ISSN 2413–9599 (Print)
ISSN 2541–870X (Online)

www.radioprom.org

DOI: 10.21778/2413-9599-2021-31-1-74-83
УДК 621.391

Направления развития существующей концепции оценки актуальности угроз утечки информации по техническим каналам в условиях современных тенденций совершенствования технической разведки

С. В. Скрыль[1], М. П. Сычев[1], А. В. Мазин[2], Т. В. Мещерякова[3], О. А. Гуляев[4], И. М. Тегенцев[5]

[1] ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана», Москва, Россия
[2] ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана», Калужский филиал, Калуга, Россия
[3] ФГКОУ ВО «Воронежский институт МВД России», Воронеж, Россия
[4] ПАО «Корпорация Иркут», филиал «Региональные самолеты», Москва, Россия
[5] Центр инженерно-технического обеспечения ФСИН России, Москва, Россия

Постановка проблемы. Обоснование требований к обеспечению конфиденциальности в процессе изготовления и производственных испытаний образцов авиационной техники, возникает необходимость решения задач оценки эффективности мер предотвращения утечки информации по каналам побочных электромагнитных излучений и наводок, и виброакустическим каналам. Эта ситуация характерна как для технологического оборудования предприятий авиапрома, так и для оборудования производимых образцов авиационной техники.

Цель. Обоснование направлений развития существующей концепции оценки актуальности угроз утечки информации по техническим каналам в условиях современных тенденций совершенствования технической разведки.

Результаты. В статье изложены результаты анализа существующей нормативно-существующей базы ФСТЭК России для адекватной оценки мер предотвращения утечки информации по каналам побочных электромагнитных излучений и наводок, и виброакустическим каналам на предприятиях авиапрома в процессе реализации технологий производства и испытания выпускаемой продукции.

Практическая значимость. Обоснованные направления совершенствования методической базы определения актуальных угроз могут быть использованы в рамках разработки методов и моделей адекватной оценки мер предотвращения утечки информации по каналам побочных электромагнитных излучений и наводок, и виброакустическим каналам на предприятиях авиапрома в процессе реализации технологий производства и испытания выпускаемой продукции.

Ключевые слова: техническая разведка, перехват информативных сигналов виброакустического поля, перехват информативных сигналов побочных электромагнитных излучений и наводок (ПЭМИН), оценка актуальных угроз безопасности информации

Для цитирования:
Направления развития существующей концепции оценки актуальности угроз утечки информации по техническим каналам в условиях современных тенденций совершенствования технической разведки / С. В. Скрыль, М. П. Сычев, А. В. Мазин, Т. В. Мещерякова, О. А. Гуляев, И. М. Тегенцев // Радиопромышленность. 2021. Т. 31, № 1. С. 74–83. DOI: 10.21778/2413-9599-2021-31-1-74-83

Directions for the development of the existing concept of assessing the relevance of information leakage through technical channels in the current trends of improving technical intelligence

S. V. Skryl[1], M. P. Sychev[1], A. V. Mazin[2], T. V. Meshcheryakova[3], O. A. Gulyaev[4], I. M. Tegentsev[5]

[1] Bauman Moscow State Technical University, Moscow, Russia
[2] Bauman Moscow State Technical University, Kaluga branch, Kaluga, Russia
[3] Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russia
[4] Corporatcia Irkut PJSC, Regional aircraft branch, Moscow, Russia
[5] The Main Department of the Federal Penitentiary Service of Russia, Moscow, Russia

Problem statement. The rationale for confidentiality requirements in the process of manufacturing and production testing of aviation equipment samples. There is a need to assess the effectiveness of measures to prevent information leakage through the channels of incidental electromagnetic radiation and interference and vibroacoustic channels. This situation is characteristic both for the technological equipment of the aviation industry enterprises and the equipment of the produced aircraft models.

Objective. The rationale for developing the existing concept of assessing the relevance of the threats of information leakage through technical channels in the current trends of improving technical reconnaissance.

Results. The article presents the analysis results of the existing regulatory and existing base of FSTEC Russia for sufficient assessment of measures to prevent information leakage through the channels of incidental electromagnetic radiation and interference and vibroacoustic channels at the enterprises of the aircraft industry in the implementation of production technologies and testing of manufactured products.

Practical implications. The substantiated directions of improving the methodological basis for determining the current threats can be used in the development of methods and models for assessment of measures to prevent information leakage through the channels of electromagnetic emissions and interference and vibroacoustic channels at aircraft industry enterprises in the implementation of production technologies and testing of manufactured products.

