ISSN 1684-2588

Электросвязь

TELECOMMUNICATIONS

Ежемесячный научно-технический,
информационно-аналитический
и учебно-методический журнал

4 2020

УДК 004.75

Проблемы безопасности детей и подростков в Интернете и их решение с применением технологий больших данных

И.Я. АЛЕКПЕРОВА, канд. техн. наук, С.С. ОДЖАГВЕРДИЕВА

Институт информационных технологий НАНА, Баку, AZ 1141, Азербайджан

E-mail: airada.09@gmail.com

DOI: 10.31044/1684-2588-2020-0-4-23-31

Статья поступила в редакцию 06.08.2019
Принята после доработки 06.08.2019
Принята к публикации 21.01.2020

В виртуальном пространстве существуют две основные проблемы, связанные с безопасностью детей и подростков: проблемы со сбором, хранением и обработкой персональных данных детей и подростков и проблема с выявлением в виртуальной среде вредных ресурсов, предназначенных для детей. Для эффективного решения обеих проблем предложено использовать технологии больших данных и разработана схема распределенной системы для обработки веб-контента.

Ключевые слова: *интернет-безопасность детей, большие данные, социальные сети, интернет вещей, персональные данные, веб-контент, распределенная обработка данных.*

In connection with the development of the modern information society, information about people and events is mainly obtained from the virtual space. The active use of the global network is part of daily life of children and adolescents. New technologies play a large role in human development, contribute to the formation of modern society, and also create new problems related to child safety. In the virtual space, there are two main problems associated with the safety of children and adolescents: problems with the collection, the storage and the processing of personal data of children and adolescents, and the problem of the identifying in a virtual environment the harmful resources intended for children. To effectively solve both problems, it was proposed to use the big data technologies and a distributed system scheme for processing web content was developed.

Keywords: *children's internet security, big data, social network, personal data, web content, distributed data processing.*

Введение

Новые технологии играют большую роль в развитии человека, способствуют в формировании современного общества, а также создают новые проблемы, связанные с безопасностью детей. В связи с развитием современного информационного общества информация о людях и событиях в основном получается из виртуального пространства. Активное использование глобальной сети является частью повседневной жизни детей и подростков. В современном мире, где информационные технологии развиваются очень быстро, дети растут в окружении

цифровых устройств. Усовершенствование, применение в различных областях и увеличение количества этих устройств меняет поведение детей. Информация об их повседневной жизни собирается в различных информационных системах. Родители, различные страховые компании, банковские учреждения и ряд организаций пытаются извлечь из этой информации максимальную пользу. Цифровые устройства, интегрированные в жизнь детей, обеспечивают простоту, скорость и точность доступа и передачи информации, но также создают и определенные проблемы для безопасности детей. Наряду со многими положительными чертами информация о здоровье и поведении детей, которая собирается в разные базы данных с помощью этих цифровых устройств, также является психологическим средством и используется для личных интересов отдельных лиц, групп, организаций с целью нанесения ущерба деятельности отдельных и социальных субъектов [1].

Остаются актуальными задачи, связанные с поведением детей в виртуальном мире. Например, как цифровые устройства влияют на поведение детей, как использовать информацию, полученную через эти устройства, знают ли родители об интересах, увлечениях и друзьях детей в виртуальной среде и как защитить детей от опасности, исходящей от Интернета. Активное использование социальных сетей, мобильной связи и участие в различных сетевых играх являются частью повседневной жизни детей и подростков. Большинство из них могут открыто и без труда размещать свою личную информацию (имя, фамилию, домашний адрес, номер школы, в которой они учатся, контактные телефоны, интересы и т.д.) в социальных сетях, вебдневниках или блогах. Для подростка сейчас стало обычным поведение, когда часто обновляются профиль и статус в социальных сетях, идет активный обмен информацией о своих повседневных делах и событиях, общение с друзьями и обмен идеями в Интернете [2].

