

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 621.3: 004.05

DOI: 10.21822/2073-6185-2021-48-3-83-92

Оригинальная статья / Original Paper

Исследование побочных электромагнитных излучений, образующихся при работе устройств с сенсорным вводом информации

Е.А. Рогозин¹, Р.Е. Рогозин², Д.Г.Силка¹, Д.И. Коробкин⁴, М.О. Мещеряков³

¹ Воронежский институт МВД России,

² Воронежский государственный технический университет,

³ МГТУ имени Н.Э. Баумана,

⁴ Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина,

¹394065, г. Воронеж, пр. Патриотов, 53, Россия,

²394006, г. Воронеж, ул. 20 лет Октября, 84, Россия,

³105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1, Россия,

⁴394016, г. Воронеж, ул. Старых Большевиков, 54а, Россия

Резюме: Цель. В целях определения «защищенности» объекта информатизации специального назначения необходимо провести расчёт показателей побочных электромагнитных излучений, образующихся при работе устройств с сенсорным вводом информации, связанных с утечкой информации по техническим каналам. Необходимо разработать перечень действий по нейтрализации потенциальных угроз (включая разработку системы защиты информации для защиты от данного вида угроз). **Метод.** Исследование побочных электромагнитных излучений, образующихся при работе устройств с сенсорным вводом информации проводится с использованием экспертно-документального и инструментального методов. **Результат.** Приведены результаты исследования побочных электромагнитных излучений, образующихся при работе устройств с сенсорным вводом информации и определены аспекты совершенствования специальных мероприятий по защите информации на объекте информатизации специального назначения. **Вывод.** Направление исследования является актуальным и требует дальнейшего развития организационно-технических мероприятий по реализации требований нормативно правовых документов по защите информации.

Ключевые слова: побочные электромагнитные излучения, опасные сигналы, сенсорные экраны, эффективность, утечка защищаемой информации, несанкционированное получение информации, расчёт показателей эффективности

Для цитирования: Е.А. Рогозин, Р.Е. Рогозин, Д.Г. Силка, Д.И.Коробкин, М.О. Мещеряков. Исследование побочных электромагнитных излучений, образующихся при работе устройств с сенсорным вводом информации. Вестник Дагестанского государственного технического университета. Технические науки. 2021; 48 (3): 83-92. DOI:10.21822/2073-6185-2021-48-3-83-92

Investigation of side electromagnetic radiation generated during the operation of devices with sensory input of information

E.A. Rogozin¹, R.E. Rogozin², D.G. Silka¹, D.I. Korobkin⁴, M.O. Meshcheryakov³

¹ Voronezh Institute of the Ministry of Internal Affairs of Russia,

² Voronezh State Technical University,

³ Moscow State Technical University named after N.E. Bauman,

⁴ Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin,

¹394065, Voronezh, 53 Patriot Ave., Russia,

²394006, Voronezh, st. 20 years of October, 84, Russia,

³105005, Moscow, 2nd Baumanskaya st., 5, building 1, Russia,

⁴394016, Voronezh, st. Old Bolsheviks, 54a, Russia

Abstract. Objectives. In order to determine the "security" of a special purpose informatization object, it is necessary to calculate the indicators of side electromagnetic radiation generated during the operation of devices with sensor input of information associated with information leakage through technical channels. It is also necessary to develop a list of actions to neutralize potential threats (including the development of an information protection system to protect against this type of threat). **Method.** The study of side electromagnetic radiation generated during the operation of devices with sensory input of information is carried out using expert documentary and instrumental methods. **Result.** The results of the study of side electromagnetic radiation generated during the operation of devices with sensor input of information are given and aspects of improving special measures for the protection of information at a special purpose informatization object are determined. **Conclusion.** The direction of this study is very relevant and requires further development of organizational and technical measures to implement the requirements of regulatory legal documents for the protection of information.

