Доверие и безопасность в информационном обществе

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ФОЛЬКЛОРА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья рекомендована членом редакционного совета А.Н. Райковым 25.08.2020.

Алигулиев Расим Магамед оглу

Доктор технических наук, профессор
Институт информационных технологий НАНА
Баку, Азербайджанская Республика
r.alguliev@gmail.com

Кулиев Хикмет Валех оглу

Доктор философии по филологическим наукам, доцент
Институт фольклора НАНА
Баку, Азербайджанская Республика
quliyevh@mail.ru

Аннотация

В статье изучены возможности использования фольклора в решении проблем информационной безопасности. Отмечается, что в настоящее время быстрый рост роли интернета в повседневной жизни помимо преимуществ имеет такие отрицательные стороны, как появление киберпреступлений и кибернасилия, скрытых социальных сетей и процессов, носящих криминальный характер, что привело к актуализации проблемы информационной безопасности. В настоящее время предложены различные методы и подходы к выявлению и предотвращению имеющих место в виртуальной среде негативных социальных процессов, в частности таких, как пропаганда преступлений и насильственных актов. В статье в контексте информационной безопасности анализируются вопросы выявления адекватных методов и средств обнаружения секретности, ориентированной на негативные действия, скрытых преступных виртуальных социальных сетей и групп с использованием уникальных возможностей фольклора, выдвинуты предложения по осуществлению деятельности в этом направлении в перспективе.

Ключевые слова

информационная безопасность, киберпреступность, дезинформация, интернет-фольклор, фольклорный факт, мультикультуральная фольклорная среда, национальная идентичность

Введение

Появление интернета кардинально повлияло на расширение возможностей общения между людьми, решение проблем, связанных с различными вопросами, начиная от доступа к информации до различных способов ее хранения и обработки. Создающий новые возможности для коммуникации и связи между людьми, интернет в настоящее время превратился еще и в динамичную среду, в которой находят место политические, экономические, социальные, культурные и другие процессы. Не случайно, что в виртуальной сфере уже появилась и электронная культура (иначе говоря, цифровая культура) [1, с. 44]. Вместе с тем быстрое развитие интернета и появление форумов привели к увеличению зависимости людей от него, созданию благодатной почвы для появления различных опасностей и угроз. С этой точки зрения в условиях существования цифровых технологий, электронной среды, глобальной информационной сети одними из основных задач национальной безопасности являются защита национально-духовных ценностей, изучение народной культуры, фольклора, что сообразно современным требованиям в контексте информационной безопасности является достаточно актуальным. С одной стороны, решение проблем информационной безопасности, изучение происходящих в виртуальной среде

процессов, в том числе связанных с киберпреступностью и кибернасилием, выявление индивидов и групп, осуществляющих деятельность криминального характера, используя специфические возможности фольклора, а с другой − изучение проблем информационной безопасности самого фольклора являются важными задачами, ждущими своего решения. Вместе с тем изучение наличествующих в социальных сетях фольклорных процессов, фольклорных фактов, являющихся социокультурной реакцией, цифровой народной культуры, фольклорного творчества нового поколения, фольклорных форм и материалов представляет собой одну из самых актуальных проблем, стоящих перед интернет-фольклором.

Таким образом, вопрос фольклора и информационной безопасности можно рассматривать в трех ключевых аспектах:

1) использование уникальных возможностей фольклора в контексте информационной безопасности, определение адекватных методов и средств для выявления секретности, ориентированной на негативные действия, скрытых преступных виртуальных сетей и групп;

2) осуществляемые с помощью возможностей компьютерных технологий цифровизация национальных фольклорных ресурсов, собранных из различных источников, ввод их в электронную среду, надежное хранение их в этой среде, обеспечение их полноты и доступности, а также определение параметров (признаков, показателей) каждого фольклорного ресурса для его идентификации, позволяющих проводить его интеллектуальный анализ;

3) анализ на основе применения мультидисциплинарных методов и подходов, а также существующих в интернете (социальных сетях, на форумах и сайтах) процессов фольклорного творчества, трендов и тенденций фольклоризации или дефольклоризации, временных фольклорных традиций, фольклорных фактов нового поколения, фольклорных форм, то есть интернет-фольклора в целом.

