МАТЕМАТИЧЕСКИЕ, СТАТИСТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ В ЭКОНОМИКЕ

Научная статья / Original article

УДК 004.056.5

DOI 10.22394/ee253.93-109

JEL C11 D83 O33

EDN XDFVCB

Лисичкин В. Г., Лисичкина Н. В.

ИНФОРМАЦИОННЫЙ ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Лисичкин Владимир Георгиевич
доктор технических наук, доцент
Академия ФСО России (г. Орел, Россия), сотрудник
lisichkin-vg@rambler.ru
https://orcid.org/0000-0001-6684-0318
SPIN 7566-7713

Лисичкина Наталия Владимировна
кандидат экономических наук, доцент
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Среднерусский институт управления (г. Орел, Россия), доцент кафедры менеджмента и управления персоналом
natalyorel@hotmail.com
https://orcid.org/0000-0002-7114-4330
SPIN 7418-9506

Vladimir G. Lisichkin
Doctor of Engineering Sciences, Associated Professor
Academy of the Federal Guard Service of the Russian Federation (Orel, Russia), Employee
lisichkin-vg@rambler.ru
https://orcid.org/0000-0001-6684-0318
SPIN 7566-7713

Nataliya V. Lisichkina
Candidate of Economic Sciences, Associated Professor
Russian Presidential Academy of National Economy and Public Administration, Central Russian Institute of Management (Orel, Russia), Associate Professor of Management and Personnel Management Department
natalyorel@hotmail.com
https://orcid.org/0000-0002-7114-4330
SPIN 7418-9506

В условиях непрерывного совершенствования технических и программных средств и растущей геополитической напряжённости система защиты информации в российских телекоммуникационных системах должна базироваться на принципах Керкхоффса, то есть предусматривать механизм, позволяющий некоторым оптимальным образом определять потенциальные возможности условного противника получить несанкционированный доступ к скрываемой информации, которая может содержать как персональные данные пользователей, так и коммерческую тайну экономических субъектов. Одним из факторов угрозы при передаче информации по телекоммуникационным сетям, даже обеспечивающим достаточно высокий уровень шифрования, является наличие побочных электромагнитных излучений, которые могут стать источниками информативного сигнала, рандомно распространяющегося за границами контролируемого периметра. Предметом исследования служит применение активных методов технической защиты информации, то есть целенаправленного зашумления информационного сигнала. Целью данного исследования является разработка модели оценки эффективности активных методов защиты информации от утечки по техническим каналам с учётом того, что современные высокоинтеллектуальные средства обработки сигналов, основанные на статистических методах, обеспечивают достаточно высокий уровень вероятности распознавания ин-

Under conditions of continuous improvement of technical and software tools and growing geopolitical tensions, information security system in Russian telecommunications systems should be based on the Kerckhoffs's principles, that is, provide a mechanism that allows some optimal way to determine potential of token enemy to gain unauthorized access to hidden information that may contain both personal data of the users and commercial secrets of economic entities. One of the threat factors in information transmission of over telecommunication networks, even those providing sufficiently high encryption level, is electromagnetic side effects, which can become sources of informative signal that randomly propagates beyond the boundaries of the controlled perimeter. The subject of the study is application of active methods of technical information protection, that is, targeted noisening of information signal. The purpose of the study is to develop effectiveness evaluation model of active methods of information protection from leak through technical channels, taking into account the fact that modern highly intelligent signal processing tools based on statistical methods provide sufficiently high probability of recognizing information signal hidden under noise if the entropy of the noise screen is not high enough. Considering the existence of correlation between the effectiveness level of

формационного сигнала, скрываемого под шумами, если энтропия шумовой завесы окажется недостаточно высокой. Принимая в качестве рабочей гипотезы существование корреляции между уровнем эффективности защиты информации от несанкционированного доступа и степенью неопределённости, создаваемой в техническом канале смеси полезного сигнала с шумом, авторы выполнили анализ статистических критериев обнаружения скрываемой информации. В качестве результата предложен информационный подход, позволяющий выполнять сравнительный анализ эффективности различных методов защиты телекоммуникационной системы от утечек замаскированной псевдошумовым сигналом информации на основе критерия Кульбака-Лейблера. При этом необходимо учитывать, что возможности оптимального детектора по достоверности обнаружения заведомо ограничены и для эффективной работы модели необходимо задать корректные ограничения допустимых значений вероятностей ошибок ложного срабатывания и пропущенного обнаружения замаскированного сигнала.

***Ключевые слова**: защита информации, коммерческая тайна, персональные данные, вероятность обнаружения, эффективность защиты, статистические критерии, энтропия, дивергенция, критерий Кульбака-Лейблера.*

***Вклад авторов**: все авторы внесли равный вклад в проведение исследования и написание статьи; выразили согласие нести публичную ответственность за все аспекты работы, связанные с точностью или достоверностью любой части рукописи; одобрили финальную версию статьи перед публикацией.*

Для цитирования: Лисичкин В. Г., Лисичкина Н. В. Информационный подход к оценке эффективности защиты информации в телекоммуникационных системах // Экономическая среда. – 2025. – Т. 14, № 3. – С. 93-109. – https://doi.org/10.22394/ee253.93-109. – EDN XDFVCB.

information protection from unauthorized access and the uncertainty degree of the mixture of useful signal with noise created in the technical channel as a working hypothesis, the authors analyzed the statistical criteria for detecting hidden information. As a result, information approach is proposed that makes it possible to perform comparative effectiveness analysis of various protection methods of telecommunications system from information leaks disguised by pseudo-noise signal based on Kullback–Leibler criterion. At the same time, it should be borne in mind that optimal detector capabilities are obviously limited in terms of detection accuracy, and it is necessary to set correct limits on the permissible probability values of false operation and missed detection of masked signal for effective operation of the model.

***Keywords**: information protection, trade secret, personal data, detection probability, protection effectiveness, statistical criteria, entropy, divergence, Kulback-Leibler criterion.*

***Authors' contribution**: All authors contributed equally to the research and writing; agreed to be publicly responsible for all aspects of the work related to the accuracy or integrity of any part of the manuscript; approved the final version of the article before publication.*

For citation: Lisichkin V.G., Lisichkina N.V. Information Approach to Effectiveness Evaluation of Information Telecommunication Systems Protection. *Economic Environment*, 2025, vol. 14, no. 3, pp. 93-109. (In Russ.). Available from: https://doi.org/10.22394/ee253.93-109.

Введение

В настоящее время проблема защиты информации является одним из важнейших аспектов обеспечения не только национальной безопасности, но и безопасности персональных данных и коммерческой тайны экономических субъектов [1–4]. Решение этой проблемы требует комплексного подхода из-за необходимости учёта большого количества самых разнообразных факторов [5–7]. Особое место в общем ряду существующих в области безопасности проблем занимает защита информации от утечки по техническим каналам (ТК) в телекоммуникационных системах (ТКС) [8–11]. В условиях растущей геополитической напряжённости информационное противостояние, в течение нескольких десятилетий развивавшееся скрытно, выходит на новый уровень. Увеличение военных бюджетов позволяет использовать новейшие достижения научно-технической мысли для совершенствования систем и средств иностранных технических разведок (ИТР) – в этой ситуации защита информации от несанкционированного доступа, искажения, уничтожения и иных неправомерных действий становится всё более актуальной.

При разработке мер защиты информации от несанкционированного доступа разумным подходом считается предположение, основанное на принципах Огюста Керкхоффса [12] – технические средства разведки условного противника обладают максимальными возможностями по перехвату, анализу и вскрытию защищаемой информации. Такое предположение позволяет разрабатывать наиболее эффективные и надёжные меры защиты.