По мере развития Интернета начали появляться новые формы взаимодействия людей с информационными технологиями. Традиционное использование цифровых устройств, снабженных технологиями больших данных и генетическими алгоритмами, не только ускорило и увеличило качество обмена информацией, но также стало важным фактором для принятия решений во всех сферах жизни граждан. Новые платформы создают благоприятные условия для социализации молодых людей, но при этом актуализируют проблему защиты их персональных данных. Быстрое увеличение и обновление персональных данных на различных цифровых устройствах при обработке требуют использования технологий больших данных [3].

Большие данные — это большой объем, высокая скорость и большое разнообразие данных, которые требуют новых форм обработки. Под технологиями больших данных понимаются программные и аппаратные обеспечения, предназначенные для анализа больших и разнообразных массивов данных на лету, которые невозможно обрабатывать традиционными приложениями из-за сложного состава и нестабильности. Технологии больших данных сегодня применяются в здравоохранении, экономике, банковском деле, государственном управлении и во многих других областях. Для решения разнообразных задач сегодня широко используются данные из социальных сетей (Facebook и Twitter), поисковых систем (Google, Yahoo!, Yandex), различных форумов и блогов. Но проблемы с хранением, структурированием и обработкой этих данных сегодня все еще остаются очень актуальными.

Из-за того, что невозможно традиционными информационными системами определить, какой из быстрорастущих и обновляющихся интернет-ресурсов полезен, а какой вреден для детей и подростков, более целесообразно использовать в подобных задачах технологии больших данных. Целью исследования являются разработка концептуальной модели, предусматривающей обработку больших данных в распределенной файловой системе для выявления полезного веб-контента для детей, и эффективное решение вопросов безопасности молодого поколения.

1. Персональные данные детей и цифровые технологии

В последнее время стали актуальными проблемы в связи с проникновением цифровых объектов в нашу повседневную жизнь. Сегодня в жизни детей особое значение имеют цифровые устройства (сенсорные игрушки, устройства-напоминания о различных задачах, устройства слежения за активностью детей и т.д.), особенно детей младшего возраста, ведь их ежедневные занятия начинаются с устройств слежения и игрушек, снабженных датчиками (цифровые игрушки). Цифровые игрушки собирают информацию о поведении детей в течение определенного периода времени с помощью световых или специальных сигналов.

Есть много устройств, которые следят за поведением детей. Например, KidFit — это фитнес-снаряжение, которое регистрирует и регулирует физическую активность детей. HereO — это специальные часы с датчиками, которые передают информацию родителям о местонахождении детей [4]. Spourting — радионяня, регистрирует время сна и другие виды продолжительности поведения ребенка и гарантирует, что он всегда виртуально находится рядом с родителем, врачом и няней [5].

Примерами цифровых игрушек являются игрушки Teddy the Guardian [5]. Эта мягкая цифровая игрушка-медведь записывает, собирает и передает важные параметры здоровья, такие как сердцебиение, недостаток кислорода, температура тела и уровень стресса, в базу данных. Вполне вероятно, что эти данные могут быть использованы не только медицинским учреждением, но и другими организациями. Через определенное время, когда ребенок становится постарше, возрастает интерес его к мобильным устройствам, компьютерам, планшетам и другим современным технологиям. Сегодня использование цифровых технологий детьми далеко от обычной традиции использования мыши и клавиатуры. Они заменены современными формами взаимодействия, такими как сенсорный экран, интеллектуальные устройства (интернет вещей, устройства распознавания жестов и т.д.).

Интеллектуальные устройства с поддержкой Интернета передают информацию, собранную из окружающей среды, с использованием встроенных датчиков, программного обеспечения и процессоров. После начальной настройки большинство интеллектуальных устройств работают автоматически, собирая и отправляя информацию в определенные базы данных. А это приводит к созданию огромного количества данных, которые должны быть надежно сохранены, обработаны и представлены в цельной, эффективной и легко интерпретируемой форме. Интеллектуальные устройства часто собирают пользовательские данные без их разрешения. Интернет вещей является примером цифровых технологий и способен получать данные о поведении, состоянии здоровья людей и социально-экономическом положении семьи [6].

