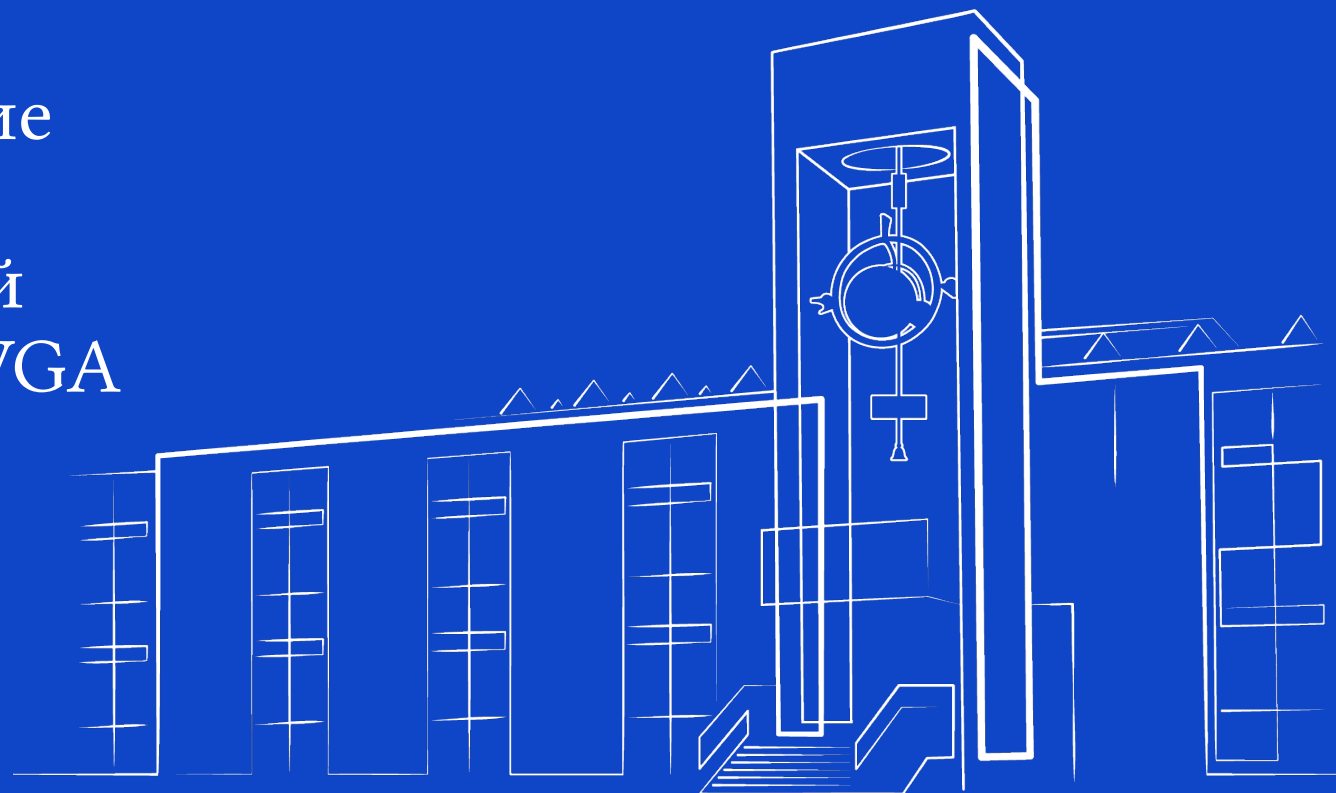


Имитационное моделирование перехвата побочных электромагнитных излучений видеосистем с интерфейсом VGA

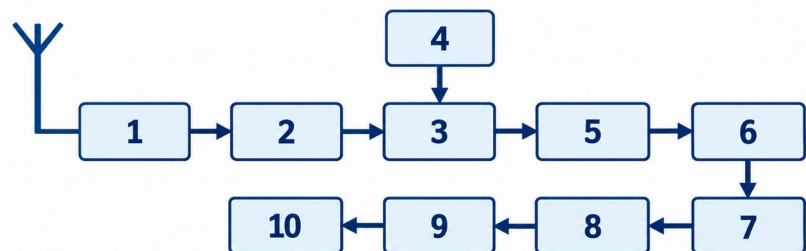


Лукманова Оксана Равилевна

Старший преподаватель кафедры
информационной безопасности, НИУ МИЭТ

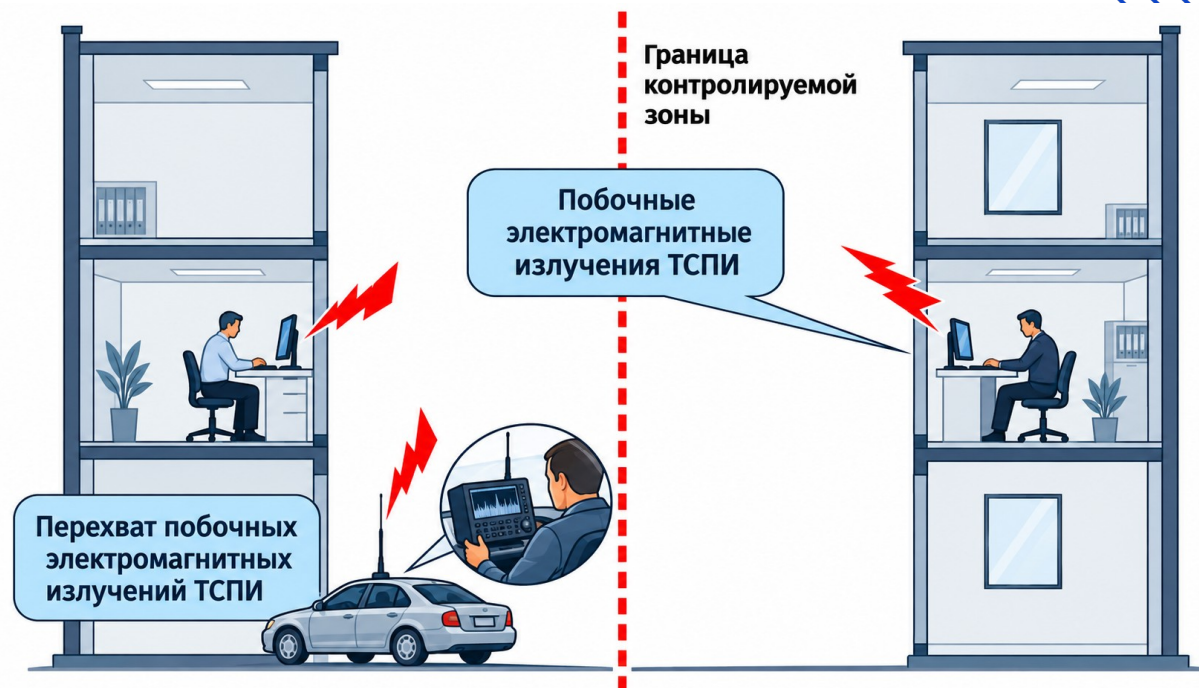


Перехват ПЭМИ технических средств



- 1 – перестраиваемый полосовой фильтр высокой частоты;
- 2 – усилитель высокой частоты;
- 3 – смеситель (для упрощения схема представлена только с одним смесителем);
- 4 – управляемый генератор (гетеродин);
- 5 – перестраиваемый полосовой фильтр промежуточной частоты;
- 6 – усилитель промежуточной частоты;
- 7 – видеодетектор;
- 8 – аналого-цифровой преобразователь;
- 9 – блок цифровой обработки сигналов;
- 10 – ЖК-монитор.

