

По проекту РНФ 18-11-00302 в 2018 году были получены следующие результаты.

1. Разработана **концепция построения и функционирования интеллектуальных систем аналитической обработки цифрового сетевого контента (ИСаОЦСК) с целью обнаружения и противодействия нежелательной, сомнительной и вредоносной информации.** Концепция включает: основные определения; принципы организации интеллектуальной аналитической обработки цифрового сетевого контента, распространяемого в сети Интернет и в социальных сетях; цели и задачи ИСаОЦСК; особенности Интернет-пространства и социальных сетей, влияющие на построение ИСаОЦСК; механизмы обеспечения интеллектуальной аналитической обработки цифрового сетевого контента в сети Интернет и в социальных сетях; структуру ИСаОЦСК; требования к ИСаОЦСК. Основной целью функционирования ИСаОЦСК определено выявление в информационных объектах сети Интернет и в социальных сетях нежелательной, сомнительной и вредоносной информации и выработка мер противодействия этим видам информации. Определены основные структурные компоненты ИСаОЦСК: (1) распределенные интеллектуальные сканеры и компоненты предварительной обработки; (2) компоненты многоаспектной оценки и категоризации ИО, включающие базовые классификаторы, аспектные классификаторы и итоговые классификаторы; (3) компоненты обеспечения своевременности анализа ИО; (4) компоненты устранения неполноты и противоречивости результатов оценки и категоризации; (5) компоненты адаптации и переобучения системы; (6) компоненты выработки и выбора мер противодействия нежелательной, сомнительной и вредоносной информации, включающие базу контрмер и модуль поддержки принятия решений; (7) компоненты реализации визуальных интерфейсов. Для каждого структурного компонента ИСаОЦСК определены выполняемые функции и обоснованы предъявляемые к ним требования.

2. Разработан **общий подход и требования, предъявляемые к компонентам сбора и предварительной обработки сетевых информационных объектов на основе применения распределенных интеллектуальных сканеров.** Подход основан на децентрализованном управлении комплексом распределенных интеллектуальных сканеров, самостоятельно организующихся для выполнения отдельных операций вычислительного процесса. Определены исходные данные для сбора и предварительной обработки сетевых ИО: (1) конечное множество сетевых адресов для сканирования; (2) уникальные сетевые адреса расположения сетевых ИО для их загрузки и предварительной обработки; (3) список ключевых слов для поиска сетевых ИО. Выделены следующие основные свойства сетевых ИО: адресность, изменчивость, доступность, структурированность и иерархичность. Предложены механизмы обеспечения доступности сетевых ИО в зависимости от их уровня. Обоснованы функциональные требования к компонентам сбора и предварительной обработки сетевых ИО: (1) обнаружение и загрузка сетевых ИО с учетом параметров заданного сегмента; (2) типизация лексем полуструктурированного и структурированного сетевого информационного контента; (3) структурная категоризация ИО; (4) выявление и преодоление механизмов блокировки автоматизированного сбора информации; (5) приоритезация ИО. Нефункциональными требованиями являются: гибкое масштабирование, децентрализованное управление, максимальная оперативность; высокая ресурсоемкость.

3. Разработан **общий подход и требования, предъявляемые к компонентам многоаспектной оценки и категоризации смыслового наполнения информационных объектов.** Подход ориентирован на решение задачи автоматической классификации сетевых ИО с использованием данных, собранных в РБД ИО с помощью интеллектуальных сканеров. Этапами решения этой задачи являются: предварительная обработка текста; извлечение признаков; сокращение размерности пространства признаков; обучение классификатора методами машинного обучения; оценка классификатора. Предварительная обработка текста включает в себя токенизацию и лемматизацию, удаление стоп-слов, стемминг и морфологический анализ. На этапе извлечения признаков формируется численная модель (индексация) текста. Сокращение признаков достигается за счет удаления сильно коррелирующих и не информативных значений атрибутов. Для оценки текстового классификатора используются стандартные метрики точности. Основными метриками являются метрики полноты, однако также учитываются метрики аккуратности и F-мера. Функциональные требования определяют необходимость: поддержки предварительной обработки текстового содержания ИО; поддержки анализа структуры html-страницы; поддержки анализа цифрового содержимого; поддержки обработки дополнительной информации об ИО; идентификации технологий на серверной стороне соответствующего ИО; извлечение исполняемых сценариев. К выделенным нефункциональным требованиям относятся: точность, гибкость (адаптивность), быстродействие и масштабируемость.

