DOI: 10.18137/RNU.V9187.22.02.P.157 УДК 004.891

С.В. Пилькевич, К.О. Гнидко, В.А. Лохвицкий, А.С. Дудкин, О.С. Иванов, Т.Р. Сабиров

ДЕМОНСТРАТОР ПРОГРАММНО-ТЕХНИЧЕСКОГО СРЕДСТВА АВТОМАТИЗИРОВАННОГО РАСПОЗНАВАНИЯ ВРЕДОНОСНЫХ МУЛЬТИМЕДИЙНЫХ ОБЪЕКТОВ В СЕТИ ИНТЕРНЕТ (ИТОГИ ИССЛЕДОВАНИЯ)

Аннотация. Представлено обобщение результатов исследования, проведенного авторским коллективом в 2018–2021 годах в рамках грантового финансирования РФФИ[1]. В частности раскрыты обоснования использованных в исследовании подходов для достижения заявленной цели; перечислены задачи, решение которых способствовало достижению требуемых результатов; обозначены концептуальные положения, в русле которых построена логика разработанных решений; описаны возможности и ограничения созданного демонстратора – программно-технического средства выявления и интеллектуальной обработки деструктивного мультимедийного интернет-контента. Представлены результаты тестовой эксплуатации разработанного программно-технического средства (демонстратора), позиционируемого авторами в качестве элемента интеллектуальной системы защиты здоровья интернет-пользователя путем автоматизированной интеллектуальной обработки интернет-трафика, выводимого на пользовательский монитор, что способствует обеспечению информационно-психологической безопасности населения. Обозначены направления дальнейшего усовершенствования демонстратора.

Ключевые слова: информационно-психологическая безопасность, здоровье интернет-пользователя, интеллектуальная система защиты, потенциально вредоносная информация, программно-технические средства.

S.V. Pilkevich, K.O. Gnidko, V.A. Lokhvitskiy, A.S. Dudkin, O.S. Ivanov, T.R. Sabirov

DEMONSTRATOR OF A HARDWARE AND SOFTWARE TOOL AUTOMATED DETECTION OF MALICIOUS MULTIMEDIA OBJECTS ON THE INTERNET (SUMMARY OF RESEARCH)

Abstract. The results of the research conducted by the author's team in 2018-2021 are presented. The rationale of the approaches used in the study to achieve the goal is disclosed; the tasks, the solution of which contributed to the achievement of the required results, are listed; the conceptual provisions, within which the logic of the developed solutions is built; the capabilities and limitations of the created hardware and software tool for identification and intelligent processing of destructive multimedia Internet content are described. The results of experimental operation of the developed tool, which is an element of the intellectual health protection system for Internet users, are presented. Directions for further improvement of the developed hardware and software complex are outlined.

Keywords: information-psychological safety, Internet-user health, intelligent protection system, potentially malicious information, software and hardware.

[1] № 18-29-22064 мк: «Модели и методы выявления и интеллектуальной обработки деструктивного мультимедийного интернет-контента».

Пилькевич Сергей Владимирович
доктор технических наук, доцент кафедры систем сбора и обработки информации. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: моделирование сложных социотехнических систем; криптографические методы защиты информации. Автор более 100 опубликованных научных работ.
Электронный адрес: ambers@list.ru

Гнидко Константин Олегович
доктор технических наук, доцент, профессор кафедры систем сбора и обработки информации. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: искусственный интеллект; машинное обучение; информационно-психологическая безопасность; моделирование социальной динамики. Автор более 100 опубликованных научных работ.
Электронный адрес: greeny598@yandex.ru

Лохвицкий Владимир Александрович
доктор технических наук, преподаватель кафедры систем сбора и обработки информации. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: моделирование сложных социотехнических систем, криптографические методы защиты информации. Автор более 100 опубликованных научных работ.
Электронный адрес: vovan296@mail.ru

Дудкин Андрей Сергеевич
кандидат технических наук, заместитель начальника кафедры систем сбора и обработки информации. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: технологии разработки программного обеспечения; методы машинного обучения; СУБД; математическое моделирование. Автор более 40 опубликованных научных работ.
Электронный адрес: andry-ll@mail.ru

Иванов Олег Сергеевич
кандидат медицинских наук, и. о. заведующего научно-исследовательской испытательной лабораторией промышленной медицины. Научно-исследовательский институт промышленной и морской медицины Федерального медико-биологического агентства России, Санкт-Петербург. Сфера научных интересов: психометрия; промышленная и морская медицина; онтологический инжиниринг; социальная психология; экспертные ассистирующие системы. Автор более 40 опубликованных научных работ.
Электронный адрес: sibivolga@ya.ru

Сабиров Тимур Римович
кандидат технических наук, старший преподаватель кафедры систем сбора и обработки информации. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: информационная безопасность; искусственный интеллект; онтологический инжиниринг. Автор более 30 опубликованных научных работ.

Введение

В первой половине текущего века одним из трендовых направлений, представленных широкомасштабными фундаментальными и прикладными исследованиями, является проблема взаимодействия человека с интернет-пространством [6; 7]. Данные исследования проводятся в русле многих научных дисциплин. Однако в качестве инструментария преи-

мущественно используются нейрокогнитивные и нейрокомпьютерные технологии [14]. И это очевидно: качественно новые знания чаще появляются с представлением новых данных и (или) их новых комбинаций. И то, и другое становится доступным при усовершенствовании инструментария – программных и аппаратных средств извлечения и обработки больших и (или) малозаметных данных.

Проблема взаимодействия человека с интернет-пространством стала актуальной в связи с тем, что настоящий этап существования мировой цивилизации ознаменован тотальным подключением индивида к Сети. То, что происходит в Сети, значительно, а в отдельных случаях критически влияет и на поведение отдельных субъектов, и на поведение масс [6]. Поведение масс является фактором безопасности в любом масштабе рассмотрения. Получение практически применимых результатов, повышающих процент распознавания и нейтрализации потенциально вредоносных мультимедийных объектов в сети Интернет, способных нанести ущерб индивидуальному, групповому и массовому сознанию и психофизиологическому состоянию граждан Российской Федерации, является деятельностью по обеспечению государственной безопасности нашей страны.

В этой связи Российский фонд фундаментальных исследований (РФФИ) в 2018 году объявил конкурс на лучшие научные проекты междисциплинарных фундаментальных исследований, в том числе по теме 26-822 «Фундаментальные проблемы взаимодействия человека с интернет-пространством: нейрокогнитивные и нейрокомпьютерные технологии» [13]. В рамках данного конкурса получили государственную финансовую поддержку такие исследовательские проекты, как «Психологическое и генетическое исследование предикторов, определяющих поведение пользователей при восприятии интернет-контента различной информационной направленности»; «Особенности реализуемых в интернет-пространстве когнитивных моделей взаимодействий между индивидуумами»; «Разработка научно-методических подходов к анализу интернет-дискурса электронного участия в социальных сетях»; «Разработка психологических агентных моделей реакций сетевых сообществ на информационные сообщения различной модальности»; «Разработка социокиберфизической системы мониторинга разнородного интернет-контента в целях противодействия проявлению агрессии, давления и других форм деструктивного воздействия на индивидуальное и групповое сознание пользователей»; «Методология построения когнитивных ассистентов, предотвращающих виктимное поведение в информационном пространстве, на основе современных концепций распределенных вычислений и технологий интеллектуального анализа данных»; «Мониторинг и выявление деструктивных информационных воздействий и негативных личностных тенденций молодого поколения при взаимодействии с интернет-пространством на основе методов нейрокомпьютерной и нейросетевой обработки интернет-контента»; «Персональные когнитивные ассистенты, сопровождающие деятельность человека в информационном пространстве»; «Разработка методов нейросетевого анализа визуального интернет-контента пользователей социальных сетей с целью автоматизированного определения выраженности личностных черт, связанных с психологическим неблагополучием»; «Разработка комплексного подхода к анализу русскоязычных аудио-, видео- и текстовых материалов с целью выявления агрессивного поведения пользователей информационного пространства на основе нейросетевых технологий»; «Разработка методологии моделирования когнитивных функций на основе данных нейропсихологии и нейрофизиологии, когнитивной психологии, лингвистики»; «Разработка моделей и методов выявления ин-

формационных угроз и защиты от них в интернет-пространстве» и др. Всего из 2018 поддержано РФФИ 24 проекта по рассматриваемой в данной публикации тематике.