Одной из возможных причин утечки защищаемой информации в процессе её обработки с использованием различных технических средств связи (ТСС) является наличие побочных электромагнитных излучений (ПЭМИ) [13]. Существование такого канала утечки обусловлено тем, что любое радиоэлектронное средство в процессе своего функционирования создаёт в пространстве вокруг себя магнитное и электрическое поля, а также электромагнитное излучение. Источниками данных излучений являются изменяющиеся токи, циркулирующие между элементами ТСС, которые могут отражать признаки обрабатываемой защищаемой информации. Эти излучения и поля, которые можно назвать информативными сигналами (ИС), могут распространяться за границы контролируемой зоны и стать доступными злоумышленнику, который, используя соответствующую аппаратуру перехвата, может получить доступ к защищаемой информации [14].

Источниками информативного сигнала могут являться виртуальные антенные устройства, которые возникают случайным образом и излучают сигналы с защищаемой информацией. Роль таких случайных излучающих антенн могут выполнять соединительные кабели, удлинители, шины, печатные проводники, а также разъёмы различных проводных интерфейсов. Данные элементы в зависимости от геометрических размеров и характеристик интерфейсов могут выступать в качестве распределённых или сосредоточенных антенн – источников ПЭМИ [13]. Возможность утечки информации по такому каналу определяется в ходе специальных исследований, например с помощью оценки напряжённости полей на границе контролируемой зоны [14]. На практике данная задача может решаться путём проведения измерений напряжённости полей вблизи исследуемого ТСС и перерасчёта полученных значений к границе контролируемой зоны с помощью разработанной методики и соответствующих коэффициентов изменения напряжённости вдоль пространственной координаты [15; 16].

Для обеспечения эффективной защиты информации от утечки по ТК важно выработать критерии защищённости, чтобы получить аргументированные ответы на такие вопросы, как: существует ли возможность утечки по данным каналам, и если да, то достаточно ли принятых мер для предотвращения такой утечки. Существуют два основных подхода к формированию таких критериев [10; 11; 17] – оценка эффективности защитных мер на качественном уровне и энергетический критерий. Первый подход не находит широкого применения в практической деятельности, так как качественная оценка уровня защищённости информации, передаваемой по каналам связи, требует наличия специалистов высокой квалификации в этой области знаний, что не всегда возможно, при этом сама оценка всегда будет субъективной, так как определяется уровнем квалификации специалиста, реализующего такой критерий оценивания [18; 19].

Большее применение находят энергетические критерии, основанные на измерении различных параметров информативных сигналов в каналах утечки и сравнении результатов измерений с установленными нормами [20]. Одним из таких критериев является соотношение мощностей информативного сигнала и шума, измеренное на выходе специального измерительного устройства, и сравнение полученного значения с максимально допустимым на границе контролируемой зоны уровнем [21]. Также находит применение энергетический критерий, основанный на измерении напряжённости поля (электрического, магнитного, электромагнитного) в пределах контролируемой зоны и сравнении с нормой [22–24]. При обработке результатов измерений могут использоваться вероятностные подходы, основанные на статистических методах [25–29].

Техническая защита информации от утечки, в отличие от криптографических методов скрытия информации, направлена на уменьшение соотношения сигнал/шум на границе контролируемой зоны и основана на двух основных направлениях [8; 11;

18]. Первое – уменьшение мощности информативного сигнала в канале утечки, для чего применяются пассивные методы защиты информации (экранирование, электрическая фильтрация, схемотехнические методы, звукоизоляция и пр.) [30–34]. Второе направление реализуется активными методами защиты и основано на создании дополнительной шумовой помехи в канале утечки, что позволяет также уменьшать соотношение сигнал/шум в контролируемой зоне за счёт увеличения мощности шума [35–37]. Практическое применение находят как пассивные, так и активные методы технической защиты информации, однако активные методы обладают большей универсальностью и проще реализуются, поэтому считаются более эффективными.

Применение для оценки эффективности активных мер защиты информации от утечки такого показателя, как отношение $P_с / P_ш$ мощности информативного сигнала $P_с$ и мощности шума $P_ш$, не всегда приводит к наилучшему результату с точки зрения обеспечения требуемого уровня безопасности связи. Современные способы обработки сигналов, основанные на статистических методах, могут позволить средствам ИТР получать доступ к передаваемой информации даже в условиях сильного зашумления информационного сигнала [38]. Чтобы противостоять таким методам, необходимо использовать такие шумовые сигналы, которые существенно увеличивают энтропию сигнала, скрываемого под шумами. В этом случае уровень защиты информации от несанкционированного доступа будет во многом зависеть от степени увеличения неопределённости смеси полезного сигнала с шумом. Для проверки эффективности мер защиты информации от утечки по ТК целесообразно использование вероятностных методов и различного рода статистических критериев.

Одним из общепринятых вероятностных критериев, позволяющим получить минимальную величину ошибки распознавания для единичного наблюдения, может быть критерий минимума апостериорной вероятности [28]. Однако в условиях априорной неопределённости применение такого критерия может приводить к существенному снижению вероятности правильного принятия решения. Представляется более целесообразным использование показателей, позволяющих оценивать изменение уровня неопределённости смеси полезного сигнала с шумом. Поскольку мерой неопределённости любого случайного процесса (в том числе и зашумлённого информационного сигнала) является энтропия, критерием эффективности защиты информации от утечки по техническим каналам может служить увеличение энтропии [39].

Постановка задачи

При реализации активных методов защиты информации приходится в техническом канале утечки создавать специальным образом сформированную смесь информационного сигнала и дополнительной шумовой помехи. Математически эту процедуру можно представить следующим образом. На вход некоторого преобразовательного устройства с оператором преобразования *G* подаётся детерминированный информационный сигнал $\xi(t)$. В результате выполненного преобразования на выходе появляется псевдослучайный шумовой сигнал $\tilde{\xi}(t): G\{\xi(t)\} = \tilde{\xi}(t)$, обладающий низкими корреляционными свойствами, что должно затруднить вероятному злоумышленнику доступ к передаваемой информации. Чтобы определить эффективность таких мер защиты вероятностными методами, необходимо оценить степень близости сформированного сигнала к идеальному шуму, в качестве которого можно выбрать белый гауссовский шум $n(t)$. В этом случае можно записать $\tilde{\xi}(t) = \xi(t) + n(t)$ и сформулировать задачу проверки эффективности мер защиты информации как задачу проверки ги-

потез, где гипотеза H_0 означает отсутствие в сигнале $\tilde{\xi}(t)$ информационной составляющей: $\tilde{\xi}(t) = n(t)$; гипотеза H_1 – в принимаемом сигнале есть скрываемая информация: $\tilde{\xi}(t) = \xi(t) + n(t)$. В этом случае задачу проверки эффективности технических мер защиты информации от утечки можно сформулировать как задачу распознавания гипотез.

Постановка задачи проверки гипотез зависит от уровня априорной определённости условного противника. Если предположить достаточно высокий уровень знаний ИТР о реализации активных мер защиты информации и наличие у противника статистических материалов наблюдений, позволяющих знать вероятностные законы распределений, то можно говорить о задаче обнаружения в виде простого гипотетического теста:

$$H_0 : \tilde{\xi} \sim f_0(x);\ H_1 : \tilde{\xi} \sim f_1(x), \tag{1}$$

где $f_0(x)$ и $f_1(x)$ – вероятностные распределения, соответствующие отсутствию и наличию скрываемой информации в сигнале $\tilde{\xi}(t)$.

Оптимальное решение в такой ситуации может быть получено условным противником на основе байесовского критерия максимального правдоподобия или критерия Неймана-Пирсона [28; 40; 41].

Альтернативный вариант априорной осведомлённости – вероятностные законы противнику неизвестны. Постановка задачи обнаружения видоизменяется:

$$H_0 : f(\tilde{\xi}) \approx f_0(x);\ H_1 : f(\tilde{\xi}) \neq f_0(x) \tag{2}$$

и становится сложной гипотетически тестовой проблемой [12].