Упрощённая структурная схема комплекса перехвата



Результаты Маркуса Кюна: перехват контрольного текста с экрана ноутбука при полосах пропускания приёмника 20 и 200 МГц

Цель и постановка исследования

Цель

Оценить влияние полосы пропускания приёмника на восстановление и распознавание текста ПЭМИ видеосистемы VGA

Объект: канал утечки информации через ПЭМИ видеосистемы VGA

Метод: имитационное моделирование в Matlab

Результат: зависимости качества изображения от RBW и времени накопления



Структура имитационной модели

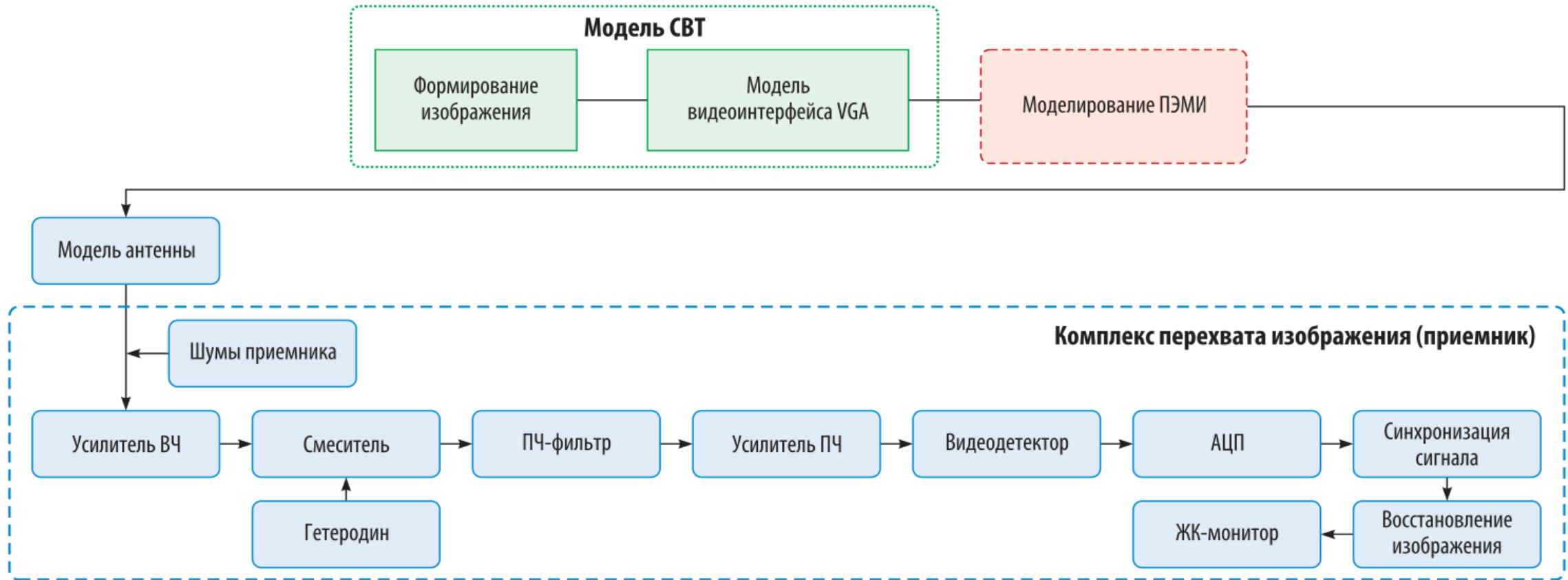


Рис. 1. Структурная схема модели канала перехвата ПЭМИ видеосистем, использующих интерфейс VGA

Формирование изображения



Рис. 1. Синтезированное эталонное Full HD-изображение

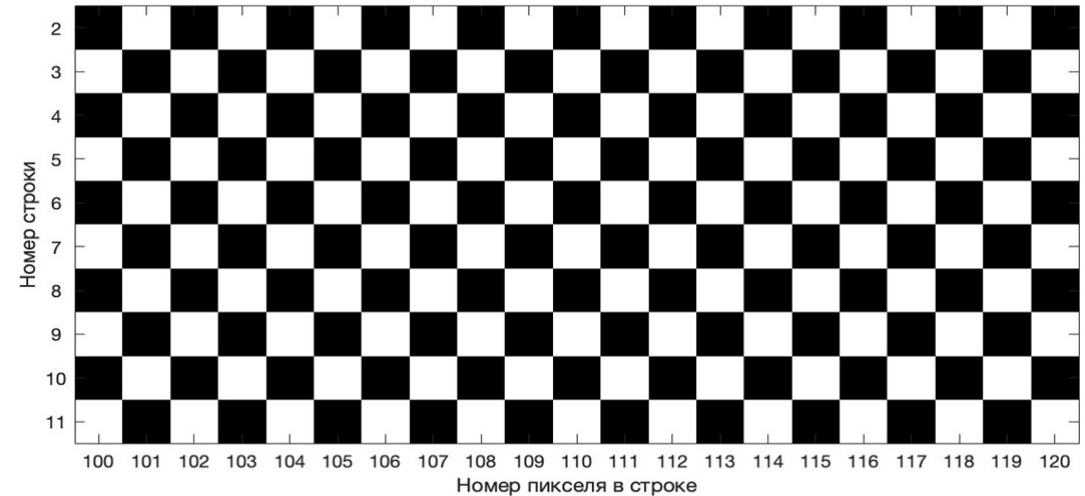


Рис. 2. Тестовый паттерн «шахматная доска» для оценки предельной пространственной частоты (увеличенный фрагмент 10 × 20 пикселей)

Full HD (1920×1080 пикселей) в цифровой области формализуется как тензор:

$$I(y, x, l) \in [0, 1],$$

где $y \in [1, 1080]$, $x \in [1, 1920]$, а $l \in \{R, G, B\}$ — глубина тензора

