



**Н.Н. Тетерин**  
*МИРЭА — Российский технологический университет,  
г. Москва, Российская Федерация*

## **Концепция архитектуры информационной системы выявления деструктивного поведения в организационных системах**

**Аннотация.** Рассмотренная в работе концепция архитектуры информационной системы реализует алгоритм выявления деструктивного поведения сотрудников. Одной из важных особенностей алгоритма является использование методов машинного обучения, в частности, NLP (Natural Language Processing), для анализа текста. Данный алгоритм может быть успешно реализован в организационных системах, что особенно актуально с применением информационных технологий при управлении персоналом. Деструктивное поведение сотрудников представляет собой серьезную угрозу для эффективности работы организаций. К преимуществам алгоритма относятся: автоматизация сбора данных рассматриваемого в работе процесса и своевременное, обоснованное принятие решений руководством. Проблемой исследования является отсутствие эффективных и систематизированных методов для своевременного выявления и предотвращения деструктивного поведения. Целью работы является описание концепции архитектуры информационной системы, реализующей алгоритм выявления деструктивного поведения, который позволит автоматизировать процесс сбора и анализа данных с помощью методов машинного обучения, а также обеспечит своевременное и обоснованное принятие решений руководством. Решение заявленной в работе проблемы, заключающейся в отсутствии эффективных и систематизированных методов для своевременного выявления и предотвращения деструктивного поведения сотрудников в организациях, заключается в разработке концепции архитектуры системы, реализующей алгоритм выявления деструктивного поведения. Представленная в работе концепция архитектуры обеспечивает комплексный подход к сбору, обработке, анализу данных и принятию решений, что позволяет минимизировать риски, связанные с деструктивным поведением сотрудников, и повысить эффективность работы организации. Результаты исследования представляют ценность для руководителей, аналитиков HR-подразделений и разработчиков корпоративных информационных систем. Внедрение предложенного алгоритма позволит предсказывать деструктивное поведение сотрудников организаций.

**Ключевые слова.** Машинное обучение, NLP, концепция архитектуры информационной системы, алгоритм, организационные системы, принятие решений, автоматизация сбора данных, деструктивное поведение сотрудников.

**Информация о статье.** Дата поступления: 14 апреля 2025 г.; дата принятия к публикации: 11 июня 2025 г.; дата онлайн-размещения: 8 июля 2025 г.

N.N. Teterin

*MIREA — Russian Technological University,  
Moscow, Russian Federation*

## The Concept of Information System Architecture for Identifying Destructive Behavior in Organizational Systems

**Abstract.** The information system architecture concept considered in the paper implements an algorithm for identifying destructive employee behavior. One of the important features of the algorithm is the use of machine learning methods, in particular NLP (Natural Language Processing), for text analysis. This algorithm can be successfully implemented in organizational systems, which is especially important with the use of information technology in personnel management. Destructive behavior of employees poses a serious threat to the effectiveness of organizations. The advantages of the algorithm include: automation of data collection of the process under consideration and timely, informed decision-making by management. The problem of the research is the lack of effective and systematic methods for timely detection and prevention of destructive behavior. The purpose of this paper is to describe the concept of an information system architecture that implements an algorithm for detecting destructive behavior, which will automate the process of data collection and analysis using machine learning methods, as well as ensure timely and informed decision-making by management. The solution to the problem stated in the paper, which is the lack of effective and systematic methods for timely detection and prevention of destructive behavior of employees in organizations, is to develop a concept for the architecture of a system that implements an algorithm for detecting destructive behavior. The architecture concept presented in this paper provides an integrated approach to data collection, processing, analysis and decision-making, which minimizes the risks associated with destructive employee behavior and increases the efficiency of the organization. The results of the study are valuable for managers, HR department analysts and developers of corporate information systems. The implementation of the proposed algorithm will allow predicting the destructive behavior of employees of organizations.