Одним из промежуточных вариантов априорной определённости может быть следующий. Информации о законах распределения вероятностей у противника нет, но может быть известен алгоритм формирования псевдослучайного шумового сигнала, скрывающего передаваемую информацию. В этом случае вероятностное распределение будет зависеть от некоторого неизвестного параметра δ, определяющего уровень изменений, происходящих с шумовым сигналом $n(t)$ после смешивания его с информационным сигналом $\xi(t)$. Гипотетически тестовая проблема (2) немного упрощается:

$$H_0 : \delta = 0;\ H_1 : \delta > 0. \tag{3}$$

Техническую реализацию задачи (1) можно представить следующим образом. Предположим, что в техническом канале утечки информации выполнены измерения псевдослучайного шумового сигнала $\tilde{\xi}(t)$ и результаты измерений представлены в дискретной форме в виде вектора скалярных значений $X = x_1, x_2, \ldots, x_n$ как независимых и одинаково распределённых реализаций случайной величины $\tilde{\xi}$. Необходимо определить, какой из гипотез, H_0 или H_1, соответствуют полученные результаты измерений:

$$H_0 : \tilde{\xi} \sim f_0(x);\ H_1 : \xi \sim f_1(x). \tag{4}$$

Аналитические исследования

Как следует из результатов наших предыдущих исследований [26; 39], алгоритм принятия решений, который позволяет определить индекс гипотезы (например, 0 или 1) для любого вектора измерений $x_i \in R^n, i=1,2,...,n$ из множества R^n, можно назвать детектором. Математически это будет отображение $F: R^n \to \{0,1\}$. Наборы

$$R_0 = \{\xi \in R^n | F(\xi) = 0\};\ R_1 = \{\xi \in R^n | F(\xi) = 1\} \quad (5)$$

некоторым образом формируют непересекающееся разделение множества R^n на две области: $R^n = R_0 \cup R_1$ и полностью будут описывать детектор F. Набор R_1 называют критической областью, потому что детектор решает H_1 тогда и только тогда, когда $\tilde{\xi} \in R_1$.

Детектор может совершить ошибки двух типов: ложные тревоги и пропущенные обнаружения информационных сигналов. Вероятность ложной тревоги P_α – это вероятность того, что случайная переменная $\tilde{\xi}$, распределённая согласно $f_0(x)$, оценивается как информационный сигнал (детектор принимает гипотезу H_1), в то время как вероятность пропущенного обнаружения P_β является вероятностью, что случайная переменная $\tilde{\xi}$, распределённая согласно $f_1(x)$, неправильно обнаружена как естественный шум $n(t)$:

$$P_\alpha = P\{F(\xi) = 1 | \xi \approx f_0\} = \int_{R_1} f_0(x)dx\ ; \quad (6)$$

$$P_\beta = P\{F(\xi) = 0 | \xi \approx f_1\} = \int_{R_0} f_1(x)dx = 1 - \int_{R_1} f_1(x)dx\ . \quad (7)$$

Представляется целесообразным в дополнение к байесовским критериям при оценке расхождения между распределениями $f_0(x)$ или $f_1(x)$, когда в качестве показателя используется отношение правдоподобия, рассмотреть информационный подход, при котором критерием эффективности защиты информации за счёт маскирующих помех может служить изменение энтропии. В качестве показателя может выступить относительная энтропия или дивергенция (КЛ отклонение) Кульбака-Лейблера $D_{KL}(f_0 \| f_1)$. Этот показатель может служить мерой расхождения (различия) между двумя распределениями вероятностей $f_0(x)$ и $f_1(x)$:

$$D_{KL}(f_0 \| f_1) = \sum_x f_0(x) \log \frac{f_0(x)}{f_1(x)}. \quad (8)$$

Предполагается, что чем меньше разница между $f_0(x)$ и $f_1(x)$, тем больше вероятность ошибочного решения условного противника о наличии скрываемой информации в наблюдаемом псевдослучайном шумовом сигнале. В идеальной ситуации, когда $D_{KL}(f_0 \| f_1) = 0$, можно считать систему маскирования необнаруживаемой и абсолютно безопасной, потому что в этом случае распределения $f_0(x)$ и $f_1(x)$ совершенно

идентичны и неразличимы по критерию Кульбака-Лейблера.

В реальной ситуации принято говорить о так называемом ε-уровне безопасности системы маскирования информации, когда выполняется неравенство

$$D_{KL}(f_0 \| f_1) \le \varepsilon. \tag{9}$$

Чтобы установить связь данного показателя с вероятностями ошибок первого и второго рода, предположим, во-первых, что в канале передаётся только шум с распределением $f_0(x)$. В этом случае вероятность гипотезы H_1 будет равна $f_0(1) = P_\alpha$, а вероятность H_0 будет составлять $f_0(0) = 1 - P_\alpha$. Во-вторых, при передаче зашумлённого информационного сигнала с распределением $f_1(x)$ эти вероятности будут составлять $f_1(1) = 1 - P_\beta$ и $f_1(0) = P_\beta$ соответственно. Полная группа событий будет составлять

$$f_0(x) = (f_0(0), f_0(1)) = (1 - f_0(1), f_0(1)); \tag{10}$$

$$f_1(x) = (f_1(0), f_1(1)) = (f_1(0), 1 - f_1(0)), \tag{11}$$

и можно вычислить в соответствии с (8) дивергенцию Кульбака-Лейблера $d_{KL}(P_\alpha, P_\beta)$ для результатов оптимального детектора в рассмотренной ситуации:

$$d_{KL}(P_\alpha, P_\beta) = \sum_{x \in X} f_0(x) \log \frac{f_0(x)}{f_1(x)} = (1 - P_\beta) \log \frac{1 - P_\beta}{P_\alpha} + P_\beta \log \frac{P_\beta}{1 - P_\alpha}. \tag{12}$$

Поскольку работа любого оптимального детектора связана с выполнением определённого алгоритма обработки сигналов, а из теории информации известно, что детерминированная обработка не может увеличить энтропию, то можно записать:

$$d_{KL}(P_\alpha, P_\beta) \le D_{KL}(f_0 \| f_1) \le \varepsilon. \tag{13}$$

Неравенство (13) принципиально ограничивает возможности любого оптимального детектора, который может использоваться при несанкционированном доступе к замаскированной информации. Если исходить из ограничения максимального значения ошибки первого рода $0 < P_\alpha < c_\alpha$, как это принято в критерии Неймана-Пирсона [40; 41], минимально возможная вероятность ошибки второго рода может быть определена из следующего выражения:

$$P_\beta(P_\alpha) = \arg \min_{P_\beta \in [0,1]} \{P_\beta \mid d_{KL}(P_\alpha, P_\beta) \le \varepsilon\}, \tag{14}$$

где минимум берётся по всем вариантам оптимальных детекторов, у которых вероятность первого рода составляет P_α. Если достоверность обнаружения информации в псевдошумовом сигнале обозначить $P_D(P_\alpha) = 1 - P_\beta(P_\alpha)$, можно построить семейство графиков зависимости P_D от вероятности ложной тревоги P_α для различных значений $\varepsilon \in (0,1)$ (рисунок 1).

