Научная статья
УДК 004.056.53; DOI: 10.61260/2218-13X-2026-1-170-181

МАТЕМАТИЧЕСКОЕ ОПИСАНИЕ И КЛАССИФИКАЦИЯ СЛОЖНЫХ ИНФОРМАЦИОННЫХ ПОТОКОВ С УЧЕТОМ ЛОЖНОЙ И ВРЕДОНОСНОЙ ИНФОРМАЦИИ

✉**Ярцева Наталия Андреевна.**
Университет ИТМО, Санкт-Петербург, Россия
✉***karmanova.ifmo@gmail.com***

Аннотация. В современных условиях информационные потоки усложняется недостоверными и вредоносными данными, что негативно влияет на системы управления и информационную безопасность. Необходимы инструменты для фильтрации информации до её обработки. Увеличение ложных и вредоносных сообщений требует эффективных алгоритмов для анализа и управления данными, обеспечивающих устойчивость автоматизированных систем. Цель исследования: создание эффективных математических и вычислительных методов анализа, классификации и управления информацией для повышения надежности систем и достоверности данных. Предложен метод имитационного моделирования, основанный на математической модели с элементами теории вероятностей, где информационный поток делится на достоверную, ложную и вредоносную информацию. Для классификации сообщений применяются вероятностные методы, учитывающие априорные и апостериорные вероятности, а также анализ сетевых, временных и семантических характеристик. В отличие от существующих методов, рассматриваемый фокусируется на анализе данных до их использования, что снижает риск деструктивных воздействий. Разработана математическая модель для анализа информационных потоков, включающих достоверную, ложную и вредоносную информацию. Модель использует вероятностные подходы и учитывает сетевые, временные и семантические характеристики сообщений для их классификации и минимизации деструктивного влияния. Модель позволяет эффективно учитывать особенности каждого источника, выделяя достоверные, ложные и вредоносные сообщения, что обеспечивает высокую точность и надежность результирующего информационного потока. Такое комплексное решение способствует повышению целостности данных и может использоваться в системах управления и информационной безопасности для минимизации влияния деструктивной информации и обеспечения принятия обоснованных решений. Результаты могут использоваться для мониторинга информационных угроз, фильтрации вредоносной информации и обеспечения безопасности критически важных систем, а также поддерживают принятие решений в государственных структурах, экономике и энергетике, повышая доверие к информационным системам.

Ключевые слова: сложный информационный поток, классификация информации, ложная информация, вредоносная информация, достоверная информация, вероятностные модели, информационная безопасность анализ потоков, энтропия

Для цитирования: Ярцева Н.А. Математическое описание и классификация сложных информационных потоков с учетом ложной и вредоносной информации // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2026. № 1. С. 170–181. DOI: 10.61260/2218-13X-2026-1-170-181

Scientific article

MATHEMATICAL DESCRIPTION AND CLASSIFICATION OF COMPLEX INFORMATION FLOWS CONSIDERING FALSE AND HARMFUL INFORMATION

✉**Yartseva Natalia A.**
ITMO University, Saint-Petersburg, Russia
✉***karmanova.ifmo@gmail.com***

Abstract. In modern conditions, information flows are complicated by unreliable and harmful data, which negatively affects management systems and information security. Tools are needed to filter information before it is processed. The increase in false and malicious messages requires effective algorithms for analyzing and managing data that ensure the stability of automated systems. The purpose of the research is to create effective mathematical and computational methods for the analysis, classification and management of information to improve the reliability of systems and the reliability of data. A method of simulation modeling based on a mathematical model with elements of probability theory is proposed, where the information flow is divided into reliable, false and harmful information. To classify messages, probabilistic methods are used, taking into account prior and posteriori probabilities, as well as the analysis of network, temporal and semantic characteristics. Unlike existing methods, this one focuses on analyzing data before it is used, which reduces the risk of destructive impacts. A mathematical model has been developed for the analysis of information flows, including reliable, false and malicious information. The model uses probabilistic approaches and considers the network, temporal and semantic characteristics of messages to classify them and minimize their destructive impact. The model allows you to effectively consider the characteristics of each source, distinguishing reliable, false and malicious messages, which ensures high accuracy and reliability of the resulting information flow. This end-to-end solution improves data integrity and can be used in management and information security systems to minimize the impact of disruptive information and enable informed decision-making. The results can be used to monitor information threats, filter malicious information and ensure the security of critical systems, as well as support decision-making in government agencies, the economy and energy, increasing trust in information systems.