С этой целью в статье были проанализированы перспективы использования фольклора с целью обеспечения информационной безопасности и выявления киберпреступности, являющихся одними из наиболее актуальных проблем современности. В статье рассматриваются особенности фольклора, которые демонстрируют его уникальность и специфичность как компонента безопасности национального самосознания, этнической идентичности и групповой идиокультуры. Кроме того, были рассмотрены перспективы многомерного анализа в цифровых фольклорных базах данных, научно-теоретические и практические проблемы использования фольклора в обеспечении информационной безопасности.

1 Понятие «информационная безопасность» и фольклор

Информационная безопасность – понятие широкое и, несмотря на актуализацию в последнее время, оно исторически существовало в контексте защиты, обеспечения секретности информации на различных носителях – камне, коже, бумаге и т.д. Можно считать, что с момента возникновения коммуникаций была осознана важность информации, поэтому ее защите, надежному хранению и передаче между людьми всегда придавалось большое значение. Вовсе не случайно, что в традиционной культурной среде строго охранялись информация и знания, связанные с различными профессиями и ремеслами, особенно со знахарством и народной медициной. В традиционной культурной среде существовали определенные эзотерические знания и практика, которые передавались в ограниченных рамках в табуированном виде. Иными словами, в традиционной культурной среде всегда существовали знания, опыт и информация, на передачу и распространение которых накладывался запрет – табу, поскольку фольклор, основанный на интересах и желаниях, обычаях и традициях, поведении и беседах различных социальных групп, вместе с тем отображает специфику, границы и общение социальной группы, к которой относится. Все это создает широкие возможности для определения фольклорного профиля различных социальных групп по имеющимся признакам, а затем для использования в проведении различного типа анализов.

В научной литературе существуют различные подходы к понятию «информационная безопасность» [2; 3; 4]. Понятие информационной безопасности часто понимается как обеспечение конфиденциальности, полноты и доступности информации. Однако это понятие имеет более широкое значение. Информационная безопасность заключается не только в компьютерной и сетевой безопасности. В современном обществе информационная безопасность проникает во все социально-культурные процессы общества, превращается в неотъемлемую часть национальной безопасности любого государства [5, с. 24; 6, с. 5; 7].

Если некогда человек испытывал трудности из-за недостатка информации, то в настоящее время наблюдается совершенно противоположная картина. Сегодня общество вплотную столкнулось с чрезвычайным изобилием информации, опасностью «захлебнуться» в информационном потоке, что поставило мир перед парадигмой информационной безопасности. Оценка места и роли фольклора в контексте подобной мультикультуральной реальности, выявление его возможностей является чрезвычайно актуальным вопросом.

Очень быстрое распространение информации, возможность ведения любых операций с информацией, наблюдающиеся сегодня, превратили ее в достаточно необходимое и даже стратегическое понятие. Манипулируя информацией, можно воздействовать на общество, распространяя дезинформацию – нарушить стабильность, создать социально-психологический хаос. Поэтому не случайно в настоящее время в интернете существуют многочисленные электронные ресурсы, ориентированные на ложные новости, слухи и клевету, угрозы и шантаж. Получив возможность временного присутствия в интернете, эти ресурсы, созданные в традиционных фольклорных моделях, обладают фольклорными формами и функциями [8, с. 1]. Сформированные на текущих событиях и новостях, эти ресурсы порой направлены на обман, на отрицательное воздействие на общество. Остаться в стороне от идущих в мире таких процессов, как информационные войны и конфликты, недопустимо. А это, естественно, делает актуальной информационную безопасность. Таким образом, наряду с проблемами техногенного характера у информационной безопасности существуют вытекающие из содержания информации проблемы инфогенного происхождения.