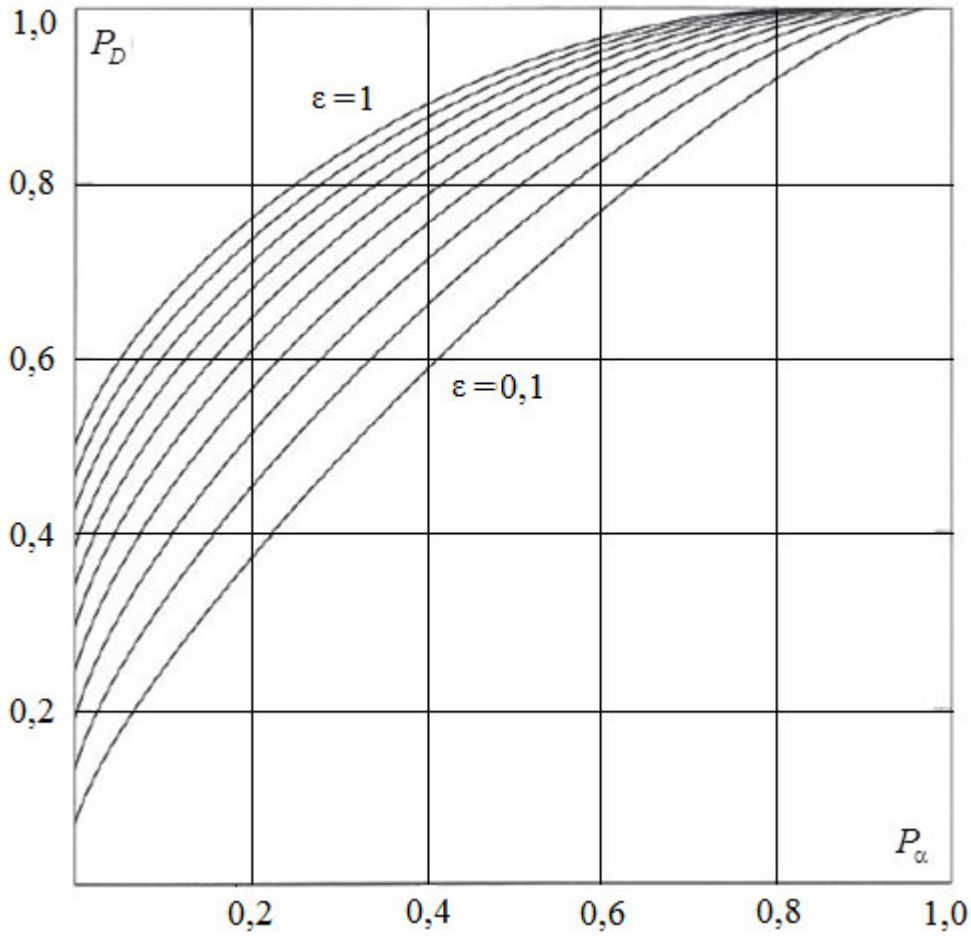

Рисунок 1 – Характеристическими кривые обнаружения (ХКО).

Математической формой этих графиков служит выражение (14). Из графиков следует, что при любом значении $\varepsilon\in(0,1)$ область под каждой соответствующей кривой ХКО определяет максимально достижимые возможности оптимального детектора по достоверности обнаружения. Кроме того, очевидно, что невозможно при разработке оптимального детектора свести к минимуму одновременно обе ошибки, необходимо искать компромисс между допустимыми значениями вероятностей ошибок первого и второго рода. В частности, если в системе распознавания условного противника будет принято нулевое значение вероятности ложной тревоги $P_\alpha = 0$, вероятность достоверного обнаружения не может превысить значение $P_D \le 1 - e^{-\varepsilon}$.

Если подставить значение $\varepsilon = 0$ в (13), то исходя из того, что энтропия не может быть отрицательной, следует равенство $d_{KL}(P_\alpha, P_\beta) = D_{KL}(f_0 \| f_1) = 0$. Как следует из теории информации, это возможно только в том случае, если распределения $f_0(x)$ и $f_1(x)$ полностью идентичны или для детектора справедливо равенство $P_\beta = 1 - P_\alpha$. В этом случае работа детектора будет основана на случайном угадывании.

В общем случае из неравенства $d_{KL}(P_\alpha, P_\beta) \le D_{KL}(f_0 \| f_1) \le \varepsilon$ следует, что чем меньше ε $(0<\varepsilon<1)$ или чем ближе два распределения $f_0(x)$ и $f_1(x)$, тем больше вероятность того, что факт наличия скрываемой информации в псевдослучайном шумовом

сигнале не будет обнаружен. Поэтому, несмотря на то, что дивергенция Кульбака-Лейблера не является метрикой в математическом значении этого слова, потому что выражение $D_{KL}(f_0\|f_1)$ не удовлетворяет свойству симметрии и неравенству треугольника [12; 39], тем не менее этот показатель может использоваться при оценке эффективности маскирования информации особенно при выполнении сравнительного анализа различных систем маскирования информационного сигнала.

Существует некоторое противоречие между оценками эффективности защиты телекоммуникационной системы от утечки по ТК с помощью показателя в виде КЛ дивергенции по результатам работы детектора для бесконечно большого и конечного числа наблюдений. Вводя критерий Кульбака-Лейблера для оценки уровня безопасности маскирования, предполагаем, что система мер защиты $S^{(1)}$ более эффективна, чем $S^{(2)}$, если справедливо неравенство $D_{KL}(f_0\|f_1)^{(1)} \le D_{KL}(f_0\|f_1)^{(2)}$. Такой подход вполне оправдан, если большее значение КЛ дивергенции предполагает возможность построения лучшей системы распознавания у вероятного противника.

Для большого числа наблюдений n со стороны условного противника такое предположение асимптотически правильно благодаря лемме Чернова-Стейна (The Chernoff-Stein lemma) [12], которая гласит: если существует ограничение на вероятность ложной тревоги $P_\alpha \le c_\alpha$, то вероятность пропуска обнаружения P_β оптимального детектора Неймана-Пирсона приближается к нулю экспоненциально быстро:

$$\lim_{n\to\infty}\frac{1}{n}\ln P_\beta(c_\alpha) = -D_{KL}(f_0\|f_1);\ P_\beta(c_\alpha) \approx e^{-nD_{KL}(f_0\|f_1)}, \tag{15}$$

что эквивалентно увеличению достоверности обнаружения скрываемой информации.

Для конечного числа наблюдений большее значение КЛ дивергенции не обязательно предполагает возможность построения лучшего детектора. Это можно показать на простом примере. Допустим, задано множество случайных чисел $C=\{1,2,...,N\}$ и на этом множестве определены два закона распределения:

$$g_N(i)=1/N, i=1,2,...,N; \tag{16}$$

$$h_N(i)=\begin{cases}1/N+\delta_N, i=1;\\ 1/N-\delta_N, i=2;\\ 1/N, i=3,4,...,N.\end{cases} \tag{17}$$

Нетрудно вычислить КЛ дивергенцию для этих распределений:

$$D_{KL}(g_N\|h_N) = -(1/N)\ln(1-N^2\delta_N^2). \tag{18}$$

Чтобы по результатам одного наблюдения x сделать обоснованный выбор между двумя гипотезами $H_0: x\in g_N$ и $H_1: x\in h_N$, можно использовать байесовский критерий отношения правдоподобия [26; 42]:

$$L(x)=h_N(x)/g_N(x)=(1/N\pm\delta_N)/(1/N)=1\pm\delta_N\geq\gamma. \quad (19)$$

При любом значении порога γ в критерии отношения правдоподобия результат будет одинаков: $P_\alpha + P_\beta \geq 1 - \delta_N$, $P_D - P_\alpha \leq \delta_N$ [12]. Если выбрать величину расхождения между двумя распределениями в виде убывающей функции *N*:

$$\delta_N = (1/N)\sqrt{1-e^{-N^2}}, \quad (20)$$

то КЛ-дивергенция будет равна $D_{KL}(g_N\|h_N)=N$.