Модель видео интерфейса VGA

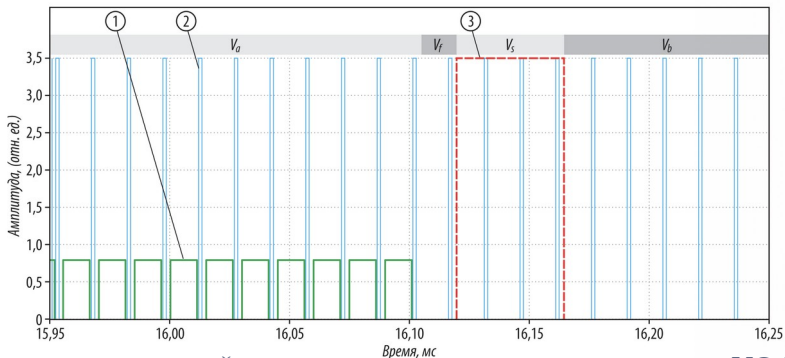


Рис. 1. Осциллограмма фрагмента структуры видеосигнала VGA-кадра

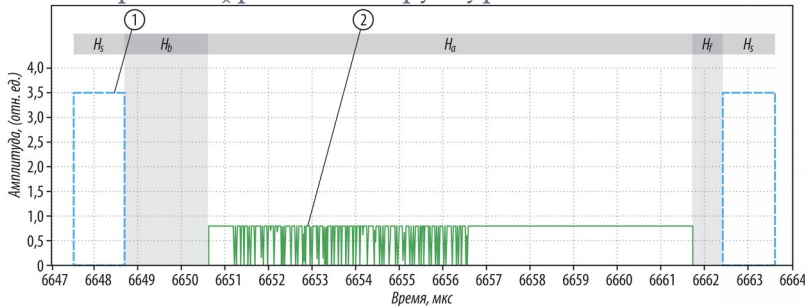


Рис. 2. Осциллограмма структуры видеосигнала 446-й строки

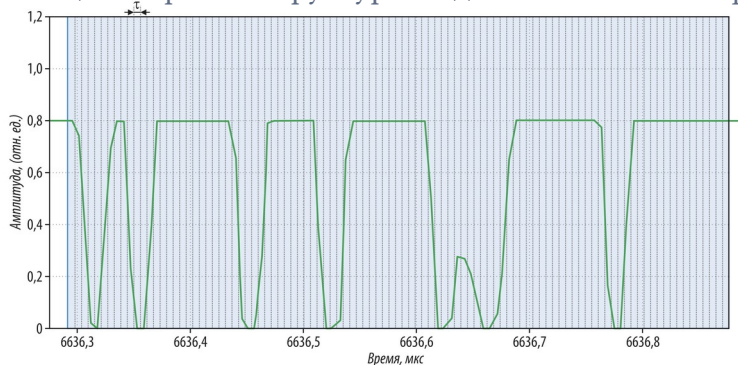


Рис. 3. Фрагмент активной части 446-й строки (пиксели 100–120) с длительностью импульса

Параметры видеокадра VGA стандарта VESA CVT
(1920 × 1080, 60 Гц)

$f_p = 172,750 \text{ МГц}$ $T_p \approx 5,789 \text{ нс}$ $F_k = 60 \text{ Гц}$

Параметр	Горизонтально, пиксели	Вертикально, строки
Активная часть (a)	$H_a = 1920$ ($\approx 11,114 \text{ мкс}$)	$V_a = 1080$ ($\approx 16,105 \text{ мс}$)
Передний гасящий интервал (f)	$H_f = 120$ ($\approx 0,695 \text{ мкс}$)	$V_f = 1$ ($\approx 14,912 \text{ мкс}$)
Синхроимпульс (s)	$H_s = 208$ ($\approx 1,204 \text{ мкс}$)	$V_s = 3$ ($44,735 \text{ мкс}$)
Задний гасящий интервал (b)	$H_b = 328$ ($\approx 1,899 \text{ мкс}$)	$V_b = 34$ ($506,999 \text{ мкс}$)
Итого (t)	$H_t = 2576$ ($\approx 14,912 \text{ мкс}$)	$V_t = 1118$ ($16,671 \text{ мс}$)

Уровни напряжений видеосигнала:
активная область (видосигнал) – H – 0,9 В

Общее количество отсчетов: $N_t = H_t \times V_t = 2\,880\,768$,
что позволяет сформировать непрерывную временную ось $t_f(n) = n \cdot T_p$,



Моделирование ПЭМИ

1. Напряженность электрической составляющей электромагнитного поля ПЭМИ на расстоянии 1 м:

$$E(f) = U(f) + K_{a.сл}(f)$$

2. Затухания ПЭМИ на трассе СВТ – ТСП ПЭМИ:

$$V(f, r) = 20 \log_{10} \left(\frac{r_0}{r} \right)^3 \cdot \sqrt{\frac{k_f^4 r^4 - k_f^2 r^2 + 1}{k_f^4 r_0^4 - k_f^2 r_0^2 + 1}},$$

где $V(f, r)$ коэффициент ослабления ПЭМИ на расстоянии r на частоте f ;

$k_f = \frac{2\pi f}{c}$ – волновое число;

$c = 3 \cdot 10^8$ – скорость света, м/с.

r_0 – расстояние, на котором производилось измерение ПЭМИ ($r_0=1$ м).

3. Напряженность электромагнитного поля ПЭМИ на расстоянии r от СТБ можно рассчитать по формуле:

$$E_r(f) = E(f) + V(f, r).$$

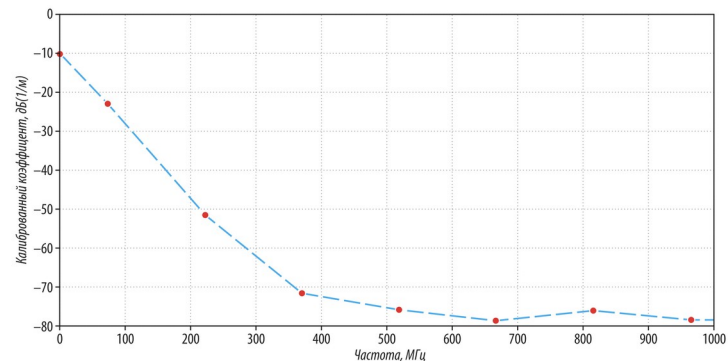


Рис. 1. График зависимости калибровочного коэффициента случайной антенны Ка.сл от частоты f

