электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель Общероссийская общественная организация "Академия инженерных наук им. А.М. Прохорова"
ISSN 2307-0609

 # 01, март 2019

УДК 004.056.53

Исследование возможной модуляции тактовых частот задающих генераторов и вторичных источников электропитания источника бесперебойного питания в магнитном поле при акустическом воздействии

Братко Д. В., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Защита информации»
bdw_@mail.ru

Научный руководитель: Ганчев А.Ю., старший преподаватель
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Защита информации»
al.ganchev@mail.ru

Аннотация: Проводится расчет значения контролируемой зоны, за пределами которой невозможен перехват опасных сигналов, возникающих за счет акустоэлектрических преобразований с учетом заданной модели нарушителя. В данной работе для вычислений используется кубический закон убывания поля. Полученные результаты подтверждаются выполнением критерия защищенности, при котором отношение сигнал/шум не должно превышать единицы. Исследование позволяет защитить информацию от неправомерного доступа к ней, а именно от утечки по побочным электромагнитным излучениям.

Ключевые слова: модуляция (modulation), контролируемая зона (controlled space), побочные электромагнитные излучения и наводки (TEMPEST).

Введение

Цели несанкционированного сбора информации можно объяснить одним понятием – коммерческий интерес. Однако, информация разноценна, а степень ее секретности (конфиденциальности) зависит от лица или группы лиц, кому она принадлежит, а также сферы их деятельности.

К одной из основных угроз безопасности информации ограниченного доступа относится утечка информации по техническим каналам, под которой понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.

Перехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов.

В результате перехвата информации возможно неправомерное ознакомление с информацией или неправомерная запись информации на носитель.

При обработке информации техническими средствами возникают побочные электромагнитные излучения и наводки, перехватив и обработав которые, становится возможным раскрытие обрабатываемой информации без прямого доступа к устройству пользователя.

Впервые теория побочных электромагнитных излучений и наводок была применена в начале 20-го века для исследования методов обнаружения, перехвата и анализа сигналов военных телефонов и радиостанций. Исследования показали, что оборудование имеет различные демаскирующие излучения, которые могут быть использованы для перехвата секретной информации. С этого времени средства радио- и радиотехнической разведки стали непременным реквизитом шпионов различного уровня. По мере развития технологии развивались как средства ПЭМИН-нападения (разведки), так и средства ПЭМИН-защиты.

Теоретическая часть

Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН) возможна по электромагнитным и проводным каналам. К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида ПЭМИН технических средств (ТС):

– излучений элементов ТС;

– излучений на частотах работы высокочастотных генераторов ТС;

– излучений на частотах самовозбуждения усилителей низкой частоты ТС.

В ТС носителем информации является электрический ток и напряжение, параметры которых (амплитуда, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам ТС вокруг них (в окружающем пространстве) возникает электрическое и магнитное поле. В силу этого элементы ТС можно рассматривать как излучатели электромагнитного поля.

В состав ТС могут входить различного рода высокочастотные (ВЧ) генераторы. К таким устройствам можно отнести: задающие генераторы (ЗГ), генераторы тактовой частоты, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д. В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся

электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ-колебаний генераторов. Кроме того, модуляция тактовых частот ЗГ и вторичных источников электропитания (ВИЭП) может происходить за счёт общей цепи питания ЗГ и источника опасного сигнала (ОС). Эти промодулированные ВЧ-колебания излучаются в окружающее пространство.

Самовозбуждение усилителей низкой частоты ТС (например, систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов.

При амплитудной модуляции в соответствии с законом передаваемого сообщения меняется амплитуда модулируемого сигнала.

В качестве тестового аналогового сообщения примем синусоидальный сигнал:

$$U_m(t) = U_m \cos \Omega t. \quad (1)$$

Несущие, то есть модулируемые колебания:

$$u(t) = U_0 \cos w_0 t, \quad (2)$$

где частота несущих колебаний w_0 больше частоты модулирующего колебания Ω.

