DOI: 10.21778/2413-9599-2020-30-4-35-46
УДК 621.391

Методические аспекты представления признаков распознавания угроз безопасности информации в условиях совершенствования технических разведок

С.В. Скрыль[1], С.С. Никулин[2], А.В. Мазин[3], В.И. Спивак[1], В.О. Крылов[1], В.В. Никулина[1]

[1] ФГБОУ ВО «Московский государственный технический университет им. Н.Э. Баумана», Москва, Россия
[2] ФГКОУ ВО «Воронежский институт МВД России», Воронеж, Россия
[3] ФГБОУ ВО «Московский государственный технический университет им. Н.Э. Баумана», Калужский филиал, Калуга, Россия

Постановка проблемы. Полнота характеристики одной из наиболее серьезных на сегодняшний день угроз безопасности информации – ее утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) от средств вычислительной техники (СВТ) определяется не только числом обнаруживаемых признаков утечки, но и рядом других параметров, характеризующих динамику реализации данной угрозы. Установленные закономерности в сценариях действий нарушителей, связанных с применением технических средств разведки (ТСР) для перехвата информативных сигналов ПЭМИН от средств вычислительной техники, позволили сформировать модель всех возможных вариантов применения ТСР для получения конфиденциальной информации, обрабатываемой средств вычислительной техники. Предложенная модель обеспечивает реализацию методических принципов теории распознавания для более полной характеристики угроз утечки информации по каналам побочных электромагнитных излучений и наводок от СВТ в процессе их выявления.
Цель. Разработка методических оснований для представления признаков осуществления нарушителем отдельных функций, связанных с использованием технических средств разведки для перехвата информативных сигналов побочных электромагнитных излучений и наводок от СВТ, в качестве признаков, идентифицирующих наиболее значимые для распознавания и предотвращения такого рода угроз состояния.
Результаты. Приводятся методические решения для идентификации трех значимых для предотвращения угроз состояний, основанные на структуризации функционального представления действий нарушителя по реализации такого рода угроз, а также математические модели для оценки прогнозируемого объема информации, раскрываемой в процессе перехвата информативных сигналов ПЭМИН от средств вычислительной техники, и оценки уровня угрозы безопасности в случае ее перехвата информации.
Практическая значимость. В работе приведены основные варианты работы разработанного в рамках представленной методики комплекса программ распознавания угроз утечки информации по каналам ПЭМИН от средств вычислительной техники.

Ключевые слова: побочные электромагнитные излучения и наводки (ПЭМИН), средства вычислительной техники (СВТ), распознавание угроз утечки информации по каналам ПЭМИН от СВТ

Для цитирования:
Методические аспекты представления признаков распознавания угроз безопасности информации в условиях совершенствования технических разведок / С.В. Скрыль, С.С. Никулин, А.В. Мазин, В.И. Спивак, В.О. Крылов, В.В. Никулина // Радиопромышленность. 2020. Т. 30, № 4. С. 35–46. DOI: 10.21778/2413-9599-2020-30-4-35-46

Methodological aspects of the presentation of information security threats recognition signs in the context of improving technical intelligence

S.V. Skryl[1], S.S. Nikulin[2], A.V. Mazin[3], V.I. Spivak[1], V.O. Krylov[1], V.V. Nikulina[1]

[1] Bauman Moscow State Technical University, Moscow, Russia
[2] Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russia
[3] Bauman Moscow State Technical University, Kaluga branch, Kaluga, Russia

Formulation of the problem. The completeness of the characteristics of one of the most serious threats to the security of information today – its leakage through the transient electromagnetic pulse emanation standard (TEMPEST) from computer equipment (CE) is determined not only by the number of detectable signs of leakage but also by several other parameters characterizing the dynamics of the implementation of such a threat. The established patterns in the scenarios of violators' actions associated with the use of technical reconnaissance equipment (TRQ) to intercept informative TEMPEST signals from computer equipment made it possible to form a model of all possible options for using TRQ to obtain confidential information processed by computer equipment. The proposed model provides the implementation of the methodological principles of the recognition theory for a more complete characterization of threats of information leakage through the channels of spurious electromagnetic radiation and interference from CE in the process of their detection.
Objective. Development of methodological grounds for presenting signs of the violator's implementation of certain functions associated with the use of technical reconnaissance equipment to intercept informative signals of spurious electromagnetic radiation and interference from computer equipment as signs that identify the most significant conditions for the recognition and prevention of such threats.
Results. Methodological solutions for the identification of three states significant for the prevention of threats are given based on the structuring of the functional representation of the intruder's actions to implement such threats. Mathematical models for assessing the predicted amount of information disclosed in the process of intercepting TEMPEST informative signals from computer equipment, and assessing the level of security threats in case of interception of information are also presented.
Practical significance. The paper presents the main options for the operation of a complex of programs for recognizing threats of information leakage through TEMPEST channels from computer equipment developed within the framework of the presented methodology.

Keywords: transient electromagnetic pulse emanation standard (TEMPEST), computer equipment (CE), recognition of threats of information leakage through TEMPEST channels from CE

For citation:
Skryl S.V., Nikulin S.S., Mazin A.V., Spivak V.I., Krylov V.O., Nikulina V.V. Methodological aspects of the presentation of information security threats recognition signs in the context of improving technical intelligence. Radio industry (Russia), 2020, vol. 30, no. 4, pp. 35–46. (In Russian). DOI: 10.21778/2413-9599-2020-30-4-35-46

Введение

Анализ сложившейся на сегодняшний день практики противодействия техническим разведкам позволяет выявить важную особенность, характерную для перехвата информации оперативного характера. Если раньше наибольший объем сведений нарушитель получал в результате перехвата техническими средствами разведки (ТСР) информативных сигналов акустического поля (речевых сигналов) [1—6], то сейчас интенсивное внедрение в практику информационной деятельности систем электронного документооборота (СЭД) привело к тому, что наиболее информационно емкими становятся сведения электронных документов, в которых концентрированно представлена вся информация по интересующим нарушителя вопросам. Учитывая тот факт, что технологической средой СЭД является инфокоммуникационная среда, серьезную угрозу стала представлять утечка информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) от средств вычислительной техники (СВТ).

Технология перехвата информативных сигналов ПЭМИН от средств вычислительной техники начала развиваться с начала 2000-х годов. В это время в США была разработана система перехвата компьютерной информации 4625-COMINT, которая

могла восстанавливать информацию, обрабатываемую средствами вычислительной техники, за счет перехвата ПЭМИН [5]. Система имела 100 каналов памяти, в которых накапливалась и анализировалась перехваченная информация. После обработки перехваченная информация восстанавливалась в том виде, в котором она выводилась на экран дисплея СВТ. Система имела следующие характеристики: диапазон рабочих частот – 25 МГц…2 ГГц, чувствительность приемного устройства – 0,15 мкВ. Существующие в настоящее время средства перехвата ПЭМИН от средств вычислительной техники имеют лучшие характеристики.

Поэтому все более актуальной становится проблема обеспечения защиты информации от утечки по таким каналам [6]. Результатом целенаправленного и системного применения технологий безопасности в этой области стало совершенствование способов выявления каналов утечки информации через ПЭМИН от средств вычислительной техники.