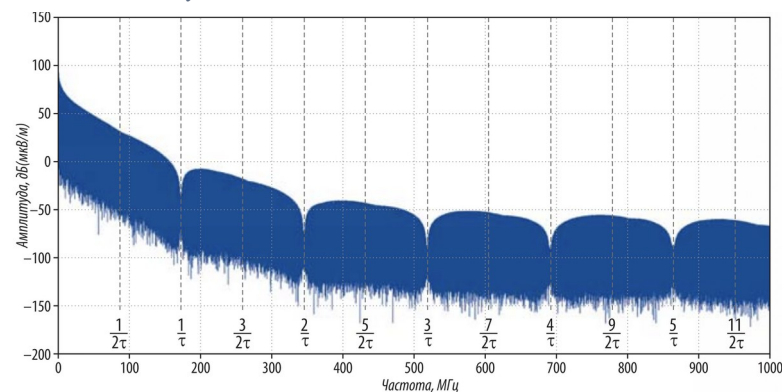


Рис. 2. Спектр ПЭМИ на расстоянии 1 м от СВТ

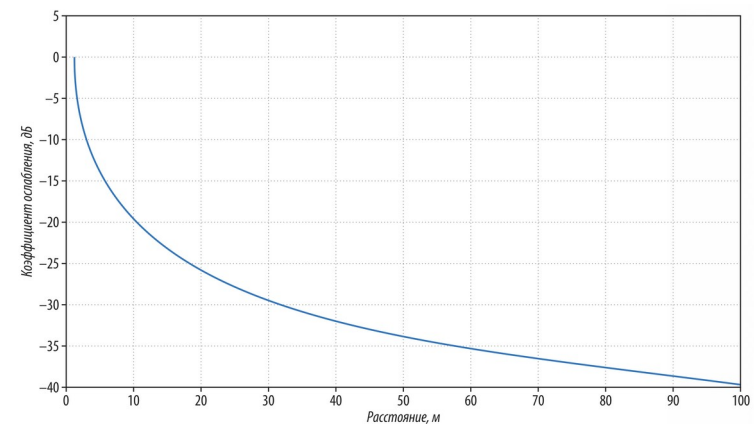


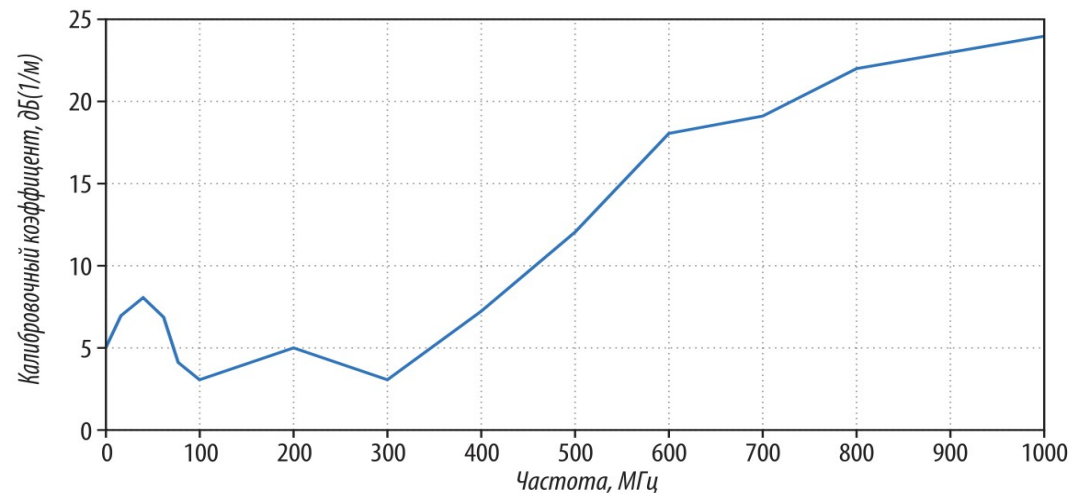
Рис. 3 Зависимость коэффициента ослабления напряженности поля ПЭМИ от расстояния r ($f = 172,75$ МГц)

Модель приёмного устройства

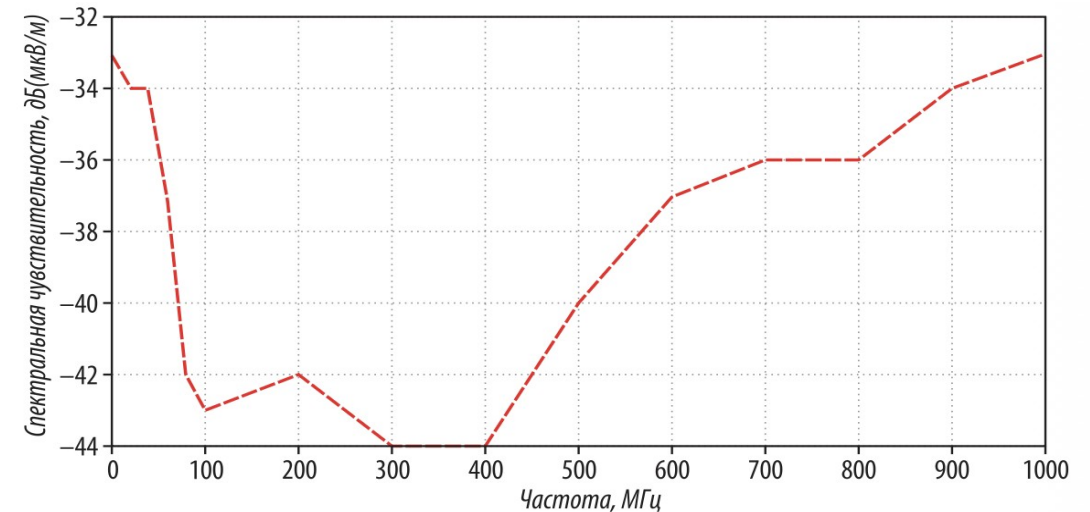
Средство перехвата: R&S FSW и антенна R&S HE600

Спектральная мощность шума анализатора спектра:

$$P_{\text{ш.пр}} = -169 \text{ дБмВт/Гц}$$
$$(U_{\text{ш.пр}} = -62 \text{ дБмкВ}/\sqrt{\text{Гц}})$$



а)



б)

Рис. 1. Характеристики антенны R&S®HE600:
а) калибровочный коэффициент; б) спектральная чувствительность ($SNR = 0$ дБ, $RBW = 1$ Гц)

Приёмный тракт: входной сигнал

1. Напряжение информативного сигнала на входе приемного устройства:

$$U_{\text{вх.пр}}(f) = E_r(f) - K_{\text{а.тср}}(f)$$

2. Принятый сигнал усиливается радиочастотным каскадом с коэффициентом усиления $G_{\text{yc}} = 100$ и поступает на вход смесителя, где происходит его преобразование с использованием гетеродина – стабильного опорного генератора.

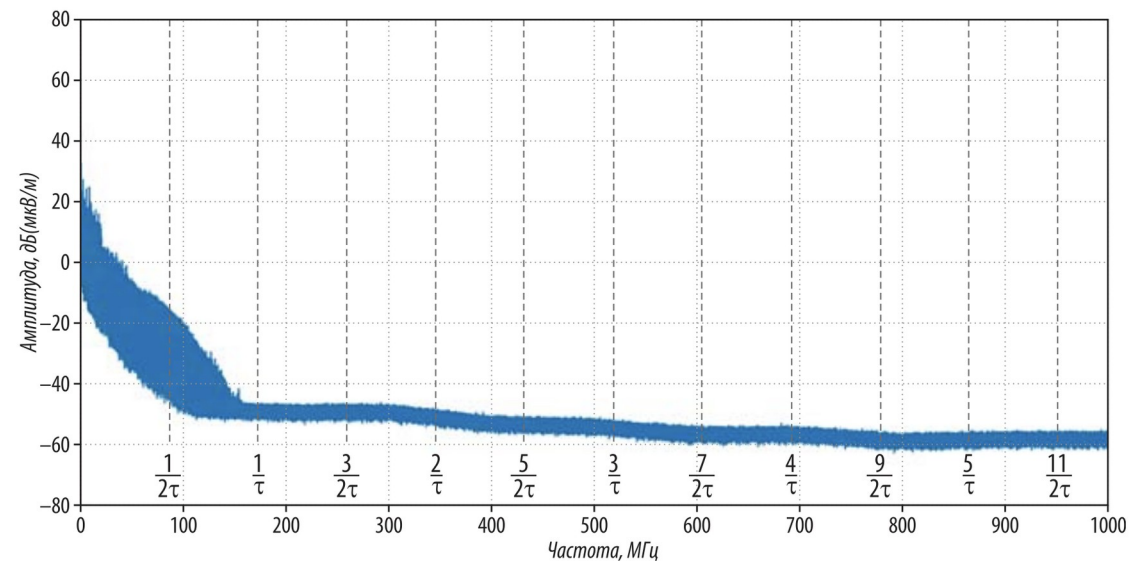


Рис. 1. Спектр сигнала на входе приёмного устройства

Приёмный тракт: преобразование и фильтрация

3. Локальный гетеродин генерирует гармоническое колебание с частотой f_{Γ} , определяемой выбранной центральной частотой настройки приёмника f_c и промежуточной частотой $f_{\text{ПЧ}}$:

$$f_{\Gamma} = f_c - f_{\text{ПЧ}}$$

В данной модели для анализа выбраны значения $f_c = 259,125$ МГц и $f_{\text{ПЧ}} = 172,75$ МГц.

