавания изображения можно определять по точности определения границ цветовых переходов на изображении. Очевидно, что, благодаря построчной развёртке, имеют значение только горизонтальные переходы, поэтому, тестовый сигнал может представлять собой чередование вертикальных полос двух цветов. Для такого сигнала можно определить несколько параметров:

- Ширина полосы в пикселях;
- Разность яркости соседних полос;
- Сглаженность перехода в пикселях.

Описанный тестовый сигнал реализован в программе «ПЭМИН тест-сигнал». Интерфейс программы представлен на рис. 1.

Раздел «Экран» определяет монитор, на котором следует отобразить тестовый сигнал. Раздел «Параметры отрисовки» определяет параметры тестового сигнала. Раздел «Частотные характеристики» является вспомогательным: он позволяет рассчитать частоту цветовых переходов заданного тестового сигнала по известной частоте пикселизации. Кнопка «Калькулятор таймингов» вызывает окно, эквивалентное программе «Калькулятор таймингов VESA» (см. выше), в котором параметры видеорежима установлены в соответствии с выбранным в разделе «Экран» монитором. Частота пикселизации, рассчитанная калькулятором таймингов, автоматически установится в разделе «Частотные характеристики».

Порядок и особенности выполнения измерений зависят от применяемого оборудования, поэтому эту задачу имеет смысл отделить от остальной части оценки. В рамках этой работы планировалось использовать спектроанализатор Rohde & Schwarz FS300. Он поддерживает удалённое управление с компьютера. Порядок удалённой работы со спектроанализатором описан в руководствах к нему [9,10].

Инструмент для выполнения измерений был реализован в виде программы «Измеритель: R&S серии FS3xx». Интерфейс программы представлен на рис. 2.

Во время тестирования измерителя, выяснилось, что достижимой частоты дискретизации спектроанализатора Rohde & Schwarz FS300 недостаточно для проведения тестов, т.к. фактически теряются практически все горизонтальные составляющие. Например, на рис. 3 изображён тестовый сигнал, и соответствующее ему перехваченное изображение. Как можно видеть, горизонтальные переходы в пределах строки практически отсутствуют.

Чтобы таких проблем не возникало, при выборе измерителя следует руководствоваться следующим правилом: если сигнал имеет частоту пикселизации f_p, и планируется оценивать распознаваемость объектов, с горизонтальными размерами не менее w пикселей (ширина полосы в тестовом сигнале из раздела 3.2 не менее w), минимальная частота дискретизации прибора вычисляется по следующей формуле:

$$f_d = \frac{2 f_p}{w} \qquad (1)$$

В данной работе, доступа к измерителю с необходимыми характеристиками получить не удалось, поэтому дальнейшую разработку придётся продолжать без проведения тестов. Наиболее простой и, возможно, эффективный способ выделения кадра – это ручное