При этом очевидно, что существующий традиционный подход к решению проблемы выявления каналов утечки информации через ПЭМИН, основанный на обнаружении отдельных признаков утечки, не может обеспечить полноту выявления такого рода угроз. Это связано с низкой достоверностью фактов обнаружения, а также со сложностью идентификации трех наиболее важных для такого рода угроз состояний, а именно:

- этапа действий нарушителя;
- прогнозируемого объема информации, раскрываемой в процессе перехвата на момент обнаружения канала;
- текущего уровня угрозы безопасности информации.

Это обусловило анализ направлений совершенствования методов выявления утечки информации по каналам ПЭМИН от средств вычислительной техники как источника угроз нарушения конфиденциальности компьютерной информации для обоснования путей совершенствования способов противодействия такого рода угрозам. Как показывает анализ, одним из таких направлений является использование в механизмах защиты информации компонентов обнаружения угроз нарушения конфиденциальности информации СВТ, построенных на основе теории распознавания [7–9]. Возможность применения методов данной теории основывается на установленных закономерностях [10] в сценариях проведения злоумышленниками противоправных действий по перехвату информации ПЭМИН от средств вычислительной техники, позволяющих создать модель всех возможных действий, осуществляемых с целью получения конфиденциальной информации при помощи технических средств разведки [11, 12]. Подобная модель является основой для реализации алгоритмов распознавания такого рода действий как источника угроз нарушения конфиденциальности информации и оценки уровня данных угроз информационной безопасности на объектах информатизации (ОИ), позволяющих не только выявлять признаки подобных действий, но и предложить способы и средства их идентификации.

Это определяет необходимость разработки методического аппарата, обеспечивающего идентификацию признаков угроз утечки информации по каналам ПЭМИН от средств вычислительной техники. Как показывают результаты исследований, подобная задача может быть решена путем построения моделей распознавания такого рода угроз. В основе этих моделей лежит упорядоченное множество признаков действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники. Упорядочивающими основаниями данного множества служат уровни структуры функционального представления действий нарушителя, а также согласованность функционального представления с математическим представлением соответствующих характеристик. Такая согласованность является предпосылкой идентифицирующего характера такого множества признаков.

Рассмотрим методические аспекты распознавания угроз утечки информации по каналам ПЭМИН от средств вычислительной техники на основе идентифицирующих признаков. С этой целью на множестве A этих признаков определим подмножества первичных признаков и вторичных. К первичным признакам будем относить признаки выполнения нарушителем отдельных функций, связанных с использованием технических средств разведки для перехвата информативных сигналов ПЭМИН, а к вторичным – признаки, полученные на основе первичных в результате их аналитической обработки.

К первичным признакам относятся объективно существующие проявления действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники. Данные признаки являются результатом декомпозиции целевой функции нарушителя [12]. Первый уровень декомпозиции этой функции позволяет идентифицировать этапы действий нарушителя, второй – реализуемые в рамках этапов процедуры использования ТСР, а третий – осуществляемые при этом функции. Именно третий, функциональный уровень позволяет идентифицировать те проявления действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники, которые характерны для осуществляемых функций. В композиционной структуре модели

распознавания угроз утечки информации по каналам ПЭМИН данный уровень является первым уровнем, а признаки осуществления соответствующих функций – первичными. Механизмы фиксации такого рода признаков реализуются как в процессе проведения организационных (оперативно-розыскных), так и организационно-технических (оперативно-технических) мероприятий, а также в процессе реализации мер контроля эффективности защиты информации от утечки по каналам ПЭМИН.

С учетом структурированности представления множества A подмножество $\{a_i^{(1)}\}$ первичных признаков будет составлять первый уровень структуры данного множества, а подмножества $\{a_j^{(2)}\},..., \{a_k^{(L)}\}$ вторичных признаков будут составлять второй и следующие уровни в порядке их возрастания.

Идентификация этапов действий нарушителя по реализации угрозы утечки информации по каналам побочных электромагнитных излучений и наводок от средств вычислительной техники

С целью идентификации этапов действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники определим подмножество $\{a_i^{(1)}\}$ первичных признаков такого рода действий, проиндексировав его элементы в соответствии со структурированным представлением множества A, т. е. представим в виде $\{a_{kji}^{(1)}\}$, где j соответствует процедуре использования определенного режима ТСР, а k – этапу действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники (табл. 1).

Для формирования подмножества $a_{kj}^{(2)}$ признаков выполнения нарушителем определенных процедур реализации режимов использования ТСР воспользуемся функциональным представлением такого рода процедур [11–12]. Пример функциональной модели одной из таких процедур – процедуры измерения параметров сигналов ПЭМИН от средств вычислительной техники параметрически-корреляционным методом, представленной в терминах функциональных диаграмм [13], приводится на рис. 1.

Сформированное на основе функционального представления такого рода процедур подмножество признаков их выполнения приводится в табл. 2.

В соответствии с приводимой в статье моделью действий нарушителя по перехвату ПЭМИН от средств вычислительной техники [11–12] подразумевается, что критерий обнаружения сигнала основывается на разнице уровня смеси перехваченного в направлении ведения разведки сигнала с шумом и уровня шума в точке проведения измерений. Это обусловлено условиями плотной городской застройки, наличия средств вычислительной техники внутри административных и офисных зданий, где помимо обычного фона также присутствуют сигналы, излучаемые в разные промежутки времени типовыми СВТ (на практике наиболее опасными обычно являются сигналы от интерфейсов и кабельных соединений мониторов, сетевого оборудования и периферийных устройств) с частотными характеристиками, схожими или идентичными побочным электромагнитным излучениям объектов информатизации. Данный критерий

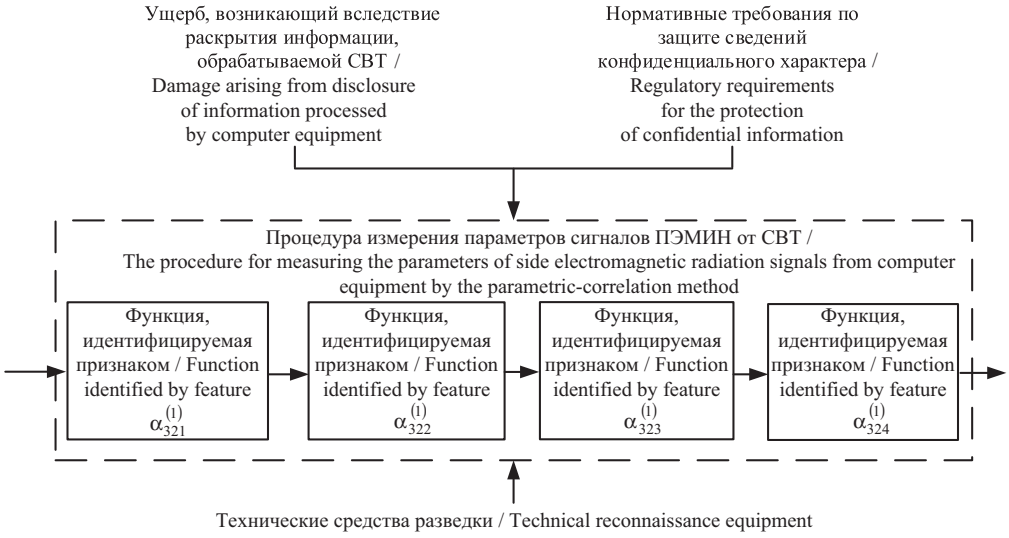

Рисунок 1. Функциональная модель процедуры измерения параметров сигналов побочных электромагнитных излучений от средств вычислительной техники параметрически-корреляционным методом
Figure 1. Functional model of the procedure for measuring the parameters of signals of spurious electromagnetic radiation from computer equipment by the parametric-correlation method