Анализ полученных соотношений позволяет сделать следующие выводы. С ростом числа наблюдений *N* КЛ дивергенция между распределениями g_N и h_N растёт до бесконечности, однако при этом вероятность распознавания на основе однократного наблюдения P_D уменьшается до случайного угадывания:

$$P_D-P_\alpha\leq\delta_N;\ \lim_{N\to\infty}\delta_N=0;\ 1-P_\beta-P_\alpha=0;\ P_\beta+P_\alpha=1. \quad (21)$$

Доказывается [12; 39], что КЛ дивергенция является функцией коэффициента изменения δ, который показывает глубину вносимых в исходный сигнал изменений, связанных с процедурой маскирования передаваемой информации активными методами защиты. Если ввести минимально допустимый коэффициент изменений $\delta_0\geq 0$, то можно предположить, что КЛ дивергенция будет ограничена снизу величиной $D_{KL}\left(f_0\|f_{\delta_0}\right)$. Обращаясь снова к лемме Чернова-Стейна, можно утверждать, что для любого заданного ограничения на вероятность ложной тревоги $0<P_\alpha<1$ система распознавания условного противника может достичь сколь угодной малой вероятности пропуска обнаружения P_β за счёт увеличения числа наблюдений (вероятность обнаружения будет стремиться к единице).

Допустим, что результаты измерений сигнала в системе распознавания условного противника представлены в виде независимых одинаково распределённых реализаций $x(i), i=1,\ldots,n$, скалярной случайной величины *X* с функцией плотности вероятности $f_0(x)$ или $f_\delta(x)$. В этом случае возникает проблема выбора между двумя гипотезами: $H_0:\delta=0$ и $H_1:\delta>0$, при условии, что коэффициент изменений δ известен. Оптимальный детектор в этом случае будет при использовании критерия отношения правдоподобия [12]:

$$L_\delta(x)=\sum_{i=1}^{n}\ln\frac{f_\delta\{x(i)\}}{f_0\{x(i)\}}. \quad (22)$$

Для малых значений коэффициента δ и большого числа наблюдений *n* функция $L_\delta(x)/n$ приближается к распределению Гаусса с одинаковыми значениями дисперсии для гипотез H_0 и H_1: $D_0=D_1=(1/n)\delta^2 I(0)$ и математическими ожиданиями

$m_0 = (-1/2)\delta^2 I(0)$ для гипотезы H_0, $m_1 = (1/2)\delta^2 I(0)$ для гипотезы H_1, где $I(\delta)$ – информация Фишера для однократного наблюдения:

$$I(\delta) = \sum_x \frac{1}{f_\delta(x)} \left\{ \frac{\partial f_\delta(x)}{\partial \delta} \right\}^2 = \sum_x f_\delta(x) \left\{ \frac{\partial \log f_\delta(x)}{\partial \delta} \right\}^2. \quad (23)$$

Между КЛ дивергенцией и информацией Фишера существует связь:

$$D_{KL}(f_0 \| f_\delta) = D_{KL}(f_\delta \| f_0) = (\delta^2 / 2) I(0). \quad (24)$$

Можно сделать вывод, что при малых значениях δ проверка отношения правдоподобия сводится к вычислению смещения среднего значения Гауссианы:

$$m_0 = (-1/2)\delta^2 I(0) \text{ или } m_1 = (1/2)\delta^2 I(0). \quad (25)$$

Качество работы детектора может быть полностью описано с помощью коэффициента отклонения

$$d^2 = n\delta^2 I(0). \quad (26)$$

Можно отметить, что большое значение коэффициента отклонения подразумевает более точную работу детектора и, таким образом, менее безопасную систему защиты от утечки по техническим каналам. Из этого следует вывод, что для малых значений коэффициента δ системы маскирования с огромной информацией Фишера менее безопасны, чем с малой величиной $I(0)$, что делает показатель (23) полезным для сравнительного анализа. Кроме того, значение информации Фишера определяет в соответствии с правилом Рао-Крамера нижнюю границу дисперсии любой несмещённой оценки $\hat{\delta}$ коэффициента изменения δ:

$$D\{\hat{\delta}\} \geq 1/nI(0). \quad (27)$$

В общем случае для параметризованной функции плотности вероятности $f(x, \theta)$ можно записать:

$$I(\theta) = M\left\{ (\partial \ln f(x, \theta) / \partial \theta)^2 \right\}_- \quad (28)$$

информация Фишера является мерой скорости изменения функции плотности вероятности $f(\xi, \theta)$ по причине изменения параметра θ в случайной величине *x*. Информация Фишера всегда неотрицательна и суммируется при осуществлении независимых наблюдений. Для результатов в виде независимых одинаково распределённых реализаций случайной величины $x(i), i = 1, \ldots, n$ можно записать

$$f(x,\theta)=\prod_{i=1}^{n} f(x_i,\theta);\ \ln f(x,\theta)=\sum_{i=1}^{n}\ln f(x_i,\theta);\ I(\theta)=\sum_{i=1}^{n} I_i(\theta), \qquad (29)$$

где $I_i(\theta)$ – информация Фишера по каждому наблюдению.

Если рассмотреть две случайные величины с нормальными законами распределения $f_1(x)$, $f_2(x)$ и различными параметрами $m_1, m_2, \sigma_1^2, \sigma_2^2$, то проверка их различимости по критерию КЛ отклонения позволяет получить:

$$D_{KL}\left(f_1 \| f_2\right)=\frac{1}{2}\left\{\ln\frac{\sigma_2^2}{\sigma_1^2}+\frac{\sigma_1^2}{\sigma_2^2}-1+\frac{(m_2-m_1)^2}{\sigma_2^2}\right\}. \qquad (30)$$

Заключение

Использование такого показателя, как дивергенция Кульбака-Лейблера для оценки уровня безопасности телекоммуникационной системы с точки зрения предотвращения утечки информации по техническим каналам, позволяет выполнять сравнительный анализ эффективности различных подходов к реализации активных методов защиты информации. При этом не следует забывать о свойственных данному подходу ограничениях: достоверность обнаружения информационного сигнала в маскирующем псевдошуме не является абсолютной. Для более эффективной работы оптимального детектора необходимо заранее выбрать (и заложить в модель соответствующие распределения критериальных вероятностей), ошибки какого типа будут являться менее допустимыми: ложные срабатывания или пропущенные обнаружения.

Кроме того, для снижения погрешности анализа, можно параллельно использовать другие методы технической защиты как активной, так и пассивной. Одним из наиболее перспективных направлений исследований представляется применение методов машинного обучения, в частности нейросетевого инструментария распознавания образов. В этом случае проблема обнаружения будет рассматриваться как классификационная задача и может решаться обучением классификатора на больших базах данных для распределений «естественный шум/замаскированный информационный сигнал». Дополнительной мерой может быть использование точной регулировки параметров классификатора с целью обеспечения минимально допустимой вероятности ложных срабатываний.

Список источников:

1. Бакшеев, А. С. Разработка методики контроля уровня защищенности информации объектов критической информационной инфраструктуры / А. С. Бакшеев, И. И. Лившиц // Вопросы кибербезопасности. – 2023. – № 2(54). – С. 85-98. – DOI 10.21681/2311-3456-2023-2-85-98. – EDN KQLCWV.

2. Бочкарев, А. М. Оценка влияния факторов НДДВ анализа на эффективность системы управления информационным обеспечением промышленного предприятия / А. М. Бочкарев // Форпост науки. – 2022. – № 4(62). – С. 35-39. – DOI 10.36683/2076-5347-2022-4-62-35-39. – EDN EWZXGD.

3. Жаринов, И. О. Критерий эффективности управления экономической системой с полисубъектным социо-киберфизическим менеджментом / И. О. Жаринов // Вестник Орел-ГИЭТ. – 2022. – № 3(61). – С. 36-42. – DOI 10.36683/2076-5347-2022-3-61-36-42. – EDN IVTEZG.