4. Для выделения информационного сигнала и подавления побочных продуктов смешения в тракте промежуточной частоты использован полосовой фильтр Баттерворта второго порядка.

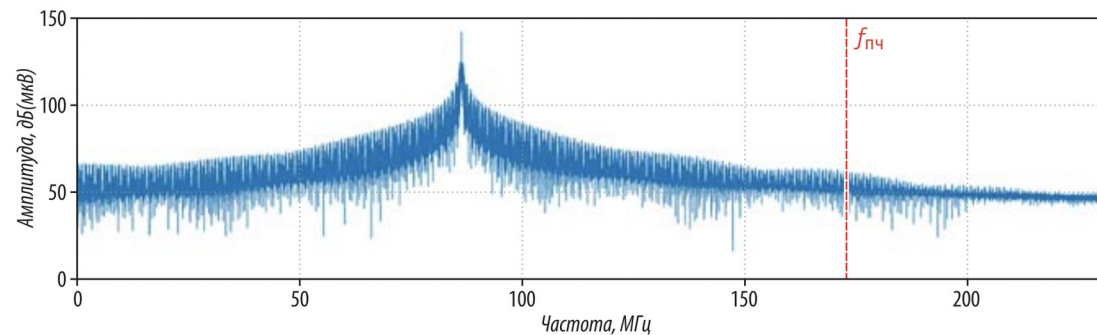


Рис. 1. Спектр информативного сигнала на выходе смесителя

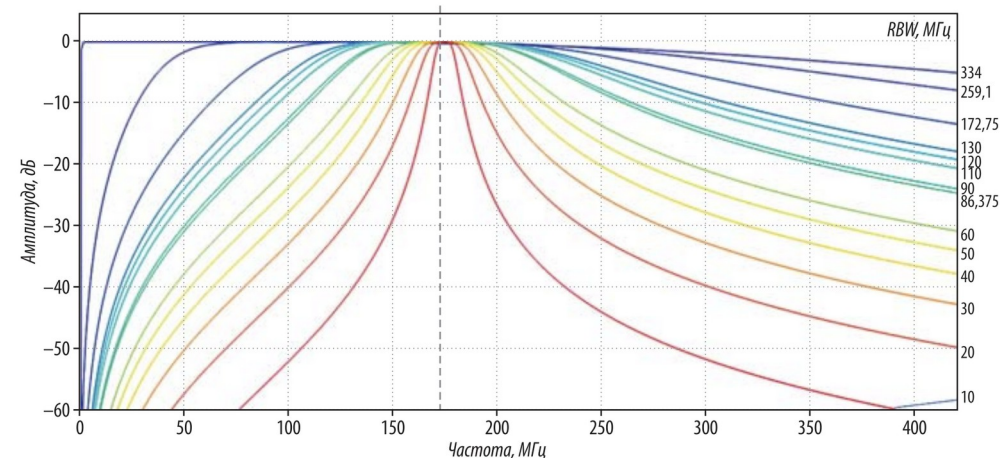
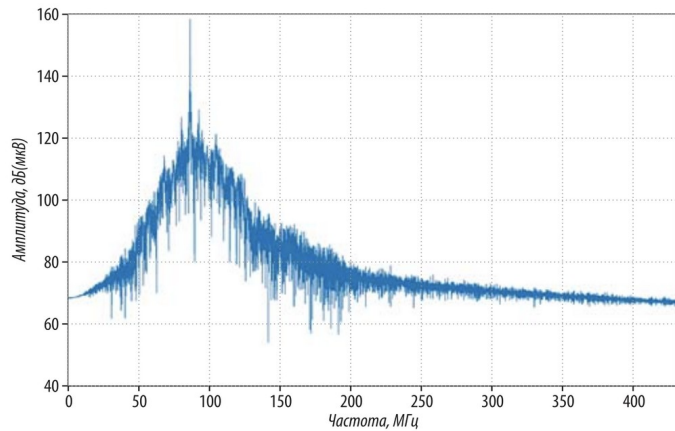
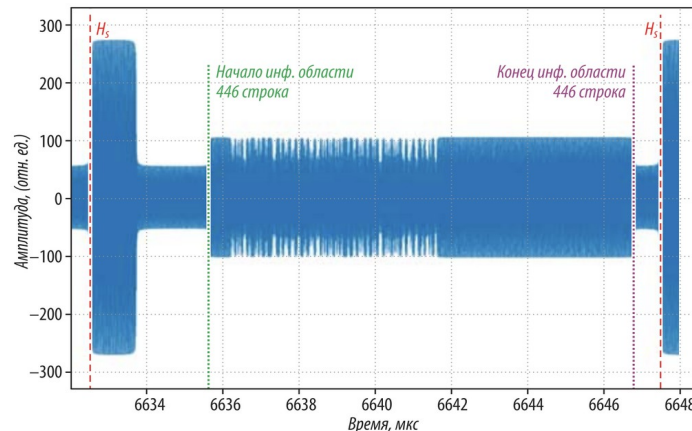


Рис. 2. АЧХ полосовых фильтров промежуточной частоты

Приёмный тракт: демодуляция сигнала



а)



б)

Рис. 1. Спектр (а) и осциллограмма (б) на выходе полосового фильтра (RBW = 172,75 МГц)

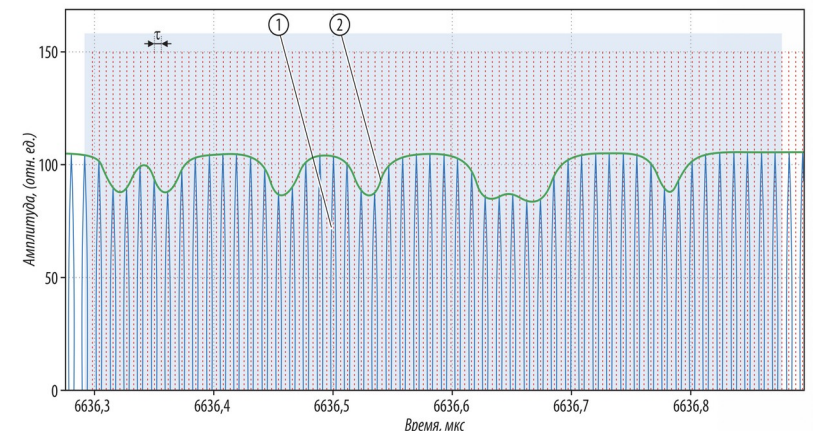


Рис. 2. Сигнал на выходе ПЧ-тракта (1) и видеодетектора (2)

После полосового фильтра сигнал усиливается каскадом с $G_{ПЧ} = 10$ до уровня, необходимого для дальнейшей обработки.