Таблица 1. Идентификации признаков действий нарушителя по перехвату информативных сигналов побочных электромагнитных излучений и наводок от средств вычислительной техники
Table 1. Identification of distinctive features of an intruder's actions to intercept informative TEMPEST signals from computer equipment

№	Обозначение признака / Feature designation	Характеристика признака / Feature characteristic
1	$a_{111}^{(1)}$	Выбор оборудования для ведения технической разведки (ТР) / Selection of equipment for technical intelligence (TE)
2	$a_{112}^{(1)}$	Занесение калибровочных данных используемых антенн / Entering the calibration data of the antennas used
3	$a_{113}^{(1)}$	Занесение нормированных характеристик сигналов ПЭМИН от средств вычислительной техники / Entering the normalized characteristics of the TEMPEST signals from computer equipment
4	$a_{114}^{(1)}$	Формирование задания для оборудования технических средств разведки на поиск сигналов ПЭМИН от средств вычислительной техники / Formation of a task for the technical reconnaissance equipment to search for TEMPEST signals from computer equipment
5	$a_{121}^{(1)}$	Настройка измерительного оборудования технических средств разведки на сигнал ПЭМИН / Setting up the measuring technical reconnaissance equipment for the TEMPEST signal
6	$a_{122}^{(1)}$	Настройка полосы пропускания измерительного оборудования технических средств разведки на сигнал ПЭМИН / Tuning the bandwidth of the measuring equipment of the technical means of reconnaissance for the TEMPEST signal
7	$a_{131}^{(1)}$	Использование оборудования технических средств разведки для выделения информативных сигналов ПЭМИН от средств вычислительной техники путем разнесения направленности сигналов / The use of technical reconnaissance equipment for the selection of informative TEMPEST signals from computer equipment by diversifying the directivity of signals
8	$a_{132}^{(1)}$	Использование оборудования технических средств разведки для выделения информативных сигналов ПЭМИН от средств вычислительной техники методами согласованной фильтрации / The use of technical reconnaissance equipment for the selection of informative signals of TEMPEST from computer equipment by methods of coordinated filtering
9	$a_{133}^{(1)}$	Использование оборудования технических средств разведки для выявления информативных сигналов ПЭМИН от средств вычислительной техники параметрически-корреляционным методом / Use of technical reconnaissance equipment to identify informative signals of TEMPEST from computer equipment by the parametric-correlation method
10	$a_{134}^{(1)}$	Заполнение банка обнаруженных информативных сигналов побочных электромагнитных излучений и наводок результатами радиомониторинга информативных сигналов ПЭМИН от средств вычислительной техники / Filling in the bank of detected informative signals of side electromagnetic radiation and interference with the results of radio monitoring of informative TEMPEST signals from computer equipment
11	$a_{211}^{(1)}$	Перемещение измерительных антенн для выявления максимальной направленности информативных сигналов ПЭМИН /
12	$a_{212}^{(1)}$	Использование оборудования технических средств разведки для определения нормированных параметров затухания информативных сигналов ПЭМИН / Moving measuring antennas to identify the maximum directivity of informative TEMPEST signals
13	$a_{213}^{(1)}$	Использование оборудования технических средств разведки для измерения информативных сигналов ПЭМИН параметрически-корреляционным методом / Use of technical reconnaissance equipment for measuring informative TEMPEST signals by the parametric-correlation method
14	$a_{214}^{(1)}$	Использование оборудования технических средств разведки для определения мест размещения СВТ на объектах информатизации / Use of technical reconnaissance equipment to determine the locations of computer equipment at information system facilities (ISF)
15	$a_{221}^{(1)}$	Настройка оптимального уровня выходных электромагнитных сигналов вспомогательного генератора на частотах сигналов ПЭМИН / Setting the optimal level of the output electromagnetic signals of the auxiliary generator at the TEMPEST signals frequencies
16	$a_{222}^{(1)}$	Измерение уровня электромагнитного поля сигналов вспомогательного генератора на расстоянии, наиболее близком к ОИ / Measurement of the electromagnetic field level of the auxiliary generator signals at a distance closest to the information system facility
17	$a_{223}^{(1)}$	Измерение уровня электромагнитного поля сигналов вспомогательного генератора на наибольшем удалении от ОИ / Measurement of the electromagnetic field level of the auxiliary generator signals at the greatest distance from the information system facility
18	$a_{224}^{(1)}$	Расчет коэффициентов затухания для информативных сигналов ПЭМИН от средств вычислительной техники / Calculation of attenuation coefficients for informative TEMPEST signals from the computer equipment
19	$a_{231}^{(1)}$	Настройка оптимального уровня выходных электрических сигналов вспомогательного генератора на частотах наведенных информативных сигналов / Setting the optimal level of the output electrical signals of the auxiliary generator at the frequencies of the induced informative signals
20	$a_{232}^{(1)}$	Использование оборудования технических средств разведки для измерения уровня мощности электрических сигналов вспомогательного генератора в исследуемых линиях на расстоянии, наиболее близком к ОИ / Use of technical reconnaissance equipment to measure the power level of electrical signals of the auxiliary generator in the lines under investigation at a distance closest to the ISF
21	$a_{233}^{(1)}$	Использование оборудования технических средств разведки для измерения уровня мощности электрических сигналов вспомогательного генератора в исследуемых линиях на наибольшем удалении от ОИ / Use of technical reconnaissance equipment to measure the power level of electrical signals of the auxiliary generator in the lines under study at the greatest distance from the ISF
22	$a_{234}^{(1)}$	Расчет коэффициентов затухания для сигналов, наведенных в цепи питания и заземления СВТ, а так же на линии периферийных устройств и линии связи / Calculation of attenuation coefficients for signals induced in the power and ground circuit of the computer equipment as well as on the line of peripheral devices and communication lines
23	$a_{241}^{(1)}$	Использование оборудования технических средств разведки для определения мест разведдоступности, максимально удаленных от ОИ / Use of technical reconnaissance equipment to determine places of reconnaissance, as far as possible from the ISF
24	$a_{242}^{(1)}$	Выбор мест ведения разведки с наименьшей заметностью / The choice of places for conducting reconnaissance with the least visibility

Таблица 1. (продолжение)
Table 1. (продолжение)