С автоматическим потоком информации и связью между цифровыми устройствами приходит новый набор рисков кибербезопасности. Если родители могут удаленно получить доступ ко всем данным о своих детях, то киберпреступники тоже смогут это сделать. Наличие большого количества устройств в одной сети дает возможность киберпреступникам иметь разные точки доступа к персональным данным. Например, телевизор, «смарт-часы» или любые другие устройства, оснащенные датчиками и подключенные к домашней сети, которая не защищена должным образом, могут стать ключом для персональных данных.

Сегодня бесконтактные датчики являются образцами улучшения сенсорных технологий. При сборе персональных данных большое значение имеет интернет вещей, хотя при решении вопроса безопасности этих данных важно учитывать вопросы нормативно-правового регулирования, кибербезопасности и стандартизации. Вопросы правового регулирования остаются пока открытыми. Не существует конкретных законов, которые охватили бы различные уровни проблем, касающихся интернета вещей. Интеллектуальные устройства, подключенные через сеть друг к другу, создают риски и множество вопро-

сов безопасности, и никакие существующие правовые законы не рассматривают такие риски.

Различные популярные веб-проекты, такие как YouTube, Facebook, Twitter, являются основными источниками информации [7]. Сбор персональных данных является результатом следующих процессов:

1) каждый день миллионы фотографий и видео загружаются в социальные сети, блоги, сайты знакомств детьми и подростками;

2) миллионы детей и подростков делятся своими идеями, эмоциями и интересами с помощью мультимедийных ресурсов через социальные сети. Эта информация очень часто остается на их личной странице, что позволяет подключаться к ним в любое время;

3) возможности социальных сетей определяют онлайн-активность детей и подростков, и чем больше активность, тем больше личной информации можно собирать и анализировать.

Захват скрытых персональных данных детей и подростков через социальные сети может создать серьезные проблемы. Социальные сети идентифицируют активность, интерес, досуг и занятость каждого ребенка. Такая ситуация может подрывать не только безопасность молодого поколения, но и безопасность целых семей и общества в целом. Например, анализ персональных данных о детях и подростках дает представление о социально-экономической и психологической ситуации в семье, а также о демографическом положении в стране [8].

Теоретически любая информация в Интернете доступна всем, в том числе детям и подросткам. Единого закона о защите детей в виртуальной среде и о запрете какой-либо веб-страницы не существует, поэтому регулирование осуществляется на основе национального законодательства. Например, американский закон о защите конфиденциальности детей в интернете 1998 г. (The Children's Online Privacy Protection Act — COPPA) обеспечивает защиту персональных данных детей и предъявляет определенные требования к операторам веб-сайтов и онлайн-служб, предназначенных для детей в возрасте до 13 лет [9]. COPPA является федеральным законом США, предназначенным для ограничения сбора и использования личной информации о детях операторами интернет-услуг и веб-сайтов. Принятый Конгрессом США в 1998 г. закон вступил в силу в апреле 2000 г. COPPA запрещает участие ребенка в игре, предложение приза или другое действие в отношении ребенка, раскрывающее больше личной информации, чем это разумно необходимо для участия в такой деятельности. А также требует от оператора любого веб-сайта или онлайн-службы, которая собирает персональные данные детей, разместить на веб-сайте уведомление о том, какая информация собирается, как оператор раскрывает и использует такую информацию. К сожалению, COPPA распространяется только на компании, ведущие бизнес в США, в то время как Интернет имеет глобальный охват.

Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» доказывает необходимость защиты детей и подростков от информационного воздействия, способного причинить вред их здоровью и психологическому состоянию. Несмотря на то что закон неоднократно подвергался изменениям и дополнениям, в нем четко сформулированы виды информации, причиняющие вред здоровью и развитию детей. К ним относятся информация, «побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий», а также «способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртсодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством» и т.д. [10].

Отсутствие единого закона в отношении защиты детей в интернет-среде переклады-

вает проблему на саморегулирование, поэтому во многих странах ответственность за доступ детей к веб-ресурсам несут родители. Известно, что своевременное получение достоверной информации о своих детях отвечает интересам родителей. Собранная информация о детях формирует большие данные в базе данных и порождает разногласия относительно того, насколько эти данные полезны или вредны для детей. Родителям часто сложно принимать решения об использовании веб-ресурсов, которые предоставляют большие данные. Возникают следующие проблемы:

- отсутствие прозрачности. Есть вероятность использования персональных данных детей преступными группами. Поскольку персональные данные детей передаются в различные базы данных, родители часто не знают о цели использования этих данных;
- сложность, разнообразие и скорость больших данных увеличивают вероятность ошибки в их анализе. В некоторых случаях системный администратор предоставляет информацию, которая не отражает правду о ребенке из-за сбоя программного обеспечения или отсутствия необходимых технологий. В результате доверие родителя к системе снижается;
- вероятность искажения данных. Статистические данные, собранные о детях, могут быть искажены из-за сбоя устройства или сети;
- недоверие между родителями и детьми. Аналитические системы, предназначенные для обработки персональных данных детей и подростков, способствуют изменению отношений между родителями и детьми. Часто мнение детей не учитывается, когда родители принимают решения исключительно на основе персональных данных.

Принимая во внимание процессы, происходящие в современном мире, мы видим, что, несмотря на существующие проблемы, родителям необходимо быстро получать нужную информацию о своем ребенке (его здоровье, поведении и т.д.). Статистические данные о поведении детей и подростков в период обучения и отдыха включаются в базы данных образовательных учреждений. Эти показатели постепенно увеличиваются и начинают работать совместно с другими системами (банковские системы, медицинские учреждения, страховые компании и т.д.).

2. Свойства больших данных в анализе веб-контента для детей

Высокая активность детей и подростков в виртуальной среде, а также увеличение объема вредоносной информации в ней указывают на актуальность технологий больших данных для решения проблем, связанных с обеспечением безопасности детей в интернет-среде. Здесь основная проблема связана с обработкой черезмерно большого количества неструктурированных данных. Неструктурированные данные, такие как текстовые сообщения, аудио- и видеофайлы, являются данными, не позволяющими осуществлять легкий доступ к элементам данных. Структурированные же данные, напротив, организованы так, чтобы каждый элемент в разных сочетаниях был доступен. Данные также могут быть полуструктурированными. Такие данные хотя и не организованы в структуру, но имеют дополнительные данные, позволяющие обращаться к элементам этих данных. Традиционные реляционные базы данных поддерживают только структурированные данные, но многие базы данных нового поколения, поддерживающие технологии больших данных, могут работать с полуструктурированными, а также неструктурированными в некоторой степени данными [11]. Анализ больших данных требует учета следующих основных параметров данных [12]:

1) объем данных. При анализе больших данных первая задача состоит в том, можно ли массив данных считать большим. Объем данных, которые предоставляют аудио- и видеофайлы, данные в виде текста, таблиц, схем и т.д., определяет, можно ли анализировать их как большие данные;

2) многообразие данных. Многообразие больших данных затрудняет процесс анализа. Для эффективного анализа данных в первую очередь требуются очистка, агрегирование и структурирование больших данных;

3) скорость обработки. Все данные, полученные через запрос браузера, сначала ге-

нерируются и сохраняются в базе данных. Выполнение быстрого анализа больших файлов в течение определенного периода времени требует использования быстрых алгоритмов. В то же время следует учитывать, что чем выше скорость обработки данных, тем лучше интерактивность;