Keywords: side electromagnetic radiation, dangerous signals, touch screens, efficiency, leakage of protected information, unauthorized obtaining of information, calculation of performance indicators

For citation: E.A. Rogozin, R.E. Rogozin, D.G. Silka, D.I. Korobkin, M.O. Meshcheryakov. Investigation of side electromagnetic radiation generated during the operation of devices with sensory input of information. Herald of Daghestan State Technical University. Technical Sciences. 2021; 48 (3): 83-92. (In Russ.) DOI:10.21822/2073-6185-2021-48-3-83-92

Введение. При работе устройств с сенсорным вводом информации наибольшую опасность для утечки информации представляют экран и различные элементы электросхемы, отвечающие за функционирование устройства [1-4].

От самой сенсорной панели ПЭМИ не образуется, так как она используется в качестве щупа для определения места касания пользователя, а вот элементы электросхемы, отвечающие за определение места касания и за вычисления действий пользователя будут представлять угрозу для данных, обрабатываемых данным устройством [5-9]. Наибольшую опасность утечки информации через ПЭМИН представляют узлы и устройства ПЭВМ, обрабатывающие информацию в последовательном коде [10-12].

Постановка задачи. Необходимо провести расчёт показателей побочных электромагнитных излучений, образующихся при работе устройств с сенсорным вводом информации, связанных с утечкой информации по техническим каналам, а также разработать перечень действий по нейтрализации потенциальных угроз (включая разработку системы защиты информации для защиты от данного вида угроз). Исследованию подлежат: экран; звуковая система контроллер сенсорной панели (табл.1).

Таблица 1. Исследуемые устройства
Table 1. Investigated devices

Устройство Device	Процессор CPU	Диагональ экрана Screen diagonal	Разрешение экрана Screen resolution
SAMSUNG Galaxy Tab A 10.1 (2019) SM-T515N	Восьмиядерный Samsung Exynos 7904	диагональ 10.1 дюйма	1900x1200 пикселей

Методы исследования. Поиск опасных сигналов производился с помощью программно-аппаратного комплекса для проведения специальных исследований на сверхнормативные побочные электромагнитные излучения «NAVIGATOR 7.0» и вручную.

Частотный диапазон измерений. По электрической составляющей электромагнитного поля: 10кГц-150МГц. По магнитной составляющей электромагнитного

поля: 10кГц-25МГц. Методика проведения измерений предусматривает следующие действия:

1. Собрать установку и настроить измерительную аппаратуру (табл.2, рис.1.).
2. Загрузить на исследуемые устройства тест-режимы.
3. Измерить уровень шумов (тест-режим выключен).
4. Включить тест-режим. При превышении уровня сигнала на 3Дб относительно шумов программа выделяет подозрительные сигналы.
5. Далее в экспертном (ручном) режиме происходит поиск и удаление лишних опасных частот.

Таблица 2. Измерительная аппаратура

Table 2. Measuring equipment

№ п/п	Наименования средств измерений и вспомогательного оборудования Names of measuring instruments and auxiliary equipment	Тип Type	Диапазон частот Frequency range
Средства измерений Measuring instruments			
1.	Измерительный приемник Measuring receiver	Анализатор спектра Spectrum analyzer «Agilent 8596E»	100 кГц – 3 ГГц
2.	Комплект измерительных антенн Measuring antenna set	Антенна измерительная дипольная типа Measuring dipole antenna АИ 5-0 с УР-1.6 № 643	9 кГц – 2000 МГц
		Антенна измерительная рамочная типа Measuring loop antenna АИР3-2 с УР-1.6 № 643	9 кГц – 30 МГц
3.	Токоъемник Current collector	ТИ 2-3	9 кГц – 300 МГц
Вспомогательное оборудование Auxiliary equipment			
4.	Ноутбук Notebook	«Toshiba»	-