25	$a_{311}^{(1)}$	Использование оборудования технических средств разведки для визуального измерения напряженности электрической составляющей электромагнитного поля информативных сигналов ПЭМИН от средств вычислительной техники на частотах из банка обнаруженных сигналов / Use of equipment of technical means of reconnaissance for visual measurement of the strength of the electrical component of the electromagnetic field of TEMPEST informative signals from the computers at frequencies from the bank of detected signals
26	$a_{312}^{(1)}$	Использование оборудования ТСР для измерения напряженности электрической составляющей шума на частотах из банка обнаруженных сигналов / Use of technical reconnaissance equipment for visual measurement of the strength of the electrical component of the electromagnetic field of informative TEMPEST signals from computer equipment at frequencies from the bank of detected signals
27	$a_{313}^{(1)}$	Использование оборудования технических средств разведки для визуального измерения напряженности магнитной составляющей электромагнитного поля информативных сигналов ПЭМИН от средств вычислительной техники на частотах из банка обнаруженных сигналов / Use of equipment of technical means of reconnaissance for visual measurement of the strength of the magnetic component of the electromagnetic field of TEMPEST informative signals from the computers at frequencies from the bank of detected signals
28	$a_{314}^{(1)}$	Использование оборудования ТСР для измерения напряженности магнитной составляющей шума на частотах из банка ранее обнаруженных сигналов / Use of technical equipment for measuring the intensity of the electrical noise component at frequencies from the bank of detected signals
29	$a_{321}^{(1)}$	Использование оборудования технических средств разведки для измерения напряженности электрической составляющей электромагнитного поля информативных сигналов ПЭМИН от средств вычислительной техники на частотах из банка ранее обнаруженных сигналов параметрически-корреляционным методом / Use of technical reconnaissance equipment for visual measurement of the strength of the magnetic component of the electromagnetic field of informative TEMPEST signals from computer equipment at frequencies from the bank of detected signals
30	$a_{322}^{(1)}$	Использование оборудования ТСР для измерения напряженности электрической составляющей шума на частотах из банка обнаруженных сигналов / Use of TCP equipment for measuring the strength of the magnetic noise component at frequencies from the bank of previously detected signals
31	$a_{323}^{(1)}$	Использование оборудования технических средств разведки для измерения напряженности магнитной составляющей электромагнитного поля информативных сигналов ПЭМИН от средств вычислительной техники на частотах из банка обнаруженных сигналов параметрически-корреляционным методом / Use of technical reconnaissance equipment for measuring the strength of the electric component of the electromagnetic field of informative signals of TEMPEST from computer equipment at frequencies from the bank of previously detected signals by the parametric-correlation method
32	$a_{324}^{(1)}$	Использование оборудования ТСР для измерения напряженности магнитной составляющей шума на частотах из банка обнаруженных сигналов / Use of technical reconnaissance equipment for measuring the intensity of the electrical noise component at frequencies from the bank of detected signals
33	$a_{411}^{(1)}$	Использование оборудования ТСР для визуального измерения напряжения наведенных сигналов на частотах из банка обнаруженных сигналов / Use of technical reconnaissance equipment for visual measurement of induced signals voltage at frequencies from the bank of detected signals
34	$a_{412}^{(1)}$	Использование оборудования технических средств разведки для визуального измерения напряжения шума в линиях, имеющих выход за пределы контролируемой зоны (КЗ) объектов информатизации, на частотах из банка обнаруженных сигналов / Use of technical reconnaissance equipment for visual measurement of noise voltage in lines that go beyond the controlled zone of information system facilities at frequencies from the bank of detected signals
35	$a_{421}^{(1)}$	Использование оборудования технических средств разведки для измерения напряжения сигналов, наведенных в линии, имеющие выход за пределы КЗ объектов информатизации, на частотах из банка обнаруженных сигналов параметрически-корреляционным методом / The use of technical reconnaissance equipment for measuring the voltage of signals induced in the line, which go beyond the controlled zone of information system facilities at frequencies from the bank of detected signals by the parametric-correlation method
36	$a_{422}^{(1)}$	Использование оборудования технических средств разведки для измерения напряжения шума в линиях, имеющих выход за пределы КЗ объектов информатизации, на частотах из банка обнаруженных сигналов параметрически-корреляционным методом / Use of technical reconnaissance equipment for measuring the noise voltage in lines that go beyond the controlled zone of information system facilities at frequencies from the bank of detected signals by the parametric-correlation method
37	$a_{511}^{(1)}$	Использование оборудования технических средств разведки для восстановления исходного вида информации, обрабатываемой средствами вычислительной техники объектов информатизации, на основе перехваченных информативных сигналов ПЭМИН / The use of technical reconnaissance equipment to restore the original type of information processed by information system facilities based on the intercepted informative signals of TEMPEST
38	$a_{512}^{(1)}$	Использование оборудования технических средств разведки для преобразования перехваченной информации ПЭМИН от средств вычислительной техники в удобный для анализа вид, подбор контрастности изображений и удаление избыточной информации / Use of technical reconnaissance equipment for converting the intercepted information of TEMPEST from computer equipment into an easy to analyze form, selection of image contrast and removal of redundant information
39	$a_{513}^{(1)}$	Использование оборудования технических средств разведки для занесения и индексирование информации, обрабатываемой СВТ объектов информатизации, в базу данных перехваченной информации / Use of technical reconnaissance equipment for entering and indexing information processed by technical reconnaissance equipment of the information system facility into the database of intercepted information
40	$a_{521}^{(1)}$	Использование оборудования ТСР для обеспечения работы нарушителя с базой данных перехваченной информации для выбора актуальной информации / The use of technical reconnaissance equipment to ensure the operation of the offender with a database of intercepted information to select relevant information
41	$a_{522}^{(1)}$	Использование оборудования ТСР для работы нарушителя со специальными программами для получения исходных форм сигналов, перехваченных корреляционными методами / The use of technical reconnaissance equipment for the operation of an intruder with special programs to obtain the original waveforms intercepted by correlation methods
42	$a_{531}^{(1)}$	Использование оборудования ТСР для анализа перехваченной информации, обрабатываемой средствами вычислительной техники объектов информатизации, на предмет её достаточности для раскрытия содержания / The use of technical reconnaissance equipment for the analysis of intercepted information processed by computer facilities for its sufficiency for disclosing the content
43	$a_{532}^{(1)}$	Использование оборудования ТСР для анализа раскрытой информации на предмет содержания в ней дезинформации / Using the technical reconnaissance equipment to analyze disclosed information for the content of disinformation in it

Таблица 2. Подмножество признаков и характеристик процедур
Table 2. Subset of features and characteristics of procedures

№	Обозначение признака / Feature designation	Характеристика признака / Feature characteristic
1	$a_{11}^{(2)}$	Настройка оборудования технических средств разведки для поиска сигналов ПЭМИН / Setting up the technical reconnaissance equipment to search for TEMPEST signals
2	$a_{12}^{(2)}$	Обеспечение максимальной чувствительности оборудования ТСР / Ensuring maximum sensitivity of technical reconnaissance equipment
3	$a_{13}^{(2)}$	Выделение информативных сигналов ПЭМИН от средств вычислительной техники / Isolation of informative TEMPEST signals from computer facilities
4	$a_{21}^{(2)}$	Определение местоположения средств вычислительной техники как источников информативных сигналов ПЭМИН / Determination of the location of computer equipment as sources of informative TEMPEST signals
5	$a_{22}^{(2)}$	Определение характеристик затухания сигналов ПЭМИН от средств вычислительной техники / Determination of attenuation characteristics of TEMPEST signals from computer equipment
6	$a_{23}^{(2)}$	Определение характеристик затухания сигналов, наведенных в цепи питания и заземления средств вычислительной техники и линии связи, выходящие за пределы КЗ / Determination of attenuation characteristics of signals induced in the power and ground circuit of computer equipment and communication lines that go beyond the controlled zone
7	$a_{24}^{(2)}$	Определение мест оптимальной разведдоступности сигналов ПЭМИН от средств вычислительной техники / Determination of places of optimal reconnaissance of TEMPEST signals from computer equipment
8	$a_{31}^{(2)}$	Визуальное определение параметров сигналов ПЭМИН / Visual determination of TEMPEST signal parameters
9	$a_{32}^{(2)}$	Измерение параметров сигналов ПЭМИН параметрически-корреляционным методом / Measurement of TEMPEST signal parameters by parametric-correlation method
10	$a_{41}^{(2)}$	Визуальное определение параметров электрических сигналов, наведенных в цепи питания и заземления средств вычислительной техники и линии связи, выходящие за пределы КЗ / Visual determination of the parameters of electrical signals induced in the power and grounding circuit of computer equipment and communication lines that go beyond the controlled zone
11	$a_{42}^{(2)}$	Измерение электрических сигналов, наведенных в цепи питания и заземления средств вычислительной техники и линии связи, выходящие за пределы КЗ, параметрически-корреляционным методом / Measurement of electrical signals induced in the power and ground circuits of computer equipment and communication lines that go beyond the controlled zone using the parametric-correlation method
12	$a_{51}^{(2)}$	Преобразование данных, перехваченных по каналам ПЭМИН от средств вычислительной техники / Conversion of data intercepted via TEMPEST channels from computer equipment
13	$a_{52}^{(2)}$	Работа с базой перехваченной информации / Working with the base of intercepted information
14	$a_{53}^{(2)}$	Анализ достаточности информации, перехваченной по каналам ПЭМИН от средств вычислительной техники, для раскрытия ее содержания / Analysis of the sufficiency of information intercepted through TEMPEST channels from computer equipment for disclosing its content