2 Возможности фольклора в контексте информационной безопасности

Известно, что в настоящее время интернет превратился в основное средство информационного обмена между народами мира. У этого процесса наряду с положительной стороной имеется и отрицательная сторона. Так, в интернете создана очень благодатная социальная среда для противоправных действий злоумышленников, организованных транснациональных, криминальных групп, которые являются носителями различных фольклорных культур. Если возможность анонимности, созданная интернетом, а также социальными медиа, с одной стороны, создает условия для устранения психологических барьеров, способных помешать социализации, общению и сближению индивидуумов, свободному и комфортному самовыражению пользователей, то с другой стороны неизвестность и неопределенность создают возможность для претворения в жизнь самых разных негативных, противозаконных действий. У. Арклан и Х. Ренджбер, особо подчеркивающие создание выгодных условий для правонарушений и преступности анонимным характером социальных медиа, пишут: «Люди, прячась за анонимностью, совершая действия, на которые не решались в повседневной жизни, легче избегают законного преследования» [9, с. 36]. В действительности причиной возникновения киберпреступности является не интернет, а противоправные действия принадлежащих к какому-либо народу и являющихся носителями его фольклорной культуры лиц, осуществляющих различные злонамеренные действия. «Вина» интернета здесь заключается в неумении определения намерений этих людей и создания условий, исключающих совершение злоумышленниками подобных действий. Говоря иначе, предоставляемые интернетом, платформами социальных медиа особые возможности вместе с тем привели к «эффективному использованию злоумышленниками этой среды» [10, с. 685].

Поэтому в интернете в соответствии с процессами, идущими на платформах социальных медиа, в законодательстве различных стран мира регулярно осуществляются изменения, принимаются решения по правовому регулированию борьбы с киберпреступлениями. Однако, несмотря на это, в настоящее время достаточно широко распространяются факты обмана людей, торговли людьми, психологического воздействия, переориентирования общества ложью и слухами посредством интернета – социальных сетей, сайтов и блогов (например, игра «Синий кит», смысл которой в устрашении, шантаже, подчинении, см.: [11, с. 51-53; 12]). В настоящее время социальные медийные платформы представляют собой сети, где ложь, слухи, обман распространяются с наибольшей скоростью [13].

Не случайно М.У. Берри М.В. и Дж. Коган, проводившие обширные исследования, связанные с анализом текстов и киберпреступности, описывают роль интернета в этом вопросе следующим образом: «...К сожалению, возможность использования новой технологии для негативных дел появляется непосредственно с ней самой. Кибернасилие и интернет-хищничество порождают

угрозу для недостаточно опытных пользователей компьютеров, в частности детей и подростков» [14, с. 161].

Формирование нормативно-правовой базы интернет-среды, правовое регулирование процессов в ней, предотвращение преступности и другие подобные вопросы делают необходимым усиление индивидуальной ответственности в интернет-среде. Однако войти в интернет и пользоваться им можно свободно. Люди при вхождении в интернет идентифицируются не какими-либо биометрическими данными – чертами лица, следами рук и пр., а IP-адресами. Хотя IP-адреса предоставляют информацию о конкретном устройстве, подключенном к интернету, очень сложно идентифицировать пользователя этого устройства. Кроме того, в контексте трансформации в виртуальной среде реальных социально-культурных процессов, а также превращения виртуальной среды, социальных сетей, блогов и сайтов в пространство, где происходят социально-культурные процессы, наблюдаются образование тайных социальных групп вне национального и международного права, а также наличие между ними зашифрованных определенными метафорическими и символическими знаками связей, в силу чего выявление подобных процессов чрезвычайно затруднено. Следовательно, некоторая информация, циркулирующая в Интернете, носит криптографический характер.