Keywords: complex information flow, classification of information, false information, malicious information, reliable information, probabilistic models, information security, flow analysis, entropy

For citation: Yartseva N.A. Mathematical description and classification of complex information flows considering false and harmful information // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2026. № 1. P. 170–181. DOI: 10.61260/2218-13X-2026-1-170-181

Введение

В современных системах обработки данных и обеспечения информационной безопасности основное внимание обычно уделяется анализу поступившей информации после её интеграции в систему. Такой подход часто игнорирует этап предварительной оценки информационных потоков, что повышает риск проникновения недостоверной, ложной или вредоносной информации. Это может привести к нарушениям в работе системы, снижению качества принимаемых решений и негативным последствиям для связанных процессов. Недостаточная проработка механизмов предварительной проверки данных до их попадания в систему отмечается и в ряде исследований, посвящённых проблеме распространения ложной или вредоносной информации [1–5]. Большинство работ сосредотачивается на анализе таких данных уже после их проникновения в системы, мало внимания уделяя

раннему фильтрованию и оценке. Это указывает на актуальность разработки методик и средств, направленных на предотвращение интеграции вредоносной информации ещё на стадии предварительной обработки.

Результаты исследований, проведенных в последние годы [6–10], подтверждают, что выявление ложной и вредоносной информации о сложных объектах и их состояниях во входящем потоке данных представляет собой сложную задачу, решение которой требует создания специализированных систем защиты. Такие системы призваны обеспечивать достоверность информации вне зависимости от её типа и области применения. Множество авторов отмечают, что для повышения целостности и достоверности информации необходим комплексный системный подход, обусловленный целым рядом факторов [11–13].

Прежде всего, разделение информации на ложную, вредоносную и достоверную – это не самоцель. Оно является лишь средством получения информации, необходимой системе управления для выработки определенного решения, стратегии поведения или стратегии управления, в рассматриваемом случае – обеспечения информационной безопасности. Следовательно, одним из важнейших требований, предъявляемых к системе определения ложной, вредоносной и достоверной информации, является обеспечение ею наибольшей эффективности вышестоящей системы управления.

Кроме того, общая результативность системы защиты данных тесно связана с эффективностью ее отдельных компонентов. К таким компонентам можно отнести устройства для получения сведений об объекте, вычислительную технику и программное обеспечение, каналы передачи данных, а также (в случае использования автоматизированных систем) персонал, обслуживающий систему обнаружения ложной, вредоносной и достоверной информации, средства визуализации нужной информации и другие аналогичные элементы [14].

Для математического описания сложного информационного потока, включающего ложную, вредоносную и достоверную информацию, рассматривается модель, основанная на вероятностных подходах и инструментах теории информации. Далее представлены основные шаги, необходимые для построения этой модели.

Модель информационного потока

Основа метода заключается в том, что сложный информационный поток представляется как совокупность трех категорий информации: достоверной, ложной и вредоносной. Для классификации сообщений используются вероятностные подходы, включая учет априорных и апостериорных вероятностей, а также анализируются сетевые, временные и семантические характеристики потока. Новизна предлагаемого метода заключается в разработке интегрированной математической модели, основанной на вероятностных подходах, инструментах теории информации и методах машинного обучения для описания и управления сложными информационными потоками, включающими достоверную, ложную и вредоносную информацию. Отличительной чертой является использование априорных и апостериорных вероятностей для автоматической классификации сообщений с учетом динамической изменчивости данных. Модель применяет семантический анализ, временные ряды и анализ сетевых связей, что обеспечивает точное выявление ложной и вредоносной информации. Метод также рассматривает оценку качества потока через энтропию, где увеличение неопределенности указывает на рост деструктивной информации. Уникальность подхода также состоит в сочетании теоретических и прикладных инструментов, позволяющих эффективно управлять информационными потоками и повышать их безопасность в условиях цифровых угроз.