проверяется в рамках режима $a_{51}^{(2)}$ использования оборудования ТСР на основе результатов выполняемых нарушителем функций, идентифицируемых признаками $a_{311}^{(1)}$, $a_{312}^{(1)}$, $a_{313}^{(1)}$, $a_{314}^{(1)}$, $a_{321}^{(1)}$, $a_{322}^{(1)}$, $a_{323}^{(1)}$, $a_{324}^{(1)}$, $a_{412}^{(1)}$, $a_{422}^{(1)}$. Указанные признаки, относящиеся к действиям нарушителя по использованию оборудования ТСР для измерения параметров электромагнитного шума в выбранной точке ведения разведки, соответствуют процедуре $a_{24}^{(2)}$ и характеризуют методику измерения сигналов в реальных условиях.

Для формирования подмножества $a_{k}^{(3)}$ признаков этапов действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники воспользуемся функциональным представлением такого рода этапов [11–12]. В качестве примера на рис. 2 приведена функциональная модель этапа измерения параметров сигналов ПЭМИН, реализация которого связана с выполнением процедуры, функциональная модель которой приводится на рис. 2.

Сформированное на основе функционального представления этапов действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники подмножество признаков их выполнения приводится в табл. 3.

С учетом изложенного, возможности по идентификации этапов действий нарушителя по реализации угрозы утечки информации по каналам ПЭМИН от средств вычислительной техники проиллюстрируем на примере оценки возможности распознавания его действий на этапе измерения параметров информативных сигналов ПЭМИН от средств вычислительной техники (табл. 4).

В качестве критерия успешности идентификации признака $a_{kj}^{(2)}$ выполнения нарушителем соответствующей процедуры определим условие:

$$g_{kj} \geq \varepsilon_{kj}, \quad (1)$$

где g_{kj} – текущее значение числа идентифицированных первичных признаков, позволяющих идентифицировать признак $a_{kj}^{(2)}$; ε_{kj} – предельное

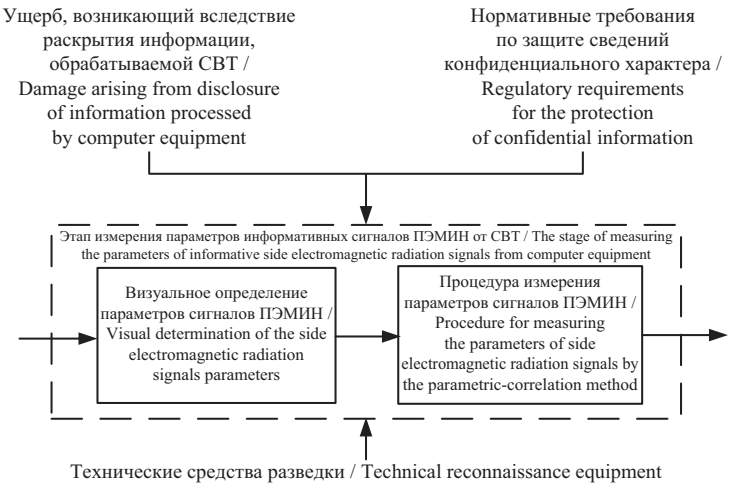

Рисунок 2. Функциональная модель процедуры измерения параметров информационных сигналов побочных электромагнитных излучений и наводок от средств вычислительной техники
Figure 2. Functional model of the procedure for measuring the parameters of information signals of side electromagnetic radiation and interference from computer technology

Таблица 3. Подмножество признаков по перехвату информативных сигналов пэмин от средств вычислительной техники
Table 3. A subset of features for intercepting informative TEMPEST signals from computer equipment

№	Обозначение признака / Feature designation	Характеристика признака / Feature characteristic
1	$a_1^{(3)}$	Поиск сигналов ПЭМИН / Search for TEMPEST signals
2	$a_2^{(3)}$	Поиск мест разведдоступности сигналов ПЭМИН / Search for places of TEMPEST signals reconnaissance
3	$a_3^{(3)}$	Измерение параметров информативных сигналов ПЭМИН от средств вычислительной техники / Measurement of parameters of informative TEMPEST signals from computer facilities
4	$a_4^{(3)}$	Измерение параметров наведенных электрических сигналов, наведенных в цепи питания и заземления средств вычислительной техники и линии связи, выходящие за пределы КЗ / Measurement of parameters of induced electrical signals induced in the power and ground circuits of computer equipment and communication lines that go beyond the controlled zone
5	$a_5^{(3)}$	Анализ количества перехваченной информации по критерию достаточности для ее раскрытия / Analysis of the amount of intercepted information according to the criterion of sufficiency for its disclosure

значение числа идентифицированных первичных признаков, позволяющее идентифицировать признак $a_{kj}^{(2)}$.

Аналогичным образом в качестве критерия идентифицированности признака $a_k^{(3)}$ реализации нарушителем соответствующего этапа определим условие:

$$h_k \geq \delta_k, \quad (2)$$

где h_k – текущее значение числа идентифицированных признаков выполнения нарушителем процедур работы с ТСР, позволяющих идентифицировать признак $a_k^{(3)}$ выполнения соответствующего этапа; δ_k – предельное значение числа идентифицированных признаков выполнения нарушителем процедур работы с ТСР, позволяющее идентифицировать признак $a_k^{(3)}$.

Прогнозируемый объем информации, раскрываемой в процессе перехвата информативных сигналов побочных электромагнитных излучений и наводок от средств вычислительной техники

Оценим прогнозируемый объем информации, раскрываемой в процессе реализации нарушителем функций процедуры измерения параметров сигналов ПЭМИН от средств вычислительной техники параметрически-корреляционным методом, функциональная модель которой приведена на рис. 1.

