Научная статья
УДК 004.056
DOI 10.35266/1999-7604-2023-3-60-65

ОЦЕНИВАНИЕ КАЧЕСТВА АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ ИНФОРМАЦИИ

Сергей Игоревич Прудников
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Москва, Россия
prudnikovscience@gmail.com, https://orcid.org/0000-0002-5136-8521

Аннотация. В статье представлены выводы из анализа угроз, возникающих в результате распространения информации, способной оказать негативное психологическое воздействие. Рассмотрены современные механизмы выявления и блокировки вредоносной информации, сформирован математический аппарат оценивания качества ее автоматизированного обнаружения и создана функциональная модель информационно-технологических процессов анализа информационного ресурса на предмет наличия вредоносной информации.

Ключевые слова: вредоносная информация, информационный ресурс, обнаружение вредоносной информации

Финансирование: работа выполнена при финансовой поддержке гранта Президента РФ по государственной поддержке ведущих научных школ РФ (грант НШ-122.2022.1.6).

Для цитирования: Прудников С. И. Оценивание качества автоматизированного обнаружения вредоносной информации // Вестник кибернетики. 2023. Т. 22, № 3. С. 60–65. DOI 10.35266/1999-7604-2023-3-60-65.

Original article

ASSESSING THE QUALITY OF AUTOMATED MALICIOUS INFORMATION DETECTION

Sergey I. Prudnikov
St. Petersburg Federal Research Center of the Russian Academy of Sciences, Moscow, Russia
prudnikovscience@gmail.com, https://orcid.org/0000-0002-5136-8521

Abstract. The article presents findings of the analysis of threats arising due to the spread of information, which can have a negative impact on a person's psychological condition. Modern mechanisms for detection and blocking of malicious information are considered; a mathematical apparatus for assessing the quality of information detection is established; and a functional model of informational and technological processes for the examination of an information source for malicious information is designed.

Keywords: malicious information, information source, malicious information detection

Funding: the study is supported by the grant of the President of the Russian Federation in the framework of state support for leading research schools in the Russian Federation (grant NSh-122.2022.1.6).

For citation: Prudnikov S. I. Assessing the quality of automated malicious information detection. *Proceedings in Cybernetics.* 2023;22(3):60–65. DOI 10.35266/1999-7604-2023-3-60-65.

ВВЕДЕНИЕ

На сегодняшний день среднестатистический пользователь интернета в возрасте 12–17 лет ежедневно проводит в сети до 6 часов, а около 74 % из них посещают информационные ресурсы, содержащие информацию, запрещенную для распространения среди детей [1]. Как показывает проведенный анализ, требования законодательства в области защиты детей от воздействия вредоносной информации, способной оказать негативное влияние на их здоровье и развитие, выполняются не в пол-

ной мере ввиду значительно расширившейся интернет-медиасферы и невозможности своевременного реагирования контролирующих и надзорных органов [2, 3]. Поэтому актуальным является совершенствование методических подходов к решению задач автоматизированного выявления такой информации для ее своевременного блокирования [4–6].

В основу исследования положен замысел использования системы автоматизированного обнаружения вредоносной информации, входными данными которой будет являться контент с медиасервисов (аудио- и видеоданные в потоковом и непотоковом режимах), возраст интернет-пользователей, особенности настройки доступа к ресурсам сети Интернет, а выходными – сведения о наличии запрещенного контента на посещенных ресурсах на основе установленных возрастных меток, список посещенных сайтов, демонстрирующих контент, запрещенный для пользователей определенных возрастных категорий, рекомендации по блокировке такого контента, список принудительно заблокированных интернет-ресурсов.

Цель исследования – математическая постановка задачи оценивания качества автоматизированного обнаружения вредоносной информации в медиасреде с учетом текущего уровня развития информационных технологий.

МАТЕРИАЛЫ И МЕТОДЫ

Хранение большого объема исходных данных и результатов анализа информационных потоков требует создания баз данных, способных не только обеспечивать качественное хранение информации, но и оперативно ее обрабатывать и предоставлять доступ для решения поставленных задач [7–9].