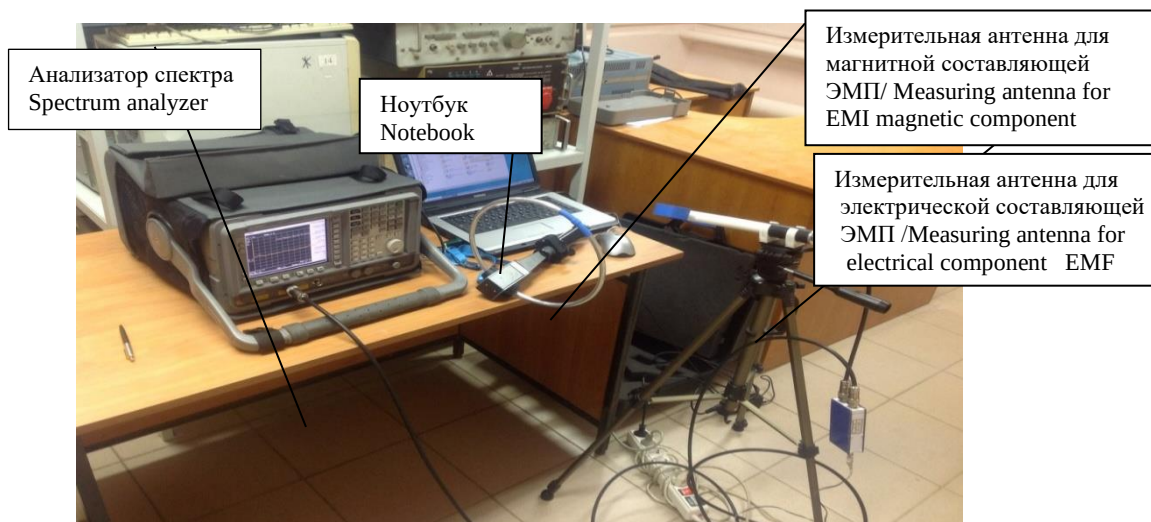


Рис. 1. Измерительное оборудование

Fig. 1. Measuring equipment

Тест режимы устройств. Во время проведения специальных исследований исследуемое устройство работало в авиарежиме (для уменьшения помех, образующихся от Wi-Fi аппаратуры, Bluetooth гарнитуры).

Вывод изображения на экран. Загрузить на исследуемое устройство рисунок, представленный на рис. 2. Рисование. Загрузить на исследуемые устройства программу, подразумевающую работу пользователя с устройством, как при рисовании на экране.

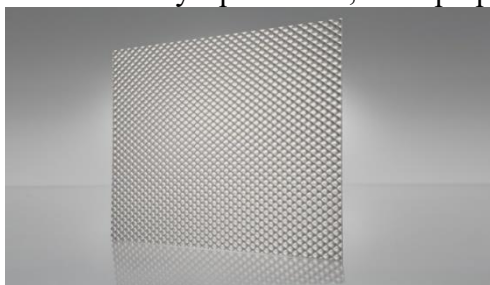


Рис. 2. Вывод изображения на экран

Fig. 2. Displaying an image on the screen

На SAMSUNG Galaxy Tab A 10.1 (2019) SM-T515N включить программу Samsung Notes. На рис. 3 приведено изображение интерфейса программы исследуемого устройства.



Рис. 3. Интерфейс программы исследуемого устройства

Fig. 3. DUT program interface

Касания, происходящие через небольшие промежутки времени. Включить на устройствах виртуальную клавиатуру и набрать текст. Во время проведения исследований все исследуемые устройства работали в авиарежиме. Расчёт зоны R2 проводился для информативных сигналов согласно методике, описанной в литературном источнике [13] для расчета зоны R2. Измерения показали, что невозможно обнаружить опасный сигнал по магнитной составляющей по следующим признакам: пропадание сигнала на экране, уменьшение амплитуды сигнала при выключении устройства. Поэтому расчет проводился только по электрической составляющей ЭМП.