4) нестабильность данных. Основной проблемой при обработке больших данных в режиме онлайн является нестабильность данных во времени, создающая определенные трудности при управлении данными. Например, если веб-ресурс, который считается полезным носителем информации для детей, ранее содержал вредоносный контент, то это следует учитывать при обработке, т.е. такие веб-страницы считаются подозрительными;

5) сложность данных. Данные для анализа поступают из разных источников. Также веб-страницы имеют сложную семантику. Ссылки между страницами бывают разных типов: внутренние ссылки, ссылки на другие веб-страницы внутри сайта и в конечном счете на внешние проекты (различные веб-сайты). И такая путаница затрудняет анализ веб-контента;

6) достоверность данных. Точность анализа зависит в первую очередь от источника и от качества собранных данных.

Данные, собранные на сервере в результате запросов детей, не всегда доступны в случайном порядке. Основная проблема здесь заключается в том, что статистический анализ больших, сложных и гетерогенных данных может привести к неправильному и неточному выбору переменных и алгоритмов. Поэтому при выявлении полезных данных для детей важно принимать во внимание риски, связанные с проверкой, отбором, измерением и получением ответов [13].

3. Распределенная обработка данных

Эффективная обработка больших данных основана на технологии распределенных файловых систем [14, 15]. При параллельной обработке информации данные распределяются по кластеру и одна и та же задача выполняется параллельно на каждом узле кластера. В распределенных системах данные хранятся и индексируются в источнике данных, расположенном на нескольких серверах, а не в одной файловой системе (рисунок). С этой точки зрения, лучше использовать параллельные и распределенные системы управления базами данных при обработке веб-контента и обрабатывать данные на пересечениях, где они расположены.

Методы анализа больших данных, полученных из Интернета, для выявления вредных и полезных ресурсов, предназначенных для детей могут быть следующие: методы статистического анализа, кластерный анализ, классификация и ассоциативные правила, прогнозирование с использованием моделей на основе машинного обучения, генетические алгоритмы и т.д. Инструменты, используемые в традиционном хранилище данных, — это многомерный анализ, регрессия, классификация, кластеризация и обнаружение данных. Используя многомерные методы анализа, можно разделить информацию по назначению, например, веб-контент предназначенный для детей младше 12 лет или для пользователей старше 18 лет и т.д. Собранная информация сохраняется и индексируется в хранилище данных. Для загрузки из разных

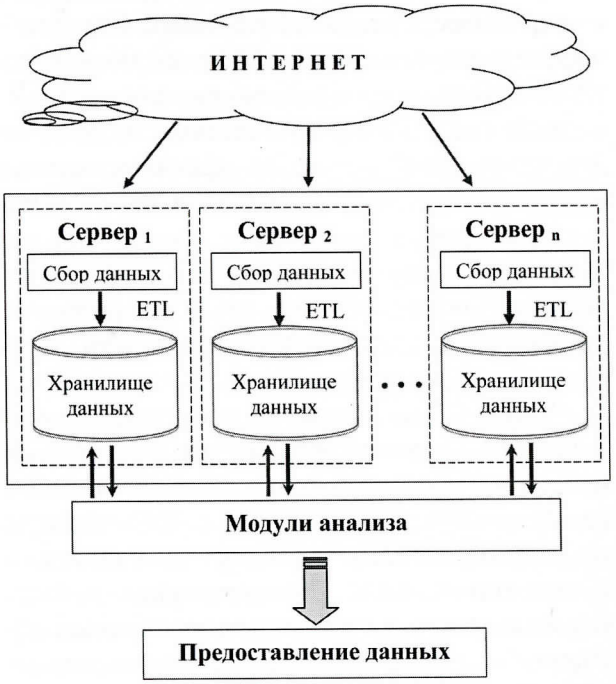

Схема распределенной системы для обработки веб-контента

источников и преобразования больших данных предлагается использовать технологию ETL (Extract, Transform, Load). ETL может использовать как временные, так и постоянные данные. При работе с традиционными хранилищами данных агрегированные данные используются для решения определенных проблем, например, при настройке несоответствий между данными [16].