1. Проблемы хранения информации

Исходя из опыта построения нейронных сетей, а также учитывая требования законодательства по защите детей от информации, причиняющей вред их здоровью и развитию, требуется формирование баз данных, содержащих следующую информацию:

1. *Справочная база* (информация, имеющая характерный информационный окрас, свойственный информации, причиняющей вред здоровью и развитию детей): возрастные категории детей и присвоенные им метки доступа; список слов и сочетаний слов; изображения; видео- и аудиоданные; обучающие, проверочные и тестовые наборы данных (датасеты).

2. *Исходные данные:* идентификатор пользователя автоматизированного рабочего места или мобильного устройства; возраст пользователя; особенности настройки доступа к интернет-ресурсам.

3. *Результаты функционирования:* список посещенных сайтов, демонстрирующих контент, запрещенный для детей различных возрастных категорий; рекомендации по присвоению возрастных меток информационным ресурсам; список принудительно заблокированных интернет-ресурсов.

4. Выявление вредоносной информации, причиняющей вред здоровью и развитию детей, предполагает формирование математического аппарата, способного обеспечивать адекватное функционирование разрабатываемого программного обеспечения (ПО) с заданными показателями качества.

2. Квалиметрия автоматизированного обнаружения вредоносной информации

В квалиметрии под оцениванием качества понимается особый тип деятельности, направленной на формирование ценностных суждений об объекте оценивания, под которым подразумеваются качество, определенные подмножества свойств или отдельное качество [10].

Исходя из этого оценка качества представляет собой результат взаимодействия четырех компонентов:

$$M = \{S, Ob, B, A\}, \qquad (1)$$

где S – субъект оценивания;

Ob – объект оценивания;

B – база сравнения;

A – алгоритм оценивания.

В классическом рассмотрении в роли субъекта оценивания S может выступать как один эксперт, так и экспертная группа (сообщество). Порядок формирования таких групп и организации их функционирования рассмотрены в [11]. Применительно к теме исследования в роли субъекта оценивания выступает специализированное ПО, разработанное с применением технологий искусственного интеллекта и предназначенное для выявления вредоносной информации в информационных ресурсах различного назначения и режима функционирования.

Так как объект оценивания может включать в себя простые информационные объекты, такие как звук, изображение, текстовое описание и т. д., то для формализации S представим его в виде пространства субъекта оценивания S в теоретико-множественном смысле со структурой отношений в нем $\wedge_S$, раскрывающей взаимосвязь между простыми информационными объектами, устанавливаемую в процессе оценивания. В таком случае субъект оценивания S конкретизируется путем представления формальных объектов двух видов $\langle S, \wedge_S \rangle$.

Под объектом оценивания Ob понимается информационный ресурс, в котором оценивается качество выявления вредоносной информации. Каждому рассматриваемому объекту соответствует пространство качеств R со структурой отношений в нем $\wedge_R$. При этом каждому качеству соответствует пространство свойств Γ со структурой отношений в нем $\wedge_\Gamma$. Измерение качества переводит пространство свойств в пространство показателей качества, или на языке мер – в пространство мер качества M с соответствующей ему структурой отношений в пространстве мер $\wedge_M$ [12].

Таким образом, объект оценивания можно представить тремя формальными объектами:

$$Ob = \langle\langle R, \wedge_R\rangle, \langle \Gamma, \wedge_\Gamma\rangle, \langle M, \wedge_M\rangle\rangle. \quad (2)$$

Базу сравнения B можно представить одной или несколькими базами сравнений, что позволяет ее формализовать с помощью теоретико-множественного пространства баз сравнения и конкретизировать в зависимости от содержания в виде группы аналогов, систем эталонов и нормативов качества.