Обсуждение результатов. Вычисляется значение напряженности ЭМП по электрической составляющей E_c , созданной информативным сигналом на частоте f , по формуле

$$E_c = \sqrt{E_{c+ш}^2 - E_{ш}^2} \text{ (мкВ/м)}$$

где $E_{c+ш}$ (мкВ/м) – уровень напряженности ЭМП при работе исследуемого технического устройства, $E_{ш}$ (мкВ/м) – уровень шума (напряженность ЭМП при выключенном исследуемом устройстве).

По формулам

$$L_1 = \frac{150}{\pi \cdot f}$$

$$L_2 = \frac{1800}{f}$$

определяются на частоте f (МГц) границы ближней, промежуточной и дальней зон. По формуле

$$R = \frac{1}{\sqrt[3]{\frac{K \cdot E_{ш}}{E_c}}}$$

где $K = 1$ для ОТСС, не имеющих в своем составе видеомониторов, и $K = 0,3$ для ОТСС, имеющих в своем составе видеомониторы, проверяется, достаточно ли уровня E_c , чтобы информативный сигнал от ОТСС распространился за границу ближней зоны.

При рассчитанном $R < L_1$ R принимается за R_2 .

При $R > L_1$ пересчитываются значение E_c на границу ближней зоны по формуле

$$E_1 = E_c \cdot \left(\frac{R_0}{L_1}\right)^3 \text{ мкВ/м}$$

По формуле

$$R = \frac{L_1}{\sqrt[3]{\frac{K \cdot E_{\text{ш}}}{E_c}}} (\text{м})$$

проверяется, достаточно ли уровня E_1 , чтобы информативный сигнал от ОТСС распространялся за границу промежуточной зоны.

Если $R < L_2$, то информативный сигнал за границу промежуточной зоны не распространяется. В этом случае требуемый радиус контролируемой зоны определяется значением R .

При $R > L_2$ пересчитывается значение E_1 к границе промежуточной и дальней зон- E_2 по формуле

$$E_2 = E_1 \cdot \left(\frac{L_1}{L_2}\right) \text{ мкВ/м}$$

По формуле

$$R = \frac{L_2 \cdot E_2}{K \cdot E_{\text{ш}}} (\text{м})$$

Определяется окончательное значение R_2 для дальней зоны.

Примечание: при условии $L_1 \leq 1$ (м) и $L_2 \leq 1$ (м) в формулах (6) и (8) значения L_1 и L_2 принимаются равными 1 м, а E_1 и E_2 равными E_c ; величина измеряется в Дб относительно 1 мкВ/м, при расчетах используется значение этой величины в мкВ/м.

Перевод выполняется по формуле

$$E = 10^{0,05 \cdot E(\text{Дб})} \text{ мкВ/м}$$

За итоговое значение зоны R_2 принимается наибольшее значение из значений, посчитанных по методике, указанной выше. Режим вывода информации на экран представлен в табл.3, 4.

Таблица 3. Электрическая составляющая ЭМП 0.3 метра от исследуемого устройства

Table 3. Electrical component of EMF 0.3 meters from the investigated device

Частота, МГц	Ес+п, дБмкВ/м	Еп, дБмкВ/м	Ес, мкВ/м	Р, м
0,27	62,35	56,29	1136,80	1,8
0,351	53,69	49,54	379,39	1,6
1,35	47,69	38,64	226,80	2,1
1,863	42,38	38,05	104,48	1,6
2,421	42,53	38,53	103,81	1,6
6,183	43,51	39,21	118,75	1,6
7,524	40,5	37,47	75,07	1,5
7,812	41,8	37,79	95,52	1,6
9,387	38,04	34,97	56,81	1,5
12,645	40,21	32,64	93,05	1,9
12,735	36,68	33,29	50,23	1,5
16,398	43,45	40,32	106,61	1,5
17,379	36,82	33,16	52,33	1,6
17,937	37,2	33,94	52,64	1,5
18,594	36,41	33,11	48,26	1,5
28,251	35,61	32,23	44,36	1,5
Rmax=2,1				

Таблица 4. Электрическая составляющая ЭМП 1 метр от исследуемого устройства
Table 4. Electrical component of EMF 1 meter from the investigated device

Частота, МГц	Ес+п, дБмкВ/м	Еп, дБмкВ/м	Ес, мкВ/м	R, м
0,513	45,49	42,20	137,13	1,5
Rmax=1,5				

Режим ввода информации при помощи сенсорного экрана представлен в табл.5, 6.
Рисование.