Информационный поток представлен автором как последовательность сообщений $\{m_t\}$, где t – метка времени, а каждое сообщение m_t принадлежит обобщенному пространству данных $_{\text{М}}$, которое включает три подмножества:

– M_T – множество достоверных сообщений (поток достоверной информации);

– M_F – множество ложных сообщений (поток ложной информации);

– M_M – множество вредоносных сообщений (поток вредоносной информации).

Каждое сообщение m_t принадлежит одному из этих типов, то есть:

$$M = M_T \cup M_F \cup M_M,$$
$$M_T \cap M_F = \varnothing,$$
$$M_T \cap M_M = \varnothing,$$
$$M_F \cap M_M = \varnothing.$$

Соотношение между этими множествами может быть выражено через вероятности (доли сообщений в общем потоке):

$$P(M_T) + P(M_F) + P(M_M) = 1,$$

где $P(M_T)$, $P(M_F)$, $P(M_M)$ – вероятность того, что случайно выбранное сообщение принадлежит соответствующему множеству.

Вероятностное описание потока

Для каждого сообщения m_t вводится априорная вероятность принадлежности к определенному типу (например, по классификации или внешним характеристикам контента):

$$P(m_t \in M_T),$$
$$P(m_t \in M_F),$$
$$P(m_t \in M_M),$$

где суммы вероятностей равны 1 для каждого t:

$$P(m_t \in M_T) + P(m_t \in M_F) + P(m_t \in M_M) = 1.$$

Сообщения в потоке могут не быть равновероятны, а их классификация может зависеть от дополнительных параметров (контекста или содержимого). Поэтому на каждом шаге t функция вероятности будет зависеть от характеристик сообщения x_t:

$$P(m_t \in M_T | x_t),$$
$$P(m_t \in M_F | x_t),$$
$$P(m_t \in M_M | x_t),$$

где x_t – вектор признаков сообщения.

Вероятностное распределение и классификация

Каждое сообщение m_t характеризуется вектором признаков $x_t \in R^n$, где n – количество характеристик сообщения (например, семантические, лексические, временные или сетевые признаки). Цель состоит в построении вероятностной модели, которая оценивает вероятность того, что сообщение принадлежит одному из классов: достоверному, ложному или вредоносному.

С использованием многоклассовой классификации определяются апостериорные вероятности для каждого сообщения:

$$P(C_k|\mathrm{x}_t), k \in \{T, F, M\},$$

где C_T – класс достоверной информации; C_F – ложной; C_M – вредоносной; x_t – признаки сообщения.

Согласно формуле Байеса:

$$P(C_k|\ x_t) = \frac{P(x_t|\ C_k)P(C_k)}{P(x_t)},$$

где $P(\ x_t\ |C_k)$ – вероятность получить такой вектор признаков при условии, что сообщение относится к классу C_k; $P(C_k)$ – априорная вероятность класса (например, рассчитанная по известным пропорциям $P(M_T)$, $P(M_F)$, $P(M_M)$; $P(\ x_t)$ – нормирующий множитель, независимый от k.

Для вычисления $P(C_k\ |\ x_t)$ могут использоваться такие методы, как наивный байесовский классификатор, модели логистической регрессии или методы на основе глубоких нейронных сетей [15–16].

Инструменты для выделения ложной и вредоносной информации

Для решения задачи классификации ложной и вредоносной информации применяется анализ сетевых взаимодействий, временных характеристик сообщений и текстового содержания.

Семантический анализ: использование эмбеддингов (например, *Word2Vec, GloVe* или трансформеров, как *BERT, GPT*) для получения векторного представления смыслового содержания. Ложная информации часто имеет такую особенность, как повторяемость шаблонов, интенсивность потока данных и стремление вызывать у потребителя информации ответную реакцию.

Модель временной корреляции: вредоносная информация часто воспринимается через распространение во времени. Для этого применимы модели временных рядов (например, *LSTM, GRU*), а также графовые подходы, анализирующие частоту отправки сообщений через временные окна.

Анализ источников: для каждого сообщения m можно сопоставить вероятности достоверности источника с помощью функций ранжирования. Если отправитель ранее распространял уже ложную или вредоносную информацию, вероятность того, что текущее сообщение также является неверным, повышается.