Алгоритм оценивания A основывается на множестве операторов оценивания и соответствующим ему формализованном пространстве операторов оценивания θ. Множество операторов оценивания θ основано на логике сравнения L и использует заданные методы оценивания K. Результатом оценивания является оценка качества OK, при этом множеству OK соответствует пространство оценок O [13].

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Учитывая изложенное, система оценивания S_{OK} описывается многокомпонентным кортежем вида:

$$S_{OK} = \{\langle S, \wedge S\rangle, \langle R, \wedge_R\rangle, \langle \Gamma, \wedge_\Gamma\rangle, \langle M, \wedge_M\rangle, B, \theta, O\}. \quad (3)$$

Для дальнейшей работы введем понятие показателя качества выявления вредоносной информации. Пусть под мерой качества выявления вредоносной информации (μ) в информационном ресурсе (массиве, потоке, отдельных файлах) понимается отображение качества системы M или подмножества – отдельных ключевых свойств системы или их групп $\{m_i\} \subset M$ на множество вещественных чисел M_e:

$$\mu: M \to M_e \text{ или } \mu: \{m_i\} \to M_e. \quad (4)$$

Для представления (1) в семантическом виде заменим множество вещественных чисел M_e множеством семантических единиц S_e. Таким образом, имеем выражение вида:

$$s: M \to S_e \text{ или } s: \{m_i\} \to S_e. \quad (5)$$

Представим систему автоматизированного обнаружения вредоносной информации в структурном виде (рис. 1).

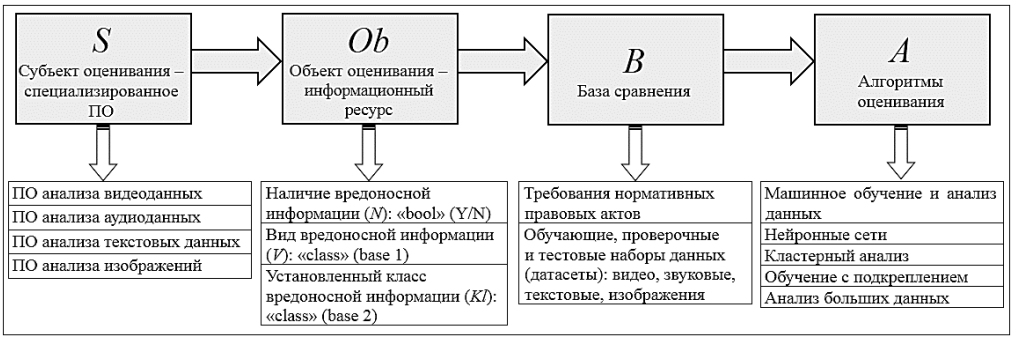

Рис. 1. Структурный вид системы автоматизированного обнаружения вредоносной информации
Примечание: составлено автором на основании данных, полученных в исследовании.

Исходя из описанной логики, в процессе оценивания (анализа) производится определение наличия вредоносной информации (*N*), вида вредоносной информации (*V*) и ее классификация с отнесением к одному из классов (*Kl*) в соответствии с федеральным законодательством.

В связи с тем, что процесс анализа информационных ресурсов является технически сложным и ресурсоемким, для его всестороннего моделирования целесообразно использовать нотацию Росса (IDEF0), основанную на концепции системного моделирования и предназначенную для описания сложных систем. На рис. 2 представлена функциональная модель информационно-технологических процессов анализа информационного ресурса на предмет наличия вредоносной информации, причиняющей вред здоровью и развитию детей.