4. Разработаны **общий подход и требования, предъявляемые к компонентам обеспечения своевременности многоуровневого и многомодульного анализа информационных объектов на основе использования параллельных вычислений.** Подход ориентирован на параллельную обработку данных в компонентах ИСАОЦСК. С учетом преимуществ и недостатков различных способов распараллеливания вычислений, принято решение использовать в проекте для обеспечения своевременности анализа ИО с помощью машинного обучения платформу Spark Hadoop и различные алгоритмы из ее библиотеки Spark MLlib. Обоснованы основные требования к компонентам, направленные на обеспечение работоспособности всей системы, которые заключаются в обеспечении высокой масштабируемости и отказоустойчивости, а также организации распределенного хранилища данных.

5. Разработаны **общий подход и требования, предъявляемые к компонентам устранения неполноты и противоречивости оценки и категоризации смыслового наполнения информационных объектов на основе использования методов обработки неполных, противоречивых и нечетких знаний.** Подход сводится к усовершенствованию классификаторов ИО с использованием методы вероятностного, нечеткого и нейросетевого оценивания ситуаций, нечеткого и нейросетевого вывода и нечеткой и нейросетевой оптимизации. Предложен состав и уровни архитектуры компонентов устранения неполноты и противоречивости с учетом «цепочки» принятия решений в условиях неопределенности. Принятие решений на каждом уровне осуществляется в условиях неопределенности, вызванной нестационарностью функционирования ИСАОЦСК, воздействиями дестабилизирующих факторов, внешней среды, нечеткостью целей и несогласованностью задач оценки и категоризации, а также другими факторами. Сформулированы частные и обобщенная постановки задач на

разработку моделей и методов устранения неполноты и противоречивости оценки и категоризации цифрового контента. К их числу относятся: (1) вероятностные методы, позволяющие устранить аспекты класса стохастической неопределенности; (2) методы теории нечетких множеств, позволяющие устранить неоднозначность, неизвестность, недостаточность или нечеткость исходных данных; (3) методы теории искусственных нейронных сетей, позволяющие устранить недостоверность, недостаточность, недоопределенность, несогласованность, неполноту, неадекватность, неточность исходных данных для оценки и категоризации. Сформулированы требования к процессам оценки и категоризации в условиях неопределенности: оперативность, комплексность, адекватность, достоверность, объективность, непрерывность, полнота, точность и открытость. Сформулированы базовые (по постоянной готовности, устойчивости, масштабируемости (мобильности-переносимости), безопасности работы, производительности) и дополнительные (по модульности, функциональной избирательности, генерируемости, виртуализации, независимости программ от внешних устройств, совместимости, открытости, многозадачности, многопользовательскому режиму, защищенности, экономичности работы, а также поддержке различных файловых систем и стандартных форматов данных) требования, которые предъявляются к компонентам устранения неопределенности оценки и категоризации смыслового наполнения ИО на основе использования методов обработки неполных, противоречивых и нечетких знаний. Выполнение данных требований позволит интеллектуальным сканерам (классификаторам) оперативно, полно (достоверно), точно и адекватно выявлять признаки и противодействовать нежелательной, сомнительной и противоречивой информации в цифровой сетевом контенте.

6. Разработаны **общий подход и требования, предъявляемые к компонентам адаптации и переобучения системы анализа информационных объектов, в том числе в режиме эксплуатации.** Цель подхода заключается в разработке и анализе архитектуры системы классификации нежелательной и вредоносной информации по множеству классификационных признаков с использованием текстовой информации сайтов, html-данных, данных о структуре документов и URL-данных с применением методов автоматизированной классификации веб-сайтов и их отдельных страниц с использованием методов машинного обучения. Особенность предлагаемого подхода заключается в иерархическом построении решающего правила в виде набора базовых классификаторов и объединяющего их выходные данные верхнеуровневого классификатора. Предложенный подход позволяет минимизировать временные затраты, связанные с изменением типов анализируемых исходных данных, модифицируя не систему классификации целиком, а лишь отдельное подмножество базовых классификаторов, соответствующий аспектный классификатор и итоговый классификатор, тем самым адаптируя имеющееся решение под изменившиеся требования. Подход обосновывает трехуровневую иерархическую архитектуру классификации содержимого веб-страниц. На первом уровне размещаются бинарные классификаторы, которые выполняют проверку принадлежности анализируемого объекта к определенной категории. Второй уровень включает классификаторы, предназначенные для определения аспектов веб-страницы. На третьем уровне располагается итоговый классификатор. Исходные наборы данных, представленные в виде файлов html-страниц, вначале обрабатываются компонентом извлечения признаков. Формируемые этим компонентом наборы признаков помещаются в

РБД ИО. Обоснованы требования к компонентам по показателям оперативности, масштабируемости и надежности.