Таблица 5. Электрическая составляющая ЭМП 1 метр от исследуемого устройства
Table 5. Electrical component of the EMF 1 meter from the device under test

Частота, МГц	Ес+п, дБмкВ/м	Еп, дБмкВ/м	Ес, мкВ/м	R, м
0,657	44,53	37,67	150,10	1,9
0,954	51,93	45,42	348,025	1,8
1,512	44,89	36,2	163,29	2,0
1,71	40,89	36,19	90,08	1,7
2,421	39,39	36,03	68,42	1,5
2,799	40,78	37,44	80,13	1,5
2,844	41,2	37,85	84,19	1,5
4,959	39,67	35,83	73,76	1,5
Rmax=2,0				

Таблица 6. Электрическая составляющая ЭМП 0.3 метра от исследуемого устройства

Table 6. Electrical component of EMF 0.3 meters from the investigated device

Частота, МГц	Ес+п, дБмкВ/м	Еп, дБмкВ/м	Ес, мкВ/м	R, м
0,198	103,07	49,13	142396,44	11,8
1,35	87,37	38,49	23361,31	9,7
3,222	70,5	44,69	3345,26	4,0
3,618	73,45	43,24	4702,11	4,8
3,798	48,31	42,57	222,92	1,8
4,095	70,79	47,99	3454,29	3,6
4,266	45,15	42,03	129,52	1,5
4,374	61,74	46,45	1203,60	2,7
4,527	64,15	42,23	1607,31	3,5
4,95	63,16	42,58	1432,49	3,3
5,121	66,94	42,66	2219,16	3,8
5,643	67,27	36,66	2308,40	4,8
6,453	49,38	37,39	284,98	2,3
6,669	61,7	38,79	1213,07	3,6
7,65	39,43	35,94	69,60	1,5
8,163	61,54	35,41	1192,53	4,1
8,874	57,16	33,81	719,44	3,7
9,243	57,87	33,27	781,17	3,8
9,576	37,53	33,65	57,84	1,6
9,792	36,27	32,97	47,49	1,5
9,945	62,57	32,86	1343,59	4,7
10,224	43,73	33,17	146,73	2,2
10,539	58,1	33,35	802,18	3,9
10,98	54,69	32,58	540,95	3,5
11,196	52,15	32,78	402,69	3,1
11,25	36,04	32,4	47,75	1,6

продолжение табл. 6				
11,574	54,91	32,21	555,05	3,6
11,718	35,95	32,27	47,42	1,6
11,835	43,59	31,75	146,15	2,3
11,898	36,73	31,92	56,16	1,7
12,348	51,47	33,45	371,58	3,0
12,456	36,32	32,85	48,56	1,5
12,825	37,8	32,34	65,66	1,7
12,906	40,68	32,11	100,35	2,0
13,014	36,2	32,17	50,20	1,6
13,176	52,82	32,48	435,49	3,3
13,383	37,48	32,8	60,76	1,7
13,545	46,4	33,56	203,42	2,4
13,635	35	31,96	39,90	1,5
13,86	48,33	33,12	256,95	2,7
14,22	42,19	32,25	121,98	2,1
14,31	38,19	33,92	64,23	1,6
14,499	38,62	33,11	72,33	1,7
14,535	37,75	33,58	60,63	1,6
14,598	42,83	32,91	131,27	2,1
14,805	50,93	34,37	348,06	2,8
14,967	39,15	34,52	73,42	1,7
18,027	45,99	32,4	194,89	2,5
18,225	37,74	33,5	60,86	1,6
18,297	38,94	34,68	69,98	1,7
18,405	39,28	32,58	81,61	1,9
18,585	41,42	33,03	108,90	2,0
19,242	36,74	31,81	56,60	1,7
19,359	40,26	34,69	87,59	1,8
19,611	42,87	34,13	129,52	2,0
19,8	40,92	35,98	91,63	1,7
19,908	44,08	37,21	159,96	1,9
19,953	40,64	35,8	88,24	1,7
19,989	41,79	35,36	108,01	1,8
20,16	42,52	36,99	113,42	1,7
20,439	45,55	37,56	173,75	2,0
21,042	45,11	37,42	164,05	1,9
22,59	44,87	37,66	157,66	1,9
22,635	41,29	36,58	94,39	1,7
Rmax=11,8				