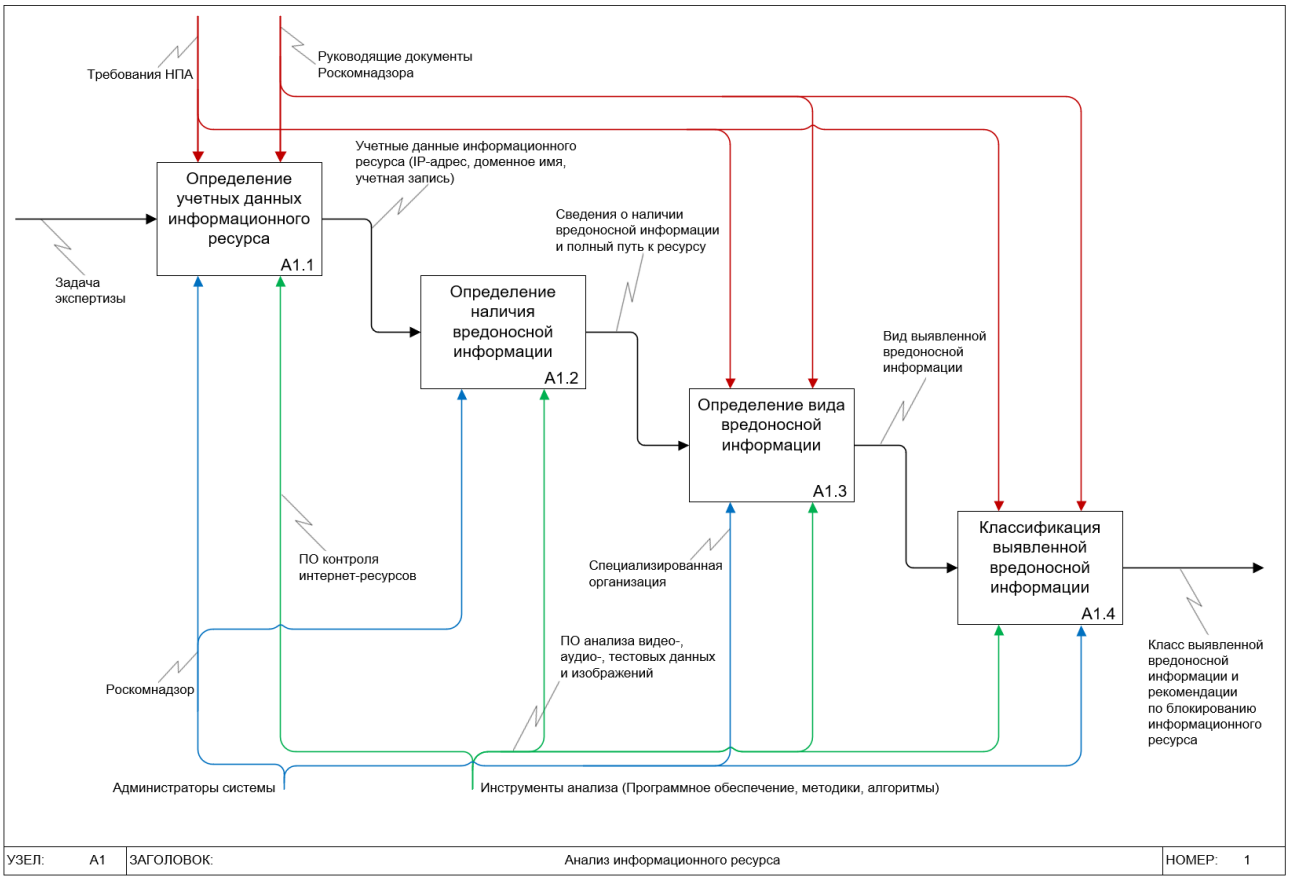

Рис. 2. Функциональная модель

Примечание: составлено автором на основании данных, полученных в исследовании.

Представленная функциональная модель анализа информационного ресурса на предмет наличия вредоносной информации в нотации IDEF0 определяет последовательность операций по выявлению вредоносной информации и ее классификации, а также механизмы, необходимые для качественного решения поставленной задачи на всех уровнях модели. Вместе с тем построение адекватной имитационной модели бизнес-процессов в системе автоматизированного выявления вредоносной информации требует перехода от описания системы в IDEF0 к дискретно-событийной модели с использованием аппарата систем массового обслуживания [14].