7. Разработаны **общий подход и требования, предъявляемые к компонентам выработки и выбора мер противодействия нежелательной, сомнительной и вредоносной информации**. Подход выделяет способы и средства, применимые для защиты от информации, и действующие в РФ механизмы защиты от информации. Определены основные объекты и субъекты, взаимодействующие в рамках данного подхода: ИО, источник информации, канал распространения информации, целевая аудитория, субъект воздействия информации. Меры противодействия вводятся для защиты субъекта воздействия информации от вредоносного воздействия информации. Они зависят от классов всех перечисленных субъектов и объектов и класса информации, представленной ИО (нежелательная, сомнительная или вредоносная). Для целевой аудитории как субъекта воздействия информации предложена трехуровневая классификация. Определены каналы распространения информации и предложена их двухуровневая классификация. Меры для защиты от нежелательной, сомнительной и вредоносной информации вначале классифицируются по способу защиты, а затем по способам их реализации. Основными этапами противодействия нежелательной, вредоносной и сомнительной информации являются: определение класса информации, определение класса мер защиты, выбор оптимальных средств/мер защиты. Функциональными требованиями к компонентам выработки и выбора мер противодействия являются: управляемость процесса; учет законов Российской Федерации; ограничение доступа к нежелательной информации; учет возможного ущерба для граждан и государства; автоматизация процесса; соблюдение прав граждан на доступ к информации.

8. Разработаны **общий подход и требования, предъявляемые к компонентам реализации визуальных интерфейсов для выявления и противодействия нежелательной, сомнительной и вредоносной информации**. Подход, названный «конвейер визуализации», заключается в последовательной обработке данных согласно следующих этапов: (1) анализа данных; (2) фильтрации данных; (3) разметки данных; (4) отрисовки данных. Кроме того, подход соотносит модели визуализации и структуры данных. Он позволяет реализовывать принцип повторяемости, когда множество моделей должны быть взаимозаменяемы. Определены требования к компоненту визуализации со стороны самого процесса визуализации и архитектуры этого компонента. Со стороны визуализации выдвинуты следующие требования: (1) возможность выявления lie factor (неправильной интерпретации графической метрики); (2) отсутствие chart junk (графические элементы, которые не несут какой-либо информации); (3) использование анимации. Со стороны архитектуры выдвинуты следующие требования: (1) реализация концепции «конвейера визуализации»; (2) унификация данных в соответствии со структурой; (3) учет способов человеко-машинного взаимодействия с результатом визуализации; (4) учет зависимости объема данных от способа их хранения.

9. Разработана **общая архитектура перспективных ИСАОЦСК с целью обнаружения и противодействия нежелательной, сомнительной и вредоносной информации**. В предложенной архитектуре компоненты взаимодействуют через РБД ИО. В РБД поступают данные от компонентов предварительной обработки и устранения

неполноты и противоречивости. Из РБД данные поступают в компоненты устранения неполноты и противоречивости, адаптации и переобучения, оценки и классификации и противодействия. Системообразующими являются компонент обеспечения оперативности и компонент визуализации. Первый из них обеспечивает реализацию методов и алгоритмов параллельной обработки данных в других компонентах. Второй компонент обеспечивает визуальный интерфейс всех компонентов и отображение результатов их работы в традиционных и специальных моделях визуализации. Для оценки архитектуры разработан стенд для экспериментальных исследований, основанный на использовании гипервизора VMware и платформ распределенных вычислений Hadoop и Spark. Сформирован тестовый набор данных, содержащий свыше 70 тыс. записей, каждая из которых является множеством атрибутов веб-страницы Интернета. Каждая веб-страница относится к одной из 18 категорий нежелательной информации. Полученный тестовый набор данных апробирован при решении задачи классификации ИО в двух сериях экспериментов: на одной машине (однопоточный режим) и на кластере параллельно работающих машин (многopоточный режим). Результаты экспериментальной оценки показали, что в обеих сериях наилучшие результаты по обучению продемонстрировали классификаторы на основе метода опорных векторов. При этом установлено, что система Spark не дала существенного выигрыша по времени обучения, что, по-видимому, связано с недостаточно большим объемом тестового набора данных.

По результатам проекта сделано **8** публикаций в изданиях, индексируемых в базе Scopus, **19** – в базе РИНЦ, получено **7** свидетельств о государственной регистрации программ для ЭВМ.