Keywords: technical reconnaissance, interception of informative signals of the vibroacoustic field, interception of informative signals of electromagnetic emissions and interference (IEMEI), assessment of current threats to information security

For citation:
Skryl S. V., Sychev M. P., Mazin A. V., Meshcheryakova T. V., Gulyaev O. A., Tegentsev I. M. Directions for the development of the existing concept of assessing the relevance of information leakage through technical channels in the current trends of improving technical intelligence. Radio industry (Russia), 2021:31(1); pp. 74–83. (In Russian). DOI: 10.21778/2413-9599-2021-31-1-74-83

Введение

Анализ ретроспектив технической разведки, как деятельности по добыванию сведений конфиденциального характера, и ее дальнейших перспектив [1–3] позволяет выявить устойчивую тенденцию целенаправленного расширения возможностей технических средств разведки (ТСР) по двум основным направлениям:

- перехват информативных сигналов побочных электромагнитных излучений и наводок (ПЭМИН) от средств вычислительной техники (СВТ);
- перехват информативных сигналов виброакустического поля.

Первое направление связано с интенсивным внедрением в практику информационной деятельности такого класса автоматизированных

информационных систем, как системы электронного документооборота [4]. Обрабатываемые в этих системах электронные документы являются наиболее информационно емкими источниками сведений, в том числе сведений конфиденциального характера, ввиду концентрированного представления в них готовых решений по интересующим нарушителя вопросам. Это приводит к тому, что целостность информации [5] электронных документов, перехватываемой ТСР через ПЭМИН, существенно превышает целостность информации, получаемой в результате перехвата информативных сигналов акустического поля (речевых сигналов) [6; 7].

Кроме того, важным обстоятельством, обусловливающим целенаправленное расширение возможностей ТСР по перехвату информативных сигналов ПЭМИН от СВТ, является постоянно возрастающий интерес производителей высокотехнологичной продукции к технологиям производства такой продукции на конкурирующих предприятиях [8]. В связи с тем что эти технологии являются технологиями с высокой степенью автоматизации и реализованы как на базе СВТ, так и на базе их отдельного класса — микропроцессорной техники [9], перехват информативных сигналов ПЭМИН от технологического оборудования дает возможность получить информацию о технологических решениях, используемых в производственной деятельности.

Таким образом, стоит отметить и то, что радиоэлектронное оборудование той продукции, которая производится на этих предприятиях, базируется на микропроцессорной технике. Возникающие в процессе производства и технологических испытаний этого оборудования ПЭМИН являются источником информации о характеристиках производимой продукции.

СВТ, как источник информативных сигналов ПЭМИН, стал рассматриваться с начала 2000-х годов. В это время в США было разработано одно из первых ТСР, ориентированных на перехват компьютерной информации — система 4625 — *COMINT* [1]. Работая по пятидесяти каналам в диапазоне рабочих частот от 25 МГц до 2 ГГц, с чувствительностью приемного устройства 0,15 мкВ, данная система позволяла восстанавливать перехваченную информацию в том виде, в котором она выводилась на экраны дисплеев СВТ. Дальнейшее развитие данного направления в технической разведке привело к появлению отдельного класса ТСР, ориентированных на перехват компьютерной информации через ПЭМИН.

Анализ проблемы

Аналогичная тенденция совершенствования средств перехвата сигналов виброакустического поля обусловила появление нового ТСР — аппаратуры виброакустической разведки.

Это определяет необходимость решения ряда проблем, связанных с предотвращением утечки информации по виброакустическим каналам и каналам ПЭМИН от СВТ и адекватности соответствующих мер. Пути решения этих проблем предполагают детальное исследование как процессов перехвата информативных сигналов виброакустического поля и информативных сигналов ПЭМИН, так и мер предотвращения утечки с целью адекватной оценки характеристик исследуемых процессов.

Указанные проблемы крайне актуальны для предприятий авиационной промышленности (авиапрома) — традиционного объекта разведдеятельности спецслужб иностранных государств [10] и иностранных производителей авиационной техники, конкурирующими на мировом авиационном рынке с российскими авиастроителями.

Именно информативные сигналы виброакустического поля, возникающего в процессе производства и технологических испытаний двигательных установок; и электромагнитного поля, возникающего в виде ПЭМИН в процессе производства и технологических испытаний радиоэлектронного оборудования, устанавливаемого на образцах производимой авиационной техники, являются наиболее характерными демаскирующими признаками предприятий авиапрома. Кроме того, серьезным демаскирующим признаком являются информативные сигналы ПЭМИН от технологического оборудования, используемого предприятиями в производственном процессе. Указанные физические поля являются источниками информации о технических характеристиках продукции, производимой на предприятиях авиапрома, и используемых при этом технологических решениях.

Это, в свою очередь, позволяет характеризовать каналы утечки информации на предприятиях авиапрома, образуемые вследствие перехвата информативных сигналов виброакустического поля, возникающего в процессе производства и технологических испытаний авиационных двигателей, и электромагнитного поля, возникающего в виде ПЭМИН в процессе производства и технологических испытаний радиоэлектронного оборудования, устанавливаемого на образцах производимой авиационной техники, как технические каналы утечки технологической информации.