Энтропия информационного потока

На основе теории информации поток сообщений можно анализировать через меры неопределенности. Энтропия информационного потока H рассчитывается как:

$$H(M) = -\sum_{k \in \{true,\ false,\ malicious\}} \mathrm{P}(C_\mathrm{k}) log \mathrm{P}(C_\mathrm{k}).$$

Здесь:

– если $P(M_T) >> P(M_F)+P(M_M)$, то поток более «чистый», с низкой энтропией;

– если $P(M_F)$ или $P(M_M)$ значительны, энтропия возрастает, так как система становится более стохастической и менее предсказуемой.

Повышение энтропии потока также свидетельствует о растущем влиянии ложной или вредоносной информации на общий поток данных [17].

Динамика взаимодействия различных информационных потоков

Пусть $N_T(t)$, $N_F(t)$, $N_M(t)$ – количество достоверных, ложных и вредоносных сообщений в момент времени t. Тогда вероятности отнесения сообщения к тому или иному классу за интервал времени T можно выразить следующим образом:

$$P(M_T) = \frac{N_{T(t)}}{T},$$

$$P(M_F) = \frac{N_{F(t)}}{T},$$

$$P(M_M) = \frac{N_{M(t)}}{T}.$$

Информационный поток можно описать системой дифференциальных уравнений, отражающих динамическое поведение классов (например, увеличение количества ложной информации через дополнительные каналы получения информации) [18]. Вся динамика сведена
к вероятностным характеристикам классификации сообщений, а не к детерминированной динамике целочисленных переменных. Переменные являются не целочисленными, а непрерывными. В данном случае анализируется не непрерывное изменение количества сообщений во времени, а отношение количества сообщений разных типов (достоверных, ложных, вредоносных) к общему числу сообщений – то есть рассматривается динамика вероятностной структуры потока, не его числовая динамика, а расчет ведется по дискретным шагам («для каждого сообщения», «на каждом шаге»).

Тогда описанием информационной динамики будет система уравнений:

$$\frac{\partial P_T}{\partial t} = -\beta_{FT} P_F(t) P_T(t) - \beta_{MT} P_M(t) P_T(t),$$

$$\frac{\partial P_F}{\partial t} = \beta_{TF} P_T(t) P_F(t) - \gamma_F P_F(t),$$

$$\frac{\partial P_M}{\partial t} = \beta_{TM} P_T(t) P_M(t) - \gamma_M P_M(t).$$

где значения β_{xy}(коэффициент влияния одного типа информации на другой); γ_{false}, $\gamma_{malicious}$ («темпы убывания») найдены комбинаторными методами из пакетов семантического анализа.

Правая часть уравнений отражает динамику долей сообщений каждого типа (достоверных, ложных, вредоносных) и строится по аналогии с уравнениями Лотки-Вольтерра системы «хищник–жертва» [19, 20]. Главный принцип – вероятности изменяются под действием поступления новых сообщений, перекрестной корреляции между источниками, удаления/отсева ложных/ненадежных сообщений, распространения информации (например, «цепной» доставки вредоносных сообщений). Коэффициенты появляются из вероятности того или иного «перехода» между классами данных на определённом временном отрезке. Данное описание позволяет затем оценивать эволюцию информационного потока в модели.

Уравнения используются как теоретическая основа моделирования динамики состава потока – для обоснования процессов изменения долей достоверных, ложных и вредоносных сообщений в совокупности данных на промежутке времени. В разделе «Экспериментальные исследования…» основное внимание уделено реализации вероятностных правил

классификации сообщений, однако аналитические уравнения позволяют прогнозировать предельное поведение потоков, например, установить стационарное распределение или критерии устойчивости «чистого» информационного потока при разных параметрах надежности источников/интенсивности шума.

Формально, параметры/структура потоков, увиденные в результатах моделирования, соотносятся с поведением решений указанных систем (например, рост доли достоверных данных при росте избыточности коррелирует с устойчивым «фиксированным» решением системы). Это позволяет проводить верификацию/калибровку модели.

Метрики оценки эффективности модели

Для оценки эффективности модели фильтрации и анализа информации важно использовать метрики, учитывающие дисбаланс классов (поскольку достоверных сообщений часто значительно больше). Среди таких метрик можно выделить:

– *Precision* (точность), *Recall* (полнота), *F1*-score отдельно для классов C_F и C_M;

– *ROC-AUC* (площадь под *ROC*-кривой) для оценки разделимости ложной и достоверной информации.