**Keywords.** Machine learning, NLP, information system architecture concept, algorithm, organizational systems, decision-making, automation of data collection, destructive behavior of employees.

**Article info.** Received 14 April, 2025; Accepted 11 June, 2025; Available online 8 July, 2025.

В современных условиях цифровизации и роста конкуренции эффективность работы организации во многом зависит от слаженности коллектива и здоровой корпоративной культуры [1]. Однако деструктивное поведение сотрудников, такое как саботаж, нарушение корпоративных норм или распространение негативной информации, представляет собой угрозу для достижения положительных результатов. Традиционные методы выявления подобных случаев, такие как ручной мониторинг HR-отделом, часто оказываются недостаточно эффективными: они требуют значительных временных и человеческих ресурсов. Внедрение автоматизированных решений, способных оперативно и объективно выявлять признаки деструктивного поведения является актуальным.

Предлагаемый алгоритм выявления деструктивного поведения сотрудников является решением поставленной проблемы. Ключевое преимущество алгоритма заключается в автоматизации процессов сбора и анализа данных в виде единой системы. Автоматический сбор данных не только снижает нагрузку на HR-отдел, но и обеспечивает оперативность выявления проблем [2]. Например, если сотрудник публикует сообщение с оскорбительным содержанием в корпоративном чате, алгоритм мгновенно анализирует текст и классифицирует его как нарушение корпоративных норм, уведомляя ответственных лиц.

В данной области проводятся исследования А.В. Минаевым и А.В. Симоновым, которые в своих работах акцентируют внимание на вопросах информационной безопасности [3–4] и исследования Никулиной И.В. направленные на изучение кадровых вопросов в психологии [5].

Одной из важных особенностей алгоритма является использование методов машинного обучения, в частности, NLP (Natural Language Processing), для анализа текста [6]. Данный метод позволяет учитывать не только ключевые слова, но и контекст, тон сообщений и эмоциональную окраску. Например, фраза «Этот проект — полный провал!» может быть классифицирована как распространение негатива, даже если она не содержит явных оскорблений. Такая глубина анализа недоступна при использовании традиционных методов или более простых алгоритмов.

В алгоритме используется многоуровневая классификация деструктивного поведения, где он не просто выявляет проблему, но и определяет ее тип: нарушение корпоративных норм, распространение негатива, саботаж или другие случаи. Такая детализация позволяет HR-отделу и руководству более точно понимать причины проблемы и принимать соответствующие меры. Например, если алгоритм выявляет саботаж, то необходимо провести индивидуальную беседу с сотрудником.

Важным преимуществом алгоритма является его гибкость и масштабируемость. Параметры алгоритма, такие как критерии классификации или список ключевых слов, могут быть настроены в зависимости от специфики организации, что делает его применимым в различных отраслях [7].

Сравнение с известными методами и другими алгоритмами также подтверждает преимущества данного подхода. Известные методы, такие как ручной мониторинг, требуют значительных ресурсов и не обеспечивают оперативность. Другие алгоритмы ограничены в функциональности: они могут анализировать только тексты, без учёта контекста, или требуют сложной настройки и интеграции. Данный алгоритм является оптимальным решением для современных организаций.

Практическая значимость внедрения данного алгоритма заключается не только в снижении рисков, связанных с деструктивным поведением, но и в улучшении корпоративной культуры. Когда сотрудники знают, что их действия анализируются объективно и прозрачно, они становятся более осознанными в своих поступках, что способствует созданию здоровой рабочей атмосферы, где каждый чувствует ответственность за общий успех. Внедрение алгоритма повышает репутацию компании как современной и технологически продвинутой организации, что может стать конкурентным преимуществом на рынке труда [8].

Исходные данные — основа для работы алгоритма выявления деструктивного поведения. Данные собираются из различных корпоративных систем, обрабатываются и анализируются с использованием методов машинного обучения и статистики, что позволяет алгоритму точно выявлять проблемы и предоставлять обоснованные рекомендации для руководства и HR-отдела [9, с. 171–174].