Чтобы подготовиться к процессу обработки информации, данные должны быть переданы на заранее подготовленные серверы. Однако проблема заключается в том, что данные в виртуальной среде приводятся в распределенном виде и каждая веб-страница отструктурирована и отформатирована в соответствии с запросом специалиста, создавшего этот материал. Учитывая это на первом этапе необходимы очистка и группировка данных.

Качество анализа зависит от правильного распределения данных. Распределение данных для аналитической базы данных приводит к минимальному количеству обмена информацией между перекрестками при выполнении запросов. Следует иметь в виду, что использование логического блока во время обработки больших данных полезно, если все данные в традиционной базе данных передаются из логического блока, ответственного за их преобразование, очистку, проверку и загрузку.

Использование интеллектуальных методов анализа и гибридных алгоритмов при решении задачи позволяет получить более эффективные результаты [13, 17, 18]. Примерами наиболее популярных технологий для работы с большими данными являются модель MapReduce, предложенная Google, и программное обеспечение Hadoop с открытым исходным кодом, предлагаемое Apache Software Foundation. В этих системах нет необходимости включать данные в таблицы и следовать строгой иерархии. Прежде чем анализировать, нужно просто сгруппировать данные.

MapReduce считается основной системой обработки больших данных благодаря своей простоте, масштабируемости и точной отказоустойчивости. MapReduce — это вычислительная модель распределенной базы данных, обеспечивающая эффективное распределение данных и используемая для параллельных вычислений на больших наборах данных. MapReduce обеспечивает безопасность системных данных. Распределенная файловая система закрывает кластер и хранит несколько копий каждого кластера на разных серверах, а также поддерживает отключения [19, 20].

Карта для начальной обработки входных данных (Map) показывает, где распределенные данные выделяются рабочим узлам, т.е. отдельным узлам, которые служат в качестве запрашиваемой части информации и хранят информацию об алгоритмах и результатах, использованных при обработке. Основное требование для эффективного распределения данных состоит в том, чтобы число узлов, соединяющих подгруппы, было минимальным. Если существует алгоритм решения какой-либо из разделенных проблем, то этот алгоритм может использоваться для решения других проблем того же класса. Результаты суммируются в конце операции (Reduce). Например, алгоритм будет вычислять промежуточные суммы в каждом соединении параллельной файловой системы, чтобы найти окончательную сумму, а затем собирать эти промежуточные цены. Чтобы повысить эффективность и компетентность каждой части информации, наиболее целесообразно хранить данные в нескольких экземплярах на выделенных серверах.

Пользовательская функция Reduce агрегирует значения с одним и тем же ключом и генерирует их. Окончательные результаты сохраняются в глобальной файловой системе. Если система Map или Reduce по какой-либо причине не работает, задача передается на другой сервер из файловой системы. После завершения всех задач пользовательская программа выполняет визуализацию данных. Вдохновленные MapReduce, существуют также специальные системы для определенных приложений, такие как машинное обучение, потоковая обработка данных и т.д. [21].

Предлагаемая система имеет несколько преимуществ:

- отказоустойчивость. Система может справиться с мелкими сбоями, минимизировать

объем потерянной работы, и не нужно перезапускать систему;
- конфигурация и установка системы относительно просты. Не требуется большого опыта программиста в работе параллельной и/или распределенной системы;
- гибкость системы. Входные данные в системе могут иметь любой формат вместо конкретной схемы;
- система может масштабироваться до тысяч процессоров. Это позволяет более точно обрабатывать большой обьем данных, предназначенных для детей любого возраста.