Результаты экспериментальных исследований по оценке формирования и предоставления достоверных данных

Экспериментальная проверка метода проводилась с использованием Python 3.10 и библиотек для анализа данных [21]. Целью было доказать, что объединение данных от нескольких источников с перекрёстной проверкой и адаптацией весов значительно повышает долю достоверных сообщений в итоговом потоке.

Блок-схема алгоритма комплексированной обработки данных предоставлена на рисунке.

Были сгенерированы синтетические многоканальные потоки данных от 10 виртуальных источников с разной начальной надёжностью. В общей сложности 10 000 сообщений имели следующую структуру: 60 % – достоверные, 30 % – ложные, 10 % – вредоносные. Для ложных и вредоносных сообщений специально искажались значения и метаданные, моделируя атаки и сбои.

Ключевой параметр – степень избыточности данных (доля сообщений, подтверждённых несколькими источниками) – варьировалась от 10 % до 90 %. Эффективность метода оценивалась по трём показателям: доля достоверных сообщений в итоговом потоке (D), доля согласованных сообщений (C) и доля исключённых недостоверных данных (E).

Результаты показали устойчивый рост достоверности (D) и согласованности (C) с увеличением избыточности. При избыточности 90 % значение D достигает 0,98, а C стабилизируется на уровне 0,93–0,97. Доля исключаемых данных (E) возрастает с ростом уровня шума, что отражает эффективное отсеивание конфликтных и вредоносных сообщений.

Динамическая настройка весов источников ускоряет адаптацию: надёжные источники усиливают своё влияние, а ненадёжные быстро теряют вес. Это повышает стабильность потока в долгосрочной перспективе.

Сравнение с базовым режимом (без перекрёстной проверки) показало, что предложенный метод повышает достоверность результирующего потока на 15–20 процентных пунктов при разных уровнях избыточности. Эксперименты подтвердили эффективность комплексированной обработки для формирования высоконадёжного информационного потока в условиях шума и целенаправленных искажений.

Табличное представление ключевых результатов по трем срезам эксперимента приведено ниже (табл. 1–3).

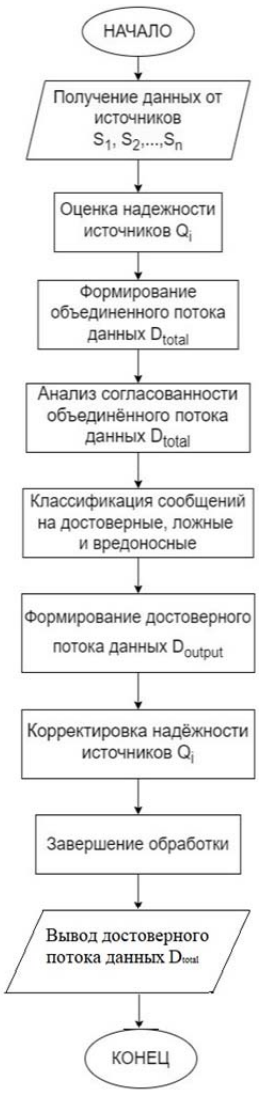

Рис. **Цикл управления рисками**

Таблица 1

Зависимость достоверности информации от избыточности данных

Уровень избыточности (%)	D (достоверность итогового потока)
10	0,75
30	0,85
50	0,90
70	0,95
90	0,98

Таблица 2

Результаты использования перекрестной корреляции

Уровень избыточности (%)	C (согласованность итогового потока)
10	0,83
30	0,89
50	0,93
70	0,97
90	0,97

Таблица 3

Результаты исключения недостоверных данных

Уровень шума в данных (%)	E (исключённые данные)
10	0,12
30	0,22
50	0,36
70	0,51

Выводы

Предложенный подход обеспечивает проактивную защиту от ложных и вредоносных данных в нестабильной информационной среде. Его основные достоинства:

1. Адаптивность. Система динамически переоценивает доверие к источникам, увеличивая вклад надёжных и снижая влияние источников с постоянными ошибками. Это позволяет гибко реагировать на изменения в потоках данных.