Ручное выявление деструктивного поведения часто оказывается неэффективным из-за субъективности и недостатка данных. Алгоритмизация процесса позволяет: систематизировать сбор и анализ данных, а также обеспечить оперативное реагирование на возникающие инциденты. [10]

Алгоритм выявления деструктивного поведения основан на автоматизированном сборе и анализе данных о сотрудниках.

Табл. 1 показывает, как данные из разных источников собираются и классифицируются по категориям поведения.

Таблица 1

#### Исходные данные по категориям поведения

ID	Текст сообщения/письма	Категория поведения
1	Этот проект — полный провал!	Распространение негатива
2	Я не буду это делать, это не моя работа	Саботаж
3	Ты вообще ничего не понимаешь!	Нарушение корпоративных норм
4	Мы должны работать вместе	Другие случаи
5	Этот дедлайн нереален	Распространение негатива

Источники данных можно разделить на внутренние и внешние.

Внутренние источники данных — это корпоративные системы и инструменты, которые уже используются в организации. Они предоставляют структурированные данные, которые легко анализировать, представлены в табл. 2.

Внешние источники данных — это публичные данные, которые можно получить из социальных сетей, форумов и других открытых платформ. Публичные данные менее структурированы, но могут предоставить ценную информацию, представлены в табл. 3.

Таблица 2

**Внутренние источники данных**

Источник данных	Тип данных	Методы сбора
HRM-системы	KPI, опоздания, нарушения	API-интеграция, экспорт данных
Системы учета времени	Время, затраченное на задачи	API, SQL-запросы
Корпоративная почта	Переписка между сотрудниками	Анализ текста, ключевые слова
Корпоративные чаты	Сообщения	NLP-анализ, логирование
Системы видеонаблюдения	Видеозаписи	Компьютерное зрение

Таблица 3

**Внешние источники данных**

Источник данных	Тип данных	Методы сбора
Социальные сети	Посты, комментарии	Веб-скрапинг, API
Форумы и блоги	Обсуждения, отзывы	Веб-скрапинг, NLP-анализ
Сайты с отзывами	Отзывы о компании	Веб-скрапинг, анализ тональности

Важно понимать, как данные поступают в систему, обрабатываются и преобразуются в полезные отчеты.

Рассмотрение алгоритма приводилось автором в работе ранее [11], а в данной работе представлена реализация этапов системы на основе алгоритма.

Далее в исследовании представлена архитектура системы, которая демонстрирует сбор, анализ и визуализацию данных. Архитектура системы представлена на нескольких уровнях и состоит из нескольких ключевых модулей, которые взаимодействуют друг с другом для обработки данных.

Логическая архитектура представлена в виде диаграммы компонентов. Рисунок 1 демонстрирует основные компоненты системы и их взаимодействие.

Диаграмма компонентов показывает, как данные поступают из внешних систем в модуль сбора данных, затем обрабатываются, анализируются и преобразуются в отчеты, которые доступны руководству и HR-отделу через пользовательский интерфейс.

Физическая архитектура представлена в виде диаграммы развертывания. Рисунок 2 демонстрирует как компоненты системы развертываются на физических или виртуальных серверах.

Диаграмма развертывания показывает, что система состоит из трех основных серверов: сервер приложений, сервер баз данных и сервер пользовательского интерфейса. Данные поступают