Анализ возможных методических подходов к реализации продекларированного выше требования детального исследования виброакустических каналов утечки информации и каналов ПЭМИН на предприятиях авиапрома, а также детальное исследование мер предотвращения утечки информации на этих предприятиях приводят к необходимости учитывать весьма важные для исследования обстоятельства — особенности технологии производства продукции на предприятиях авиапрома, не позволяющие проводить натурные эксперименты по исследованию виброакустических каналов утечки информации и каналов ПЭМИН, а также по исследованию мер предотвращения утечки информации на этих предприятиях. Это связано со значительными временными издержками на проведение таких экспериментов в ущерб технологическому процессу, а также риску демаскирования признаков, позволяющих раскрыть информацию о продукции, производимой на предприятии.

Альтернативой натурным экспериментам по исследованию виброакустических каналов утечки информации и каналов ПЭМИН, а также по исследованию мер предотвращения утечки информации на этих предприятиях, является исследование этих процессов при помощи математических методов [11–13].

Анализ возможностей применяемого на практике методического аппарата оценки угроз утечки информации по техническим каналам дает основание констатировать, что в его основе лежит концепция вероятностной оценки актуальности угроз безопасности информации, положения которой отражены в ряде нормативно-методических документов ФСТЭК России.

Методический аппарат

В основу методики оценки актуальных угроз безопасности информации положена экспертиза обстоятельств, позволяющих отнести факторы, влияющие на защищенность информации, к потенциальным источникам угроз ее безопасности, выявить уязвимости к такого рода угрозам и определить сами угрозы.

Проанализируем возможность применения данного методического аппарата для оценки уровня угрозы утечки конфиденциальной информации через ПЭМИН от СВТ и через информативные сигналы виброакустического поля в ходе реализации технологических процессов на предприятии отечественного авиапрома.

В соответствии с положениями рассматриваемой методики отнесение факторов, влияющих на защищенность технологической информации от утечки по техническим каналам, к потенциальным источникам угроз ее безопасности осуществляется путем экспертной оценки соответствия между такого рода источниками и их признаками. В результате формируется множество $\{x_i\}$, $i = 1, 2, \ldots, I$, элементы которого составляют признаки источников, а индексы — номера источников.

Для рассматриваемого примера:

$i = 1$ — иностранные спецслужбы;

$i = 2$ — иностранные производители авиационной техники;

x_1 — наличие интереса у иностранных спецслужб к образцам боевой авиационной техники, выпускаемой предприятием авиапрома;

x_2 — наличие интереса у иностранных производителей авиационной техники, конкурирующих на мировом авиационном рынке с предприятием авиапрома.

Особенность выявления уязвимостей, через которые возможна реализация угроз утечки технологической информации по техническим каналам на предприятии авиапрома, — использование инструментальных и расчетных методик, позволяющих установить факт потенциальной возможности утечки.

Для установления фактора уязвимости технологической информации предприятия авиапрома к реализации угроз ее утечки по техническим каналам проводится экспертный анализ технологической среды. В результате формируется множество $\{y_j\}$, $j = 1, 2, \ldots, J$, элементы которого составляют факторы уязвимостей, а индексы — их номера.

Для рассматриваемого примера:

y_1 — наличие зданий и сооружений вокруг предприятия.

y_2 — превышение допустимого значения на границе контролируемой зоны (КЗ) уровня собственных побочных электромагнитных излучений (ПЭМИ) от находящегося в производственных помещениях предприятия технологического радиоэлектронного оборудования и работающего радиоэлектронного оборудования;

y_3 — превышение допустимого значения на границе КЗ уровня электромагнитных излучений (ЭМИ) на частотах работы высокочастотных генераторов технологического радиоэлектронного оборудования и работающего радиоэлектронного оборудования образцов производимой продукции;

y_4 — превышение на границе КЗ допустимого уровня ЭМИ на частотах самовозбуждения низкой частоты технологического радиоэлектронного

оборудования и работающего радиоэлектронного оборудования образцов производимой продукции;

y_5 — превышение допустимого уровня наводки ЭМИ ОТСС на соединительных линиях технологического радиоэлектронного оборудования и посторонних проводниках, выходящих за пределы КЗ;

y_6 — превышение допустимого уровня просачиваемых информативных сигналов в цепях электропитания технологического радиоэлектронного оборудования;

y_7 — превышение допустимого уровня просачиваемых информативных сигналов в цепях заземления технологического радиоэлектронного оборудования;

y_8 — территориальная доступность производственных помещений предприятия для ведения по ним технической разведки;

y_9 — наличие труб отопления, водоснабжения, газоснабжения и канализации в производственных помещениях предприятия;