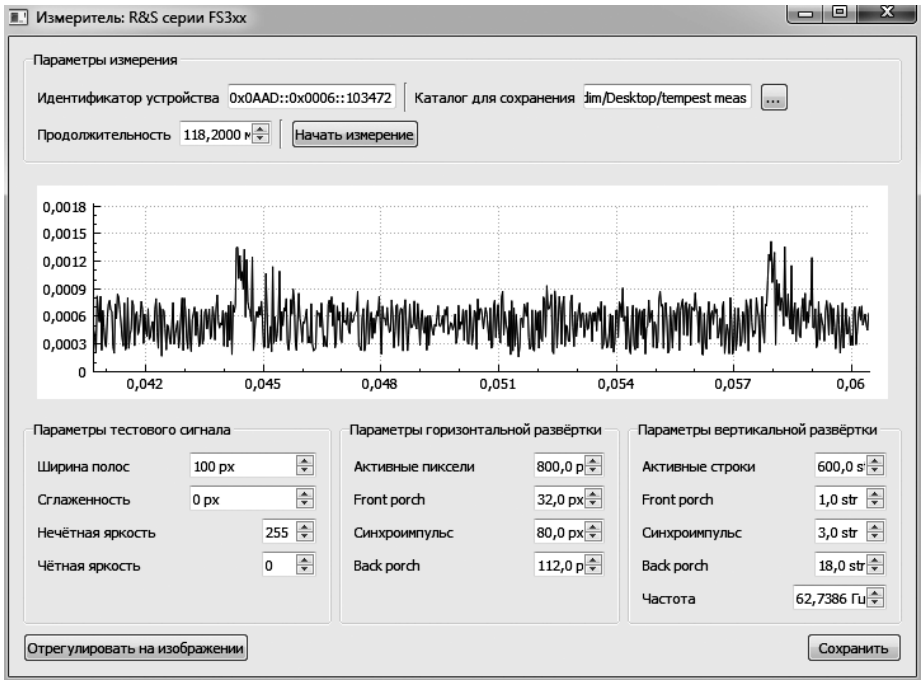

Рис. 2. Интерфейс программы « Измеритель: R&S серии FS3xx»

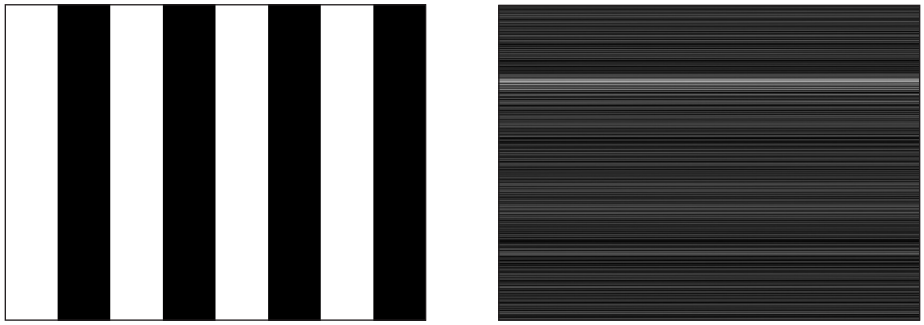

Рис. 3. Пример тестового сигнала (слева) и соответствующее ему перехваченное изображение (справа).

выделение оператором. Однако при обработке большого количества измерений такой метод создаёт большую нагрузку на человека. В этом разделе предпринята попытка предложить метод автоматического выделения кадра.

Зная параметры исследуемого монитора, параметры тестового сигнала и способ его образования, можно попытаться предсказать форму сигнала ПЭМИН. Для тестового сигнала, описанного выше, ПЭМИН должен представлять собой последовательность коротких импульсов. Ниже дано описание правил определения положения этих импульсов.

Пусть определены следующие характеристики сигнала: T_{pulse} – период следования цветовых переходов тестового сигнала; T_h – период горизонтальной развёртки; t_{h_active} – продолжительность горизонтальной «активной» области; t_{h_fp} – время начала строкового «front porch» от начала строки; t_{h_sync} – время начала строкового синхроимпульса от начала строки; t_{h_bp} – время начала строкового «back porch» от начала строки; T_v – период вертикальной развёртки; t_{v_active} – продолжительность вертикальной «активной» области; t_{v_fp} – время начала вертикального «front porch» от начала кадра; t_{v_sync} – время начала вертикального синхроимпульса от начала кадра; t_{v_bp} – время начала вертикального «back porch» от начала кадра; b_1 – нечётная яркость; b_2 – чётная яркость. Яркость последней полосы в строке b_{last} можно определить следующим образом: $b_{last} = b_1$, если $\left[\frac{T_h}{T_{pulse}}\right]$ – нечётное, $b_{last} = b_2$, если $\left[\frac{T_h}{T_{pulse}}\right]$ – чётное. Здесь […] – взятие целой части.