ЗАКЛЮЧЕНИЕ

Результаты исследования позволяют сделать следующие выводы:

1. Проведенный анализ показал, что защита детей и подростков от воздействия вредоносной информации требует комплексного применения современных информационных технологий, способных осуществлять поиск, выявле-

ние, классификацию и адресную блокировку вредоносных информационных ресурсов с заданными показателями качества.

2. Определен вид системы автоматизированного обнаружения вредоносной информации, учитывающий требования нормативных правовых актов по защите детей и подростков от воздействия вредоносной информации, а также возможности современных информационных технологий.

3. Сформирован и обоснован математический аппарат оценивания качества автоматизированного обнаружения вредоносной информации, разработана функциональная модель информационно-технологических процессов анализа информационного ресурса на предмет наличия вредоносной информации. Для повышения качества дальнейшей работы требуется переход от описания системы в IDEF0 к дискретно-событийной модели с использованием аппарата систем массового обслуживания, что позволит разработать инструментарий для выработки и оценивания управленческих решений.

Список источников

1. Медиапотребление 2022. URL: https://mediascope.net/upload/iblock/883/f11rt3k24o0ju2jkak4v0s0wr836wobp/MEDIAPOTREBLENIE_DIGITAL_14092022.pdf (дата обращения: 11.01.2023).
2. Симонова В. А., Лифинцева Е. А. Защита несовершеннолетних от негативной информации в Интернет // Научные известия. 2022. № 26. С. 128–131.
3. Титор С. Е., Каменева Т. Н. Деструктивное влияние интернета на поведение несовершеннолетних: результаты эмпирического исследования // Caucasian Science Bridge. 2022. Т. 5, № 4. С. 126–135.
4. Богомолов А. В., Чуйков Д. С., Запорожский Ю. А. Средства обеспечения безопасности информации в современных автоматизированных системах // Информационные технологии. 2003. № 1. С. 2–8.
5. Аветисян А. И. Кибербезопасность в контексте искусственного интеллекта // Вестник Российской академии наук. 2022. Т. 92, № 12. С. 1119–1123. DOI 10.31857/S0869587322120039.
6. Мамченко М. В., Мещеряков Р. В., Галин Р. Р. и др. Социокиберфизическая система для выявления и блокирования деструктивного Интернет-контента // Современные проблемы радиоэлектроники и телекоммуникаций : материалы 18-й Междунар. молодежной науч.-технич. конф., 10–14 октября 2022 г., г. Севастополь. Севастополь : Севастопол. гос. ун-т., 2022. С. 159.
7. Иванов А. А., Богомолов А. В. Архитектура гетерогенной информационной среды интеграции информационных ресурсов предприятий, решающих задачи инвестирования в человеческий капитал // Математические методы в технологиях и технике. 2022. № 8. С. 76–79.
8. Мещеряков Р. В., Исхаков С. Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. 2022. № 5. С. 82–99. DOI 10.21681/2311-3456-2022-5-82-99.
9. Тобин Д. С., Голосовский М. С., Богомолов А. В. Технология обеспечения достоверности информации при проведении сетевых экспертиз // Современные информационные технологии и ИТ-образование. 2020. Т. 16, № 3. С. 623–632.