В результате воздействия колебания (1) на амплитуду несущих колебаний (2) получим сигнал с амплитудной модуляцией:

$$u(t) = U_0(1 + m \cos \Omega t) \cos w_0 t, \quad (3)$$

где $m = {}^{U_m}/_{U_0} \leq 1$ – коэффициент амплитудной модуляции.

Графики трех приведенных колебаний представлены на рисунках 1, 2, 3:

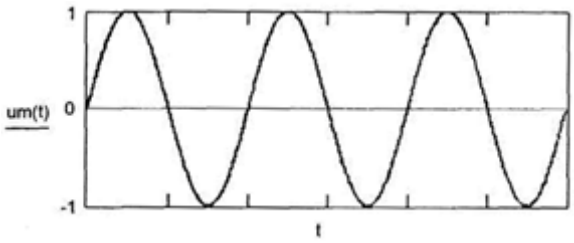

Рис. 1. Тестовый синусоидальный сигнал

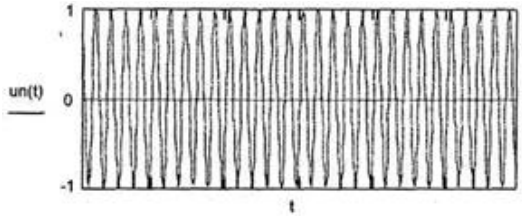

Рис. 2. Модулируемое колебание

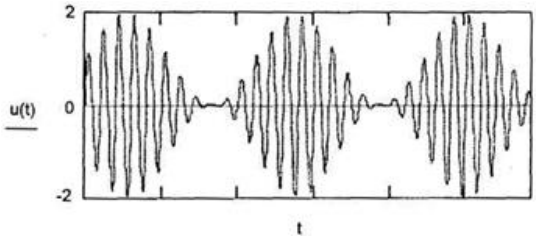

Рис. 3. Сигнал с амплитудной модуляцией

Из формулы (3) получим выражение:

$$u(t) = U_0 \cos w_0 t + U_0 m \cos \Omega t \cos w_0 t, \quad (4)$$

которое в соответствии с формулой для произведения тригонометрических функций приведет к виду:

$$u(t) = U_0 \cos w_0 t + 0{,}5 m U_0 \cos(w_0 - \Omega) t + 0{,}5 m U_0 \cos(w_0 + \Omega) t, \quad (5)$$

из которого следует, что спектр колебания при амплитудной модуляции тональным сигналом состоит из трех составляющих с частотами: w_0 (совпадает с частотой несущей), $(w_0 - \Omega)$ (нижняя боковая), $(w_0 + \Omega)$ (верхняя боковая):

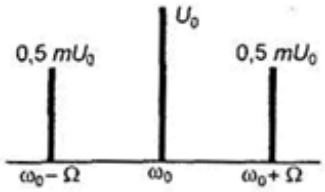

Рис. 4. Спектр колебания при амплитудной модуляции

Модель нарушителя

В рамках проводимых работ и предполагаемой модели нарушителя установлено, что нарушитель нацелен на перехват информации с использованием каналов ПЭМИН, при этом имеет в своем распоряжении приемные технические средства разведки (ТСР) общего назначения (неспециализированные) и не реализующие специализированные методы обработки принимаемых сигналов и восстановления информации. Таким образом, целью нарушителя является перехват откликов сигналов на тактовых частотах ЗГ ТС в магнитной составляющей электромагнитного поля, промодулированных акустическим информационным сигналом, с целью восстановления акустической информации, циркулирующей в помещении, в котором располагается объект исследований.

В качестве нарушителей, осуществляющих перехват обрабатываемой ТС информации с использованием каналов ПЭМИН, рассматриваются только внешние нарушители, осуществляющие атаки из-за пределов контролируемой зоны (КЗ).

Критерий защищенности.

Техническое средство является защищенным, если отношение сигнал/шум меньше или равно 1:

$$S/N \leq 1, \quad (6)$$

при этом для оценки защищенности в качестве шума будет использоваться объектовый шум.

Практическая часть

Оборудование:

1. Источник бесперебойного питания (ИБП) FSP EP1500.
2. Акустический излучатель (экранированная колонка) «Акустик».
3. Анализатор спектра Anritsu MS2712.
4. Цифровой осциллограф BK Precision 2190E.
5. Антенна измерительная рамочная АИР 3-2.