y_{10} — наличие подведенных коммуникаций (кабелей электропитания и телефонии) в производственных помещениях предприятия;

y_{11} — наличие металлоконструкций в производственных помещениях предприятия;

y_{12} — наличие окон в производственных помещениях предприятия;

y_{13} — наличие вентиляционных систем в производственных помещениях предприятия;

y_{14} — наличие в производственных помещениях предприятия охранно-пожарной сигнализации;

y_{15} — наличие на предприятии собственной радиосети;

y_{16} — наличие на предприятии трансляционной сети и громкоговорящей связи;

y_{17} — наличие в производственных помещениях предприятия выхода на внешние автоматические телефонные станции;

y_{18} — наличие в производственных помещениях предприятия бытовой техники;

y_{19} — наличие в производственных помещениях предприятия технологического радиоэлектронного оборудования;

y_{20} — наличие в производственных помещениях предприятия продукции с работающим радиоэлектронным оборудованием;

y_{21} — наличие выхода кабелей питания и цепей заземления технологического оборудования за пределы предприятия;

y_{22} — наличие на предприятии собственной трансформаторной подстанции;

y_{23} — наличие в технологическом процессе фазы проведения испытаний двигательных установок без их запуска («холодных» испытаний) [14; 15];

y_{24} — наличие в технологическом процессе фазы проведения испытаний двигательных установок с их запуском [14; 15].

Перечисленные факторы характеризуют потенциальный перечень уязвимостей. Возможность возникновения на основе таких уязвимостей угроз перехвата информативных сигналов ПЭМИН и виброакустического поля на предприятии оценивается с помощью соответствующих инструментально-расчетных методик.

Количественно уязвимость, через которую возможна утечка технологической информации по техническим каналам на предприятии авиапрома, характеризуется вероятностью наличия благоприятных условий ее использования для реализации угрозы. Данная вероятность оценивается путем анкетирования специалистов в области противодействия техническим разведкам (ПДТР). В систематизированном виде результаты экспертной оценки данной характеристики представляются лингвистической переменной Λ_{ij}, принимающей одно из значений — «да», «вероятно», «возможно», «маловероятно» и «нет» — в зависимости от того, насколько возможно использование i-м потенциальным источником угроз утечки технологической информации j-ой уязвимости. Каждому из пяти лингвистических значений ставится в соответствие вероятность использования i-м источником j-ой уязвимости — p_{ij}. Данная вероятность позволяет формально определить вероятность P_i использования j-й уязвимости (в приводимом примере j = 1, 2, …, 25) от всех возможных (в приводимом примере от обоих) источников угроз [16]:

$$P_j = 1 - (c_{j,1}(1 - p_{j,1})c_{j,2}(1 - p_{j,2})), \quad (1)$$

где $c_{j,1}$ — коэффициент соответствия, равный 1, если j-я уязвимость характерна i-му источнику и 0 – в противном случае.

Множество источников угроз утечки технологической информации по техническим каналам на предприятии авиапрома и множество уязвимостей, через которые возможна реализация такого рода угроз, позволяет сформировать само множество угроз утечки $\{l_k\}$, k = 1, 2, …, K.

Для рассматриваемого примера:

l_1 — утечка информации за счет собственных ПЭМИ при прохождении тока по элементам технологического радиоэлектронного оборудования и элементам работающего радиоэлектронного оборудования образцов производимой продукции;

l_2 — утечка информации за счет ЭМИ на частотах работы высокочастотных генераторов

технологического радиоэлектронного оборудования и работающего радиоэлектронного оборудования образцов производимой продукции;

l_3 — утечка информации за счет ЭМИ на частотах самовозбуждения усилителей никой частоты технологического радиоэлектронного оборудования и работающего радиоэлектронного оборудования образцов производимой продукции;

l_4 — утечка информации за счет ЭМИ технологического радиоэлектронного оборудования на соединительных линиях и посторонних проводниках, выходящих за пределы КЗ;

l_5 — утечка информации за счет просачивания информативных сигналов в цепи электропитания и заземления технологического радиоэлектронного оборудования;

l_6 — утечка информации за счет преднамеренного «высокочастотного облучения» из-за пределов КЗ;

l_7 — утечка акустической информации от производимых двигательных установок по вибрационному каналу;

l_8 — утечка акустической информации от производимых двигательных установок по акустическому (прямому воздушному) каналу;

l_9 — утечка информативного акустического сигнала по оптико-электронному каналу.

Соответствие между уязвимостями и характерными им угрозами утечки технологической информации по техническим каналам определяется коэффициентом актуальности $a_{j,k}$, принимающего значение 1, если *j*-я уязвимость инициирует *k*-ю угрозу и 0 – в противном случае.