С этой целью на множестве $\{\Phi_{kji}\}$ функций, идентифицируемых первичными признаками действий нарушителя по перехвату информативных сигналов ПЭМИН от средств вычислительной техники, определим функции, соответствующие

Таблица 4. Таблица идентификации признаков этапа измерение параметров информативных сигналов побочных электромагнитных излучений и наводок от средств вычислительной техники
Table 4. Features identification table for the stage of measurement of parameters of informative signals side electromagnetic radiation and interference from computer equipment

Признак $a_3^{(3)}$ идентифицирующий выполнение этапа / Feature $a_3^{(3)}$ that identifies the completion of the stage							
Признаки, идентифицирующие выполнение процедур этапа / Features identifying the execution of stage procedures							
$a_{31}^{(2)}$				$a^{32(2)}$			
Первичные идентифицирующие признаки / Primary identifying features							
$a_{311}^{(1)}$	$a_{312}^{(1)}$	$a_{313}^{(1)}$	$a_{314}^{(1)}$	$a_{321}^{(1)}$	$a_{322}^{(1)}$	$a_{323}^{(1)}$	$a_{324}^{(1)}$

представленной на рис. 1 функциональной модели: Φ_{321} – измерение напряженности электрической составляющей электромагнитного поля на частотах обнаруженных информативных сигналов ПЭМИН от средств вычислительной техники параметрически-корреляционным методом; Φ_{322} – измерение напряженности электрической составляющей шума на частотах обнаруженных сигналов; Φ_{323} – измерение напряженности магнитной составляющей электромагнитного поля на частотах обнаруженных информативных сигналов ПЭМИН от средств вычислительной техники параметрически-корреляционным методом; Φ_{324} – измерение напряженности магнитной составляющей шума на частотах обнаруженных сигналов.

Оценим прогнозируемый объем v информации, раскрываемой в процессе перехвата информативных сигналов ПЭМИН от средств вычислительной техники, с помощью выражения

$$v = \gamma\tau, \tag{3}$$

где τ – продолжительность перехвата; γ – количество информации, перехватываемое в единицу времени.

Таким образом, прогнозируемый объем v информации, раскрываемой в процессе перехвата информативных сигналов ПЭМИН от средств вычислительной техники, может быть оценен с помощью следующих выражений:

1) при идентификации функции Φ_{321} выражением:

$$v_{321} = \gamma\omega_{321}, \tag{4}$$

где ω_{321} – среднее значение случайной величины времени реализации функции Φ_{321};

2) при идентификации последовательности, состоящей из функций Φ_{321} и Φ_{322}, выражением

$$v_{321,322} = \gamma\ (\omega_{321} + \omega_{322}), \tag{5}$$

где ω_{322} – среднее значение случайной величины времени реализации функции Φ_{322};

3) при идентификации последовательности, состоящей из функций Φ_{321}, Φ_{322} и Φ_{323}, выражением

$$v_{321,\,322,\,323} = \gamma\ (\omega_{321} + \omega_{322} + \omega_{323}), \tag{6}$$

где w_{323} – среднее значение случайной величины времени реализации функции Φ_{323};

4) при идентификации всей процедуры измерения параметров сигналов ПЭМИН от средств вычислительной техники параметрически-корреляционным методом выражением

$$v_{32} = \gamma(\omega_{321} + \omega_{322} + \omega_{323} + \omega_{324}), \tag{7}$$

где ω_{324} – среднее значение случайной величины времени реализации функции Φ_{324}.

Оценка уровня угрозы безопасности информации, обусловленной ее утечкой по каналам побочных электромагнитных излучений и наводок от средств вычислительной техники

Уровень U угрозы безопасности информации, обусловленной ее утечкой по каналам ПЭМИН от средств вычислительной техники, оценивается при помощи математической модели своевременности S реагирования на такого рода угрозу [14]:

$$S = \frac{1}{2}\left[\begin{array}{l} e^{\frac{1}{2}\lambda(2\bar{\tau}_{(y)}+\sigma^2\lambda-2\bar{\tau}_{(p)}-\bar{\tau}_{(o)})}\times \\ \times\left(1-erf\left(\dfrac{\bar{\tau}_{(y)}+\sigma^2\lambda-\bar{\tau}_{(p)}-\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right)\right)+ \\ +erf\left(\dfrac{\bar{\tau}_{(y)}-\bar{\tau}_{(p)}-\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right)-e^{\frac{1}{2}\lambda(\sigma^2\lambda-\bar{\tau}_{(p)}-\bar{\tau}_{(o)})}\times \\ \times\left(1-erf\left(\dfrac{\sigma^2\lambda-\bar{\tau}_{(p)}-\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right)\right)+erf\left(\dfrac{\bar{\tau}_{(p)}-\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right) \end{array}\right], \tag{8}$$

где $\lambda = \dfrac{1}{T(y)}$; $T_{(y)}$ и $\bar{\tau}_{(y)}$ – периодичность и средняя продолжительность угрозы утечки информации, соответственно; $\bar{\tau}_{(o)}$ – среднее значение времени обнаружения угрозы; $\bar{\tau}_{(p)}$ – среднее значение времени, затрачиваемого на принятие мер по предотвращению утечки; σ – среднеквадратическое отклонение времени обнаружения угрозы.

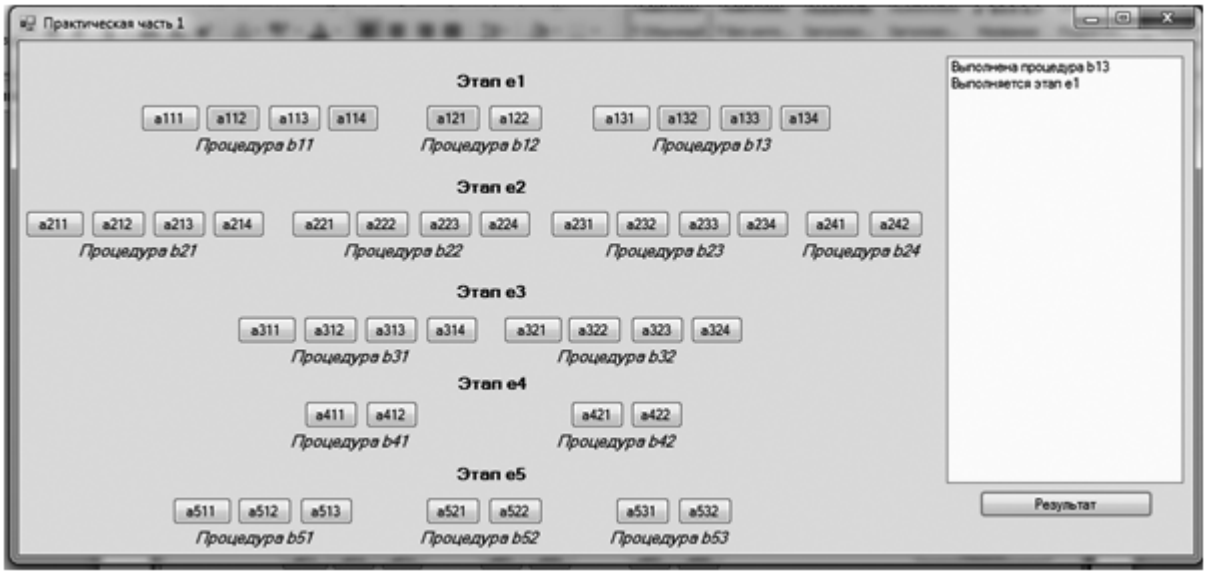

Рисунок 3. Результат распознавания угрозы утечки по каналам побочных электромагнитных излучений и наводок от средств вычислительной техники на ранней стадии ее реализации
Figure 3. The result of recognizing the threat of leakage through the channels of side electromagnetic radiation and interference from computer equipment at an early stage of its implementation