Среди перечисленного списка исследовательских работ был представлен и авторский проект «Модели и методы выявления и интеллектуальной обработки деструктивного мультимедийного интернет-контента» [15].

Цель проекта – получить практически применимые результаты, повышающие результативность распознавания и нейтрализации потенциально вредоносных мультимедийных объектов в сети Интернет, способных нанести ущерб индивидуальному, групповому и массовому сознанию и психофизиологическому состоянию граждан Российской Федерации.

В рамках работ по достижению цели авторским коллективом были сформулированы следующие **задачи**.

1. Осуществить системный анализ угроз информационно-психологической безопасности пользователей автоматизированных систем, а также применяемых в Российской Федерации и за рубежом нормативно-правовых, организационных и технических мер по обеспечению защиты пользователей от негативного контента, способного причинить вред их здоровью и развитию.

2. Выполнить исследование путей повышения результативности выявления скрытых информационных вложений в мультимедийных потоках данных. Разработать концептуальную модель системы распознавания потенциально вредоносных конструкций в потоках данных специального вида.

3. Разработать методы и алгоритмы обнаружения потенциально вредоносной информации в мультимедийных потоках данных и снижения скорости ее распространения в социальных сетях с применением математического аппарата интеллектуального анализа данных (Data Mining) и нейросетевых технологий, осуществление их программной реализации.

4. Провести экспериментальные исследования по практическому обнаружению и блокированию потенциально вредоносной информации в файлах мультимедийных форматов, а также по анализу топологии больших графов с целью обнаружения ключевого подмножества дуг, влияющих на возможность неконтролируемого (эпидемиологического) распространения информации по сети.

Обзор работ по вопросу исследования

Решение поставленных задач осуществлялось путем декомпозиции их на подзадачи, результаты решения которых, а также концепция всего исследования излагаются ниже.

Обоснование актуальности исследования описано в работе [16]. В публикации перечислены угрозы национальной безопасности в информационной сфере, которые создают предпосылки для расширения спектра междисциплинарных фундаментальных исследований, ориентированных на решение проблем нейрокомпьютерного и нейрокогнитивного взаимодействия человека с интернет-пространством. Существующая ситуация и тренды в данной области обосновывают востребованность программно-технических средств защиты от вредоносного информационного контента. Обозначенная проблематика сопряжена с необходимостью формирования системы формализованных признаков, позволяющих построить решающие правила объективного отнесения тех или иных информационных сообщений, распространяемых по сети Интернет к классу потенциально вредоносных. Развитие положений цитируемой выше публикации изложено в работе, описывающей требуемую функциональность программно-технических средств мониторинга и защиты потребителей (пользователей) интернет-контента от психотравмирую-

щей информации, «Признаковое пространство потенциально вредоносного контента: от гипотезы к эксперименту» [18]. В частности, в работе изложен подход к проведению экспериментального исследования, направленного на получение признаков, характерных для потенциально вредоносного контента. На основе экспериментально полученной информации стало возможным выработать решающие правила для автоматического обнаружения деструктивного мультимедийного интернет-контента.

В ходе разработки темы исследования стало также понятно, что необходимо уточнить смысловое наполнение терминов, которыми будут описываться различные аспекты выполняемой работы. Решению этой подзадачи посвящена публикация [11], где рассматривается проблема совместного использования терминологического аппарата разных предметных областей для описания процесса воздействия информационных сообщений на мышление, эмоциональную сферу и поведение индивида и группы. Описан алгоритм формализованного перехода от номинальной к интервальной шкале оценок информационного воздействия контента на состояние психики индивида. Обосновывается перечень методов исследования проявлений контаминации психики человека, взаимоувязанных с уровнями рассматриваемой проблематики: индивидуальным, групповым и массовым. Обозначена актуальность разработки и создания специализированного программного обеспечения для выявления и предотвращения распространения деструктивного мультимедийного контента в сети Интернет.

В статье [32] описан подход к оценке оперативности процесса выявления контаминационного контента в потоках мультимедийных объектов. Показана возможность разделения мультимедийных объектов на составляющие – текст, видео, аудио и др., их параллельная обработка, анализ и последующее объединение результатов. Выполнена формализация указанного процесса с помощью модели системы массового обслуживания типа Split-Join, а также представлена реализация численного метода расчета его вероятностно-временных характеристик. Результаты оценки представлены в виде набора начальных моментов распределения случайной длительности обработки запроса в системе. В работе [20] помимо текстового описания представлены иллюстрации архитектуры программно-технической системы (демонстратора).

В работе [34] рассмотрена проблема, связанная с вероятностным и иррациональным характером поведения человека, а также представлен вариант ее решения в рамках концепции исследования. Эта особенность поведения является главной трудностью для его математического моделирования: прочной теоретической основы для прогностического статистического моделирования иррациональных решений, принимаемых человеком, до сих пор не выработано. В статье описывается один из вариантов моделирования иррациональности в поведении человека при осуществлении выборов.

Разработка алгоритмов автоматической проверки мультимедийных информационных потоков, выводимых на мониторы пользователей оконечных устройств доступа к сети Интернет, требует объективных критериев отнесения информационных сообщений к категории токсичного и, напротив, позитивного контента. Решение данной задачи требует соответствующей методики отбора образцов контаминационного графического (вербально-графического) контента, а также процедур первичной статистической обработки результатов тестирования испытуемых. В публикации [17] представлено описание того, как решалась данная подзадача. Среди прочего отмечено, что инертность усовершенствования правовых механизмов и невозможность своевременного обнаружения и

блокирования потенциально вредоносных мультимедийных объектов приводит к тому, что токсичная информация проникает в массовое сознание. Выходом из сложившегося положения может явиться ввод в эксплуатацию интеллектуальной системы автоматической обработки потоков информации, способной классифицировать контент, выявлять потенциально вредоносный и блокировать или снижать скорость распространения в интернет-пространстве того или иного контента. Рассматривается ассоциированная с решаемой задачей проблематика категоризации объектов контента, относимых к классу негативных (потенциально вредоносных) или, напротив, позитивных. Авторский подход отличается сведением к минимуму субъективной составляющей процесса классификации мультимедийного контента по степени его влияния на интернет-пользователя. Информационные сообщения по механизмам их влияния на пользователя сети рассматриваются в двух аспектах: подпороговое воздействие (реализуется на бессознательном уровне посредством специально организованного синтаксического содержания) и сознательное воздействие (осуществляется посредством семантики сообщения). Классификация мультимедийных информационных сообщений, содержащих специфические цветографические схемы, аудиоэффекты, мерцания, кадры-вставки и др., реализуется посредством мониторинга вызываемых предъявляемым стимульным материалом психофизиологических (нейросенсорных) эффектов и позволяет отнести любой мультимедийный объект к положительным, нейтральным или негативным. Предложен апробированный подход к получению объективной интегральной характеристики, позволяющей относить графический стимульный материал к классам позитивного или негативного контента.