Данные *табл. 1* позволяют дать количественную оценку уровня угроз утечки технологической информации по техническим каналам на предприятии авиапрома в виде вероятности $P_k^{(y)}$ реализации *k*-ой угрозы, k = 1, 2, …, 9:

$$P_k^{(y)} = 1 - \prod_{j=1}^{24}(1 - \alpha_{j,k} P_j), \qquad (2)$$

где P_j соответствует выражению (1).

Анализируя в целом существующий уровень проработки математических методов как в проблематике технической защиты информации в целом, так и в вопросах предотвращения угроз утечки информации по техническим каналам в условиях современных тенденций совершенствования технической разведки, можно выявить три весьма серьезных обстоятельства, не позволяющих характеризовать разработанный на настоящий момент математический аппарат как адекватный.

Таблица 1. Соответствие значений коэффициентов актуальности уязвимостей технологической информации для инициализации угроз ее утечки по техническим каналам на предприятии авиапрома
Table 1. Compliance of the values of vulnerability ratios of technological information for the initiation of threats of its leakage through technical channels in the aviation industry enterprise

Уязвимости / Vulnerabilities	Угрозы / Threats								
	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1
2	1	0	0	0	0	0	0	0	0
3	0	1	0	0	0	0	0	0	0
4	0	0	1	0	0	0	0	0	0
5	0	0	0	1	0	0	0	0	0
6	0	0	0	0	1	0	0	0	0
7	0	0	0	0	1	0	0	0	0
8	1	1	1	1	1	1	1	1	1
9	0	0	0	1	1	0	1	0	0
10	0	0	0	1	1	0	1	0	0
11	0	0	0	0	0	1	1	0	0
12	1	1	1	0	0	1	1	1	1
13	0	0	0	0	0	1	0	1	0
14	0	0	0	0	0	1	0	0	0
15	0	0	0	0	0	1	0	0	0
16	0	0	0	0	0	1	0	0	0
17	0	0	0	0	0	1	0	0	0
18	0	0	0	0	0	1	0	0	0
19	1	1	1	1	1	1	0	0	0
20	1	1	1	0	0	1	0	0	0
21	0	0	0	1	1	0	0	0	0
22	0	0	0	0	0	1	0	0	0
23	0	0	0	0	0	0	1	1	1
24	0	0	0	0	0	0	1	1	1

Первое обстоятельство связано с неоправданно широким применением эвристического подхода к оценке возможностей нарушителя по перехвату информативных сигналов физических полей. Характерным примером здесь может служить рассмотренная выше методика ФСТЭК по оценке указанных возможностей, реализующая экспертный подход в вопросах вероятностного представления субъектно-объектных отношений в исследуемых процессах. Примененный здесь эмпирический подход к переходу от лингвистического к количественному представлению вероятностных характеристик угроз утечки информации

по техническим каналам способствует доминированию субъективного влияния экспертных оценок как на сам процесс исследования, так и на его результаты, что является предпосылкой низкой адекватности используемого методического аппарата. Кроме того, данный методический аппарат не учитывает те случайные состояния исследуемых процессов, которые характеризуют их динамику. В п. 5 «Определение вероятностей реализации угроз» нормативно-методического документа, определяющего порядок оценки актуальных угроз безопасности информации, прямо указывается на этот недостаток: «вероятность угрозы характеризует динамику ее возникновения и реализации… Такие модели в настоящее время отсутствуют, а их разработка представляет собой достаточно длительный процесс. Для парирования сложностей, связанных с отсутствием математических моделей расчета вероятностей реализации угроз, принято следующее допущение: <…> вероятность реализации угрозы в условиях отсутствия мер защиты приравнивается к единице, если данная угроза имеет место, и к нулю, если угроза отсутствует. Последнее допущение равносильно тому, что выбирается такое время, за которое реально существующая угроза может быть реализована с вероятностью, близкой к единице. В последующем предполагается расширить данную методику путем разработки необходимых математических моделей расчета вероятности реализации угрозы и устранить данное допущение».

Второе обстоятельство связано с тем, что в тех моделях, которые все же позволяют оценить характеристики исследуемых процессов в их динамике [11; 17], учитывается лишь продолжительность этих процессов, но не учитываются случайные состояния, связанные с динамикой возникновения угроз и их обнаружением. Как и в предыдущем случае, это обстоятельство является предпосылкой низкой адекватности этих моделей.

Третье обстоятельство связано с отсутствием методического аппарата математического моделирования, позволяющего оценить основную характеристику эффективности мер предотвращения утечки информации — их полноту. Исключение составляют попытки оценить эффективность таких мер соотнося их длительность и длительность процесса перехвата информативных сигналов физических полей [18]. Адекватность такой оценки невысока, так как даже в случае, когда за время существования угрозы меры предотвращения утечки информации будут осуществлены, что может характеризовать их как эффективные, полнота контроля не позволит идентифицировать каналы утечки. А это уже характеризует меры как неэффективные.