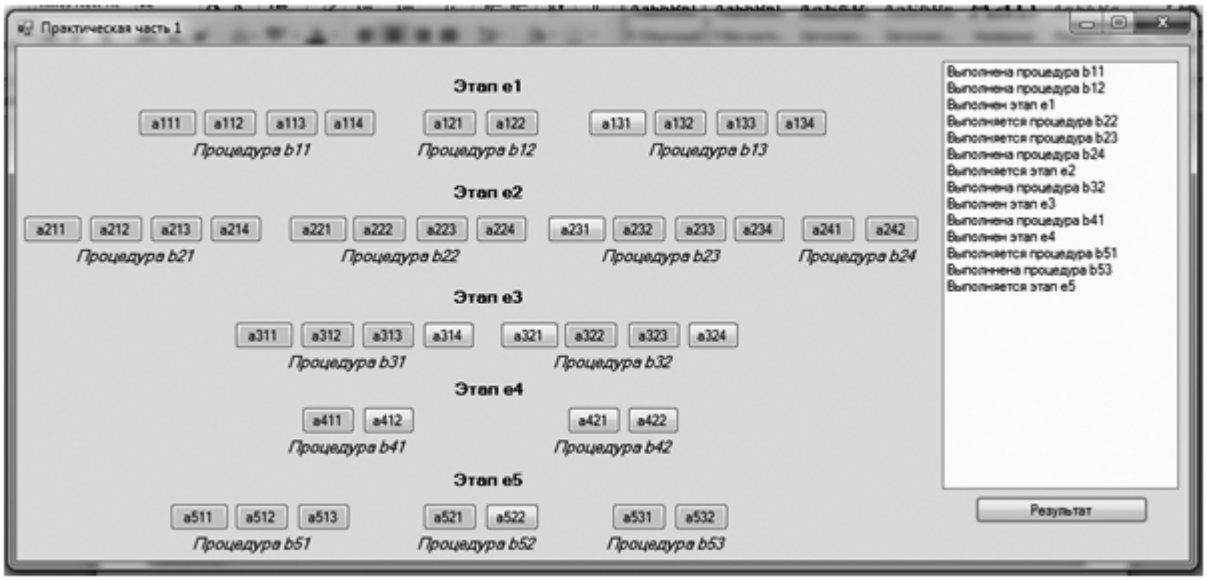

Рисунок 4. Результат распознавания угрозы утечки по каналам побочных электромагнитных излучений и наводок от средств вычислительной техники на завершающей стадии ее реализации
Figure 3. The result of recognizing the threat of leakage through the channels of side electromagnetic radiation and interference from computer equipment at the final stage of its implementation

Исходя из того, что события, связанные с перехватом информативных сигналов ПЭМИН от средств вычислительной техники и реагирование на такого рода угрозы являются случайными событиями, составляющими полную группу, уровень U угрозы безопасности информации, обусловленной ее утечкой по каналам ПЭМИН от средств вычислительной техники определяется в соответствии с выражением:

$$U = 1 - S, \quad (9)$$

где S соответствует (8).

Выводы

Рассмотренные методические положения позволили авторам разработать комплекс программ для распознавания угроз утечки по каналам ПЭМИН

от средств вычислительной техники. Основные варианты работы программы распознавания такого рода угрозы на ранней и завершающей стадиях ее реализации представлены на рис. 3 и 4 соответственно [15].

Таким образом, предложенный методический аппарат распознавания угроз утечки информации по каналам ПЭМИН от средств вычислительной техники позволяет дать более полную информацию о них в случае появления таких угроз.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И.* Методы защиты акустической речевой информации от утечки по техническим каналам: монография. М.: РЦИБ «Факел», 2008. 258 с.
2. *Хорев А.А.* Техническая защита информации. М.: НПЦ «Аналитика», 2008. 436 с.
3. *Меньшаков Ю.К.* Виды и средства иностранных технических разведок. М:. Изд-во МГТУ им. Н.Э. Баумана, 2009. 656 с.
4 *Меньшаков Ю.К.* Теоретические основы технических разведок. М.: ИПЦ «Маска», 2017. 638 с.
5. *Меньшаков Ю.К.* Теоретические основы технических разведок / под ред. Ю.Н. Лаврухина. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 536 с.
6. *Авсентьев А.О.* Комплексность проблематики технической защиты информации как системная основа ее исследования // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сб. материалов Всероссийской научно-практической конференции. Воронеж: Воронежский институт МВД России, 2010. С. 3–4.
7. *Горелик А.Л., Скрипкин В.А.* Методы распознавания. М.: Высшая школа, 1977. 222 с.
8. *Фу К.* Структурные методы в распознавании образов. М.: Мир, 1977. 319 с.
9. *Фукунага К.* Введение в статистическую теорию распознавания образов. М.: Наука, 1979. 368 с.
10. *Никулин С.С., Пономаренко С.А.* Характеристика личности злоумышленника, совершающего противоправные действия в отношении информации с использованием технических средств / Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: материалы Всероссийской научно-практической конференции. Воронеж: Воронежский институт МВД России, 2014. С. 76–78.
11. *Авсентьев О.С., Гомова Н.И.* Функциональная модель перехвата информации по каналам наводок электромагнитных излучений / Охрана. Безопасность. Связь – 2011: материалы международной научно-практической конференции. Часть 1. Воронеж: Воронежский институт МВД России, 2011. С. 70–74.
12. *Скрыль С.В., Никулин С.С., Щербаков А.В., Спивак В.И., Пономарев М.В.* Функциональные аспекты моделирования процесса перехвата информативных сигналов побочных электромагнитных излучений и наводок на объектах информатизации // Телекоммуникации. 2019. № 3. С. 35–41.
13. *Калянов Г.Н.* CASE: Структурный системный анализ (автоматизация и применение). М.: Лори, 1996. 242 с.
14. *Кондаков С.Е., Мещерякова Т.В., Скрыль С.В., Стадник А.Н., Суворов А.А.* Вероятностное представление условий своевременного реагирования на угрозы компьютерных атак // Вопросы кибербезопасности. 2019. № 6 (34). С. 59–68.
15. *Оценка* этапов реализации угрозы утечки информации по каналам побочных электромагнитных излучений и наводок на объектах информатизации / С.С. Никулин, С.В. Скрыль и др. Свидетельство о государственной регистрации программы для ЭВМ от 11.03.2020. № 2020613206, Российская Федерация.