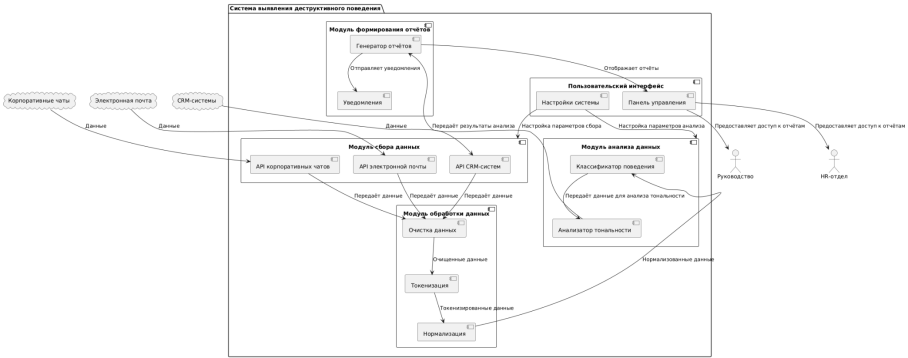


Рис. 1. Диаграмма компонентов

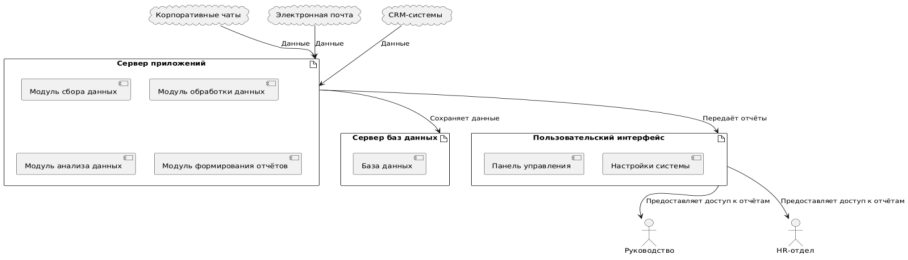


Рис. 2. Диаграмма развертывания

из внешних систем на сервер приложений, где они обрабатываются и сохраняются в базе данных. Результаты анализа передаются на сервер пользовательского интерфейса, где они доступны руководству и HR-отделу.

Поведенческая архитектура представлена в виде диаграммы последовательности. Рисунок 3 демонстрирует, как данные проходят через систему.

Диаграмма последовательности показывает, как данные поступают от пользователя в модуль сбора данных, затем обрабатываются, анализируются и преобразуются в отчеты, которые доступны пользователю через интерфейс.

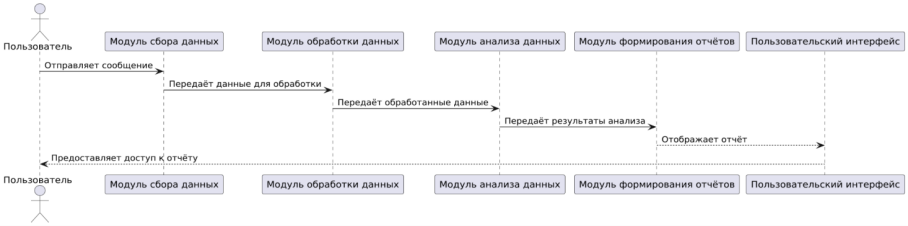


Рис. 3. Диаграмма последовательности

Данная архитектура помогает понять, что система работает как единый механизм, где каждый модуль выполняет свою роль.

Представленные далее диаграмма классов и диаграмма использования демонстрируют, какие компоненты системы взаимодействуют друг с другом и как пользователи взаимодействуют с системой.

Диаграмма классов описывает основные компоненты системы и их взаимосвязи, представлена на рис. 4.