В связи с этим для повышения идентификационных возможностей интернет-пользователей очень актуален анализ звука, изображения, почерка, стиля (лексикона). Например, профиль какого-либо лица определяется его стилем, лексиконом, повторяющимися в устной или письменной речи словами, лексическими, синтаксическими, семантическими и семиотическими свойствами. Для этого разрабатываются методы и средства компьютерного анализа текстов с использованием компьютерных технологий языковой обработки естественного языка. Исследователи отмечают, что «изучая транскрипты из разных источников о кибернасилии и киберпреступности, мы сталкиваемся со схожими тактиками, используемыми кибернасильниками и киберхищниками в целях сокрытия своей личности и обмана» [14, с. 150]. Подчеркиваемую авторами схожесть можно наблюдать не только в тактиках, но и в фольклорном выражении, реакции и поведении, основывающихся на коллективной реакции и отношении.

В целом для идентификации интернет-пользователей существует ряд способов. В проведенных в этой области исследованиях было предложено различных методов анализа и выявления создаваемого пользователями контента больше, чем методов анализа и выявления самих пользователей. В частности, существуют определенные исследования по выявлению распространяемых в социальных сетях и на других онлайн-платформах ложных новостей и слухов [15, с. 729-736; 16, с. 1-8; 13], а также методы борьбы с ними, их предотвращения или же уменьшения их влияния [17, с. 2406-2414; 18, с. 108-114]. Однако иногда эти методы сами бывают недостаточными. Даже если и имеется какая-то информация об опасных или подозрительных объектах, необходимых сведений об их действительном занятии незаконной деятельностью получить не удается. Доступны бывают лишь отправленные этим объектом тексты, отдельные фрагменты речи или же предложения, и именно на их основе возникает необходимость проведения анализа. Фольклорная культура, присущая интернет-пользователям, в борьбе с кибепреступностью превращается в очень значимый источник информации, то есть фольклор играет важнейшую роль в обеспечении информационной безопасности.

В контексте обеспечения информационной безопасности с точки зрения идентификации личности или группы, фольклор обладает уникальными и специфическими признаками. Так, каждый индивид является носителем фольклорного профиля социальной группы, к которой он относится – традиционного и устоявшегося, а также «признанного» поведения и дискурса со стороны других членов группы. Вместе с тем, фольклор как этнический идентификатор может играть ключевую роль в определении национальной идентичности (этнической и групповой идентичности), национального характера и типологии его создателя. Также фольклор в качестве криптографической информации представляет собой метафорическую систему, отображающую символами реальность или ситуации. Фольклорный факт – это «индекс» [19, с. 16] выражающий определенную информацию или послание.

Эти уникальные и специфические особенности фольклора проявляются в процессе общения, самовыражения и поведения реальных или виртуальных социальных групп, являющихся его носителями, объединенных вокруг определенных интересов и потребностей, что еще больше конкретизирует идентификационные возможности изучаемого объекта. Иначе говоря, в качестве одного из специфических признаков для выявления исследуемого объекта (индивида, группы, сети и т.д.) в каком-либо происходящем киберпреступлении важную роль может сыграть его фольклорный портрет. С этой точки зрения можно сказать, что фольклор – это закодированный

источник информации с большим потенциалом защиты информации. На основании этой информации можно определить первичные признаки изучаемого объекта, так как каждый индивид, включая пользователя интернета, невольно выражает фольклорную среду, фольклорную группу и, наконец, фольклорную идентичность, к которой он принадлежит, в коммуникативном процессе или в любом акте поведения. А это дает возможность для создания посредством фольклора в контексте информационной безопасности фольклорного профиля автора определенного контента, письменной или устной речи, тайных социальных групп и процессов. С помощью компьютерных технологий и соответствующих аналитических методов можно охарактеризовать данный фольклорный профиль по самым различным параметрам. Естественно, что при этом «использование технологии интеллектуального анализа для определения ключевых терминов, свойств, событий и атрибутов из широкого спектра текстов в таких ресурсах, как статьи, веб-сайты, дискуссионные форумы, блоги», автоматически обнаруживает неявную информацию из различных текстов и аудиоисточников» [20, с. 19].