Для некоторого момента времени t, время от начала кадра t_v, время от начала строки t_h и время от последнего цветового перехода t_{pulse} определяются следующим образом:

$$t_v = t - \left[\frac{t}{T_v}\right] \times T_v, \; t_h = t_v - \left[\frac{t}{T_h}\right] \times T_h,$$
$$t_{pulse} = t_h - \left[\frac{t}{T_{pulse}}\right] \times T_{pulse} \tag{2}$$

Если задана ширина импульса w_{pulse}, то t принадлежит импульсу образцового сигнала, если оно удовлетворяет следующему условию:

$$\begin{aligned}
&\left(\left(t_v < w_{pulse}/2\right) \wedge \left(b_1 > 0\right)\right) \vee \left(\left|t_v - t_{v_sync}\right| < w_{pulse}/2\right) \vee \\
&\left(\left(t_v < w_{pulse}/2\right) \wedge \left(b_1 > 0\right)\right) \vee \left(\left|t_v - t_{v_bp}\right| < w_{pulse}/2\right) \vee \\
&\left(\left(T_v - t_v < w_{pulse}/2\right) \wedge \left(b_1 > 0\right)\right) \vee \left(\left(t_h < w_{pulse}/2\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v > t_{v_fp}\right)\right) \vee \\
&\left(\left(\left|t_h - t_{h_fp}\right| < w_{pulse}/2\right) \wedge \left(b_{last} > 0\right) \wedge \left(t_v > t_{v_fp}\right)\right) \vee \\
&\left(\left(\left|t_h - t_{h_sync}\right| < w_{pulse}/2\right) \wedge \left(\left(t_v < t_{v_sync}\right) \vee \left(t_v > t_{v_bp}\right)\right)\right) \vee \\
&\left(\left(\left|t_h - t_{h_bp}\right| < w_{pulse}/2\right) \wedge \left(\left(t_v < t_{v_sync}\right) \vee \left(t_v > t_{v_bp}\right)\right)\right) \vee \\
&\left(\left(T_h - t_h < w_{pulse}/2\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v < t_{v_fp} - w_{pulse}/2\right)\right) \vee \\
&\left(\left(t_{pulse} < w_{pulse}/2\right) \wedge \left(t_h > w_{pulse}/2\right) \wedge \left(t_h < t_{h_fp} - w_{pulse}/2\right)\right) \vee \\
&\left(\left(T_{pulse} - t_{pulse} < w_{pulse}/2\right) \wedge \left(t_h > w_{pulse}/2\right) \wedge \left(t_h < t_{h_fp} - w_{pulse}/2\right)\right)
\end{aligned} \tag{3}$$

здесь: $\wedge$ – логическое «И», $\vee$ – логическое «ИЛИ». Используя условия из формулы (3), можно сгенерировать образцовый сигнал в любом временном диапазоне.

Так как продолжительность кадра T_v известна, необходимо только определить смещение кадра в исследуемом сигнале. Для этого можно воспользоваться способом определения смещения между похожими сигналами по максимуму функции корреляции [12]. Порядок операций следующий:

1) сгенерировать образцовый сигнал на временном диапазоне $[0, T_v)$;

2) на промежутке $[0; T_v)$ рассчитать значения функции корреляции между исследуемым и образцовым сигналами;

3) смещение принять равным положению максимума функции корреляции.

Как уже было указано выше, качество распознавания изображения можно определять по точности определения границ цветовых переходов на изображении. Можно выделить два вида ошибок: потеря цветового перехода и обнаружение ложного цветового перехода. Соответственно, можно определить две метрики информативности ПЭМИН: процент потерянных цветовых переходов и процент ложных цветовых переходов (относительно ожидаемого числа цветовых переходов). Ниже предложен способ вычисления этих метрик. Расчёт описанных метрик был реализован в программе «Оценка ПЭМИН».