На основе проработанной концепции исследования были описаны требования к разрабатываемому демонстратору. Сформулированные к интеллектуальной системе защиты пользователей от деструктивного мультимедийного интернет-контента требования изложены в публикации [3]. В работе обобщены результаты исследований, проведенных авторами в области распознавания и блокирования потенциально опасного мультимедийного контента, способного оказать негативное воздействие на психику пользователей автоматизированных систем. Представленная концепция построения системы защиты пользователей реализует многомодельный подход к обнаружению потенциально вредоносного воздействия в информационных потоках. Четкая классификация с последующим дообучением осуществляется на основе нейронных сетей. Семантические распознаватели наличия деструктивного контента в мультимедийных потоках данных построены на основе адаптированных алгоритмов фрактального, фоносемантического и сентимент-анализа, дискретного вейвлет-преобразования, перцептивного хеширования, быстрого преобразования Фурье и др. Для подтверждения вредоносного информационно-психофизиологического воздействия на потребителей мультимедийного контента используется нечеткий классификатор на основе аппарата размытых множеств.

Проблемы построения обучающих выборок вредоносного графического контента в сети Интернет с применением нейросетевого распознавателя и программно-аппаратного комплекса получения данных окулометрии Gazepoint HD3, а также структура сверточной нейросети, потенциально способной в рамках парадигмы глубокого обучения к обобщению и выделению на различных уровнях иерархии слабоформализуемых признаков, отличающих графический контент негативного содержания, способный нанести ущерб психике и физиологическому состоянию пользователей, рассмотрены в работе [5]. Для обучения нейросетевого классификатора распознавать контент того или иного класса,

был предложен способ отбора изображений с различным смысловым наполнением и экспрессией [8]. Формирование системы признаков потенциально вредоносных мультимедийных объектов и отнесение информационных объектов к классу вредоносных в рамках исследовательской концепции осуществляется на основе анализа проведения испытуемых [33]. Анализ реакции испытуемых на разный контент принимается в качестве внешних критериев отнесения контента к тому или иному классу. В работах [2; 4] рассматривается проблематика формирования набора данных, который может быть использован в качестве обучающей выборки для интеллектуального классификатора деструктивного визуального контента. Описана методика проведения экспериментального исследования с применением видеоокулографа, процедуры детектирования аномалий в данных и получения категориальных оценок эмоциональной значимости изображений. Техническая реализация, включая дизайн целевого обследования испытуемых, изложена в [28].

Обоснование критериев оценки влияния интернет-контента на психологическое здоровье потребителя информации представлено в [10; 29].

Проработка концепции исследования, проведенные эксперименты и полученный в ходе их выполнения опыт и практически применимые результаты предоставили данные для создания демонстратора программно-технического средства, повышающего результативность распознавания и нейтрализации потенциально вредоносных мультимедийных объектов в сети Интернет, способных нанести ущерб индивидуальному, групповому и массовому сознанию и психофизиологическому состоянию граждан Российской Федерации.

Ключевые моменты при реализации демонстратора изложены в публикациях [9; 12; 19].

Помимо публикаций теоретические положения концепции исследования реализованы следующими программно-техническими средствами и базами данных.

1. Программное средство разработки онтологических моделей стратифицированного представления состояний сложных иерархических систем [27]. Программа предназначена для построения моделей представления состояний сложных иерархических систем в виде онтологии в форматах RDF, RDFS, OWL2 для инструментального обеспечения проведения системного анализа сложных гетерогенных иерархических систем.

2. Программный модуль параметризации логико-лингвистического описания классов деструктивного медиаконтента на основе окулографических данных [22]. Программа предназначена для описания параметров, полученных с систем видеоокулографии. Программа позволяет эксперту производить различные операции над выделенными в ходе разметки виртуальными объектами, их связями, атрибутами: объединять в одну категорию (класс = rdfs: Class), разводить по разным категориям, определять степень их пересечения и др.; давать новым классам (категориям) человекопонятное описание, характеристику.

3. Программное средство выявления ключевых признаков негативного интернет-контента в мультимедийных объектах на основе метода латентно-семантического анализа с динамическим определением ранговых значений [26]. В данном программно-техническом средстве программные модули основаны на симбиозе применения методов предварительной обработки данных и метода латентно-семантического анализа с динамическим определением ранговых значений, позволяющем всесторонне описать семантическую структуру анализируемых данных, автоматически выделить оптимальные значения сингулярных чисел и провести оценку смысловой близости ключевых признаков негативного Интернет-контента в мультимедийных объектах. Подробнее функциональность программного средства изложена в работе [30].

4. Программа оценивания результативности выявления скрытых информационных вложений в мультимедийных потоках данных на основе алгоритмически реализованной модели многоканальной неэкспоненциальной системы массового обслуживания с разделением задач и агрегированием результатов их параллельной обработки [25]. Программа предназначена для повышения результативности процесса выявления скрытых информационных вложений в мультимедийных потоках данных за счет использования модели многоканальной неэкспоненциальной системы массового обслуживания с разделением задач и агрегированием результатов их параллельной обработки.

5. Программное средство унифицированного хранения и обработки результатов экспериментов по влиянию деструктивного медиаконтента на оператора ЭВМ [23]. Данное средство предназначено для хранения и обработки результатов экспериментов, состоящей в автоматизированном интеллектуальном анализе числовых параметров психофизиологических характеристик, полученных по объединенным каналам окулографии и психометрии. Заявленная функциональность предназначена для реализации логико-аналитической обработки результатов окулографии и психометрии с целью подготовки исходных данных для обучения нейросетевого распознавания.

6. Программный модуль фильтрации окулографических данных и выявления ключевых признаков деструктивного медиаконтента на основе статистической обработки результатов измерений с определением пороговых значений случайных величин [24]. Модуль предназначен для статистической обработки результатов измерений, а именно: подбора типа и параметров вероятностного распределения с последующей фильтрацией исходных данных на основе выявления аномалий в поступающей статистической выборке и выявления ключевых признаков в окулографических данных на основе анализа распределения частот проявления признаков деструктивного медиаконтента.

7. Фактографическая база данных результатов экспериментов по влиянию деструктивного информационного воздействия потенциально опасного мультимедийного контента на оператора ЭВМ [21]. Это реляционная база данных, содержащая результаты экспериментов по влиянию деструктивного медиаконтента на оператора ЭВМ.

Окулографические данные поступают из различных источников: GazepointHD3, «Цветомер», Biomouse, после чего выполняется их предварительная обработка и усвоение в базе данных, где реализовано хранение более 60 различных параметров окулографических измерений, каждое из которых имеет привязку к временной шкале. Реализация совместного хранения данных, получаемых из различных измерительных систем, открывает возможности для последующей комплексной аналитической обработки с использованием интеллектуальных методов.