Ввод информации на сенсорной панели при помощи клавиатуры (табл. 7).

Таблица 7. Электрическая составляющая ЭМП 0.3 метра от исследуемого устройства

Table 7. Electrical component of EMF 0.3 meters from the investigated device

Частота, МГц	Ес+п, дБмкВ/м	Еп, дБмкВ/м	Ес, мкВ/м	R, м
0,198	89,43	50,2	29612,43	6,7
0,954	78,8	53,88	8695,60	3,9
3,231	68,58	44,15	2680,50	3,8
3,492	59,5	43,17	933,01	2,8
3,663	63,02	42,37	1409,69	3,3

продолжение табл. 7				
3,807	47,48	44,04	175,00	1,5
3,987	61,61	42,72	1195,86	3,1
4,086	58,28	48,64	774,51	2,1
4,572	62,45	44,81	1314,40	2,9
4,752	55,43	43,48	571,71	2,3
5,112	61,9	40,13	1240,37	3,4
5,382	51,01	40,57	338,79	2,2
5,643	60,74	37,96	1086,06	3,6
5,805	51,74	39,27	375,27	2,4
6,021	39,6	36,01	71,62	1,6
6,183	61,66	38,42	1207,72	3,6
7,02	53,55	37,12	470,44	2,8
7,092	45,93	37,43	183,41	2,0
7,272	53,93	38,01	490,73	2,7
7,398	46,52	36,65	200,63	2,1
7,533	47,62	36,88	230,07	2,2
7,803	57,28	34,57	729,18	3,6
7,965	51,19	35,01	358,26	2,8
8,163	44,77	35,38	162,91	2,1
8,343	54,74	33,37	543,76	3,4
8,541	49,21	34,08	284,27	2,7
8,874	52,74	33,4	430,98	3,1
9,684	51,02	32,27	353,25	3,1
9,945	41,76	32,61	114,77	2,1
10,215	38,4	33,02	70,10	1,7
10,809	45,67	31,92	187,99	2,5
10,881	36,51	31,87	54,21	1,7
11,025	46,78	33,11	213,53	2,5
11,196	47,93	32,35	245,70	2,7
11,304	35,74	32,58	44,03	1,5
11,394	39,52	31,76	86,34	2,0
11,565	44,93	33,24	170,32	2,3
11,826	44,15	32,66	155,42	2,3
11,961	40,75	32,34	100,85	2,0
12,258	46,56	32,76	208,33	2,5
12,483	35,53	32,06	44,34	1,5
12,645	37,56	31,86	64,55	1,8
12,708	40,55	32,4	98,04	2,0
12,906	38,27	32,51	70,23	1,8
13,068	37,19	33,57	54,41	1,6
13,698	40,89	32,81	101,81	2,0
13,842	38,98	32,84	77,35	1,8
13,986	41,9	32,81	116,53	2,1
14,238	41,95	33,43	116,04	2,0
14,409	39,13	33,05	78,53	1,8
17,847	37,82	32,28	66,05	1,7
19,944	37,44	34,12	54,44	1,5
20,7	39,52	36,11	69,79	1,5
Rmax=6,7				

Исследования показали, что невозможно обнаружить опасный сигнал по магнитной составляющей по следующим признакам: пропадание сигнала на экране, уменьшение амплитуды сигнала при выключении устройства.