4. Илюхин, А. А. Проблемы и прогнозы развития технологий беспроводных коммуникаций в рамках реализации национального проекта "Цифровая экономика" / А. А. Илюхин, Н. А. Илюхина // Экономическая среда. – 2022. – № 2(40). – С. 4-13. – DOI 10.36683/2306-1758/2022-2-40/4-13. – EDN WFTANI.

5. Дворников, С. В. Управление параметрами устойчивости инфокоммуникационной системы в условиях деструктивных воздействий / С. В. Дворников, С. А. Якушенко // Радиотехника. – 2023. – Т. 87, № 6. – С. 23-31. – DOI 10.18127/j00338486-202306-03. – EDN EXKZOH.

6. Кругликов, С. В. Методический подход к комплексному описанию объекта информационной защиты / С. В. Кругликов, С. Н. Касанин, Ю. В. Кулешов // Вопросы кибербезопасности. – 2022. – № 4(50). – С. 39-51. – DOI 10.21681/2311-3456-2022-4-39-51. – EDN XNTZSU.

7. Лубенцов, А. В. Синтез метода оценки эффективности системы информационной безопасности / А. В. Лубенцов // Известия высших учебных заведений. Электроника. – 2024. – Т. 29, № 1. – С. 118-129. – DOI 10.24151/1561-5405-2024-29-1-118-129. – EDN UJNZBJ.

8. Железняк, В. К. Защита информации от утечки по техническим каналам / В. К. Железняк. – Санкт-Петербург : Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2006. – 187 с. – ISBN 5-8088-0230-X. – EDN QMQZGT.

9. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия - Телеком, 2012. – 196 с. – ISBN 978-5-9912-0240-4. – EDN RBAWTZ.

10. Хорев, А. А. Техническая защита информации : Том 1. Технические каналы утечки информации / А. А. Хорев. – Москва : НПЦ "Аналитика", 2008. – 435 с. – EDN QMTDKT.

11. Ворона, В. А. Способы и средства защиты информации от утечки по техническим каналам / В. А. Ворона, В. О. Костенко // Computational Nanotechnology. – 2016. – № 3. – С. 208-223. – EDN WKNGZD.

12. Fridrich, J. Steganography in digital media: Principles, algorithms, and applications / J. Fridrich // Cambridge: Cambridge University Press, 2009. – 450 p. – ISBN 978-0-521-19019-0. – DOI 10.1017/CBO9781139192903.

13. Таранов, А. Б. Определение граничных условий при мажорирующей оценке коэффициентов ослабления уровней побочных электромагнитных излучений технических средств / А. Б. Таранов, О. О. Басов // Вопросы защиты информации. – 2015. – № 3(110). – С. 85-90. – EDN UXLMKX.

14. Дамм, В. А. Модель канала утечки информации за счет паразитной модуляции, возникающей при работе криптографических средств / В. А. Дамм, В. А. Шалагинов // Вопросы защиты информации. – 2007. – № 4(79). – С. 22-27. – EDN KAQTAJ.

15. Паршуткин, А. В. Повышение защищенности информации от утечки через побочные электромагнитные излучения / А. В. Паршуткин, М. Р. Неаскина // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 82-89. – DOI 10.21681/2311-3456-2022-3-82-89. – EDN ARQCJO.

16. An adaptive error-based observer method in electro-optical tracking system / W. Xia, Ya. Mao, M. Tang [et al.] // Measurement. – 2024. – Vol. 232. – P. 114638. – DOI 10.1016/j.measurement.2024.114638. – EDN WMYKPZ.

17. Ibrahimov, B. G. Research methods for increasing the security of communication systems important objects of critical information infrastructure / B. G. Ibrahimov, T. H. Mammadov // T-Comm. – 2024. – Vol. 18, No. 6. – P. 61-66. – DOI 10.36724/2072-8735-2024-18-6-61-66. – EDN AMPBTO.

18. Махов, Д. С. Анализ некриптографических методов защиты информации в радиоканалах информационных систем / Д. С. Махов // Вопросы кибербезопасности. – 2024. – № 1(59). – С. 82-88. – DOI 10.21681/2311-3456-2024-1-82-88. – EDN SJOITN.

19. Ненадович, Д. М. Методика формирования оценочных значений экспертных показателей производительности перспективных автоматизированных цифровых телекоммуникаионных систем / Д. М. Ненадович, И. В. Маркин // Вестник Тамбовского государственного технического университета. – 2021. – Т. 27, № 3. – С. 368-379. – DOI 10.17277/vestnik.2021.03.pp.368-379. – EDN NTFDQP.

20. Kozachok, A. V. Model of Pseudo-Random Sequences Generated by Encryption and Compression Algorithms / A. V. Kozachok, A. A. Spirin // Programming and Computer Software. – 2021. – Vol. 47, No. 4. – P. 249-260. – DOI 10.1134/S0361768821040058. – EDN LMELHQ.

21. Аналитическое описание функций информационной эффективности телекоммуникационных систем с различными структурами / А. М. Межуев, А. В. Коренной, Т. Ю. Урывская, Д. Л. Стуров // Радиотехника. – 2022. – Т. 86, № 9. – С. 113-125. – DOI 10.18127/j00338486-202209-12. – EDN UZMGOG.

22. Event-triggered sequential fusion filter for nonlinear multi-sensor system with random packet dropout and composite correlated noise / W. Liu, Yu. Yang, Sh. Wang, Sh. Song // Digital Signal Processing. – 2024. – Vol. 150. – P. 104522. – DOI 10.1016/j.dsp.2024.104522. – EDN YOKCCW.

23. Sensor fusion noise suppression method based on finite impulse response complementary filters / J. Wang, L. Wang, J. Lin [et al.] // Measurement. – 2024. – Vol. 232. – P. 114680. – DOI 10.1016/j.measurement.2024.114680. – EDN ESBRPM.

24. Dual-functional radar-communication based on frequency modulated continuous wave exploiting constraint frequency hopping / R. Xu, R. Wen, G. Li [et al.] // Signal Processing. – 2024. – Vol. 219. – P. 109403. – DOI 10.1016/j.sigpro.2024.109403. – EDN PYKQHZ.

25. Костогрызов, А. И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии / А. И. Костогрызов // Вопросы кибербезопасности. – 2022. – № 6(52). – С. 71-82. – DOI 10.21681/2311-3456-2022-6-71-82. – EDN SGNKNH.

26. Лисичкин, В. Г. Модель оценки достоверности контроля параметров телекоммуникационных систем на основе вероятностно-статистического подхода / В. Г. Лисичкин // T-Comm: Телекоммуникации и транспорт. – 2014. – Т. 8, № 12. – С. 51-54. – EDN TFKKPZ.

27. Сьерра-Теран, К. М. Статистические характеристики системы относительной передачи информации на основе хаотических импульсов в канале с гауссовским шумом / К. М. Сьерра-Теран, А. И. Рыжов // Журнал радиоэлектроники. – 2022. – № 9. – DOI 10.30898/1684-1719.2022.9.1. – EDN PAOUVX.

28. Тихонов, В. И. Статистический анализ и синтез радиотехнических устройств и систем / В. И. Тихонов, В. Н. Харисов ; В. И. Тихонов, В. Н. Харисов. – 2-е изд., испр. – Москва : Радио и связь, 2004. – ISBN 5-256-01701-2. – EDN QMNTAT.

29. Уханов, Е. В. Статистические характеристики сигнала на выходе оптимальной радиолокационной системы распознавания подвижных воздушных объектов / Е. В. Уханов // T-Comm: Телекоммуникации и транспорт. – 2023. – Т. 17, № 4. – С. 26-31. – DOI 10.36724/2072-8735-2023-17-4-26-31. – EDN JBGOXA.