Изложенная функциональность разработанных программных элементов потребовалась для итеративного уточнения и корректировки возможностей демонстратора. Все перечисленные модули вошли в состав специализированного программного обеспечения, вошедшего в состав демонстратора.

Полный список разработанной научно-технической документации по выполненному исследованию представлен на сайте проекта [15].

Помимо публикаций, разработанных программных средств и баз данных результатом исследования явился демонстратор. Демонстратор – это программно-техническое средство, принимающее данные из интернета, автоматически обрабатывающее их в соответствии с заложенными алгоритмами и выводящее на монитор пользователя преобразованный в соответствии с пользовательскими настройками контент.

Аппаратная часть демонстратора представлена высокопроизводительным сервером, подключаемым к сети Интернет. Архитектура специального программного обеспечения (далее – СПО) демонстратора имеет модульную структуру.

На Рисунке 1 показана реализованная целевая функциональность СПО демонстратора.

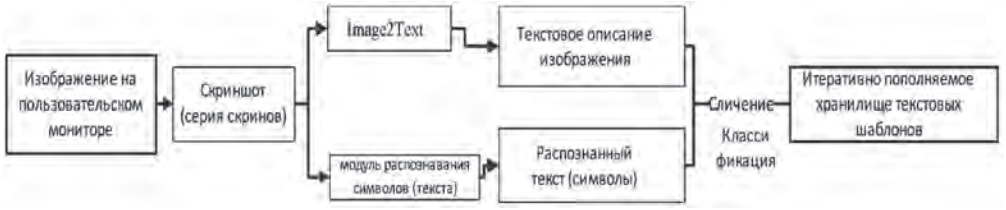

Рисунок 1. Этапы обработки пиксельного изображения на дисплее пользовательского ПК средствами СПО демонстратора

Вышеизложенная концепция программно-технического средства, изготовленного для повышения результативности автоматизированного интеллектуального распознавания вредоносных мультимедийных «объектов» в сети Интернет, реализована в демонстраторе. На момент завершения исследования демонстратор функционирует с контентом, размещенном на ограниченном (избранном) перечне IP-адресов.

СПО демонстратора функционирует как десктопное опционально настраиваемое фоновое приложение. После установки приложения на свой ПК пользователь посредством фильтров настраивает «поведение» программы при обнаружении ей ключевых слов и (или) словосочетаний. В зависимости от настроек программа либо накладывает маску на область монитора, которая распознается как токсичная, либо сигнализирует о наличии в изображении признаков деструктивного воздействия на пользователя, либо, не отвлекая пользователя, сохраняет в журнал факты срабатывания СПО на вредоносные виртуальные объекты с возможностью последующего более подробного ознакомления с этими объектами.

В реализованной версии СПО демонстратор работает с текстовым контентом и статичной графикой. Однако возможность автоматической интеллектуальной обработки мультимедийного контента (видеороликов), аудиозаписей, а также яркостно-частотных пульсаций заложена в архитектуру.

Результаты и их обсуждение

Последовательность обработки контента средствами СПО демонстратора следующая. Через типовой браузер на монитор пользователя выводится контент с заданного IP-адреса. СПО демонстратора делает скриншот экрана и отправляет сделанное изображение в обработку по технологии Image2Text technology [31]. Символьные элементы (в том числе текст) автоматически анализируется алгоритмами посимвольного сравнения входящих символов с символами, словами, фразами, имеющимися в хранилище слов и фраз. Также тесты с монитора анализируются на предмет их смыслового содержания [35] с последующим отнесению к классам «токсичный», «не токсичный», «подозрительный».

Технология Image2Text обеспечивает конвертацию пиксельной области в ее текстовый описательный эквивалент. После того как описание изображения получено, оно (текстовое описание) направляется на анализ в модуль обработки текстов.

На Рисунке 2, *а, б* продемонстрированы примеры конвертации статичного изображения в текст.

а *б*

Рисунок 2. Примеры конвертации статичного изображения в текст: *а* – азиатка в красной блузке поедает белой ложкой гусениц (насекомых) из тарелки; *б* – брюнетка с бородой в бело-зеленом платье на фоне белой стены с черными линиями (фото Кончиты Вурст)

Варианты конвертации изображения (Рисунок 2, *а*) в его текстовое описание средствами СПО демонстратора следующие:

- картина будущего китайской пищевой промышленности;
- картина крупнейшей в мире фермы по разведению насекомых;
- картина мира насекомоядных субъектов;
- картина мира насекомоядных;
- картина будущего китайской общины…

Таким образом, первые 2-3 строки текста вполне соответствуют по смыслу человеческому описанию изображения.

Варианты конвертации изображения (Рисунок 2, *б*) в его текстовое описание средствами СПО демонстратора следующие:

- картина человека, который родился мужчиной, но стал женщиной;
- изображение мужчины с бородой;
- Иисус Христос;
- фотография женщины с черными волосами;
- фотография мужчины, который не является мужчиной;
- фото мужчины, который не мужчина, а женщина;
- изображение мужчины, который не мужчина, а женщина;
- изображение женщины с длинными-предлинными волосами;
- изображение женщины, которая не является женщиной;
- изображение человека, который не является женщиной...

Семантический анализ данных вариантов описаний также может вывести на класс изображений гомосексуальной направленности, который отнесен к категории «токсичных».

Другие алгоритмы (реализующие их программные модули) автоматической обработки контента также могут итеративно подключаться в СПО демонстратора, что позволит увеличить интеллектуальность классификации выводимого на монитор пользователя интернет контента.

В зависимости от активированных классификационных критериев одни и те же изображения относятся демонстратором к разным категориям. На Рисунке 3, *а*, *б* показана

точность классификации. Выделены изображения, отнесение которых к определенному классу с экспертной точки зрения является спорным. Однако определенный граф ассоциаций вполне имеет основание для отнесения выделенных изображений к данным классам.

