ОТЗЫВ

официального оппонента
на диссертационную работу Царёва Дмитрия Владимировича на тему: «Методы и программные средства анализа поведения пользователей при работе с текстовыми данными для решения задач информационной безопасности», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Диссертационная работа Царёва Д. В. посвящена решению задачи выявления ранних признаков нетипичной работы пользователя с текстовой информацией. Примерами таких признаков могут являться следующие ситуации: пользователь работает с документами определённых категорий в несвойственное для себя время или пользователь стал обращаться к документам (читать или копировать), к которым ранее не обращался. Очевидно, что подобное поведение пользователя может быть вызвано вполне легальными обстоятельствами, возникшими в процессе его текущей рабочей деятельности, однако оно также может свидетельствовать о том, что пользователь не является тем, от имени кого он авторизовался, или пользователь стал искать документы для подготовки к организации утечки информации. Так или иначе, о подобном аномальном поведении следует информировать службу информационной безопасности организации для своевременного принятия соответствующих мер. В первом случае требуется совершенствование процесса идентификации пользователей при допуске к работе с документами, а во втором технически и технологически обеспечить возможность раннего обнаружения попыток хищения информации.

В настоящее время доступных для широкого использования универсально эффективных решений в области предотвращения утечек информации на рынке не существует. Этот факт подтверждается как многочисленными примерами промышленного шпионажа, которые регулярно освещаются в СМИ, так и просочившимися в них данными об утечках служебной информации из государственных органов и организаций, в том числе в рамках последней широкомасштабной вирусной атаки. Результаты анализа таких фактов утечки информации показывает, что наибольший ущерб наносится внутренними нарушителями, то есть либо сотрудниками организации, либо лицами, получившими тем или иным способом доступ к вычислительным ресурсам организации. Поэтому актуальность исследований, направленных на разработку новых подходов к предотвращению внутренних атак, а, следовательно, и актуальность темы рассматриваемой диссертации, не вызывает сомнений.

В работе справедливо отмечено, что существующие системы обнаружения аномального поведения пользователей используют модели поведения, основанные на методах машинного обучения, анализирующих только лишь структурированное описание операций, выполняемых пользователем. Реализованные в них поведенческие профили напрямую не учитывают контент пользовательских данных. Поэтому на их основе выявить случаи нелегитимной активности пользователя при характерных для него действиях, но с нелегальным контентом, не представляется возможным. Следовательно, расширение традиционных источников поведенческой информации за счёт добавления информации о содержимом обрабатываемых пользователем текстовых данных и разработки соответствующих методов выявления аномалий является актуальной научной задачей, новое решение которой представлено в диссертации Царёва Д. В.

Практическая ценность работы Царёва Д. В. Заключается в том, что на основе результаты его теоретических исследований составили основу для проектирования и реализации экспериментальной системы для обнаружения аномального поведения пользователей по особенностям работы с текстовой информацией. Данная система включает в себя модули сбора поведенческой информации, модули построения и применения поведенческих моделей.

Диссертационная работа Царёва Д. В. состоит из введения, четырёх глав, заключения и списка литературы. Полный объём диссертации составляет 143 страницы.

Во введении обосновывается актуальность темы диссертации на примере типового сценария утечки данных, после чего ставится цель и формулируются задачи исследования.

В первой главе приводится аналитический обзор существующих индустриальных решений по управлению информационными ресурсами предприятий. При этом основное внимание уделяется моделям представления текстовых данных, а также методам их анализа.

Во второй главе решается задача разработки модели представления поведенческой информации пользователя при работе с текстовыми данными. Автором предложена модель многомерного временного ряда, соответствующая изменению весов тематик в текстовых данных, с которыми взаимодействует пользователь в течение времени. Для этого выделяются ключевые тематики текстовых документов, входящих в пользовательский поток, с использованием метода неотрицательной матричной факторизации и рассчитываются их веса для соответствующих текстовых данных. Для уменьшения объёма анализируемых текстовых данных и минимизации влияния различных шумовых составляющих в тексте предложен новый метод, основанный на расчёте релевантности отдельных фрагментов анализируемого текста.

Третья глава посвящена решению задачи разработки методов машинного обучения, предназначенных для обнаружения аномального поведения пользователя при работе с текстовыми данными. В рамках этих методов автор предложил два новых метода обнаружения аномального поведения пользователя на основе разработанной во второй главе модели представления поведенческой информации:

1. Метод прогнозирования тематической направленности пользователя по длительным интервалам времени на основе идентификации отрезков времени, в которые пользователь вёл аномальную работу с документами, с учетом значений отклонений фактических весов тематик от спрогнозированных;
2. Метод оценки принадлежности документа к характерным тематикам пользователя, основанный на обнаружении фактов работы пользователя с несвойственным документом, исходя из оценки принадлежности текста документа к характерным тематикам анализируемого пользователя.