Условия проведения исследований:

– расстояние от ИБП до антенны $d_{\text{ант}} = 0{,}25$ м;

– расстояние от ИБП до акустического излучателя $d_{\text{аи}} = 0{,}03$ м.

Экспериментальная часть.

В данной работе объектом исследования является ИБП.

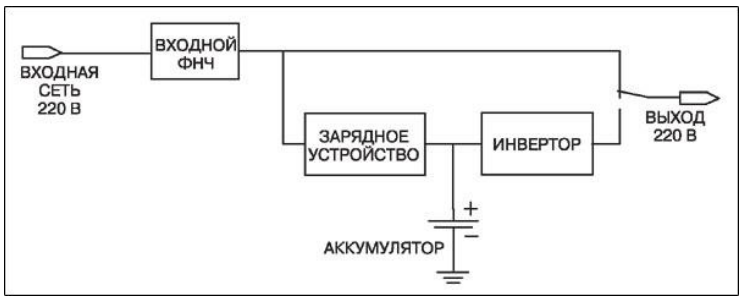

Рис. 5. Обобщенная схема ИБП

При проведении исследования в магнитной составляющей электромагнитного поля обнаружена тактовая частота ЗГ на плате зарядного устройства на частоте $f_т = 20$ кГц.

Далее измерения проводятся на первых десяти гармониках $f_{1…}f_{10} =$ 20кГц…200кГц. При проведении исследования в качестве источника информационного сигнала будет использоваться акустический излучатель с тестовым сигналом синусоидальной формы с частотой $f_{аи} = 1$ кГц. При облучении тестовым сигналом ИБП обнаружен эффект модуляции тактовой частоты тестовым сигналом.

Для исследования временной формы исходного высокочастотного колебания ИБП воспользуемся осциллографом:

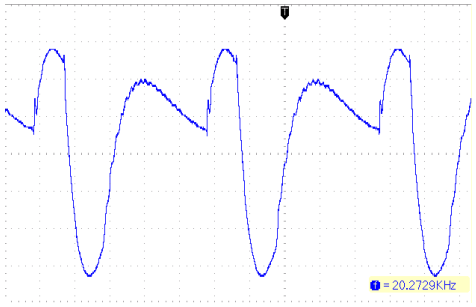

Рис. 6. Представление сигнала во временной форме

На рисунке 6 можно наблюдать последовательность прямоугольных импульсов.

Чтобы обнаружить модуляцию, необходимо представить сигнал в следующем виде:

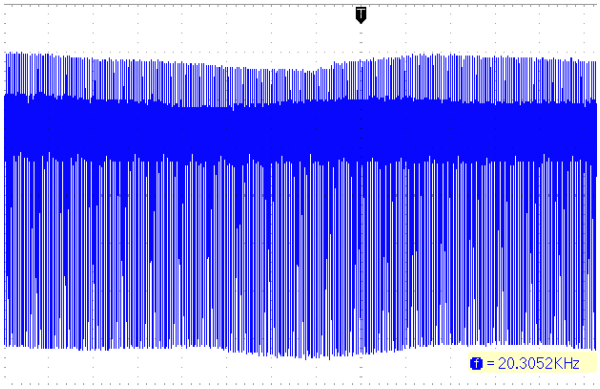

Рис. 7. Высокочастотное колебание ИБП

При включении акустического излучателя наблюдаем амплитудную модуляцию сигнала:

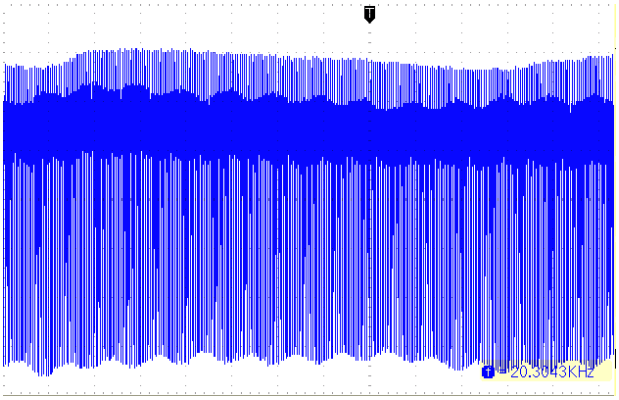

Рис. 8. Промодулированный высокочастотный сигнал ИБП

Для наблюдения модуляции в спектральной области воспользуемся анализатором спектра *Anritsu*.