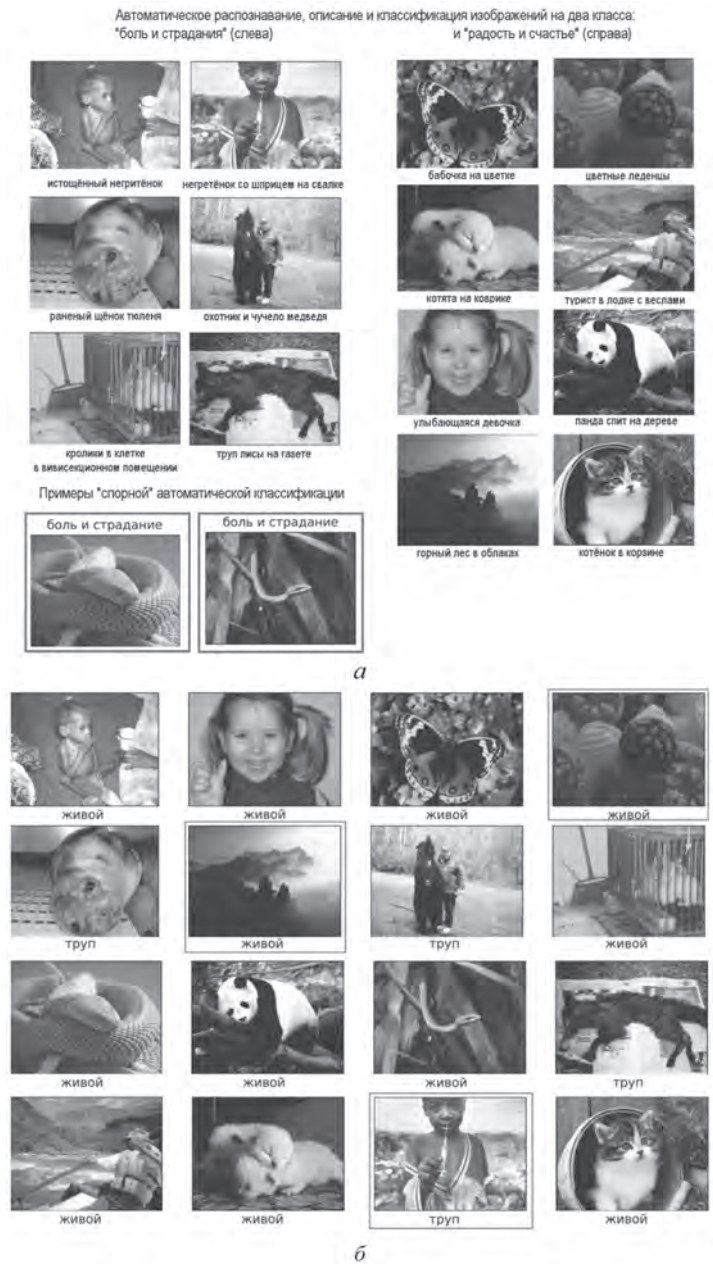

Рисунок 3. Результат автоматического распознавания изображений, их вербализация и отнесение к одному из классов (категорий) (*а*) к одной из категорий (альтернативные настройки критериев классификации) (*б*)

Способность автоматического классификатора в составе СПО демонстратора распознавать изображения представлена на Рисунке 4.

Рисунок 4. Мера косинусового сходства между автоматически распознанным изображением и экспертным описанием этого же изображения

Также стоит отметить такую функцию в СПО демонстратора, как возможность помещать шаблоны в репозиторий в ручном режиме. Это опция позволяет каждому пользователю сформировать свои классы, которые для него нежелательны, и осуществлять фильтрацию контента исходя из решения своих задач.

Выводы

Проведенное исследование позволило детально оценить актуальное положение дел в рассматриваемых предметных областях, а также установить имеющие место тенденции в их развитии. Сформулированная концепция решения задач позволила провести серию экспериментальных исследований, позволивших уточнить некоторые частные моменты, получить фактические разноплановые целевые данные и на основе проведенных работ создать модель программно-технического средства интеллектуальной автоматизированной обработки интернет-контента с целью защиты пользователя от негативного влияния информации, а затем реализовать модель в демонстраторе.

Вместе с тем исследование показало, что высокая вариативность данных на разных уровнях и этапах обработки трафика, а также цели пользователя накладывают большое количество нюансов, которые следует учитывать, чтобы юзабилити демонстратора не снижало эргономические характеристики программно-технической системы.

Таким образом, цель исследования можно считать достигнутой в полном объеме. Однако дальнейшая работа в продолжение данной тематики лежит в направлении проверки возможностей и органичений демонстратора на более разнообразном наборе данных.

Заключение

Выполненное исследование показало наличие широких возможностей создавать программно-аппаратные средства для интеллектуальной обработки контента, выводимого на

монитор пользователя. Однако ввиду огромного разнообразия форм этого контента, а также целей его восприятия пользователями формулировка классификационных критериев не является тривиальной. Один из подходов к формулировке и обоснованию таких критериев представлен в материалах исследования. Авторами описана концепция анализа и программной обработки интернет-контента, реализованная в созданном демонстраторе. Ввиду высокой вариативности параметров контента, требующих обработки, возможности демонстратора (в его актуальном на момент завершения исследования состоянии) ограничены функциями регистрации и обработки текста и статичных изображений. Анализ мультимедийного и аудиоматериала, а также динамики частотно-яркостных характеристик изображений технически возможен, но на данный момент не реализован в СПО демонстратора.

Таким образом, поставленные задачи выполнены, заявленная цель достигнута. Совершенствование функциональности демонстратора по обозначенным выше векторам возможно при продолжении исследования.

Литература

1. *Бурлаева Е.И., Зори С.А.* Сравнение некоторых методов машинного обучения для анализа текстовых документов // Проблемы искусственного интеллекта. 2019. № 1 (12). С. 42–51.

2. *Гнидко К.О., Дудкин А.С., Иванов О.С.* Концептуальная модель интеллектуальной системы защиты пользователей от деструктивного интернет-контента // Суперкомпьютерные технологии: сборник трудов молодых ученых. Ростов-на-Дону: Южный федеральный университет, 2020. С. 178–183.

3. *Гнидко К.О., Дудкин А.С., Лохвицкий В.А.* Концептуальная модель интеллектуальной системы защиты пользователей от деструктивного мультимедийного интернет-контента // Социотехнические и гуманитарные аспекты информационной безопасности: сборник трудов конференции (Пятигорск, 10–13 апреля 2019 г.). С. 117–132.

4. *Гнидко К.О., Ломако А.Г.* Экспериментальное исследование бессознательных реакций потребителей мультимедийного контента на эмоционально значимые визуальные стимулы // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 21–23.

5. *Гнидко К.О., Макаров С.А., Сабиров Т.Р.* Разработка нейросетевого классификатора для формирования обучающих выборок вредоносного графического контента в сети Интернет // Региональная информатика и информационная безопасность: сборник трудов. Вып. 7. СПб.: СПОИСУ, 2019. С. 242–245.

6. *Жуйков А.А.* Современные проблемы информационной безопасности // Вестник КРУ МВД России. 2015. № 4 (30). С. 270–273.

7. *Жуйков А.А., Мащенко И.В.* Трансформация качества информации как системный вызов постиндустриального социума XXI в. // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2020. № 1 (254). С. 91–96.

8. *Иванов О.С., Пилькевич С.В., Рознова И.А., Лохвицкий В.А., Дудкин А.С.* Отбор изображений с различным содержанием для обучения нейросети, идентифицирующей «токсичный» интернет-контент.// Интернаука 2019. № 40 (122). С. 18–23.

9. *Иванов О.С., Лохвицкий В.А., Дудкин А.С., Титов С.С.* Комплексная автоматическая интеллектуальная обработка интернет-контента, выводимого на монитор в ходе пользовательской сессии // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2021. Вып. 1. С. 103–110. DOI: 10.25586/RNU.V9187.21.01.P.103.