При распределенной обработке данных отдельные компоненты системы могут быть реализованы на разных языках программирования, что облегчает работу системных программистов. Различные типы данных в распределенных системах повышают надежность системы. Поскольку здесь используется клиент-серверная архитектура, порты сервера и клиента системы расположены на отдельных серверах, что обеспечивает надежность и прозрачность системы. Интеллектуальная система, которая выполняет распределенный анализ данных, разнообразна. Другими словами, анализ данных детей и подростков, а также анализ веб-контента предназначенного для детей, могут проводиться как индивидуально, так и в составе групп.

Предлагаемая система также может предсказать проблему, которая важна при принятии решений. Например, анализируя индивидуальные данные детей, можно определить их интересы, здоровье и психологическое состояние, что, в свою очередь, покажет, какие дети из группы риска могут иметь в будущем серьезные проблемы.

Основная проблема при параллельной обработке — предоставление результатов и вероятность ошибок при обработке. В идеале визуализация результатов должна быть автоматической и прозрачной, чтобы избавить пользователей от необходимости иметь дело с деталями обработки и изменениями конфигурации программ. Удачная визуализация результатов может привести к более эффективному использованию ресурсов, позволит без особых усилий применять системные ресурсы среди разных пользователей, изолируя и защищая их друг от друга для обеспечения конфиденциальности и безопасности. Обработка больших данных может быть завершена только с использованием специальных технологий, которые обеспечивают параллельную обработку данных. Важные параметры, типичные для больших данных, также должны учитываться при обработке. Например, интенсивность взаимодействия в сети, контроль компьютера со стороны родителей, опыт специалистов, скорость обработки и т.д. Следует иметь в виду, что измерение ошибок является одной из важных проблем, когда данные слишком велики.

Большие данные требуют много усилий для обработки, и лучший метод для решения этой проблемы — распределенная обработка данных. Такой подход может помочь быстро анализировать большие данные, обеспечить информационную безопасность детей и подростков, защищая их от вредного веб-контента. Распределенная обработка данных важна не только для реализации процесса обработки с более быстрым и точным результатом, но и для обеспечения безопасности персональных данных детей и подростков.

Заключение

Анализ проблем, связанных с информационной безопасностью детей и подростков в Интернете, показал, что безопасность детей во Всемирной сети тесно связана с проблемой больших данных и имеет два направления:
- проблема больших данных, возникающая из личной информации детей. Это проблема, созданная данными, собранными через Интернет, социальные запросы, различные аналитические и статистические системы;
- проблема с большими данными при определении полезного или вредного веб-контента для детей. Таким образом, эффективное решение вопроса о том, являются ли большие данные, собранные в виртуальной среде, полезными или вредными для детей и подростков, создает трудности и требует применения новых научных подходов.

Существующие проблемы со сбором, обработкой и предоставлением больших данных

позволяют предположить, что для эффективного структурирования и хранения обрабатываемых данных детей и подростков требуются особые условия, и, поскольку эти данные отличаются, сбор и обработка их на традиционном сервере неэффективны. Быстрый анализ больших данных и многократный рост производительности, полученный за счет параллельной обработки задач, важны для обеспечения информационной безопасности любого государства. А безопасность персональных данных детей и подростков является необходимым условием для защиты доверия и репутации граждан страны путем предотвращения рисков для их социально-экономической жизни.