Первое, что необходимо определить, это ожидаемое расположение цветовых переходов. Определим яркость последней полосы в строке b_{last}. Для некоторого момента времени t, в соответствии с формулой (2), определим время от начала кадра t_v, время от начала строки t_h и время от последнего цветового перехода t_{pulse}. Тогда t является ожидаемым положением цветового перехода, если оно удовлетворяет следующему условию:

$$\begin{aligned}
&\left(\left(t_h = 0\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v < t_{v_active}\right)\right) \vee \left(\left(t_h = t_{h_active}\right) \wedge \left(b_{last} > 0\right) \wedge \left(t_v < t_{v_active}\right)\right) \vee \\
&\left(\left(t_h = T_h\right) \wedge \left(b_1 > 0\right) \wedge \left(t_v < t_{v_active}\right)\right) \vee \left(\left(t_{pulse} = 0\right) \wedge \left(t_v < t_{v_active}\right) \wedge \left(t_h > 0\right)\right) \vee \\
&\left(\left(t_{pulse} = T_{pulse}\right) \wedge \left(t_v < t_{v_active}\right) \wedge \left(t_h < t_{h_active}\right)\right)
\end{aligned} \tag{4}$$

Используя условия из формулы (4), можно сгенерировать массив ожидаемых расположений цветовых переходов в любом временном диапазоне. Следующее, что необходимо определить – это расположение цветовых переходов в исследуемом сигнале. Эта задача сводится к поиску и определению положения пиков. К сожалению, из-за наличия шумов, простой поиск точек локального максимума может не дать нужного результата. В этой работе предлагается другой способ поиска пиков в сигнале:

1) Задать размер окна w (в секундах) и значение порога для углового коэффициента $k_{\min}$. На интуитивном уровне, w определяет ширину пика, а $k_{\min}$, определяет минимальную скорость роста сигнала до точки пика и минимальную скорость падения сигнала после точки пика.

2) Для каждой точки сигнала t выделить два диапазона: $\left[t-\frac{w}{2};t\right]$ и $\left[t;t+\frac{w}{2}\right]$.

3) Используя метод наименьших квадратов [10], аппроксимировать оба диапазона линейной зависимостью. Обозначим полученные угловые коэффициенты как k_1, для диапазона $\left[t-\frac{w}{2};t\right]$ и k_2, для диапазона $\left[t;t+\frac{w}{2}\right]$.

4) Рассматриваемая точка t будет считаться точкой пика, если $k_1 > k_{\min}$ и $k_2 < -k_{\min}$.

5) Если, согласно предыдущему правилу, к точке пика были отнесены несколько соседних точек сигнала, то их следует заменить одной, равной их среднему.

Порядок вычисления процента потерянных цветовых переходов $p_{пот}$ и процента ложных цветовых переходов $p_{лож}$ можно определить следующим образом:

1) Задать пороговое значение $\Delta_{\max}$, задающее максимально допустимое отклонение реального пика от его ожидаемого положения.

2) Создать счётчики числа ложных импульсов $n_{лож}$ и числа потерянных импульсов $n_{пот}$. Установить их равными нулю.

3) Сгенерировать массив ожидаемых расположений цветовых переходов (образцовый массив) на промежутке времени, соответствующему исследуемому сигналу. Записать его длину в переменную n.

4) Сгенерировать массив расположений цветовых переходов в исследуемом сигнале (исследуемый массив).

5) Создать вспомогательный массив.

6) Создать переменную для хранения текущего положения в исследуемом массиве и установить её равной -1.

7) Для каждого значения в образцовом массиве выполнить следующие действия:

- найти ближайший элемент в исследуемом массиве;
- рассчитать точность, как разницу между значением образцового массива и значением ближайшего элемента исследуемого массива;

рассчитать смещение s в исследуемом массиве, как разницу между индексом найденного элемента исследуемого массива и текущим положением в исследуемом массиве;

- если $s = 0$, то увеличить $n_{пот}$ на 1, и, если последний элемент вспомогательного массива больше точности, установить его равным точности;
- если $s = 1$, то добавить значение точности во вспомогательный массив;
- если $s > 1$, увеличить $n_{лож}$ на $s-1$ и добавить значение точности во вспомогательный массив.