30. Глушанков, Е. И. Анализ качества алгоритмов адаптивной пространственной и пространственно-частотной фильтрации сигналов в системах спутниковой навигации / Е. И. Глушанков, В. И. Царик // Труды учебных заведений связи. – 2022. – Т. 8, № 3. – С. 37-43. – DOI 10.31854/1813-324X-2022-8-3-37-43. – EDN KJNXBY.

31. Использование информационного резервирования для повышения надежности устройств хранения, обработки и передачи информации / А. А. Павлов, А. Н. Царьков, Ю. А. Романенко [и др.] // Радиотехника. – 2024. – Т. 88, № 2. – С. 127-137. – DOI 10.18127/j00338486-202402-16. – EDN BMLFXR.

32. Чехонина, Е. А. Обзор состязательных атак и методов защиты для детекторов объектов / Е. А. Чехонина, В. В. Костюмов // International Journal of Open Information Technologies. – 2023. – Т. 11, № 7. – С. 11-20. – EDN HEACZA.

33. Borecki, M. Variety of attenuation of RF suppression filters / M. Borecki, Ja. Sroka // Measurement. – 2024. – Vol. 232. – P. 114584. – DOI 10.1016/j.measurement.2024.114584. – EDN MOMPYE.

34. Bayesian Recognition of the State of the Information-Measuring System of a Moving Object: Study of the Algorithm for Correcting the Weight of A Priori Information / O. V. Ermolin, S. M. Muzhichek, V. I. Pavlov [et al.] // Journal of Computer and Systems Sciences International. – 2022. – Vol. 61, No. 4. – P. 505-511. – DOI 10.1134/s1064230722040062. – EDN SRMOYK.

35. Калинин, В. И. Корреляционная оценка при передаче дискретной информации на основе шумовых хаотических сигналов с временными окнами / В. И. Калинин, О. А. Бышевский-Конопко // Журнал радиоэлектроники. – 2021. – № 8. – DOI 10.30898/1684-1719.2021.8.12. – EDN ZCGDST.

36. Artyushenko, V. M. Quasi-optimal on polygaussian algorithms for receiving discrete signals / V. M. Artyushenko, V. I. Volovach // Radioengineering. – 2021. – Vol. 85, No. 3. – P. 158-159. – DOI 10.18127/j00338486-202103-15. – EDN ULEVJB.

37. Tian, T. Fusion estimation against mixed network attacks for systems with random parameter matrices, correlated noises, and quantized measurements / T. Tian, Sh. Sun // Digital Signal Processing. – 2024. – Vol. 150. – P. 104523. – DOI 10.1016/j.dsp.2024.104523. – EDN KVVMCA.

38. Будников, С. А. Методика оценки эффективности систем безопасности автоматизированных систем управления / С. А. Будников, С. М. Коваленко, А. И. Бочарова // Вопросы кибербезопасности. – 2023. – № 3(55). – С. 2-12. – DOI 10.21681/2311-3456-2023-3-2-12. – EDN QLNWEP.

39. Лисичкин, В. Г. К вопросу о выборе критерия при разработке оптимального детектора для стегоанализа / В. Г. Лисичкин // Фундаментальные и прикладные проблемы техники и технологии. – 2019. – № 5(337). – С. 47-53. – EDN HIEUEE.

40. Куликов, Е. И. Оценка параметров сигналов на фоне помех / Е. И. Куликов, А. П. Трифонов. – Москва : Советское Радио, 1978. – 296 с.

41. Тихонов, В. И. Статистическая радиотехника / В. И. Тихонов. – Москва : Радио и связь, 1982. – 624 с.

42. Акименко, Т. А. Байесовский подход при оценке достоверности двухпараметрового резонансного контроля / Т. А. Акименко, А. А. Горшков, В. Г. Лисичкин // Известия Тульского государственного университета. Технические науки. – 2015. – № 8-1. – С. 208-216. – EDN VHVHHB.

References:

1. Baksheev A.S., Livshitz I.I. Development of a methodology for monitoring the level of information security of critical information infrastructure objects. *Voprosy kiberbezopasnosti*, 2023, no. 2(54), pp. 85-98. https://doi.org/10.21681/2311-3456-2023-2-85-98.

2. Bochkarev A.M. Assessment of the Impact of the ASAD Analysis Factors on the Effectiveness of Information Management System of an Industrial Enterprise. *Science Outpost*, 2022, no. 4 (62), pp. 35-39. https://doi.org/10.36683/2076-5347-2022-4-62-35-39.

3. Zharinov I.O. Managerial Effectiveness Criterion of Economic System with Multi-Subject Socio-Cyberphysical Management. *OrelSIET bulletin*, 2022, no. 3 (61), pp. 36-42. https://doi.org/10.36683/2076-5347-2022-3-61-36-42.

4. Ilyukhin A.A., Ilyukhina N.A. Development problems and forecasts of wireless communication technologies in the framework of the national project digital economy. *Economic environment,* 2022, no. 2 (40), pp. 4-13. https://doi.org/10.36683/2306-1758/2022-2-40/4-13.

5. Dvornikov S.V., Yakushenko S.A. An approach to managing the stability parameters of complex infocommunication systems under destructive influences. *Radiotekhnika*, 2023, vol. 87, no. 6, pp. 23-31, https://doi.org/10.18127/j00338486-202306-03.

6. Kruglikov S.V., Kasanin S.N., Kuleshov Yu.V. Methodical approach to the complex description of information protection object. *Voprosy kiberbezopasnosti,* 2022, no. 4(50), pp. 39-51, https://doi.org/10.21681/2311-3456-2022-4-39-51.

7. Lubentsov A.V. Synthesis of a method for evaluating the effectiveness of an information security system. *Proceedings of universities. Electronics*, 2024, vol. 29, no. 1, pp. 118-129, https://doi.org/10.24151/1561-5405-2024-29-1-118-129.

8. Zheleznyak V.K. *Protection of information from leakage through technical channels,* St. Petersburg: St. Petersburg State University of Aerospace Instrumentation, 2006. 187 p. ISBN 5-8088-0230-X. Available from: https://www.elibrary.ru/QMQZGT.

9. Vorona V.A., Tikhonov V.A. *Conceptual foundations of creation and application of an object protection system,* Moscow: Hotline-Telecom, 2012. 196 p. ISBN 978-5-9912-0240-4. Available from: https://www.elibrary.ru/RBAWTZ.

10. Khorev A.A. *Technical protection of information,* vol. 1. Technical channels of information leakage, Moscow: NPC "Analytika. 2008. 435 p. Available from: https://www.elibrary.ru/QMTDKT.

11. Vorona V.A., Kostenko, V.O. “Ways and means of information protection from leaks

through technical channels. *Computational nanotechnology,* 2016, no. 3, pp. 208-223. Available from: https://www.elibrary.ru/WKNGZD.

12. Fridrich J. *Steganography in Digital Media: Principles, Algorithms, and Applications,* Cambridge: Cambridge University Press, 2010. 450 p. ISBN 978-0-521-19019-0. https://doi.org/10.1017/CBO9781139192903.

13. Taranov A.B., Basov O.O. The definition of boundary conditions in the majorizing estimate of the extinction coefficient levels of side electromagnetic radiation technical means. *Information security questions,* 2015, no. 3 (110), pp. 85-90. Available from: https://www.elibrary.ru/UXLMKX.

14. Damm V.A., Shalaginov V.A. Model of information leakage channel due to parasitic modulation arising during operation of cryptographic tools. *Information security questions,* 2007, no. 4(79), pp. 22-27. Available from: https://www.elibrary.ru/KAQTAJ.

15. Parshutkin A.V., Neaskina M.R. Increasing the security of information from leakage through side electromagnetic emissions. *Voprosy kiberbezopasnosti*, 2022, no. 3(49), pp. 82-89. https://doi.org/10.21681/2311-3456-2022-3-82-89.