REFERENCES

1. Gerasimenko V.G., Lavrukhin Yu. N., Tupota V.I. *Metody zashchity akusticheskoi rechevoi informatsii ot utechki po tekhnicheskim kanalam: monografiya* [Methods for protecting acoustic speech information from leakage through technical channels: monograph]. Moscow, RTSIB «Fakel» Publ., 2008, 258 p. (In Russian).
2. Khorev A.A. *Tekhnicheskaya zashchita informatsii* [Technical protection of information]. Moscow, SPC «Analytica» Publ., 2008, 436 p. (In Russian).
3. Menshakov Yu.K. *Vidy i sredstva inostrannykh tekhnicheskikh razvedok* [Types and means of foreign technical intelligence]. Moscow, Izdatelstvo MGTU im. N.E. Baumana Publ., 2009, 656 p. (In Russian).
4. Menshakov Yu.K. *Teoreticheskie osnovy tekhnicheskikh razvedok* [Theoretical foundations of technical intelligence]. Moscow, IPTs «Maska» Publ., 2017, 638 p. (In Russian).
5. Menshakov Yu.K. *Teoreticheskie osnovy tekhnicheskikh razvedok* [Theoretical foundations of technical intelligence]. In Yu.N. Lavrukhin ed, Moscow, Izdatelstvo MGTU im. N.E. Baumana Pubi., 2008, 536 p. (In Russian).
6. Avsentiev A.O. Kompleksnost problematiki tekhnicheskoi zashchity informatsii kak sistemnaya osnova ee issledovaniya. *Aktualnye voprosy ekspluatatsii sistem okhrany i zashchishchennykh telekommunikatsionnykh sistem: sbornik materialov Vserossiiskoi nauchno-prakticheskoi konferentsii* [Topical issues of operation of security systems and secure telecommunication systems: collection of materials of the All-Russian scientific-practical conference]. Voronezh, Voronezhskii institut MVD Rossii Publ., 2010, pp. 3–4. (In Russian).
7. Gorelik A.L., Skripkin V.A. *Metody raspoznavaniya* [Recognition methods]. Moscow, Vysshaya shkola Publ., 1977, 222 p. (In Russian).
8. Fu K. *Strukturnye metody v raspoznavanii obrazov* [Structural methods in pattern recognition]. Moscow, Mir Publ., 1977, 319 p. (In Russian).
9. Fukunaga K. *Vvedenie v statisticheskuyu teoriyu raspoznavaniya obrazov* [Introduction to the statistical theory of pattern recognition]. Moscow, Nauka Publ., 1979, 368 p. (In Russian).

10. Nikulin S. S., Ponomarenko S. A. Kharakteristika lichnosti zloumyshlennika, sovershayushchego protivopravnye deistviya v otnoshenii informatsii s ispolzovaniem tekhnicheskikh sredstv / *Prestupnost v sfere informatsionno-telekommunikatsionnykh tekhnologii: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenii: materialy Vserossiiskoi nauchno-prakticheskoi konferentsii* [Crime in the field of information and telecommunication technologies: problems of prevention, disclosure and investigation of crimes: materials of the All-Russian scientific and practical conference]. Voronezh, Voronezhskii institut MVD Rossii Publ., 2014, pp. 76–78. (In Russian).
11. Avsentev O. S., Gomova N. I. Funktsionalnaya model perekhvata informatsii po kanalam navodok elektromagnitnykh izluchenii. *Okhrana. Bezopasnost. Svyaz – 2011: materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii. Chast 1* [Security. Safety. Communication – 2011: materials of the international scientific and practical conference. Part 1]. Voronezh, Voronezhskii institut MVD Rossii Publ., 2011, pp. 70–74. (In Russian).
12. Skryl S. V., Nikulin S. S., Shcherbakov A. V., Spivak V. I., Ponomarev M. V. Functional aspects of interception process simulation of informative signals of e-field radiations and pick-ups at computer entities. *Telekommunikatsii,* 2019, no. 3, pp. 35–41. (In Russian).
13. Kalyanov G. N. *CASE: Strukturnyi sistemnyi analiz (avtomatizatsiya i primenenie)*[CASE: Structural Systems Analysis (Automation and Application)]. Moscow, Lori Publ., 1996, 242 p. (In Russian).
14. Kondakov S. E., Meshcheryakova T. V., Skryl S. V., Stadnik A. N., Suvorov A. A. Probabilistic representations of conditions for timely response to computer attack threats. *Voprosy kiberbezapasnosti,* 2019, no. 6 (34), pp. 59–68. (In Russian).
15. *Otsenka etapov realizatsii ugrozy utechki informatsii po kanalam pobochnykh elektromagnitnykh izluchenii i navodok na obektakh informatizatsii* [Assessment of the stages of the implementation of the threat of information leakage through the channels of spurious electromagnetic radiation and interference at the objects of informatization]. S. S. Nikulin, S. V. Skryl et al. Certificate of state registration of a computer program dated 03.11.2020. No. 2020613206, Russian Federation. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Скрыль Сергей Васильевич, д. т. н., профессор, ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», 105005, Москва, ул. 2-я Бауманская, д. 5, стр. 1, тел.: +7 (960) 125-51-05, e-mail: karel105@mail.ru.

Никулин Сергей Сергеевич, к. т. н., доцент кафедры радиотехники и электроники, ФГКОУ ВО «Воронежский институт Министерства внутренних дел Российской Федерации», 394065, Воронеж, просп. Патриотов, д. 53, тел.: +7 (950) 751-59-42, e-mail: nikcc@mail.ru.

Мазин Анатолий Викторович, д. т. н., профессор, заведующий кафедрой, ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», Калужский филиал, 248000, Калуга, ул. Баженова, д. 2, тел.: +7 (910) 915-58-25, e-mail: mazinav@yandex.ru.

Спивак Вадим Игоревич, аспирант кафедры «Защита информации», ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», 105005, Москва, ул. 2-я Бауманская, д. 5, стр. 1, тел.: +7 (903) 270-32-88, e-mail: vadimspivack@yandex.ru.

Крылов Владислав Олегович, аспирант кафедры «Защита информации», ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», 105005, Москва, ул. 2-я Бауманская, д. 5, стр. 1, тел.: +7 (906) 720-87-25, e-mail: kvo@runsec.ru.

Никулина Валентина Вячеславовна, аспирант кафедры «Защита информации», ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», 105005, Москва, ул. 2-я Бауманская, д. 5, стр. 1, тел.: +7 (905) 747-58-38, e-mail: pretty.nikulina@mail.ru.

AUTHORS

Sergey V. Skryl, D.Sc. (Engineering), professor, Bauman Moscow State Technical University, 5, str. 1, ulitsa 2-ya Baumanskaya, Moscow, 105005, Russia, tel.: +7 (960) 125-51-05, e-mail: karel105@mail.ru.

Sergey S. Nikulin, Ph.D. (Engineering), associate professor of the Department of Radio Engineering and Electronics, Voronezh Institute of the Ministry of Internal Affairs of Russia, 53, prospekt Patriotov, Voronezh, 394065, Russia, tel.: +7 (950) 751-59-42, e-mail: nikcc@mail.ru.

Anatoliy V. Mazin, D.Sc. (Engineering), professor, head of the department, Bauman Moscow State Technical University, Kaluga branch, 2, ulitsa Bazhenova, Kaluga, 248000, Russia, tel.: +7 (910) 915-58-25, e-mail: mazinav@yandex.ru.

Vadim I. Spivak, postgraduate student of the Department of Information Security, Bauman Moscow State Technical University, 5, str. 1, ulitsa 2-ya Baumanskaya, Moscow, 105005, Russia, tel.: +7 (903) 270-32-88, e-mail: vadimspivack@yandex.ru.

Vladislav O. Krylov, postgraduate student of the Department of Information Security, Bauman Moscow State Technical University, 5, str. 1, ulitsa 2-ya Baumanskaya, Moscow, 105005, Russia, tel.: +7 (906) 720-87-25, e-mail: kvo@runsec.ru.

Valentina V. Nikulina, postgraduate student of the the Department of Information Security, Bauman Moscow State Technical University, 5, str. 1, ulitsa 2-ya Baumanskaya, Moscow, 105005, Russia, tel.: +7 (905) 747-58-38, e-mail: pretty.nikulina@mail.ru.

Поступила 29.04.2020; принята к публикации 15.09.2020; опубликована онлайн 04.12.2020
Submitted 29.04.2020; revised 15.09.2020; published online 04.12.2020