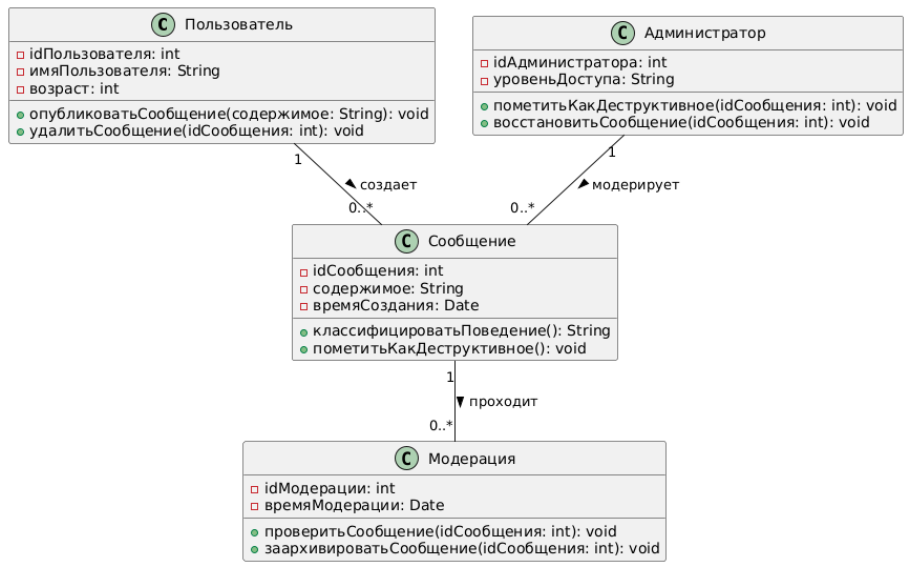


Рис. 4. Диаграмма классов

Диаграмма классов показывает, что система состоит из четырех основных классов: «Пользователь», «Сообщение», «Администратор» и «Модерация». Пользователь создаёт сообщения, которые могут быть проверены администратором и помечены как деструктивные. Сообщения также проходят через процесс проверки, где они анализируются и классифицируются.

Диаграмма использования показывает, как пользователи взаимодействуют с системой, представлена на рис. 5.

Диаграмма использования показывает, что «Пользователь» может публиковать и удалять сообщения, а «Администратор» может помечать сообщения как деструктивные или восстанавливать их. Это позволяет четко разделить роли и обязанности пользователей в системе.

Следовательно, после детального рассмотрения архитектуры системы, включая ее логическую, физическую и поведенческую составляющие, становится очевидным, что алгоритм выявления деструктивного поведения сотрудников представляет собой сложный, но хорошо структурированный механизм, где каждый компонент системы играет важную роль в обеспечении ее эффективности.



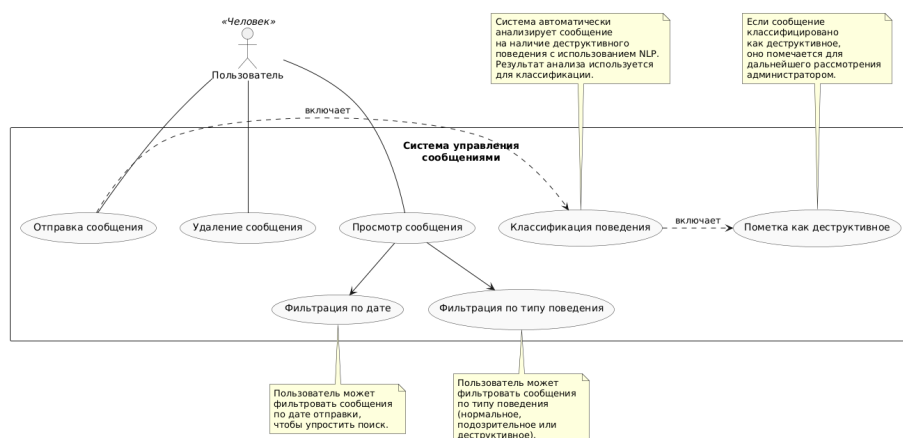


Рис. 5. Диаграмма использования

Таким образом, решение заявленной в работе проблемы, заключающейся в отсутствии эффективных и систематизированных методов для своевременного выявления и предотвращения деструктивного поведения сотрудников, заключается в разработке концепции архитектуры информационной системы, реализующей алгоритм выявления деструктивного поведения. Эта концепция архитектура обеспечивает комплексный подход к сбору, обработке, анализу данных и принятию решений, что позволяет минимизировать риски, связанные с деструктивным поведением, и повысить эффективность работы организации.

Применение предложенного проекта системы, реализующей алгоритм выявления деструктивного поведения является необходимым шагом для организаций, стремящихся к повышению эффективности и улучшению корпоративной культуры.