Для демодуляции АМ-сигнала используется детектор огибающей на основе преобразования Гильберта. Огибающая фильтруется ФНЧ для выделения низкочастотной составляющей яркости изображения. Частота среза ФНЧ выбирается по полосе анализа приёмного тракта и не превышает 80 МГц.

Для устранения фазовых искажений применяется двунаправленная фильтрация с нулевым фазовым сдвигом.

Синхронизация и восстановление изображения

$$f_{\text{АЦП}} = 4 \text{ ГГц}$$

Нормализация амплитуды в диапазон $[0, 1]$

Адаптивный порог: $V_{\text{thr}} = 0,3 \cdot \max(U_{\text{norm}}[n])$

Проверка периодичности синхроимпульсов

Выделение активных строк и сборка кадра

Бинаризация и морфологическая обработка

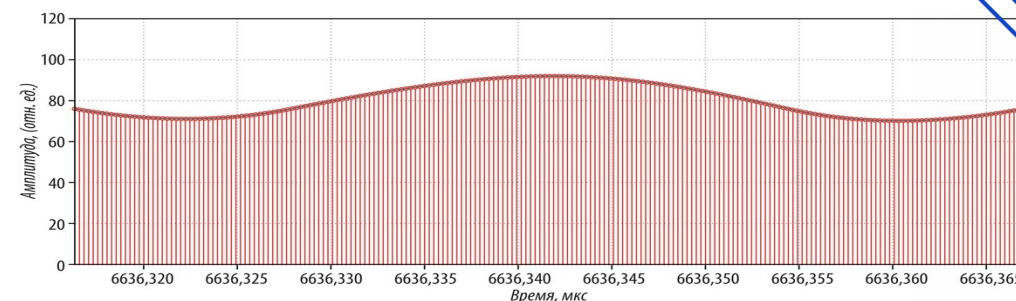


Рис. 1. Дискретизация аналогового ПЧ-сигнала с частотой $f_{\text{АЦП}} = 4 \text{ ГГц}$

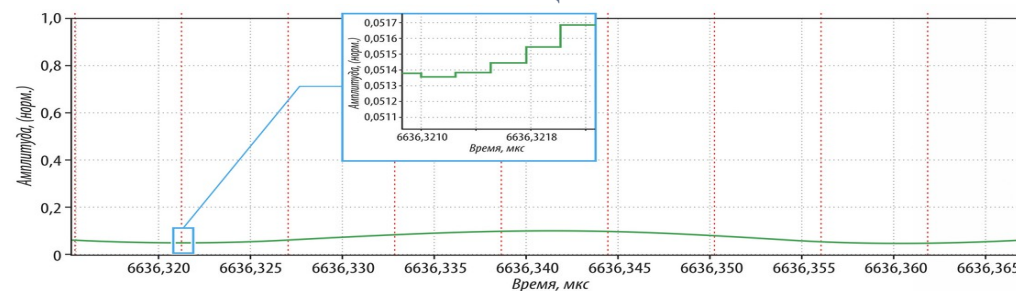


Рис. 2. Нормализованный цифровой видеосигнал

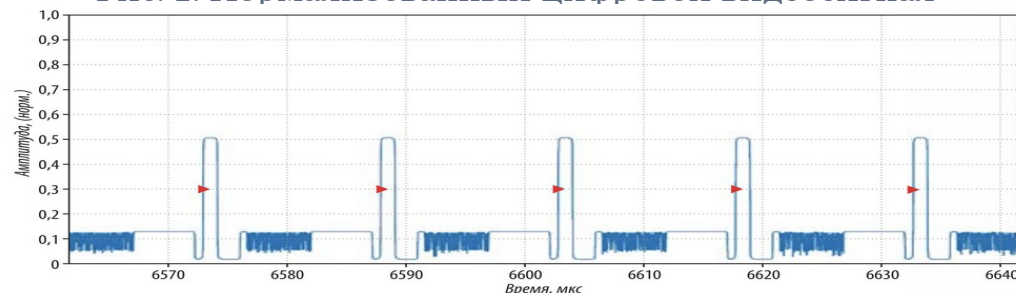


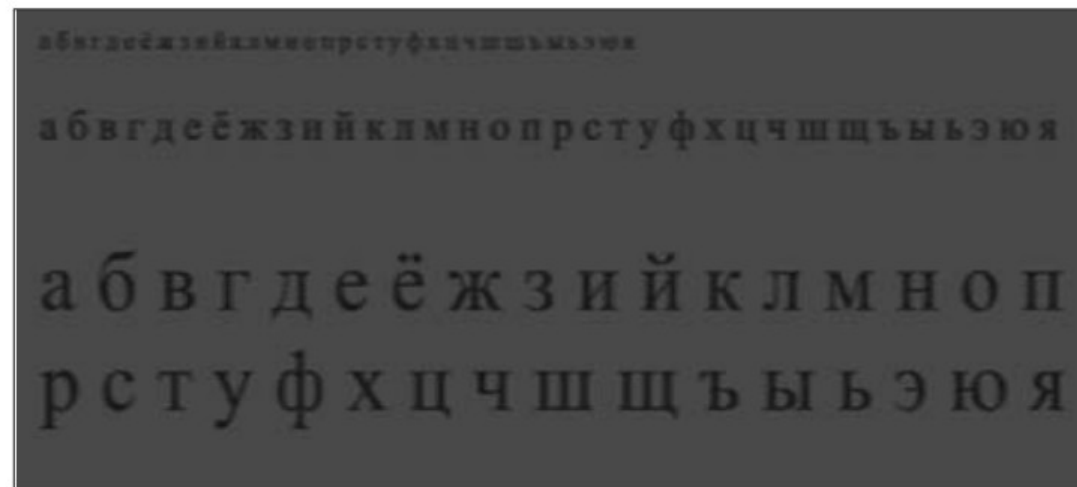
Рис. 3. Нормализованный сигнал: порог детектирования и фронты синхроимпульсов, отмеченные красным