Производим замер фонового шума:

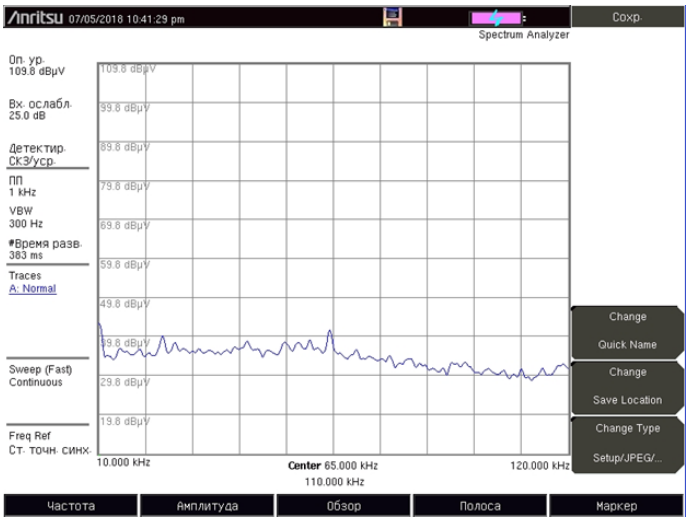

Рисунок 9. Спектр фоновых шумов

Таблица 1

Средний уровень фонового шума на частотах, кратных тактовой частоте ИБП

Характеристика	Значение									
Частота f, кГц	20	40	60	80	100	120	140	160	180	200
Средний уровень фонового шума L, *dBuV*	34,8	35,4	35,3	33,1	35,8	35,1	33,9	33,9	33,0	32,0
Средний уровень фонового шума L_1, мкА/м	8,01	5,61	5,48	4,25	5,8	5,35	4,66	4,66	4,2	3,75

При включении ИБП в сеть электропитания наблюдается набор спектральных составляющих, кратных тактовой частоте ИБП:

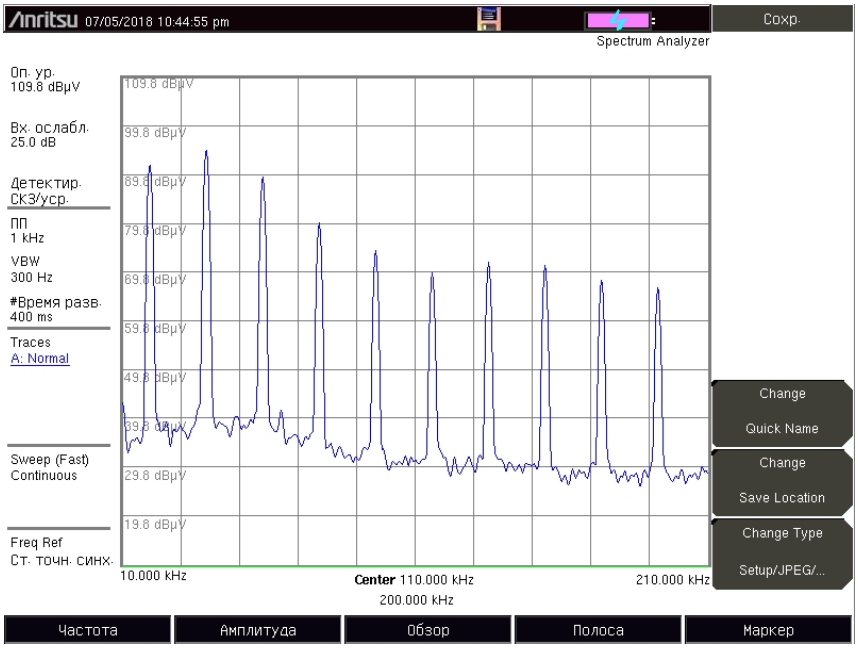

Рис. 10. Спектр отклика тактовой частоты в магнитном поле

Настраиваемся на каждую частоту в заданном частотном диапазоне и фиксируем уровень сигнала с помощью маркера:

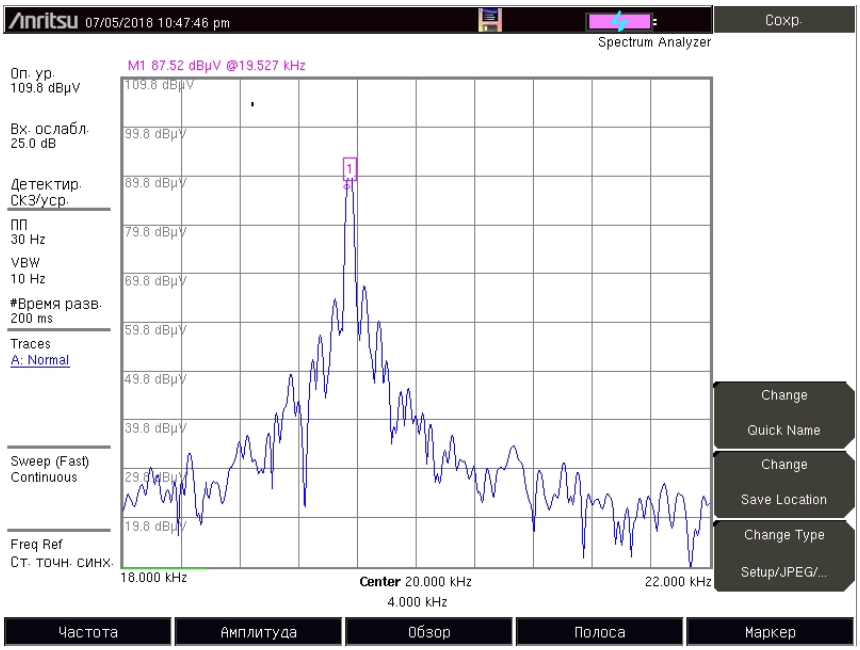

Рис. 11. Спектральная составляющая на частоте 20 кГц

При включении тестового сигнала наблюдается модуляция, а именно появляются боковые составляющие (значение маркера 2, 3), что подтверждается теоретическими данными:

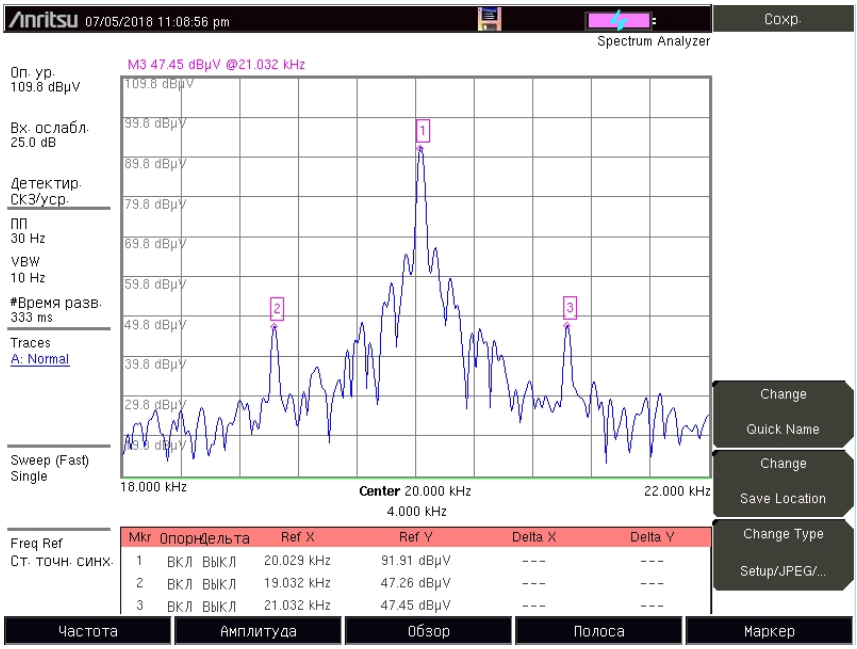

Рис. 12. Спектр при амплитудной модуляции

Далее проводим аналогичные измерения на частотах 40, 60, 80, 100, 120, 140, 160, 180 и 200 кГц. Результаты представлены в таблице 7:

Таблица 2

Уровень основных и боковых спектральных составляющих

Характеристика	Значение									
Частота, кГц	19	**20**	21	39	**40**	41	59	**60**	61	79
Уровень, *dBuV*	47,3	**92**	47,5	50,4	**94,7**	50,8	47,2	**89,1**	45,6	36,1
$H_{ос}$, мкА/м	34,6	**587**	34,6	31,5	**5172,**	33,0	21,6	**2683,**	17,9	6,0

Продолжение табл. 2

Характеристика	Значение									
Частота, кГц	**80**	81	99	**100**	101	119	**120**	121	140	**141**
Уровень, *dBuV*	**79,2**	39,2	35,7	**72,4**	33	43,1	**68,9**	41	40,3	**71,6**
$H_{ос}$, мкА/м	**858,3**	8,6	5,7	**392,3**	4,2	13,4	**262,2**	10,6	9,7	**357,8**

Окончание табл. 2

Характеристика	Значение									
Частота, кГц	142	160	**161**	162	180	**181**	182	200	**201**	202
Уровень, *dBuV*	40,7	36,8	**70,8**	37,3	30,9	**67**	31	31,5	**64,6**	34,4
$H_{ос}$, мкА/м	10,2	6,5	**326,3**	6,9	3,3	**210,7**	3,3	3,5	**159,8**	4,9

Расчет зоны R_2

1. *Доказательство кубической зависимости убывания поля.*

Для определения закона убывания сигнала в электромагнитном поле проведены измерения его уровня на расстояниях $r_1 = 0{,}25$ м, $r_2 = 0{,}4$ м и $r_3 = 0{,}6$ м. Далее проведен сравнительный анализ полученных значений:

Таблица 3

Данные для построения графика убывания поля

Характеристика	Значение		
Расстояние, м	0,25	0,4	0,6
Уровень L, *dBuV*	92,2	82,5	72,2
Уровень L_1, мкА/м	6007,0	1966,3	600,7

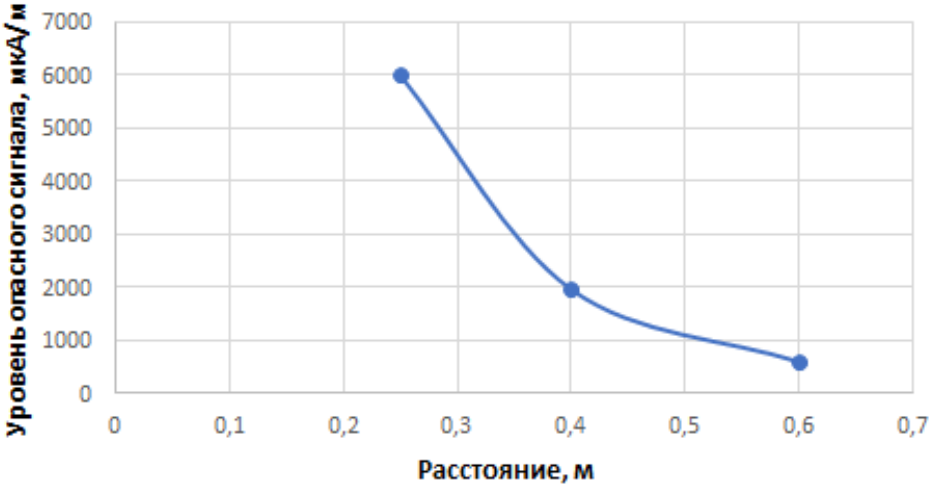

Рис. 13. График зависимости уровня сигнала от расстояния до антенны $d_{\text{ант}}$

Анализ полученных результатов показал, что убывание уровня сигнала происходит по формуле (7) с учетом погрешности измерений:

$$H_2 = H_1 * \left(\frac{d_1}{d_2}\right)^3, \quad (7)$$

где d_1 – расстояние, на котором проводится измерение для точки A_1, [м];

d_2 – расстояние, на котором проводится измерение для точки A_2, [м];

H_1 – уровень измеренного сигнала для точки A_1, [мкА/м];

H_2 – уровень измеренного сигнала для точки A_2, [мкА/м].