Следует отметить, что при разработке первого метода был предложен алгоритм прогнозирования временных рядов, основанный на нахождении взаимосвязей между элементами временного ряда, путём применения ортонормированной неотрицательной матричной факторизации к матрице многомерного временного ряда.

Четвёртая глава посвящена программной реализации экспериментальной системы обнаружения аномального поведения пользователей при работе с текстовыми данными. В главе содержатся описание архитектуры системы и экспериментальные исследования производительности основных программных модулей.

Обоснованность представленных результатов подтверждается проведёнными экспериментальными исследованиями, которые продемонстрировали возможность практического применения

разработанных методов обнаружения аномального поведения пользователя и метода удаления информационного шума. А предложенный автором алгоритм оценки релевантности отдельных фрагментов текста, который используется для фильтрации информационного шума, был апробирован при решении задачи автоматического аннотирования на общепринятом эталонном наборе данных DUC.

Достоверность полученных результатов обеспечивается корректным применением адекватного математического аппарата и подтверждается их широким обсуждением на российских и международных конференциях, а также публикациями в рецензируемых изданиях, а также использованием результатов диссертационной работы в четырёх государственных научно-исследовательских работах, касающихся как обработки и анализа текстовых данных, так и информационной безопасности.

Оценивая научную новизну работы в целом, можно согласиться с автором, что в ней разработаны методы моделирования и анализа поведения пользователей при работе с текстовыми данными, которые в отличие от известных, учитывают несколько ранее не принимавшихся в расчет факторов, использование которых позволяет повысить эффективность таких методов. Некоторые полученные в диссертации результаты могут быть использованы в системах информационной безопасности организаций и предприятий, имеющих внутреннюю техническую и технологическую документацию конфиденциального характера. Считаю, что в диссертационной работе Царёва Д. В., выполненной на достаточном для квалификационной работы уровне, представлено новое решение актуальной научной задачи. Содержание автореферата полностью соответствует содержанию текста диссертации.

Однако, несмотря на не вызывающие сомнения теоретическую значимость и практическую ценность выполненной Царёвым Д. В.

диссертационной работы, она имеет целый ряд недостатков, основными из которых, по моему мнению, являются следующие.

1. Во введении приводится список задач информационной безопасности (задача раннего обнаружения попыток хищения информации, задача аутентификации пользователей), на решение которых направлены разрабатываемые в работе методы обнаружения аномального поведения пользователей. Однако он автором необоснованно ограничен, тем более, что с помощью предложенных им методов также можно, например, определять факты работы пользователя с контентом, не относящимся к его рабочей деятельности, т.е. решать задачу обнаружения нецелевого использования корпоративных ресурсов и т.п.
2. В работе упоминаются вероятностные тематические модели для представления текстовых данных, но в тексте нет исследования их применимости в разработанных методах обнаружения аномалий.
3. В тексте имеется несколько опечаток, например, на стр. 79: «Данная модель также оценивает семантическую близость между словами на основе их контекстной встречаемости, использую обучение нейронной сети с единственным скрытым слоем».

Вывод.

Несмотря на отмеченные недостатки, которые не снижают общей положительной оценки результатов проведённых автором исследований, диссертационная работа Царёва Д. В. представляет собой завершённое научное исследование, содержит ценные научные и практические результаты. Она в полной мере удовлетворяет требованиям ВАК РФ, предъявляемым к диссертациям, представляемым на соискание учёной степени кандидата физико-математических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных

машин, комплексов и компьютерных сетей, а её автор, Царёв Дмитрий Владимирович, заслуживает присуждения ему такой учёной степени.

Официальный оппонент
доктор технических наук, профессор
Заместитель руководителя
Центра кибербезопасности
ОАО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ОАО «НИИАС»)

Б.Ф. Безродный

«31» мая 2017 г.

Контактные данные:

Телефон: 8 (985) 774-28-26

Электронная почта: b.bezrodnyi@vniias.ru

Адрес: 109029, Москва, ул. Нижегородская, 27, стр. 1

Подпись Безродного Бориса Федоровича
УДОСТОВЕРЯЮ.
Нач. Управления по работе
с персоналом ОАО "НИИАС"
О.А. Песоцкая
31.05.2017