10. *Иванов О.С., Пилькевич С.В., Гнидко К.О., Лохвицкий В.А., Дудкин А.С., Сабиров Т.Р.* Обоснование критериев оценки влияния интернет-контента на психологическое здоровье потребителя информации // Социология. 2020. № 5. С. 275–282.
11. *Иванов О.С., Пилькевич С.В., Гнидко К.О., Лохвицкий В.А., Дудкин А.С., Сабиров Т.Р.* Обоснование терминологического базиса исследований форм проявления контаминации психики человека // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 3 С. 69–76. DOI: (CrossRef): 10.25586/RNU.V9187.19.03.P.069.
12. *Иванов О.С., Пилькевич С.В., Гнидко К.О., Лохвицкий В.А., Дудкин А.С., Сабиров Т.Р.* Онтологическое проектирование программного средства оценивания влияния интернет-контента на психологическое здоровье пользователя. // Мир науки. Педагогика и психология. 2020. Т. 8, № 5. С. 37–48.
13. Итоги конкурса на лучшие научные проекты междисциплинарных фундаментальных исследований 2018 года (конкурс «мк», тема 26-822) [Электронный ресурс]. URL: https://www.rfbr.ru/rffi/eng/rffi_contest_results/o_2079896 (дата обращения: 06.02.2022).
14. *Косоруков А.А.* Перспективные технологические решения в сфере построения нейроцифрового государственного управления // Социодинамика. 2021. № 6. С. 53–66.
15. Модели и методы выявления и интеллектуальной обработки деструктивного мультимедийного интернет-контента в русле исследования «Фундаментальные проблемы взаимодействия человека с интернет-пространством: нейрокогнитивные и нейрокомпьютерные технологии» [Электронный ресурс]. https://www.rffigrantvka.ru/#1611865041356-c4354f59-3010 (дата обращения: 05.02.2022).
16. *Пилькевич С.В. Иванов О.С., Сабиров Т.Р.* Формирование системы признаков потенциально вредоносных мультимедийных объектов. Пятигорск: Изд-во Пятигорского государственного университета, 2019. С. 264–271.
17. *Пилькевич С.В., Иванов О.С., Дудкин А.С.* Формирование множества информационных объектов, относимых к негативному и позитивному классам // Региональная информатика и информационная безопасность: сборник трудов. Вып. 7. СПб.: СПОИСУ, 2019. С. 266–271.
18. *Пилькевич С.В., Лускатов И.В.* Признаковое пространство потенциально вредоносного контента: от гипотезы к эксперименту. СПб.: Изд-во Политехнического университета, 2019. С. 54–55.
19. *Сабиров Т.Р., Еремеев М.А., Гнидко К.О.* Подход к онтологическому представлению субъективных оценочных характеристик интернет-контента // Защита информации. Инсайд. 2021. № 2 (98). С. 65–67.
20. *Сабиров Т.Р., Лохвицкий В.А., Андрушкевич Д.В.* К вопросу о необходимости классификации проблемных областей при принятии решений по противодействию деструктивному контенту // Региональная информатика и информационная безопасность: сборник трудов конференции. Вып. 7. СПб.: СПОИСУ, 2019. С. 206–209.
21. Свидетельство о регистрации базы данных 2021620808. Фактографическая база данных (БД) результатов экспериментов по влиянию деструктивного информационного воздействия потенциально опасного мультимедийного контента на оператора ЭВМ / Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Дудкин А.С., Иванов О.С., 2021.
22. Свидетельство о регистрации программы для ЭВМ 2020666435. Программный модуль параметризации логико-лингвистического описания классов деструктивного медиаконтента на основе окулографических данных / Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Дудкин А.С., Иванов О.С., 2020.
23. Свидетельство о регистрации программы для ЭВМ 2020666621 Программное средство унифицированного хранения и обработки результатов экспериментов по влиянию деструктивного

медиаконтента на оператора ЭВМ / Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Дудкин А.С., Иванов О.С., 2020.

24. Свидетельство о регистрации программы для ЭВМ 2021611851. Программный модуль фильтрации окулографических данных и выявления ключевых признаков деструктивного медиаконтента на основе статистической обработки результатов измерений с определением пороговых значений случайных величин / Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Дудкин А.С., Иванов О.С., 2021.

25. Свидетельство о регистрации программы для ЭВМ 2021611075. Программа оценивания результативности выявления скрытых информационных вложений в мультимедийных потоках данных на основе алгоритмически-реализованной модели многоканальной неэкспоненциальной системы массового обслуживания с разделением задач и агрегированием результатов их параллельной обработки / Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Дудкин А.С., Иванов О.С., 2021.

26. Свидетельство о регистрации программы для ЭВМ RU 2019616036. Программное средство выявления ключевых признаков негативного интернет-контента в мультимедийных объектах на основе метода латентно-семантического анализа с динамическим определением ранговых значений / Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Краснов С.А., Дудкин А.С., Иванов О.С., 2019.

27. Свидетельство о регистрации программы для ЭВМ RU 2019616488, Программное средство разработки онтологических моделей стратифицированного представления состояний сложных иерархических систем / Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Краснов С.А., Дудкин А.С., Иванов О.С., 2019.

28. *Ivanov O.S., Chermianin S.V., Kapitanaki V.E., Pilkevich S.V.* (2020) Verifaication of the results of psychosemantic survey by eyes-gaze-tracking. Proc. of Models and Methods of Information Systems Research Workshop, pp. 15–20.

29. *Ivanov O.S., Chermyanin S.V., Kapitanaki V.E., Pilkevitch S.V., Sabirov T.R.* (2021) Approach to verification of psychometric test results by integrating the methods of tempometry and video-oculography. The Neuropsychological Trends, No. 30, pp. 29–53.

30. *Krasnov S., Lokhvitckii V., Dudkin A.* (2020) On the Applicability of the Modernized Method of Latent-Semantic Analysis to Identify Negative Content in Multimedia Objects. In: Kotenko I., Badica C., Desnitsky V., El Baz D., Ivanovic M. (eds.) Intelligent Distributed Computing XIII. IDC 2019. Studies in Computational Intelligence, vol. 868, Springer, Cham, https://doi.org/10.1007/978-3-030-32258-8_27.

31. *Liu C., Wang C., Sun F., Rui Y.* (2016). Image 2 Text: A Multimodal Caption Generator. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/07/Image2Text.pdf

32. *Lokhvickii V., Ryzhikov Y., Dudkin A.* (2020) Applying the Split-Join Queuing System Model to Estimating the Efficiency of Detecting Contamination Content Process in Multimedia Objects Streams. In: Kotenko I., Badica C., Desnitsky V., El Baz D., Ivanovic M. (eds) Intelligent Distributed Computing XIII. IDC 2019. Studies in Computational Intelligence, vol. 868. Springer, Cham, https://doi.org/10.1007/978-3-030-32258-8_26.

33. *Pilkevich S., Gnidko K.* (2019) Formation of the system of signs of potentially harmful multimedia objects. Intelligent Distributed Computing XIII, pp. 266–271.

34. *Surov I.A., Pilkevich S.V., Alodjants A.P. and Khmelevsky S.V.* (2019) Quantum Phase Stability in Human Cognition. Front. Psychol, 10:929. doi: 10.3389/fpsyg.2019.00929.