Появление опасных сигналов от исследуемого устройства заметно сильнее при работе пользователя с сенсорной панелью, чем при выводе информации на экран (пользователь не работает с сенсорной панелью). Наиболее опасный режим работы представляет рисование на сенсорной панели.

Получены значения зоны R2: антенна расположена на расстоянии 0.3 метра от устройства: зона R2 = 11,8; антенна расположена на расстоянии 1 метра от исследуемого устройства: зона R2 = 2м

Вывод. В ходе проведенных исследований установлено, что большую известность и популярность приобрели резистивные и проекционно-ёмкостные сенсорные экраны. Такие экраны используют большинство производителей мобильных устройств и гаджетов (планшеты, плееры и др.).

В работе проводились измерения ПЭМИН на техническом устройстве с проекционно-ёмкостным сенсорным экраном (SAMSUNG Galaxy Tab A 10.1 (2019) SM-T515N). Измерения показали, что ПЭМИ от данного устройства существуют. Наиболее опасный режим работы устройства - это режим ввода информации с помощью сенсорного экрана, а, именно, рисование.

В ходе исследования рассмотрены принципы работы различных видов устройств с сенсорным вводом информации, изучена структура ЭМИ, а также механизмы образования канала утечки информации за счет ПЭМИ.

Описано образование канала утечки информации за счет ПЭМИН от устройств с сенсорным вводом информации; проведено ознакомление с методикой проведения специальных исследований, получен навык работы с измерительным оборудованием, изучена методика расчета зоны R2.

В ходе выполнения исследования и расчетов, проведенных в работе, получены значения зоны R2: антенна расположена на расстоянии 0.3 метра от устройства: зона R2 = 11,8; антенна расположена на расстоянии 1 метра от исследуемого устройства: зона R2 = 2м.

Библиографический список:

1. Липаев В.В. Системное проектирование программных средств, обеспечивающих безопасность функционирования информационных систем // Информационные технологии. - 2000. - №11. - С. 49-55.
2. Мельников В.В. Основы теории защиты информации в автоматизированных системах // Вопросы защиты информации. -2000. - № 3. -С. 39-49.
3. Технические методы и средства защиты информации / Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров и др. - СПб.: Изд-во «Полигон», 2000.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах. - М.: Логос, ППОЮЛ Егоров Н.А., 2001. - 264 с.
5. Хорев А.А. Защита информации от утечки по техническим каналам. – М.: Гостехкомиссия РФ, 1998. - 320 с.
6. Методы оценки информационной безопасности автоматизированных систем управления критических приложений / В.И. Сумин, О.Ю. Макаров, Ю.Е. Иванкина и др. // Телекоммуникации. - 2001. - № 7. - С. 45-48.
7. Волобуев С.В. О систематизации выявления и анализа каналов утечки. Алгоритм выявления и классификации каналов утечки //Вопросы защиты информации. - 2000. - № 2. - С. 14-19.
8. Расторгуев С.П. Программные методы защиты информации в компьютерных сетях.- М.: Изд-во “Яхтсмен”, 1993. - 188 с.
9. Кобзарь М.Т. Общие критерии оценки безопасности информационной технологии и перспективы их использования // Безопасность информационных технологий . - 1998. - № 1. - С. 22-24.
10. Программирование алгоритмов защиты информации /А.В. Домашев, В.О. Попов, Д.И. Правиков и др. - М.: Нолидж, 2000. - 288 с.

11. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков С.В. Скрыль, И.В. Голубятников «Технические средства и методы защиты информации». Москва, «Машиностроение», 2009. – 24с.
12. Ю. Н. Рагозин «Инженерно-техническая защита информации. Лабораторный практикум» МГИУ 2008. -16с
13. Хорев А.А., Способы и средства защиты информации. Учебное пособие. – М.: МО РФ, 2000. – 316 с.