Результат цифровой обработки

До цифровой обработки



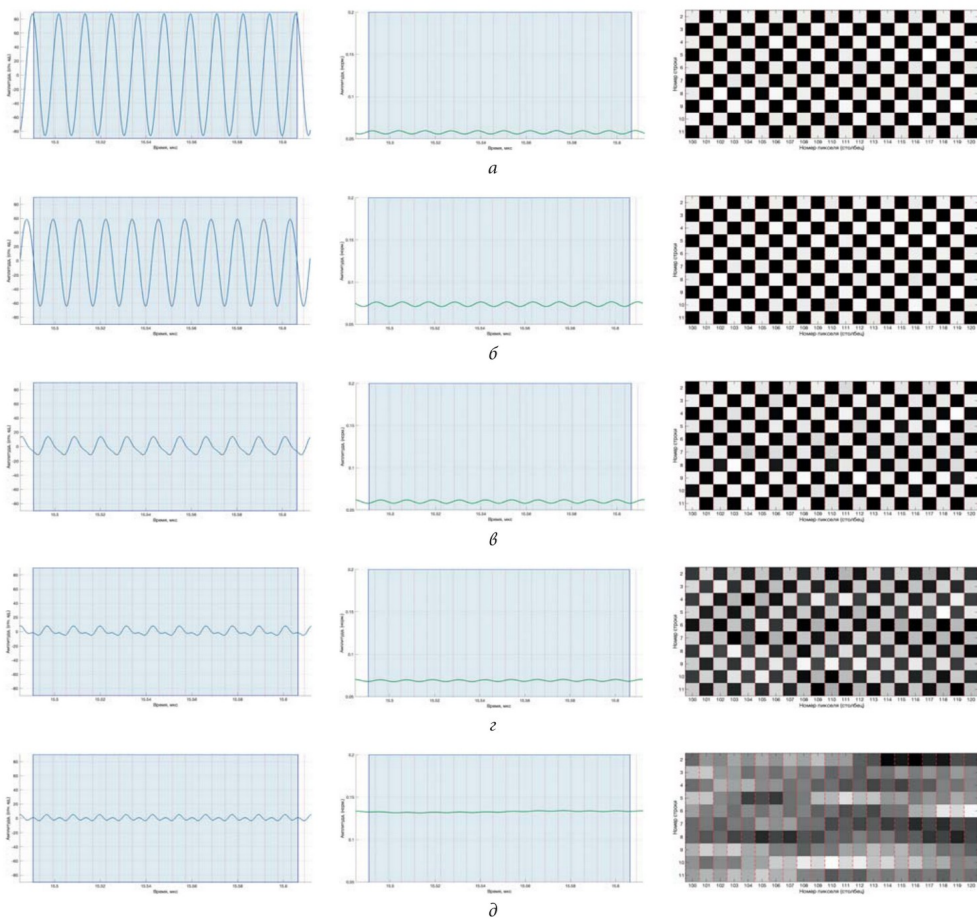
После цифровой обработки



RBW = 40 МГц, расстояние 1 м

Бинаризация и морфологические операции повышают разборчивость восстановленного текстового изображения

Влияние полосы на детализацию



Однопиксельные клетки
паттерна = $f_p/2 = 86,375$ МГц

Сужение полосы
сглаживает фронты

Контраст мелких
деталей снижается

При $RBW \approx 0,23f_p$
структура паттерна
разрушается

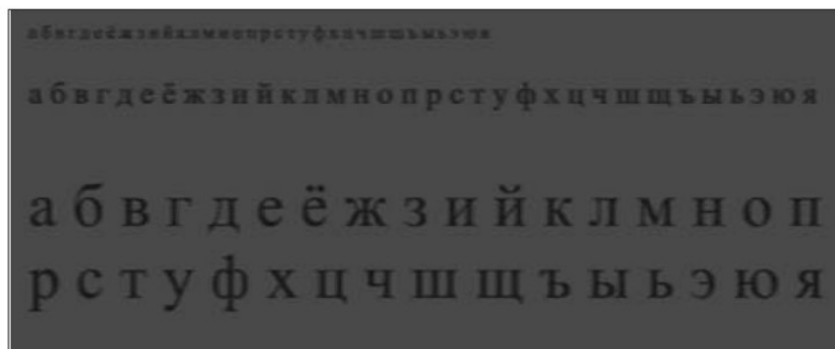
Рис. 1. Результаты экспериментальных исследований влияния полосы пропускания приёмника (RBW) на форму сигнала, сформированного шахматным паттерном.

Для каждой полосы показаны: сигнал на выходе ПЧ-тракта (слева), сигнал на выходе видеодетектора (в центре) и итоговое восстановленное изображение (справа):

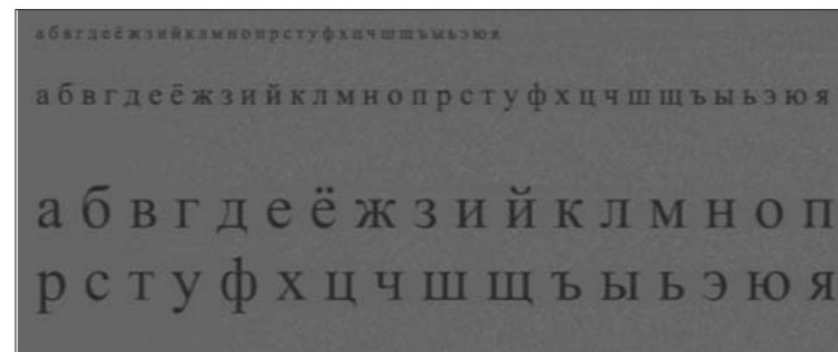
Сверху вниз $RBW = 259; 172,75; 86,375; 60; 40$ МГц

Восстановленный текст при разных RBW

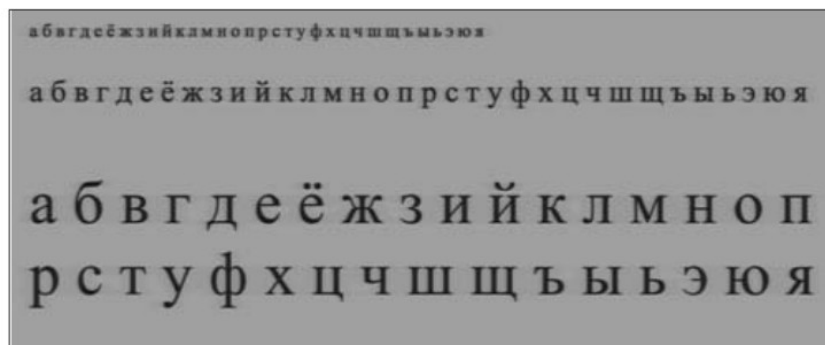
40 МГц $\approx 0,23f_p$



60 МГц $\approx 0,35f_p$



110 МГц $\approx 0,64f_p$



172,75 МГц $= f_p$

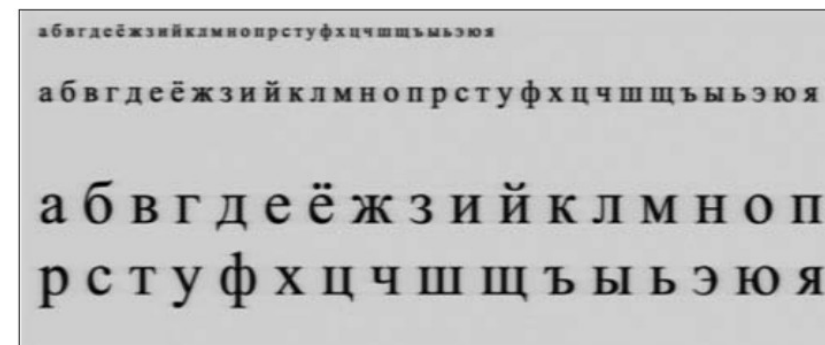


Рис. 1. Фрагменты тестовых изображений . Расстояние 1 м. В каждом фрагменте представлены масштабы 75 %, 125 % и 250 %