Особенности алгоритма, такие как использование машинного обучения и многоуровневая классификация, позволяют достичь высокой точности и гибкости.

Таким образом, внедрение данного алгоритма является обоснованным и целесообразным решением для организаций.

### Список использованной литературы

1. Енгибарян М.М. Развитие системы управления персоналом в условиях цифровых трансформаций / М.М. Енгибарян, М.Д. Шалагинова. — EDN RWODXH // Молодой исследователь Дона. — 2024. — Т. 9, № 1. — С. 42–48.
2. Тетерин Н.Н. Общие вопросы анализа деструктивного поведения пользователей в социальных сетях / Н.Н. Тетерин. — EDN OWDJUT // Актуальные проблемы деятельности подразделений уголовно-исполнительной системы : материалы Всерос. науч.-практ. конф., Воронеж, 24 окт. 2024 г. — Воронеж, 2024. — Т. 2. — С. 96–99.



3. Минаев В.А. Выявление деструктивного контента в социальных МЕДИА на основе Моделей машинного обучения / В.А. Минаев, А.Д. Реброва, А.В. Симонов. — DOI 10.36622/VSTU.2021.24.1.001. — EDN JDPDQC // Информация и безопасность. — 2021. — Т. 24, № 1. — С. 7–20.

4. Минаев В.А. Повышение точности идентификации контента экстремистского характера в социальных медиа / В.А. Минаев, А.В. Симонов. — EDN WHQAMO // Информационная безопасность: вчера, сегодня, завтра : материалы V Междунар. науч.-практ. конф., Москва, 14 апр. 2022 г. — Москва, 2022. — С. 80–86.

5. Никулина И.В. Психология кадровой безопасности : учеб. пособие / И.В. Никулина. — Самара : Изд-во Самар. ун-та, 2021. — 80 с. — EDN BCLMWC.

6. Широких И.В. Специфика текста как продукта искусственного интеллекта / И.В. Широких, А.Г. Фомин. — EDN OZGSHW // Искусственный интеллект в автоматизированных системах управления и обработки данных : сб. статей II Всерос. науч. конф., Москва, 27–28 апр. 2023 г. — Москва, 2023. — Т. 1. — С. 349–355.

7. Тетерин Н.Н. Влияние новой информационной системы на управление организационными системами / Н.Н. Тетерин, Ю.В. Чебернова. — EDN RUSECQ // Конкурентоспособность в глобальном мире: экономика, наука, технологии. — 2023. — № 6. — С. 71–72.

8. Тарасова А.В. Методика оценки деловой репутации и ее роль в оптимизации бизнес-процессов / А.В. Тарасова. — DOI 10.22394/1997-4469-2021-55-4-161-168. — EDN ZUDVAE // Регион: системы, экономика, управление. — 2021. — № 4. — С. 161–168.

9. Москвитин А.А. Данные, информация, знания: методология, теория, технологии / А.А. Москвитин. — Санкт-Петербург : Лань, 2022. — 236 с.

10. Булетова Н.Е. Управление информационными рисками в организации : учеб. пособие / Н.Е. Булетова, Н.Н. Карпухина. — Москва : Изд-во МГТУ МИРЭА, 2024. — 85 с.

11. Тетерин Н.Н. К вопросу формализации задачи выявления деструктивного поведения с применением технологий искусственного интеллекта / Н.Н. Тетерин, В.В. Смоленцева. — DOI 10.18411/trnio-10-2024-440. — EDN EEBVGI // Тенденции развития науки и образования. — 2024. — № 114-10. — С. 81–83.

## References

1. Engibaryan M.M., Shalaginova M.D. Human Resource Management System Development in the Context of Digital Transformations. *Molodoi issledovatel' Dona = Young Don Researcher*, 2024, vol. 9, no. 1, pp. 42–48. (In Russian). EDN: RWODXH.