References

1. Burlaeva E.I., Zori S.A. (2019) *Sravnenie nekotorykh metodov mashinnogo obucheniya dlya analiza tekstovykh dokumentov* [Comparison of some machine learning methods for the analysis of text documents]. *Problemy iskusstvennogo intellekta*, No. 1, pp. 42–51 (in Russian).
2. Gnidko K.O., Dudkin A.S., Ivanov O.S. (2020) *Kontseptual'naya model' intellektual'noi sistemy zashchity pol'zovatelei ot destruktivnogo internet-kontenta* [Conceptual model of an intelligent system for protecting users from destructive Internet content]. *Superkomp'yuternye tekhnologii: sbornik trudov molodykh uchenykh* [Supercomputer technologies: a collection of works of young scientists.Rostov-on-Don: Southern Federal University]. Rostov-na-Donu, Yuzhnyi federal'nyi universitet, pp. 178–183 (in Russian).
3. Gnidko K.O., Dudkin A.S., Loxviczkij V.A. (2019) *Kontseptual'naya model' intellektual'noi sistemy zashchity pol'zovatelei ot destruktivnogo mul'timediinogo internet-kontenta* [Conceptual model of an intelligent system for protecting users from destructive multimedia Internet content]. *Sotsiotekhnicheskie i gumanitarnye aspekty informatsionnoi bezopasnosti: sbornik trudov konferentsii (Pyatigorsk, 10–13 aprelya 2019 g.)* [Sociotechnical and humanitarian aspects of information security: conference proceedings (Pyatigorsk, April 10–13, 2019)], pp. 117–132 (in Russian).
4. Gnidko K.O., Lomako A.G. (2020) *Eksperimental'noe issledovanie bessoznatel'nykh reaktsii potrebitelei mul'timediinogo kontenta na emotsional'no znachimye vizual'nye stimuly* [Experimental study of unconscious reactions of multimedia content consumers to emotionally significant visual stimuli]. *Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii*, No. 29, pp. 21–23 (in Russian).
5. Gnidko K.O., Makarov S.A., Sabirov T.R. (2019) *Razrabotka neirosetevog oklassifikatora dlya formirovaniya obuchayushchikh vyborok vredonosnogo graficheskogo kontenta v seti Internet* [Development of a neural network classifier for the formation of training samples of malicious graphic content on the Internet]. *Regional'naya informatika i informatsionnaya bezopasnost'* [Regional informatics and information security], Iss. 7, pp. 242–245 (in Russian).
6. Zhujkov A.A. (2015) *Sovremennye problem informatsionnoi bezopasnosti* [Modern problems of information security]. *Vestnik KRU MVD Rossii*, Iss. 4 (30), pp. 270–273 (in Russian).
7. Zhujkov A.A., Mashhenko I.V. (2020) *Transformaciya kachestva informacii kak sistemnyj vyzov postindustrial'nogo sociuma XXI v.* [Transformation of information quality as a systemic challenge of post-industrial society XXI century]. *Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya 1: Regionovedenie: filosofiya, istoriya, sociologiya, yurisprudenciya, politologiya, kul'turologiya*, Iss. 1 (254), pp. 91–96 (in Russian).
8. Ivanov O.S., Pil'kevich S.V., Roznova I.A., Loxviczkij V.A., Dudkin A.S. (2019) *Otbor izobrazhenij s razlichnym soderzhaniem dlya obucheniya nejroseti, identificiruyushhej «toksichnyj» internet-kontent* [Selection of images with different content for training a neural network identifying "toxic" Internet content]. *Internauka*, Iss. 40 (122), pp. 18–23 (in Russian).
9. Ivanov O.S., Loxviczkij V.A., Dudkin A.C., Titov S.S. (2021) *Kompleksnaya avtomaticheskaya intellektual'naya obrabotka internet-kontenta, vyvodimogo na monitor v xode pol'zovatel'skoj sessii* [Complex automatic intelligent processing of Internet content displayed on the monitor during a user session]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie*, Iss. 1, pp. 103–110. DOI: 10.25586/RNU.V9187.21.01.P.103 (in Russian).
10. Ivanov O.S., Pil'kevich S.V., Gnidko K.O., Loxviczkij V.A., Dudkin A.S., Sabirov T.R. (2020) *Obosnovanie kriteriev ocenki vliyaniya internet-kontenta na psixologicheskoe zdorov'e potrebitelya informacii*

[Rationale for the evaluation criteria of the impact of Internet content on the psychological health of the information consumer]. *Sociologiya*, Iss. 5, pp. 275–282 (in Russian).

11. Ivanov O.S., Pil'kevich S.V., Gnidko K.O., Loxviczkij V.A., Dudkin A.S., Sabirov T.R. (2019) *Obosnovanie terminologicheskogo bazisa issledovanij form proyavleniy akontaminacii psixiki cheloveka* [Rationale for the terminological basis of research forms of human mental contamination]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie*, Iss. 3, pp. 69–76 DOI: (CrossRef): 10.25586/RNU.V9187.19.03.P.069 (in Russian).

12. Ivanov O.S., Pil'kevich S.V., Gnidko K.O., Loxviczkij V.A., Dudkin A.S., Sabirov T.R. (2020) *Ontologicheskoe proektirovanie programmnogo sredstva ocenivaniya vliyaniya internet-kontenta na psixologicheskoe zdorov'e polzovatelya* [Ontological design of a software tool for assessing the impact of Internet content on the psychological health of the user]. *Mir nauki. Pedagogika i psixologiya*, Iss. 8, No. 5, pp. 37–48 (in Russian).

13. *Itogi konkursa na luchshie nauchnye proekty mezhdisciplinarnyh fundamental'nyh issledovanij 2018 goda (konkurs «MK», tema 26–822)* [Results of the competition for the best scientific projects of interdisciplinary basic research in 2018 (contest "mc", theme 26–822)]. https://www.rfbr.ru/rffi/eng/rffi_contest_results/o_2079896 (in Russian).

14. Kosorukov A.A. (2021) *Perspektivnye tehnologicheskie resheniya v sfere postroeniya nejrocifrovogo gosudarstvennogo upravleniya* [Prospective technological solutions in the construction of neurodigital public administration]. *Sociodinamika*, Iss. 6, pp. 53–66 (in Russian).

15. *Modeli i metody vyyavleniya i intellektual'noj obrabotki destruktivnogo mul'timedijnogo internet-kontenta v rusle issledovaniya «Fundamental'nye problem vzaimodejstviya cheloveka s interne-prostranstvom: nejrokognitivnye i nejrokompyuternye tehnologii»* [Models and Methods of Detection and Intelligent Processing of Destructive Multimedia Internet Content in the Framework of the Study of "Fundamental Problems of Human Interaction with the Internet Space: Neurocognitive and Neurocomputing Technologies"]. https://www.rffigrantvka.ru/#1611865041356-c4354f59-3010 (in Russian).

16. Pil'kevich S.V. Ivanov O.S., Sabirov T.R. (2019) *Formirovanie sistemy priznakov potencial'no vredonosnyh mul'timedijnyh ob''ektov* [Formation of the system of signs of potentially malicious multimedia objects]. Pyatigorsk, Izd-vo Pyatigorskogo gosudarstvennogo universiteta, pp. 264–271 (in Russian).

17. Pil'kevich S.V., Ivanov O.S., Dudkin A.S. (2019) *Formirovanie mnozhestva informacionnyh ob''ektov, otnosimyh k negativnomu i pozitivnomu klassam* [Formation of a set of information objects referred to negative and positive classes]. *Regional'naya informatika i informacionnaya bezopasnost'*, vol. 7. St. Petersburg, SPOISU Publihing, pp. 266–271 (in Russian).

18. Pil'kevich S.V., Luskatov I.V. (2019) *Priznakovoe prostranstvo potencial'no vredonosnogo kontenta: ot gipotezy k eksperimentu* [Sign space of potentially malicious content: from hypothesis to experiment]. St. Petersburg, Polytechnic University Press, pp. 54–55 (in Russian).

19. Sabirov T.R., Eremeev M.A., Gnidko K.O. (2021) *Podxod k ontologicheskomu predstavleniyu sub''ektivnyh ocenochnyh harakteristik internet-kontenta* [Approach to the ontological representation of subjective evaluative characteristics of Internet content]. *Zashhita informacii. Insajd*, Iss. 2 (98), pp. 65–67 (in Russian).