Подчеркивая важность технологий text mining в борьбе с кибернасилием и киберпреступностью, исследователи отмечают, что «эта интересная и социально значимая подобласть text mining умоляет о привлечении внимания к ней научной общественности» [14, с. 161]. Исследователи предлагают также мультидисциплинарный подход в этом вопросе: очень важны «в вопросе понимания, выявления и предотвращения киберпреступности взаимоотношения сетевых специалистов, ученых-психологов, социологов, правоохранительных органов и специалистов по коммуникациям» [14, с. 161].

3 Роль цифровых фольклорных баз и перспективы компьютерного анализа в обеспечении информационной безопасности

В различных странах мира существует практика цифровизации, а также классификации каждой фольклорной единицы по различным параметрам в рамках единой системы фольклорных ресурсов – фольклорного банка. Так, еще во времена отсутствия современных технологических возможностей осуществлялись работы по каталогизации, коллекционированию и архивации фольклорных текстов по мотивам или сюжетам. Венгерский фольклорист Э. Ильефальви, анализируя существующие цифровые базы данных, организованные из фольклорных текстов (WossiDiA, Sagragrunnur, ETKSpace, Danish Folklore Nexus, Nederlandse VolksverhalenBank, The Schools' Collection), пишет, что при этом систематизация велась в двух основных направлениях. Первое направление – это систематизация по фольклорным жанрам, второе – по собирателю (или сети собирателей) [21, с. 218].

При изучении опыта ряда стран становится ясно, что осуществлены важные работы в сфере цифровизации фольклорных архивов на основе применения информационных технологий, их классификации по различным параметрам, проведению анализов на этих фольклорных ресурсах [22].

Известный специалист по компьютерной фольклористике Т.Р. Танджерлини нынешнее время, характеризуемое как эра «больших данных», расценивает как «первичный этап, в котором ведутся компьютерные исследования на насыщенных данными фольклорных ресурсах (исторических, созданных в цифровом формате (т.е., не цифровизированных, а созданных непосредственно в цифровой среде – *Р.А., Х.К.*), или же в гибридной форме [23, с. 10]). Ученый пишет, что большинство фольклорных коллекций, согласно применяемым специалистами общим стандартам, больше соответствуют «средним и малым» данным, чем «большим данным», поэтому актуальность этих подходов для фольклора не должна оставаться вне поля зрения [23, с. 10]. Вместе с тем, выдвинутые ученым подходы и модели по геоиндексации, картофикации и геонавигации в интегрированной среде фольклорных историй также представляют широкие перспективы для определения и системного поиска координат фольклорных ресурсов в интернете [24].

Можно полагать, что компьютерная фольклористика и другие ее области, возникшая в контексте развития информационно-коммуникационных технологий, придаст толчок к расширению и углублению самой фольклористики и к достижению значимых результатов в других сферах. В настоящее время были проделаны определенные работы по созданию фольклорных баз данных и проведению в них многопараметрических анализов. Несомненно, перспективы использования фольклора для защиты информации, особенно для выявления киберпреступлений, напрямую зависят от состояния цифровых баз данных фольклора, их пригодности для многомерного компьютерного анализа, обилия таких ресурсов в интернете и ряда других вопросов.