Отношение сигнал/шум и полоса приёмника

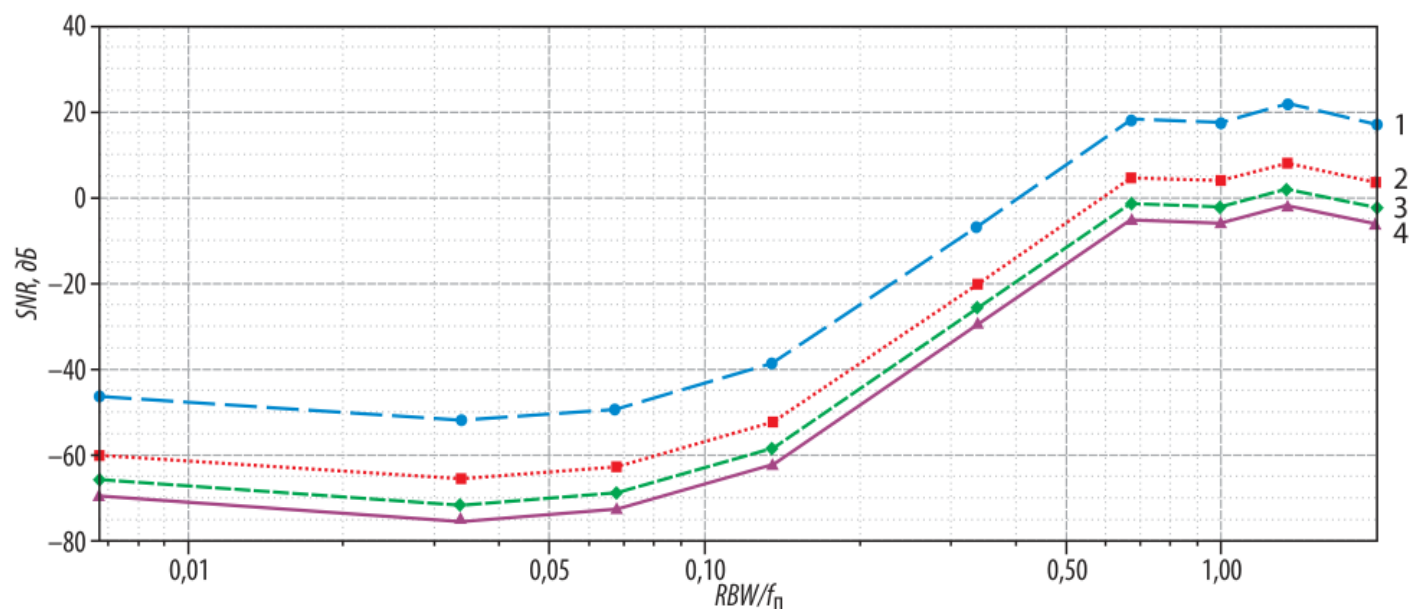


Рис. 1. Зависимость SNR от RBW/f_p для расстояний:
1 — 1 м; 2 — 5 м; 3 — 10 м; 4 — 15 м

$$SNR = 20 \cdot \log_{10} \left(\frac{\bar{U}_{\text{бел}} - \bar{U}_{\text{черн}}}{\sqrt{\frac{\sigma_{\text{бел}}^2 + \sigma_{\text{черн}}^2}{2}}} \right)$$

Оптимальной полосой в модели:
 $RBW \approx 0,7f_p \approx 121 \text{ МГц}$

При $RBW < 0,2f_p$
качество резко снижается

Накопление кадров и время наблюдения

$$\text{SNR}_n = \text{SNR} + 10 \cdot \log_{10} N, \quad N = F_k \cdot T_a$$

$$T_a \geq 10^k / F_k, \quad k = (15 - \text{SNR}) / 10, \quad F_k = 60 \text{ Гц}$$

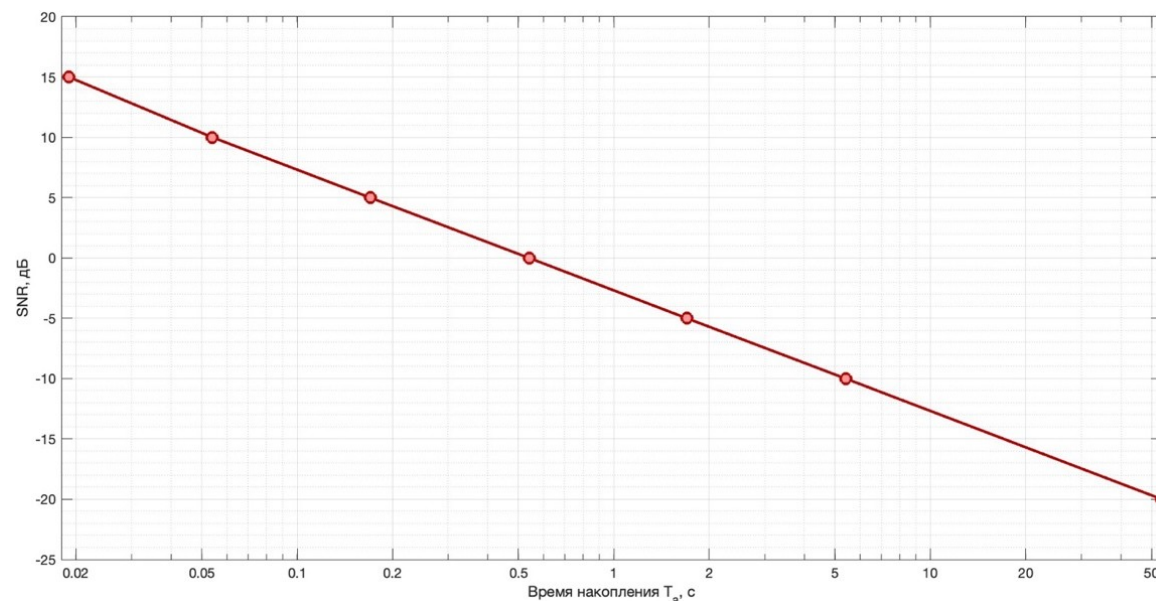


Рис. 1. Минимальное время накопления T_a в зависимости от исходного SNR для распознавания текста с вероятностью, близкой к 100 %

Условия расчёта

Статичное изображение

Усреднение кадров

Целевой $\text{SNR}_n \geq 15$ дБ

Результаты экспериментальных исследований

Модель в Matlab воспроизводит полный тракт перехвата и восстановления текстовых изображений VGA

Показатель / масштаб	RBW относительно f_p	Для $f_p = 172,75$ МГц
Максимум SNR в модели	$\approx 0,7f_p$	≈ 121 МГц
Распознавание, близкое к 100 %	$\geq 0,3f_p$, SNR ≥ 15 дБ	$\geq 51,8$ МГц
75 %, после цифровой обработки	$\approx 0,29f_p$ и выше	≈ 50 МГц и выше
125 % и 250 %, после обработки	$\approx 0,23f_p$ и выше	≈ 40 МГц и выше

Меньший размер букв требует большей полосы

Пороги относятся к тесту Times New Roman 14 пт и условиям исследования

Благодарю за внимание

Лукманова Оксана Равилевна

Старший преподаватель кафедры информационной безопасности
Национальный исследовательский университет
«Московский институт электронной техники» (НИУ МИЭТ)

Доклад на тему:

Имитационное моделирование перехвата побочных
электромагнитных излучений видеосистем с интерфейсом VGA