20. Sabirov T.R., Loxviczkij V.A., Andrushkevich D.V. (2019) *K voprosu o neobhodimosti klassifikacii problemnyh oblastej pr iprinyatii reshenij po protivodejstviyu destruktivnomu kontentu* [On the need for classification of problem areas when making decisions to counteract destructive content]. *Regional'naya informatika i informacionnaya bezopasnost'*, vol. 7. St. Petersburg, SPOISU Publihing, pp. 206–209 (in Russian).

21. Pil'kevich S.V., Gnidko K.O., Sabirov T.R., Loxviczkij V.A., Dudkin A.S., Ivanov O.S. (2021) *Faktograficheskaya baza dannykh (BD) rezul'tatov eksperimentov po vliyaniyu destruktivnogo informatsionnogo vozdeistviya potentsial'no opasnogo mul'timediinogo kontenta na operatora EVM* [Factual database (DB) of the results of experiments on the influence of the destructive information impact of potentially dangerous multimedia content on the computer operator]. *Svidetel'stvo o registratsi ibazy dannykh 2021620808* [Registration certificate of the database 2021620808] (in Russian).
22. Pil'kevich S.V., Gnidko K.O., Sabirov T.R., Loxviczkij V.A., Dudkin A.S., Ivanov O.S. (2020) *Programmnyi modul' parametrizatsii logiko-lingvisticheskogo opisaniya klassov destruktivnogo mediakontenta na osnove okulograficheskikh dannykh* [Software module for parameterization of the logical-linguistic description of destructive media content classes based on oculographic data]. *Svidetel'stvo o registratsii programmy dlya EVM 2020666435* [Registration certificate of the computer program 2020666435] (in Russian).
23. Pil'kevich S.V., Gnidko K.O., Sabirov T.R., Loxviczkij V.A., Dudkin A.S., Ivanov O.S. (2020) *Programmnoe sredstvo unifitsirovannogo khraneniya i obrabotki rezul'tatov eksperimentov po vliyaniyu destruktivnogo mediakontenta na operatora EVM* [Software tool for unified storage and processing of the results of experiments on the impact of destructive media content on the computer operator] *Svidetel'stvo o registratsii program dlya EVM 2020666621* [Registration certificate of the computer program 2020666621] (in Russian).
24. Pil'kevich S.V., Gnidko K.O., Sabirov T.R., Loxviczkij V.A., Dudkin A.S., Ivanov O.S. (2021) *Programmnyi modul' fil'tratsii okulograficheskikh dannykh i vyyavleniya klyuchevykh priznakov destruktivnogo mediakontenta na osnove statisticheskoi obrabotki rezul'tatov izmerenii s opredeleniem porogovykh znachenii sluchainykh velichin* [Software module for filtering oculographic data and identifying key features of destructive media content based on statistical processing of measurement results with the determination of threshold values of random variables] *Svidetel'stvo o registratsii programmy dlya EVM 2021611851* [Registration certificate of the computer program 2021611851] (in Russian).
25. Pil'kevich S.V., Gnidko K.O., Sabirov T.R., Loxviczkij V.A., Dudkin A.S., Ivanov O.S. (2021) *Programma otsenivaniya rezul'tativnosti vyyavleniya skrytykh informatsionnykh vlozhenii v mul'timediinykh potokakh dannykh na osnove algoritmicheski realizovannoi modeli mnogokanal'noi neeksponentsial'noi sistemy massovogo obsluzhivaniya s razdeleniem zadach i agregirovaniem rezul'tatov ikh parallel'noi obrabotki* [The program for evaluating the effectiveness of identifying hidden information attachments in multimedia data streams based on an algorithmically implemented model of a multichannel non-exponential queuing system with task division and aggregation of the results of their parallel processing]. *Svidetel'stvo o registratsii programmy dlya EVM 2021611075* [Certificate of registration of the computer program 2021611075] (in Russian).
26. Pil'kevich S.V., Gnidko K.O., Sabirov T.R., Loxviczkij V.A., Krasnov S.A., Dudkin A.S., Ivanov O.S. (2019) *Programmnoe sredstvo vyyavleniya klyuchevykh priznakov negativnogo internet-kontenta v mul'timediinykh ob"ektakh na osnove metoda latentno-semanticheskogo analiza s dinamicheskim opredeleniem rangovykh znachenii* [Software tool for identifying key features of negative Internet content in multimedia objects based on the method of latent semantic analysis with dynamic determination of rank values]. *Svidetel'stvo o registratsii programmy dlya EVM RU 2019616036, 16.05.2019* [Certificate of registration of the computer program RU 2019616036, 05/16/2019] (in Russian).
27. Pil'kevich S.V., Gnidko K.O., Sabirov T.R., Loxviczkij V.A., Krasnov S.A., Dudkin A.S., Ivanov O.S. (2019) *Programmnoe sredstvo razrabotki ontologicheskikh modelei stratifitsirovannogo predstavleniya sostoyanii slozhnykh ierarkhicheskikh system* [Software tool for developing ontological models of stratified

representation of the states of complex hierarchical systems]. *Svidetel'stvo o registratsii programmy dlya EVM RU 2019616488, 23.05.2019.* [Certificate of registration of the computer program RU 2019616488, 05/23/2019] (in Russian).

28. Ivanov O.S., Chermianin S.V., Kapitanaki V.E., Pilkevich S.V. (2020) Verifaication of the results of psychosemantic survey by eyes-gaze-tracking. Proc. of Models and Methods of Information Systems Research Workshop, pp. 15–20.

29. Ivanov O.S., Chermyanin S.V., Kapitanaki V.E., Pilkevitch S.V., Sabirov T.R. (2021) Approach to verification of psychometric test results by integrating the methods of tempometry and video-oculography. The Neuropsychological Trends, No. 30, pp. 29–53.

30. Krasnov S., Lokhvitckii V., Dudkin A. (2020) On the Applicability of the Modernized Method of Latent-Semantic Analysis to Identify Negative Content in Multimedia Objects. In: Kotenko I., Badica C., Desnitsky V., El Baz D., Ivanovic M. (eds.) Intelligent Distributed Computing XIII. IDC 2019. Studies in Computational Intelligence, vol. 868, Springer, Cham, https://doi.org/10.1007/978-3-030-32258-8_27.

31. Liu C., Wang C., Sun F., Rui Y. (2016). Image 2 Text: A Multimodal Caption Generator. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/07/Image2Text.pdf (датаобращения 13.02.22).

32. Lokhvickii V., Ryzhikov Y., Dudkin A. (2020) Applying the Split-Join Queuing System Model to Estimating the Efficiency of Detecting Contamination Content Process in Multimedia Objects Streams. In: Kotenko I., Badica C., Desnitsky V., El Baz D., Ivanovic M. (eds) Intelligent Distributed Computing XIII. IDC 2019. Studies in Computational Intelligence, vol. 868. Springer, Cham, https://doi.org/10.1007/978-3-030-32258-8_26.

33. Pilkevich S., Gnidko K. (2019) Formation of the system of signs of potentially harmful multimedia objects. Intelligent Distributed Computing XIII, pp. 266–271.

34. Surov I.A., Pilkevich S.V., Alodjants A.P. and Khmelevsky S.V. (2019) Quantum Phase Stability in Human Cognition. Front. Psychol. 10:929. doi: 10.3389/fpsyg.2019.00929.