Преодоление указанных недостатков возможно лишь в том случае, когда формальное описание исследуемых процессов позволяет математически представить все условия, характерные для динамики перехвата информативных сигналов виброакустического поля и ПЭМИН, и полноты мер предотвращения утечки информации по виброакустическим каналам и каналам ПЭМИН.

Характеризуя в этой связи исследовательский потенциал методологии технической защиты информации в целом, можно констатировать, что исследования в данной области позволили дать всестороннюю характеристику как угроз утечки информации по техническим каналам, так и способов защиты информации от утечки. Вместе с тем методические подходы к исследованию качества обеспечения мер технической защиты информации, приводимые в работах известных специалистов в области противодействия техническим разведкам [1–3; 19; 20], не обладают той степенью системности, которая позволила бы учесть особенности динамики перехвата информативных сигналов физических полей и полноты мер предотвращения утечки информации по техническим каналам в рамках однотипного формализованного представления исследуемых процессов.

Выводы

Реализованные в рамках данной методологии подходы к систематизации проявлений эффекта защищенности информации от утечки по техническим каналам носят субъективный характер и в крайне ограниченном виде отражают системные проявления субъектно-объектных отношений в процессах, характерных для данной предметной области [21], включая формальную интерпретацию динамики перехвата информации ТСР и полноты реализации мер предотвращения ее утечки.

Возрастающие требования к противодействию техническим разведкам в целом и требования к обоснованности мер предотвращения утечки информации по техническим каналам в условиях современных тенденций совершенствования технической разведки в частности, вопросы оценки эффективности таких мер являются актуальными и нуждаются в проработке как в методическом, так и в прикладном плане.

ПРИСТАТЕЙНЫЙ БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Хорев А. А.* Технические каналы утечки информации, обрабатываемой средствами вычислительной техники // Специальная техника. 2010. № 2. С. 39–57.
2. *Хорев А. А.* Контроль защищённости вспомогательных технических средств и систем от утечки по акустоэлектрическим каналам // Специальная техника. 2014. № 6. С. 48–63.
3. *Исследование* непреднамеренных электромагнитных излучений средств вычислительной техники / Ю. В. Кузнецов, А. Б. Баев, М. А. Коновалюк, А. А. Горбунова // Специальная техника. 2017. № 1. С. 2–15.
4. *Бобылева М. П.* Управленческий документооборот: от бумажного к электронному. Вопросы теории и практики. М. : ТЕРМИКА, 2016. 360 с. ISBN 978-5-6040204-6-3.
5. *Шаньгин В. Ф.* Информационная безопасность и защита информации. М. : ДМК Пресс, 2014. 702 с. ISBN 978-5-94074-768-0.
6. *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.
7. *Хорев А. А.* Способы и средства защиты речевой информации от утечки по акустоэлектрическим каналам // Специальная техника. 2014. № 1. С. 49–57.
8. *Ющук Е. Л.* Конкурентная разведка. Маркетинг рисков и возможностей. М. : Вершина, 2006. 240 с. ISBN 5-9626-0027-4.
9. *Жежера Н. И.* Микропроцессорные системы автоматизации технологических процессов. М. : Инфра-Инженерия, 2020. 240 с. ISBN 978-5-9729-0517-1.
10. *Тобольский А.* Экспансия иностранного шпионажа. Угроза модернизации России. М. : Вече, 2011. 496 с. ISBN 978-5-9533-5783-8.
11. *Джоган В. К., Авсентьев А. О.* Способ представления математических моделей для оценки характеристик противодействия перехвату речевой информации // Вестник Воронежского института МВД России. 2013. № 2. С. 248–252.
12. *Математические* модели функциональных характеристик мер комплексного технического контроля защищенности информации от утечки по виброакустическим каналам на предприятиях авиакосмической промышленности / С. В. Скрыль , В. В. Зеленцов , Д. А. Холод , С. А. Литовченко , В. И. Спивак , О. А. Гуляев. // Авиакосмическое приборостроение. 2019. № 10. С. 31–43.
13. *Математическая* модель полноты реализации функций защиты информации как инструмент научного обоснования мер обеспечения ее безопасности / С. В. Скрыль , Т. В. Мещерякова , О. А. Гуляев , Е. А. Гайфулин, И. М. Маньков , О. А. Тегенцев // Промышленные АСУ и контроллеры. 2020. № 5. С. 42–52.
14. *Двигатели* боевых самолетов России / В. Р. Котельников , В. А. Зрелов , В. А. Пономарев , О. В. Хробыстова. М. : Медиарост, 2020. 312 с.
15. *Двигатели* гражданских самолетов России / В. Р. Котельников , О. В. Хробыстова , В. А. Зрелов , В. А.Пономарев. М. : Медиарост, 2020. 564 с.
16. *Экспертный* подход к оценке уровня угрозы утечки информации по каналам ПЭМИН и ее защищенности от такого рода угроз / С. В. Скрыль , С. С. Никулин , М. В. Пономарёв , И. М. Тегенцев , М. В. Кузнецов // Промышленные АСУ и контроллеры. 2018. № 4. С. 45–53.
17. *Джоган В. К., Думачев В. Н., Здольник В. В.* О математических аспектах расчета эффективности систем технической защиты информации // Вероятностные методы в дискретной математике: материалы Седьмой Международной Петрозаводской конференции. Обозрение прикладной и промышленной математики. 2009. Том 16. Вып. 1. С. 70–71.
18. *Прикладные* аспекты оценки нераскрываемости информации: обоснование характеристики и модель исследования / С. В. Скрыль, Т. В. Мещерякова, В. В. Гайфулин, В. В. Зеленцов, М. В. Пономарев // Авиакосмическое приборостроение. 2020. № 2. С. 23–33.
19. *Гончаров Н. И., Сирота А. А., Гончаров И. В.* Анализ защищённости сетевых систем обработки данных по отношению к техническим каналам утечки информации // Специальная техника. 2017. № 1. С. 39–47.
20. *Авдеев В. Б., Анищенко А. В., Петигин А. Ф.* Методический подход к оценке защищённости информации, обрабатываемой компьютером с использованием сложных сигналов, от утечки за счёт побочных электромагнитных излучений // Специальная техника. 2017. № 3. С. 40–47.
21. *Громов Ю. Ю., Никулин С. С., Сычев А. М.* Формальные предпосылки решения проблемы оценки защищенности информации от утечки по техническим каналам // Промышленные АСУ и контроллеры. 2014. № 5. С. 69–74.