References

1. Mediapotreblenie 2022. URL: https://mediascope.net/upload/iblock/883/f11rt3k24o0ju2jkak4v0s0wr836wobp/MEDIAPOTREBLENIE_DIGITAL_14092022.pdf (accessed: 11.01.2023). (In Russian).
2. Simonova V. A., Lifintseva E. A. Protecting children from negative information on the internet. *Scientific News*. 2022;(26):128–131. (In Russian).
3. Titor S. E., Kameneva T. N. Destructive influence of the Internet on behavior of minors: Results of empirical study. *Caucasian Science Bridge.* 2022;5(4):126–135. (In Russian).
4. Bogomolov A. V., Chuikov D. S., Zaporozhsky Yu. A. Sredstva obespecheniia bezopasnosti informatsii v sovremennykh avtomatizirovannykh sistemakh. *Information Technologies.* 2003;(1):2–8. (In Russian).
5. Avetisyan A. I. Kiberbezopasnost v kontekste iskusstvennogo intellekta. *Vestnik Rossiiskoi akademii nauk.* 2022;92(12):1119–1123. DOI 10.31857/S0869587322120039. (In Russian).
6. Mamchenko M. V., Meshcheryakov R. V., Galin R. R. et al. Socio-cyberphysical system for detecting and blocking destructive internet content. In: *Proceedings of the 18th International Young Scientists Conference "Modern Issues in Radioelectronics and Telecommunications "RT – 2022"",* October 10–14, 2022, Sevastopol. Sevastopol: Sevastopol State University; 2022. p. 159. (In Russian).
7. Ivanov A. A., Bogomolov A. V. Architecture of heterogeneous information environment for integration of information resources of enterprises solving problems of investing in human capital. *MMTT*. 2022;(8):76–79. (In Russian).
8. Meshcheryakov R. V., Iskhakov S. Yu. Study of compрometation indicators for improvement of information and cyberphysical systems protection facilities. *Voprosy kiberbezopasnosti*. 2022;(5):82–99. DOI 10.21681/2311-3456-2022-5-82-99. (In Russian).
9. Tobin D. S., Golosovsky M. S., Bogomolov A. V. Technology for ensuring the accuracy of information during network examinations. *Modern Information Technologies and IT-Educatio*n. 2020;16(3):623–632. (In Russian).

10. Шапошников В. А. Квалиметрия. Екатеринбург : Изд-во Рос. гос. проф.-пед. ун-та, 2016. 134 с.
11. Прудников С. И., Котляр А. В. Метод формирования ведомственных сетевых экспертных сообществ // Математические методы в технологиях и технике. 2023. № 3. С. 104–107. DOI 10.52348/2712-8873_MMTT_2023_3_104.
12. Субетто А. И. Квалиметрия: малая энциклопедия. Вып. 1. СПб. : ИПЦ СЗИУ – фил. РАНХиГС, 2015. 244 с.
13. Вечеркин В. Б., Галанкин А. В., Прохоров М. А. Методика оценивания устойчивости функционирования автоматизированной системы управления критической информационной инфраструктурой в условиях информационного воздействия // Известия Тульского государственного университета. Технические науки. 2018. № 6. С. 160–170.
14. Тихонов С. В. Методика перехода от IDEF0 к модели в терминах теории систем массового обслуживания при исследовании бизнес-процессов организации // Управление большими системами. 2008. Вып. 21. С. 5–15.

10. Shaposhnikov V. A. Kvalimetriia. Yekaterinburg: Publishing House of the Russian State Vocational Pedagogical University; 2016. 134 p. (In Russian).
11. Prudnikov S. I., Kotlyar A. V. Method of forming departmental network expert communities. *MMTT*. 2023(3):104–107. DOI 10.52348/2712-8873_MMTT_2023_3_104. (In Russian).
12. Subetto A. I. Kvalimetriia: malaia entsiklopediia. Is. 1. St. Petersburg: Publishing House of the North-West Institute of Management – Branch of the RANEPA; 2015. 244 p. (In Russian).
13. Vecherkin V. B., Galankin A. V., Prokhorov M. A. The methods for estimation of sustainability operation of automated control system of critical information infrastructure in the conditions of information influence. *News of the Tula State University. Technical Sciences.* 2018;(6):160–170. (In Russian).
14. Tikhonov S. V. Metodika perekhoda ot IDEF0 k modeli v terminakh teorii sistem massovogo obsluzhivaniia pri issledovanii biznes-protsessov organizatsii. *Large-Scale Systems Control.* 2008;21:5–15. (In Russian).

Информация об авторе

С. И. Прудников – кандидат технических наук, старший научный сотрудник.

Information about the author

S. I. Prudnikov – Candidate of Sciences (Engineering), Senior Researcher.