2. Многоуровневая обработка. Архитектура сочетает анализ отдельных сообщений, их метаданных и согласование на уровне совокупности потоков. Это повышает устойчивость к локальным аномалиям и обеспечивает глубокую интерпретацию данных.

3. Целенаправленное подавление вредоносного контента. Встроенные вероятностные и статистические механизмы своевременно выявляют и блокируют сообщения с признаками преднамеренного искажения, снижая риски для системы.

4. Повышенная устойчивость к внешним воздействиям. Комплекс алгоритмов минимизирует успешность манипуляций информационными потоками и предотвращает появление систематических ошибок на выходе.

5. Улучшение качества последующего анализа. Сформированный поток отличается высокой согласованностью и достоверностью, что повышает надёжность любых последующих моделей и процедур принятия решений, построенных на его основе.

Работа выполнена и апробирована в рамках ОКР Интегратор-С «Создание комплекса средств автоматизации для реализации требований по обеспечению кибербезопасности при разработке и испытаниях судовых компьютеризированных систем» на предприятии ЗАО «Институт телекоммуникаций».

Список источников

1. Fake news detector using deep learning / A. Akshansh [et al.] // International Journal of Advanced Research. 2023. № 11. Vol. 4. P. 1612–1621. DOI: 10.21474/IJAR01/16831

2. Revisiting Fake News Detection: Towards Temporality-aware Evaluation by Leveraging Engagement Earliness / J. Kim [et al.] // arXivLabs. 2024. № 2411. Vol. 12775. P. 1–11. DOI: 10.1145/3701551.370352

3. Zhou X., Zafarani R. A survey of fake news: Fundamental theories, detection methods, and opportunities // ACM Computing Surveys. 2020. № 53 (5). P. 1–40. DOI: 10.1145/3395046

4. Привалов А.Н., Смирнов В.А. Поиск фейковых сайтов с использованием метода определения визуального сходства страниц // Известия ТулГУ. Технические науки. 2022. № 9. С. 260–264. DOI: 10.24412/2071-6168-2022-9-260-265

5. Zhou X., Zafarani R., Wu J. SAFE: Similarity-Aware Multi-Modal Fake News Detection. // Advances in Knowledge Discovery and Data Mining. Lecture Notes in Computer Science. 2020. Vol. 12085. P. 1–13. DOI: 10.48550/arXiv.2003.04981

6. Hammouchi H., Ghogho M. Evidence-Aware Multilingual Fake News Detection // IEEE Access. 2022. № 99. P. 1–11. DOI: 10.1109/ACCESS.2022.3220690

7. Zhou Y. The Silent Saboteur: The Impact and Management of Malicious Word-Of-Mouth in The Digital Age // Highlights in Business Economics and Management. 2024. № 41. P. 381–386. DOI: 10.54097/et0yen43

8. The impact of malicious nodes on the spreading of false information / Z. Ruan [et al.] // Chaos: An Interdisciplinary Journal of Nonlinear Science. 2020. № 30. P. 083101. DOI: 10.1063/5.0005105

9. Satija T., Kar N. Detecting Malicious Twitter Bots Using Machine Learning // Communications in Computer and Information Science. 2020. P. 182–194. DOI: 10.1007/978-981-15-3666-3_16

10. Wesam H.A., Ragheed A., Yossra H.A. Opinion mining for fake recommendations in e-commerce: A machine learning approach using LightGBM // AIP Conference Proceedings. 2025. № 3169. Vol. 030015. P. 1–11. DOI: 10.1063/5.0255957

11. Минаков С.С., Михайленко Н.В. Проблемы обеспечения достоверности технических данных и сведений, сопряжённых с выявлением и расследованием инцидентов и преступлений, совершённых с использованием информационно-телекоммуникационных технологий // Вестник экономической безопасности. 2023. № 6. С. 107–112. DOI: 10.24412/2414-3995-2023-6-107-112

12. Козлов В.В., Лагун А.В., Харченко В.А. Обоснование облика системы защиты стартового комплекса от деструктивных воздействий // Известия ТулГУ. Технические науки. 2023. № 1. DOI: 10.24412/2071-6168-2023-1-259-266

13. Лубенцов А.В. Синтез метода оценки эффективности системы информационной безопасности // Известия вузов. Электроника. 2024. Vol. 29. № 1. P. 118–129. DOI: 10.24151/1561-5405-2024-29-1-118-129

14. Карманова Н.А. Метод комплексированной обработки информации для достижения достоверности данных в цифровых сенсорных системах // Информация и космос. 2025. № 2. С. 77–85.