16. Xia W., Mao Y., Tang M., Zhang B., Liu C. An adaptive error-based observer method in electro-optical tracking system. *Measurement*, 2024, vol. 232, pp. 114638. https://doi.org/10.1016/j.measurement.2024.114638.

17. Ibrahimov B.G., Mammadov T.H. Research methods for increasing the security of communication systems important objects of critical information infrastructure. *T-Comm*, 2024, vol. 18, no. 6, pp. 61-66. https://doi.org/10.36724/2072-8735-2024-18-6-61-66.

18. Makhov D.S. Analysis of non-cryptographic information protection methods in wireless information systems. *Voprosy kiberbezopasnosti*, 2024, no. 1(59), pp. 82-88. https://doi.org/10.21681/2311-3456-2024-1-82-88.

19. Nenadovich D.M., Markin I.V. Methodology for the Formation of Assessment Values of Expert Performance Indicators for Perspective Automated Digital Telecommunication Systems. *Transactions of the Tambov State Technical University*, 2021, vol. 27, no. 3, pp. 368-379. https://doi.org/10.17277/vestnik.2021.03.pp.368-379.

20. Kozachok A.V., Spirin A.A. Model of Pseudo-Random Sequences Generated by Encryption and Compression Algorithms. *Programming and Computer Software,* 2021, vol. 47, no. 4, pp. 249-260. https://doi.org/10.1134/S0361768821040058.

21. Mezhuev A.M., Korennoi A.V., Uryvskaya T.Yu., Sturov D.L. The analytical description of functions of information efficiency of telecommunication systems with various structures. *Radiotekhnika*, 2022, vol. 86, no. 9, pp. 113-125. https://doi.org/10.18127/j00338486-202209-12.

22. Liu W., Yang Y., Wang S., Song S. Event-triggered sequential fusion filter for nonlinear multi-sensor system with random packet dropout and composite correlated noise. *Digital Signal Processing*, 2024, vol. 150, pp. 104522. https://doi.org/10.1016/j.dsp.2024.104522.

23. Wang J., Wang L., Lin J., Xiao R., Chen J., Jin P. Sensor fusion noise suppression method based on finite impulse response complementary filters. *Measurement,* 2024, vol. 232, pp. 114680. https://doi.org/10.1016/j.measurement.2024.114680.

24. Xu R., Wen R., Li G., Chu C., Wen G. Dual-functional radar-communication based on frequency modulated continuous wave exploiting constraint frequency hopping. *Signal Processing*, 2024, vol. 219, pp. 109403, https://doi.org/10.1016/j.sigpro.2024.109403.

25. Kostogryzov A.I. On models and methods of probabilistic analysis of information security in standardized processes of system engineering. *Voprosy kiberbezopasnosti*, 2022, no. 6(52), pp. 71-82, https://doi.org/10.21681/2311-3456-2022-6-71-82. Available from: https://www.elibrary.ru/SGNKNH.

26. Lisichkin V.G. Control reliability estimation model of telecommunication system paramters on basis of possibilisticstatistical approach. *T-Comm*, 2014, vol. 8, no. 12, pp. 51-54. Available from: https://www.elibrary.ru/TFKKPZ.

27. Sierra-Teran C.M., Ryzhov A.I. Statistical characteristics of differentially coherent communication system based on chaotic radio pulses over a channel with Gaussian noise. *Journal of Radio Electronics*, 2022, no. 9. https://doi.org/10.30898/1684-1719.2022.9.1.

28. Tikhonov V.I., Kharisov V.N. *Statistical analysis and synthesis of radio engineering*

devices and systems, Moscow: Radio and Communications, 1991. 608 p. ISBN 5-256-01701-2. Available from: https://www.elibrary.ru/QMNTAT.

29. Ukhanov E.V. Statistical characteristics of the signal at the output of the optimal radar system for identifying mobile air objects. *T-comm*, 2023, vol. 17, no. 4, pp. 26-31. https://doi.org/10.36724/2072-8735-2023-17-4-26-31.

30. Glushankov E.I., Tsarik V.I. Quality analysis of space and space-frequency adaptive signal processing algorithms in satellite navigation systems. *Proceedings of Telecommunication Universities*, 2022, vol. 8, no. 3, pp. 37-43, https://doi.org/10.31854/1813-324X-2022-8-3-37-43.

31. Pavlov A.A., Tsarkov A.N., Romanenko Yu.A., Pashintsev V.P., Romanenko A.Yu., Makeev M.I., Pavlov F.A. Use of information re-dundancy to increase the reliability of devices for storing, processing and transmitting information. *Radiotekhnika*, 2024, vol. 88, no. 2, pp. 127-137. https://doi.org/10.18127/j00338486-202402-16.

32. Chekhonina E.A., Kostyumov V.V. Overview of adversarial attacks and defenses for object detectors. *International Journal of Open Information Technologies*, 2023, vol. 11, no. 7, pp. 11-20. Available from: https://www.elibrary.ru/HEACZA.

33. Borecki M., Sroka J. Variety of attenuation of RF suppression filters. *Measurement,* 2024, vol. 232, pp. 114584. https://doi.org/10.1016/j.measurement.2024.114584.

34. Ermolin O.V., Muzhichek S.M., Pavlov V.I., Sebryakov G.G., Skrynnikov A.A., Tolstykh S.V. Bayesian Recognition of the State of the Information-Measuring System of a Moving Object: Study of the Algorithm for Correcting the Weight of A Priori Information. *Journal of Computer and Systems Sciences International*, 2022, vol. 61, no. 4, pp. 505-511, https://doi.org/10.1134/s1064230722040062.

35. Kalinin V.I., Byshevski-Konopko O.A. Correlation estimation for digital communications based on the noise chaotic signals with time windows. *Journal of Radio Electronics,* 2021, no. 8. https://doi.org/10.30898/1684-1719.2021.8.12.

36. Artyushenko V.M., Volovach V.I. Quasi-optimal on polygaussian algorithms for receiving discrete signals. *Radioengineering*, 2021, vol. 85, no. 3, pp. 158-159, https://doi.org/10.18127/j00338486-202103-15.

37. Tian T., Sun S. Fusion estimation against mixed network attacks for systems with random parameter matrices, correlated noises, and quantized measurements. *Digital Signal Processing*, 2024, vol. 150, pp. 104523. https://doi.org/10.1016/j.dsp.2024.104523.

38. Budnikov S.A., Kovalenko S.M., Bocharova A.I. Methodology for assessing the effectiveness of security systems of automated control systems. *Voprosy kiberbezopasnosti*, 2023, no. 3(55), pp. 2-12, https://doi.org/10.21681/2311-3456-2023-3-2-12.

39. Lisichkin V.G. To a question on a criterion choice by working out of the optimum detector for steganalysis. *Fundamental and Applied Problems of Technics and Technology,* 2019, no. 5(337), pp. 47-53. Available from: https://www.elibrary.ru/HIEUEE.

40. Kulikov E.I., Trifonov A.P. *Estimation of signal parameters against the background of interference,* Moscow: Sov. Radio, 1978. 296 p.

41. Tikhonov V.I. *Statistical radio engineering*, Moscow: Radio and Communications, 1982. 624 p.

42. Akimenko T.A., Gorshkov A.A., Lisichkin V.G. Bayesian framework for reliability estimation of two-parameter resonance control. *Izv. Tulsk. Gos. Univ. Tekh. Nauki,* 2015, no. 8-1, pp. 208-216. Available from: https://www.elibrary.ru/VHVHHB.

Статья поступила в редакцию / Received: 01.04.2025
Принята к публикации / Accepted: 26.06.2025
Подписано в печать / Passed for printing: 24.10.2025
Дата выхода в свет / Date of publication: 30.10.2025