8) Для каждого элемента во вспомогательном массиве, если значение элемента больше $\Delta_{\max}$, увеличить счётчики $n_{лож}$ и $n_{пот}$ на 1.

9) Рассчитать процент потерянных цветовых переходов по следующей формуле: $p_{пот} = \frac{n_{пот}}{n} \times 100\%$.

10) Рассчитать процент ложных цветовых переходов по следующей формуле: $p_{лож} = \frac{n_{лож}}{n} \times 100\%$.

В ходе настоящей работы разработаны метрики информативности ПЭМИН аналогового видеосигнала и составлена методика оценки защищённости монитора от утечки информации по каналу ПЭМИН и выполнена программная реализация полученной методику оценки защищённости.

Примечания

1. Kuhn M. G., Anderson R. J. Soft Tempest: Hidden data transmission using electromagnetic emanations. – United Kingdom.: University of Cambridge, 1998. – 19 p.

2. Мотуз О. В. Побочные электромагнитные излучения: моменты истории // Сайт проекта Агентура. Ru. – URL: http://www.agentura.ru/culture007/history/tempest/ (дата обращения: 17.11.2016).

3. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 1 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenki-pemin-tsifrovykh-signalov-tft-monitory.php (дата обращения: 17.11.2016).

4. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 2 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenki-pemin-tsifrovykh-signalov-tft-monitory-chast-2.php (дата обращения: 17.11.2016).

5. Кондратьев А. В. К вопросу оценки ПЭМИН цифровых сигналов. TFT мониторы. Часть 3 // Официальный сайт группы компаний МАСКОМ. – URL: http://www.mascom.ru/library/statyi/k-voprosu-otsenki-pemin-tsifrovykh-signalov-tft-monitory-chast-3.php (дата обращения: 17.11.2016).

6. VGA Hardware // Wiki проекта OS Project. – URL: http://wiki.osdev.org/VGA_Hardware (дата обращения: 17.11.2016).

7. Video signals and timing // Wiki проекта OS Project: URL: http://wiki.osdev.org/Video_Signals_And_Timing (дата обращения: 17.11.2016).

8. VESA Display Monitor Timing Standard «VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT)» // Video Electronics Standards Association. – 2007.

9. Remote Control Manual Series300 Spectrum Analyzer. VXI Plug & Play Style Instrument Driver. – Germany.: ROHDE & SCHWARZ GmbH & Co. KG, 2006. – 185 p.

10. Rohde & Schwarz Smart Instruments Family300 Basic Programming Guide. – Germany.: ROHDE & SCHWARZ GmbH & Co. KG, 2007. – 23 p.

НОСОВ Леонид Сергеевич, заведующий кафедрой информационной безопасности института точных наук и информационных технологий ФГБОУ ВО «Сыктывкарский государственный университет имени Питирима Сорокина», к.ф.-м.н., доцент. 167001, г. Сыктывкар, Октябрьский пр., д. 55. E-mail: nosov@syktsu.ru

ЗУДИН Вадим Станиславович, студент института точных наук и информационных технологий ФГБОУ ВО «Сыктывкарский государственный университет имени Питирима Сорокина». 167001, г. Сыктывкар, Октябрьский пр., д. 55. E-mail: nosov@syktsu.ru

NOSOV Leonid, Head of Department of Information Security of The Institute of Exact Sciences and Information Technology of Federal State Budget Educational Institution of Higher Education «Syktyvkar State University named after Pitirim Sorokin», Physics and Mathematics PhD, assistant professor. Bld. 55, Oktyabrsky pr, Syktyvkar, 167001. E-mail: nosov@syktsu.ru

ZUDIN Vadim, student of The Institute of Exact Sciences and Information Technology of Federal State Budget Educational Institution of Higher Education «Syktyvkar State University named after Pitirim Sorokin». Bld. 55, Oktyabrsky pr, Syktyvkar, 167001. E-mail: nosov@syktsu.ru