15. Тымчук А.И. Информационная система контроля достоверности данных приборов учёта в автоматизированной информационно-измерительной системе контроля и учёта электроэнергии // Международный научно-исследовательский журнал. 2024. № 6 (144). С. 1–9. DOI: 10.60797/IRJ.2024.144.79

16. Лебедев И.С. Адаптивное применение моделей машинного обучения на отдельных сегментах выборки в задачах регрессии и классификации // Информационно-управляющие системы. 2022. № 3 (118). С. 20–30. DOI: 10.31799/1684-8853-2022-3-20-30

17. Ефимов А.Ю. Использование энтропийных характеристик сетевого трафика для определения его аномальности // Программные продукты и системы. 2021. Т. 34. С. 83–90. DOI: 10.15827/0236-235X.133.083-090

18. Куприянов В.В. Теоретическое обоснование возможности снижения потерь информации при измерениях непрерывных случайных величин при наличии шумов // Горный информационно-аналитический бюллетень. 2021. № 8. С. 70–79. DOI: 10.25018/0236-1493-2021-8-0-70

19. Lotka A. Elements of Physical Biology. Baltimore, 1925. 460 p.

20. Вольтерра В. Математическая теория борьбы за существование. М.: Наука, 1976. 288 с.

21. Карманова Н.А. Алгоритм для реализации метода комплексированной обработки данных с целью формирования и предоставления достоверной информации // Научно-аналитический журнал «Вестник Санкт-Петербургского университета ГПС МЧС России». 2025. № 1. С. 160–173. DOI: 10.61260/2218-13X-2025-1-160-173

References

1. Fake news detector using deep learning / A. Akshansh [et al.] // International Journal of Advanced Research. 2023. № 11. Vol. 4. P. 1612–1621. DOI: 10.21474/IJAR01/16831

2. Revisiting Fake News Detection: Towards Temporality-aware Evaluation by Leveraging Engagement Earliness / J. Kim [et al.] // arXivLabs. 2024. № 2411. Vol. 12775. P. 1–11. DOI: 10.1145/3701551.370352

3. Zhou X., Zafarani R. A survey of fake news: Fundamental theories, detection methods, and opportunities // ACM Computing Surveys. 2020. № 53 (5). P. 1–40. DOI: 10.1145/3395046

4. Privalov A.N., Smirnov V.A. Poisk fejkovyh sajtov s ispol'zovaniem metoda opredeleniya vizual'nogo skhodstva stranic // Izvestiya TulGU. Tekhnicheskie nauki. 2022. № 9. S. 260–264. DOI: 10.24412/2071-6168-2022-9-260-265

5. Zhou X., Zafarani R., Wu J. SAFE: Similarity-Aware Multi-Modal Fake News Detection. // Advances in Knowledge Discovery and Data Mining. Lecture Notes in Computer Science. 2020. Vol. 12085. P. 1–13. DOI: 10.48550/arXiv.2003.04981

6. Hammouchi H., Ghogho M. Evidence-Aware Multilingual Fake News Detection // IEEE Access. 2022. № 99. P. 1–11. DOI: 10.1109/ACCESS.2022.3220690

7. Zhou Y. The Silent Saboteur: The Impact and Management of Malicious Word-Of-Mouth in The Digital Age // Highlights in Business Economics and Management. 2024. № 41. P. 381–386. DOI: 10.54097/et0yen43

8. The impact of malicious nodes on the spreading of false information / Z. Ruan [et al.] // Chaos: An Interdisciplinary Journal of Nonlinear Science. 2020. № 30. P. 083101. DOI: 10.1063/5.0005105

9. Satija T., Kar N. Detecting Malicious Twitter Bots Using Machine Learning // Communications in Computer and Information Science. 2020. P. 182–194. DOI: 10.1007/978-981-15-3666-3_16