2. Teterin N.N. General issues of analysis of destructive behavior of users in social networks. In *Current problems of the activities of the units of the penal system. All-Russian Scientific and Practical Conference, Voronezh, October 24, 2024*. Voronezh, 2024. Vol. 2, pp. 96–99. (In Russian). EDN: OWDJUT.

3. Minaev V.A., Rebrova A.D., Simonov A.V. Detection Destructive Content in Social Media Based on Machine Learning Models. *Informatsiya i bezopasnost' = Information and Security*, 2021, vol. 24, no. 1, pp. 7–20. (In Russian). EDN: JDPDQC. DOI: 10.36622/VSTU.2021.24.1.001.

4. Minaev V.A., Simonov A.V. Improving the Accuracy of Identifying Extremist Content in Social Media. In *Information Security: Yesterday, Today, Tomorrow. Proceedings of the V International Scientific and Practical Conference, Moscow, April 14, 2022*. Moscow, 2022, pp. 80–86. (In Russian). EDN: WHQAMO.

5. Nikulina I.V. *Psychology of personnel security*. Samara National Research University Publ., 2021. 80 p. EDN: BCLMWC.

6. Shirokikh I.V., Fomin A.G. Specifics of Artificial Intelligence Generated Text. In *Artificial Intelligence in Management, Control, and Data Processing Systems. Proceedings of the II All-Russian Scientific Conference, Moscow, April 27-28, 2023*. Moscow, 2023. Vol. 1, pp. 349–355. (In Russian). EDN: OZGSHW.

7. Teterin N.N., Chebernova Yu.V. The Impact of the New Information System on the Management of Organizational Systems. *Konkurentosposobnost' v global'nom mire: ekonomika, nauka, tekhnologii = Competitiveness in the Global World: Economics, Science, Technology*, 2023, no. 6, pp. 71–72. (In Russian). EDN: RUSECQ.

8. Tarasova A.V. Methods for Assessing Business Reputation and its Role in the Optimizing Business Processes. *Region: sistemy, ekonomika, upravlenie = Region: Systems, Economics, Management*, 2021, no. 4, pp. 161–168. (In Russian). EDN: ZUDVAE. DOI: 10.22394/1997-4469-2021-55-4-161-168.

9. Moskvitin A.A. *Data, information, knowledge: methodology, theory, technology*. Saint Petersburg, Lan Publ., 2022. 236 p.

10. Buletova N.E., Karpukhina N.N. *Information risk management in an organization*. Moscow, Russian Technological University Publ., 2024. 85 p.

11. Teterin N.N., Smolentseva V.V. On the issue of formalizing the task of identifying destructive behavior using artificial intelligence technologies. *Tendentsii razvitiya nauki i obrazovaniya = Trends in the Development of Science and Education*, 2024, no. 114-10, pp. 81–83. (In Russian). EDN: EEBVGI. DOI: 10.18411/trnio-10-2024-440.

### Информация об авторе

**Тетерин Николай Николаевич** — ассистент, кафедры прикладной математики, МИРЭА — Российский технологический университет, г. Москва, e-mail: teterin@mirea.ru.

### Information about the Author

**Nikolay N. Teterin** — Assistant, Department of Applied Mathematics, MIREA — Russian Technological University, Moscow, e-mail: teterin@mirea.ru.

### Для цитирования

Тетерин Н.Н. Концепция архитектуры информационной системы выявления деструктивного поведения в организационных системах / Н.Н. Тетерин. — DOI 10.17150/2713-1734.2025.7(2).204-213. — EDN GWHHYV // System Analysis & Mathematical Modeling. — 2025. — Т. 7, № 2. — С. 204–213.

### For Citation

Teterin N.N. The Concept of Information System Architecture for Identifying Destructive Behavior in Organizational Systems. *System Analysis & Mathematical Modeling*, 2025, vol. 7, no. 2, pp. 204–213. (In Russian). EDN: GWHHYV. DOI: 10.17150/2713-1734.2025.7(2).204-213.