REFERENCES

1. Khorev A. A. Technical channels of computer-rpocessed information leakage. *Spetsialnaya tekhnika*. 2010;2:39–57. (In Russian).
2. Khorev A. A. Monitoring the protection of auxiliary equipment and systems from leakage through acoustoelectric channels. *Spetsialnaya tekhnika*, 2014;6:48–63. (In Russian).
3. Kuznetsov Yu. V., Baev A. B., Konovalyuk M. A., Gorbunova A. A. Research of computer equipment spontaneous electromagnetic radiation. *Spetsialnaya tekhnika*, 2017;1:2–15. (In Russian).
4. Bobyleva M. P. *Upravlencheskii dokumentooborot: ot bumazhnogo k elektronnomu. Voprosy teorii i praktiki* [Document management: from paper to electronic. Theory and practice issues]. Moscow, TERMIKA Publ., 2016, 360 p. (In Russian). ISBN: 978-5-6040204-6-3.

5. Shangin V. F. *Informatsionnaya bezopasnost i zashchita informatsii* [Information security and protection]. Moscow, DMK Press Publ., 2014, 702 p. (In Russian). ISBN 978-5-94074-768-0.
6. Gerasimenko V. G., Lavrukhin Yu. N., Tupota V. I. Methods of protection of acoustic speech information from leakage through technical channels : monograph. Moscow, RCIB Fakel Publ., 2008. 258 p. (In Russian).
7. Khorev A. A. Methods and means of speech protection against leakage viaacoustoelectric channels. *Spetsialnaya tekhnika*, 2014;1:49–57. (In Russian).
8. Yushchuk E. L. *Konkurentnaya razvedka. Marketing riskov i vozmozhnostei* [Competitive reconnaissance. Risk and opportunity marketing]. Moscow, Vershina Publ., 2006, 240 p. (In Russian). ISBN 5-9626-0027-4.
9. Zhezhera N. I. *Mikroprotsessornye sistemy avtomatizatsii tekhnologicheskikh protsessov* [Microprocessor-based process automation systems]. Moscow, Infra-Inzheneriya Publ., 2020. 240 p. (In Russian). ISBN 978-5-9729-0517-1.
10. Tobolskii A. *Ekspansiya inostrannogo shpionazha. Ugroza modernizatsii Rossii* [Expansion of foreign espionage. Threat of modernization of Russia]. Moscow, Veche Publ., 2011, 496 p. (In Russian). ISBN 978-5-9533-5783-8.
11. Dzhogan V. K., Avsentev A. O. A method for presenting mathematical models for evaluating the characteristics of countering the interception of speech information. *Vestnik Voronezhskogo instituta MVD Rossii*, 2013;2:248–252. (In Russian).
12. Skryl S. V., Zelentsov V. V., Kholod D. A., Litovchenko S. A., Spivak V. I., Gulyaev O. A. Mathematical models of functional characteristics of measures of complex technical control of information security from leakage through vibroacoustic channels at enterprises of the aerospace industry. *Aviakosmicheskoe priborostroenie*, 2019;10:31–43. (In Russian).
13. Skryl S. V., Meshcheryakova T. V., Gulyaev O. A., Gaifulin E. A., Mankov I. M., Tegentsev O. A. .Mathematical model of completeness of implementation of information security functions as a tool for scientific justification of measures to ensure its security. *Promyshlennye ASU i kontrollery*, 2020;5:42–52. (In Russian).
14. Kotelnikov V. R., Zrelov V. A., Ponomarev V. A., Khrobystova O. V. *Dvigateli boevykh samoletov Rossii* [Engines of Russian combat aircraft]. Moscow, Mediarost Publ., 2020, 312 p. (In Russian).
15. Kotelnikov V. R., Khrobystova O. V., Zrelov V. A., Ponomarev V. A. *Dvigateli grazhdanskikh samoletov Rossii* [Engines of Russian civil aircraft]. Moscow, Mediarost Publ., 2020, 564 p. (In Russian).