2. *Расчет коэффициента модуляции по формуле (8):*

$$m = \frac{2 * U_{\text{бок}}}{U_{\text{нес}}}. \quad (8)$$

Таблица 4

Данные для расчета коэффициента модуляции

Характеристика	Значение									
Частота, кГц	20	40	60	80	100	120	140	160	180	200
Коэффициент модуляции	0,02	0,02	0,02	0,02	0,03	0,08	0,06	0,04	0,04	0,05

3. Оценка защищенности и расчет контролируемой зоны.

Контролируемая зона рассчитывается по кубическому закону убывания поля (формула (9)):

$$R_{\text{кз}} = d_{\text{ант}} * \sqrt[3]{\frac{\text{Н}_{\text{ос}}}{\text{Н}_{\text{шум}}}}, \quad (9)$$

где $d_{\text{ант}}$ – расстояние от ИБП до антенны, [м];

$\text{Н}_{\text{ос}}$ – уровень опасного сигнала, [мкА/м];

$\text{Н}_{\text{шум}}$ – уровень объектового шума, [мкА/м].

Рассчитаем $R_{\text{кз}}$ для каждой частоты:

Таблица 5

Расчет контролируемой зоны

Характеристика	Значение									
Частота, кГц	20	40	60	80	100	120	140	160	180	200
$R_{\text{кз}}$, м	0,41	0,45	0,4	0,29	0,25	0,34	0,32	0,28	0,24	0,25

Таким образом, наибольшее расстояние, с которого нарушитель может перехватить ПЭМИН: $R_{\text{кз}} = 0{,}45$ м на частоте $f = 40$ кГц.

Техническое средство является защищенным, если на границе КЗ выполняется соотношение (6).

В качестве проверки проведем расчет $R_{\text{кз}}$ методом итерационных последовательных приближений, на которых выполняется указанное соотношение. В формуле (7), изменяя d_2, добьемся, чтобы выполнялся критерий защищенности, то есть должно выполняться следующее соотношение:

$$\frac{U_{\text{ос}}}{U_{\text{ш}}} = \delta_{\text{изм}} \leq \delta_{\text{доп}} \quad (10)$$

Таблица 6

Расчет $R_{кз}$ методом итерационных последовательных приближений

Характеристика	Значение					
$R_{кз}$, м	0,25	0,3	0,35	0,4	0,44	0,45
Уровень опасного сигнала $U_{ос}$, мкА/м	31,5	18,2	11,5	7,69	5,78	5,4
Уровень шума $U_{ш}$, мкА/м	5,61	5,61	5,61	5,61	5,61	5,61
$U_{ос} / U_{ш} = \delta_{изм}$	5,61	3,24	2,04	1,37	1,03	0,96

При расчете $\delta_{изм}$ по формулам (7) и (10) получаем $\delta_{изм} = 0{,}96$. Следовательно, критерий защищенности (6) выполняется на расстоянии $R_{кз} = 0{,}45$ м.

Заключение

В ходе проведения исследования было установлено, что расстояние, за пределами которого предполагаемый нарушитель не сможет осуществить перехват информационного акустического сигнала в магнитной составляющей электромагнитного поля, возникающего за счет модуляции тактовой частоты ЗГ на плате зарядного устройства, составляет $R_{кз} = 0{,}45$ м, с учетом измеренных объектовых шумов.

Список использованной литературы

[1]. Петраков. А. В. Утечка и защита информации в телефонных каналах. 6-е изд., доп. - Москва: РадиоСофт, 2014. 415 с.

[2]. Хорев А. А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники // Специальная техника. 2010. №2. С. 39-57.

[3]. Киреева Н. В., Семенов А.В. Утечка информации по каналам ПЭМИ и способы их защиты // Международный журнал прикладных и фундаментальных исследований. 2016. № 8-4. С. 499-504.