СПИСОК ЛИТЕРАТУРЫ

1. **Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.** Социальные сети: модели информационного влияния, управления и противоборства. М.: Издательство физико-математической литературы, 2010. 228 с.
2. **Оджагвердиева С.С.** Проблемы формирования законодательной базы детской интернет-безопасности в среде электронного государство // «Актуальные междисциплинарные научно-практические проблемы информационной безопасности». Материалы IV Республиканской конференции. 14 декабря 2018 г. Баку. С. 228—232.
3. **Alguliyev R.M., Imamverdiyev Y.N.** Big Data: Big Promises for Information Security // Proceedings of the 8th International Conference on Application of Information and Communication Technologies. 15—17 Oct. 2014. IEEE, Astana. P. 1—4.
4. **http:**//www.smartwatches4u.com/news/Top-Kids-GPS-Tracking-Smartwatches. Top 10 Kids GPS Tracking Smartwatches 2018, online.
5. **Marches A., Duncan P., Plovman L., Sabeti S.** Three questions about the Internet of things and children // TechTrends. 2015. V. 59. Is. 1. P. 76—83.
6. **Алгулиев Р.М., Махмудов Р.Ш.** Интернет вещей // Информационное общество. 2013. Вып. 3. С. 42—48.
7. **Алгулиев Р.М., Алекперова И.Я.** Оценка социального кредита граждан по персональным данным в среде электронного государства: проблемы и перспективы // Проблемы информационного общества. 2019. № 1. С. 3—13.
8. **Ziegeldorf J.H., Morchon O.G., Wehrle K.** Privacy in the Internet of Things: Threats and Challenges // Security and Communication Networks. 2015. V. 7. No 12. P. 1—14.
9. **http:**//www.coppa.org/. Children's Online Privacy Protection Act, online.
10. **Федеральный** закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», online: http://ivo.garant.ru/#/document/12181695/paragraph/39:0.
11. **Carlin S., Curran K.** Cloud Computing Technologies // International Journal of Cloud Computing and Services Science (IJ-CLOSER). 2012. V. 1 P. 59—65.
12. **Andreu-Perez J., Poon C.C. Y., Merrifield R.D., Wong S.T.C., Yang G.-Z.** Big Data for Health // Journal of Biomedical and Health Informatics. 2015. V. 19. No 4. P. 1193—1208.
13. **Couper M.** Is the sky falling? New technology, changing media, and the future of surveys // Survey Research Methods. 2013. V. 7. No 3. P. 145—156.
14. **Suthaharan S.** Big Data Classification: Problems and Challenges in Network Intrusion Prediction with Machine Learning // ACM Sigmetrics Performance Evaluation Review archive. 2014. V. 41. No 4. P. 70—73.
15. **Parhami B.** Parallel Processing with Big Data // Springer International Publishing AG, Encyclopedia of Big Data Technologies, 2018, https://www.ece.ucsb.edu/~parhami/pubs_folder/parh19b-ebdt-parallel-proc-big-data.pdf.
16. **Das S., Abraham A., Konar A.** Automatic clustering using an improved differential evolution algorithm // IEEE Transaction on Systems, Man, and Cybernetics — Part A: Systems and Humans 38. 2008. P. 218—237.
17. **Thusoo A., Sarma J.S., Jain N., Shao Z., Chakka P., Zhang N., Antony A., Liu H., Murthy R.** Hive — A Petabyte Scale Data Warehouse Using Hadoop // Proceedings of the 26th International Conference on Data Engineering (ICDE), 2010 IEEE, 1—6 March, 2010. Long Beach. P. 996—1005.
18. **Hunt P., Konar M., Junqueira F.P., Reed B.** ZooKeeper: wait-free coordination for internet-scale systems // Proceedings of the 2010 USENIX conference on USENIX annual technical conference. Berkeley, CA, USA: USENIX Association. 2010. P. 11—12.
19. **Валинуров К.Р., Михайлова М.В.** Распределенные системы вычислений на примере Apache Hadoop // Международной научно-практической конференции «Научное сообщество студентов XXI столетия. Технические науки», г. Новосибирск, 30 марта 2017 г. 2017. № 3 (50). С. 76—79.
20. **Zhang Y., Cao T., Li Sh., Tian X., Yuan L., Jia H., Vasilakos A.V.,** Parallel Processing Systems for Big Data: A Survey // Proceedings of the IEEE. 2016. V. 104. Is. 11. P. 2114—2136.