16. Skryl S. V., Nikulin S. S., Ponomarev M. V., Tegentsev I. M., Kuznetsov M. V. Expert approach to assessment of level of threat of information leakage on PEMIN channels and her security from such threats. *Promyshlennye ASU i kontrollery*, 2018;4:45–53. (In Russian)
17. Dzhogan V. K., Dumachev V. N., Zdolnik V. V. On the mathematical aspects of calculating the effectiveness of technical information security systems. Probabilistic methods in Discrete Mathematics: Proceedings of the Seventh International Petrozavodsk Conference. *Obozrenie prikladnoi i promyshlennoi matematiki*, 2009;16(1):70–71. (In Russian).
18. Skryl S. V., Meshcheryakova T. V., Gaifulin V. V., Zelentsov V. V., Ponomarev M. V. Application aspects of assessment of non-disclosure of information: substantiation of the characteristic and model of the study. *Aviakosmicheskoe priborostroenie*. 2020;2:23–33. (In Russian).
19. Goncharov N. I., Sirota A. A., Goncharov I. V. Analysis of the security of network data processing systems in relation to technical channels of information leakage. *Spetsialnaya tekhnika*, 2017;1:39–47. (In Russian).
20. Avdeev V. B., Anishchenko A. V., Petigin A. F. Methodological approach to assessing the security of information processed by a computer using complex signals from leakage due to spurious electromagnetic radiation. *Spetsialnaya tekhnika*, 2017;3:40–47. (In Russian).
21. Gromov Yu. Yu., Nikulin S. S., Sychev A. M. Formal prerequisites of the solution of the problem of the assessment securities of information from leak on technical channels. *Promyshlennye ASU i kontrollery*, 2014;5:69–74. (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, e-mail: karel105@mail.ru.

Сычев Михаил Павлович, 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, e-mail: mpsichov@sm.bmstu.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, e-mail: mazinav@yandex.ru.

Мещерякова Татьяна Вячеславовна, к. ф.-м. н., начальник кафедры, ФГКОУ ВО «Воронежский институт Министерства внутренних дел Российской Федерации», 394065, Воронеж, просп. Патриотов, д. 53, e-mail: tmeshcheriakova4@mvd.ru.

Гуляев Олег Анатольевич, директор филиала, ПАО «Корпорация Иркут», филиал «Региональные самолеты», 115280, Россия, Москва, ул. Ленинская Слобода, д. 26, e-mail: pt@utw.su.

Тегенцев Иван Михайлович, начальник отделения, Центр инженерно-технического обеспечения ФСИН России, 119049, Москва, ул. Житная, д. 14, e-mail: tegentsev-im@fsin.gov.ru.

AUTHORS

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

Mikhail P. Sychev, D.Sc. (Engineering), professor, Bauman Moscow State Technical University, 5, str. 1, ulitsa 2-ya Baumanskaya, Moscow, 105005, Russia, e-mail: mpsichov@sm.bmstu.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, e-mail: mazinav@yandex.ru.
Tatiana V. Meshcheriakova, candidate of physical and mathematical sciences, head of the Department**,** Voronezh Institute of the Ministry of Internal Affairs of Russia, 53, prospekt Patriotov, Voronezh, 394065, Russia, e-mail: tmeshcheriakova4@mvd.ru.
Oleg A. Gulyaev, branch Director, Corporatcia Irkut PJSC, Regional aircraft branch, 26, ulitsa Leninskaya Sloboda, Moscow, 115280, Russia, e-mail: pt@utw.su.
Ivan M. Tegentzhev, head of the Department, The Main Department of the Federal Penitentiary Service of Russia, 14, ulitsa Zhitnaya, Moscow, 119049, Russia, e-mail: tegentsev-im@fsin.gov.ru.

Поступила 29.07.2020; принята к публикации 28.12.2020; опубликована онлайн 26.03.2021.
Submitted 29.07.2020; revised 28.12.2020; published online 26.03.2021.