10. Wesam H.A., Ragheed A., Yossra H.A. Opinion mining for fake recommendations in e-commerce: A machine learning approach using LightGBM // AIP Conference Proceedings. 2025. № 3169. Vol. 030015. P. 1–11. DOI: 10.1063/5.0255957

11. Minakov S.S., Mihajlenko N.V. Problemy obespecheniya dostovernosti tekhnicheskih dannyh i svedenij, sopryazhyonnyh s vyyavleniem i rassledovaniem incidentov i prestuplenij, sovershyonnyh s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij // Vestnik ekonomicheskoj bezopasnosti. 2023. № 6. S. 107–112. DOI: 10.24412/2414-3995-2023-6-107-112

12. Kozlov V.V., Lagun A.V., Harchenko V.A. Obosnovanie oblika sistemy zashchity startovogo kompleksa ot destruktivnyh vozdejstvij // Izvestiya TulGU. Tekhnicheskie nauki. 2023. № 1. DOI: 10.24412/2071-6168-2023-1-259-266

13. Lubencov A.V. Sintez metoda ocenki effektivnosti sistemy informacionnoj bezopasnosti // Izvestiya vuzov. Elektronika. 2024. Vol. 29. № 1. P. 118–129. DOI: 10.24151/1561-5405-2024-29-1-118-129

14. Karmanova N.A. Metod kompleksirovannoj obrabotki informacii dlya dostizheniya dostovernosti dannyh v cifrovyh sensornyh sistemah // Informaciya i kosmos. 2025. № 2. S. 77–85.

15. Tymchuk A.I. Informacionnaya sistema kontrolya dostovernosti dannyh priborov uchyota v avtomatizirovannoj informacionno-izmeritel'noj sisteme kontrolya i uchyota elektroenergii // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2024. № 6 (144). S. 1–9. DOI: 10.60797/IRJ.2024.144.79

16. Lebedev I.S. Adaptivnoe primenenie modelej mashinnogo obucheniya na otdel'nyh segmentah vyborki v zadachah regressii i klassifikacii // Informacionno-upravlyayushchie sistemy. 2022. № 3 (118). S. 20–30. DOI: 10.31799/1684-8853-2022-3-20-30

17. Efimov A.Yu. Ispol'zovanie entropijnyh harakteristik setevogo trafika dlya opredeleniya ego anomal'nosti // Programmnye produkty i sistemy. 2021. T. 34. C. 83–90. DOI: 10.15827/0236-235X.133.083-090

18. Kupriyanov V.V. Teoreticheskoe obosnovanie vozmozhnosti snizheniya poter' informacii pri izmereniyah nepreryvnyh sluchajnyh velichin pri nalichii shumov // Gornyj informacionno-analiticheskij byulleten'. 2021. № 8. S. 70–79. DOI: 10.25018/0236-1493-2021-8-0-70

19. Lotka A. Elements of Physical Biology. Baltimore, 1925. 460 p.

20. Vol'terra V. Matematicheskaya teoriya bor'by za sushchestvovanie. M.: Nauka, 1976. 288 s.

21. Karmanova N.A. Algoritm dlya realizacii metoda kompleksirovannoj obrabotki dannyh s cel'yu formirovaniya i predostavleniya dostovernoj informacii // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta GPS MCHS Rossii». 2025. № 1. S. 160–173. DOI: 10.61260/2218-13H-2025-1-160-173

Информация о статье:
Статья поступила в редакцию: 15.01.2026; одобрена после рецензирования: 16.03.2026;
принята к публикации: 17.03.2026

Information about the article:
The article was submitted to the editorial office: 15.01.2026; approved after review: 16.03.2026;
accepted for publication: 17.03.2026

Информация об авторах:
Ярцева Наталия Андреевна, ассистент факультета безопасности информационных технологий университета ИТМО (197101, Санкт-Петербург, Кронверкский пр., д. 49), e-mail: karmanova.ifmo@gmail.com, https://orcid.org/0000-0002-7007-3120, SPIN-код: 3628-9988

Information about authors:
Yartseva Nataliya A., assistant of the faculty of information technology security of ITMO university (197101, Saint-Petersburg, Kronverksky ave., 49), e-mail: karmanova.ifmo@gmail.com, https://orcid.org/0000-0002-7007-3120, SPIN: 3628-9988