References:

1. Lipaev V.V. System design of software that ensure the security of information systems functioning. *Information technologies*. 2000; 11: 49-55. (In Russ)
2. Melnikov V.V. Fundamentals of the theory of information security in automated systems [Voprosy zashchity informatsii] *Information security issues*. 2000; 3:39-49. (In Russ)
3. Technical methods and means of information protection / Yu.N. Maximov, V.G. Sonnikov, V.G. Petrov et al. - St. Petersburg: *Polygon Publishing House*, 2000. (In Russ)
4. Zavgorodniy V.I. Comprehensive information protection in computer systems. - М.: Logos, PPOYUL Egorov N.A., 2001; 264. (In Russ)
5. Khorev A.A. Protection of information from leakage through technical channels. - М.: Gostekhkomiissiya RF, 1998; 320. (In Russ)
6. Methods for assessing information security of automated control systems for critical applications / V.I. Sumin, O. Yu. Makarov, Yu.E. Ivankina et al. *Telecommunications*. 2001; 7: 45-48. (In Russ)
7. Volobuev S.V. On the systematization of the identification and analysis of leakage channels. Algorithm for identifying and classifying leakage channels. [Voprosy zashchity informatsii] *Information security issues*. 2000; 2:14-19. (In Russ)
8. Rastorguev S.P. Software methods of information protection in computer networks. - М.: Publishing house "Yachtsman", 1993; 188. (In Russ)
9. Kobzar M.T. General criteria for assessing the security of information technology and the prospects for their use. [Bezopasnost' informatsionnykh tekhnologiy] *Information technology security*. 1998;1: 22-24. (In Russ)
10. Programming algorithms for information protection / A.V. Domashev, V.O. Popov, D.I. Pravikov and others. М.: Knowledge, 2000; 288. (In Russ)
11. A.P. Zaitsev, A.A. Shelupanov, R.V. Meshcheryakov S.V. Skryl, I.V. Golubyatnikov "Technical means and methods of information protection" Ed. A.P. Zaitsev and A.A. Shelupanova, Moscow, [Mashinostroenie] *Mechanical engineering*, 2009; 24. (In Russ)
12. Yu. N. Ragozin "Engineering and technical protection of information. Laboratory workshop "MGIU 2008; 16. (In Russ)
13. Khorev AA, Methods and means of protecting information. Tutorial. - М.: Ministry of Defense of the Russian Federation, 2000; 316. (In Russ)

Сведения об авторах:

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел, e-mail: evgenirogozin@yandex.ru

Рогозин Руслан Евгеньевич, аспирант, e-mail: ruslan-96-01-09@mail.ru.

Коробкин Игорь Дмитриевич, докторант, e-mail: office@main.vsu.ru

Силка Дмитрий Григорьевич, инженер-электроник отдела информационно технического обеспечения учебного процесса, e-mail: sdg.silka@gmail.com

Мещеряков Михаил Олегович, студент кафедры ИУ-10, e-mail: keuvrn12012014@icloud.com

Information about the authors:

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof. of the Department of Automated Information Systems of Internal Affairs Bodies, e-mail: evgenirogozin@uaandekh.ru

Ruslan E. Rogozin, Postgraduate student, e-mail: ruslan-96-01-09@mail.ru.

Igor D. Korobkin, Doctoral student, e-mail: office@main.vsu.ru

Dmitry G. Silka, Electronic engineer of the Department of Information and Technical support of the Educational process, e-mail: sdg.silka@gmail.com

Mikhail O. Meshcheryakov, Student of the Department IU-10, e-mail: keuvrn12012014@icloud.com

Конфликт интересов / Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/ The authors declare no conflict of interest.

Поступила в редакцию/Received 30.07.2021.

Поступила после рецензирования/ Revised 16. 08.2021.

Принята в печать/Accepted for publication 17.08.2021.