Справедливости ради следует отметить, что периодически в определенных источниках – учебниках, монографиях, атласах и т.д. были опубликованы различные фольклорные ресурсы, которые были собраны в результате исследований, проводимых в рамках фольклористики, этнографии, антропологии, этнопсихологии и др. наук. Однако наряду с положительными сторонами этой работы, существуют и негативные, заключающиеся в том, что эти ресурсы в основном неструктурированны и сталкиваются с традиционными проблемами, встречающимися при компьютерной обработке данных на естественном языке. Поэтому руководствуясь международным опытом и рекомендациями, при поддержке специалистов в соответствующей области науки эти ресурсы, т.е. каждая фольклорная единица, должна быть заново паспортизирована на основании определенных структур, обладая при этом такими характеризующими ее признаками принадлежности, как региональные (страна, район), национально-этнические, религиозные, жанровые и др. На основе этого должны быть созданы, а также переведены на другие языки и предоставлены интернет-сообществу для публичного использования структурированные цифровые фольклорные ресурсы, которые могут быть использованы на онлайн-платформе. Иными словами, в ближайшее время должна быть сформирована сеть мультикультуральных цифровых фольклорных ресурсов, которая будет отражать реальную фольклорную среду в виртуальной среде.

Выполняя эту работу, а также обеспечивая актуальность идущих в социальной среде фольклорных процессов, можно внести вклад в использование этих цифровых ресурсов в различных целях, в том числе в повышение эффективности борьбы с киберпреступностью, являющейся одной из основных задач информационной безопасности. Так, применением цифровых фольклорных ресурсов в фильтрах трафика, на сетевых экранах, используемых с этой целью интернет-среде, можно добиться большей интеллектуализации методов и алгоритмов, используемых в процессе транспортировки и обработки принадлежащих пользователям текстов, аудиофайлов и прочего контента, то есть получения критически важных сведений для локализации и даже идентификации лиц, являющихся потенциальным источником опасности.

С другой стороны, одной из основных проблем, волнующих в настоящее время мировое сообщество, является обнаружение киберпреступных элементов и сообществ, индивидуально или в групповой форме злонамеренно, деструктивно функционирующих в социальных сетях под анонимными именами (fake profile или nickname), порождающих или распространяющих ложную информацию. В связи с этим в результате анализа социальных сетей в последнее время были разработаны различные интеллектуальные методы и алгоритмы для дешифровки криптосообществ, занимающихся криминальной деятельностью [25; 26]. Анализ показывает, что при разработке этих интеллектуальных технологий среди характеризующих пользователей интернета признаков не учитываются показатели их психики, поведения, религиозной и этнической принадлежности, а самое главное, особенности фольклорных ресурсов, обладающих большим информационным потенциалом. Поэтому в ходе борьбы с киберпреступностью на международном и национальном уровнях использованием сообразно исторически сложившимся и динамичным социальным процессам быстро возникающих и распространяющихся фольклорных ресурсов можно качественнее и эффективнее локализовать объекты, входящие в группу риска. Все эти работы могут быть успешно выполнены с использованием наиболее распространенных методов теории искусственного интеллекта – распознавания изображений, классификации и кластеризации объектов, извлечения данных, NLP (Natural Language Processing – обработка естественного языка) и других смарт-технологий.

Общий анализ проводимых в этой области исследований и осуществленных работ показывает, что существуют следующие научно-теоретические и практические проблемы использования фольклора в обеспечении информационной безопасности и выявлении случаев киберпреступности:

- проблемы формирования в соответствии с международной практикой структурированных мультимедийных фольклорных ресурсов на основе многопараметрических национальных фольклорных ресурсов, их интеграция в интернет-среду, а также регулярное обогащение;
- проблема создания принадлежащих пользователям индивидуальных фольклорных досье, иными словами, «фольклоризации» IP-адресов, имеющихся в распоряжении пользователей, на основании сравнения трафика, сформированного в результате деятельности пользователей в интернет-среде (социальные сети, форумы и блоги, переписка по электронной почте, беседы) с национальными цифровыми фольклорными ресурсами, существующими в онлайн-среде;

- проблемы идентификации действующих в интернет-среде неявных (скрытых) социальных групп и сетей на основе интеллектуального анализа (кластеризации) принадлежащих пользователям индивидуальных фольклорных досье;
- проблемы комплексного анализа диалектологического, текстологического и других аспектов путем использования интеллектуальных фольклорных сенсоров с применением методов обработки естественного языка и искусственного интеллекта, получения новых знаний и т.д.

Как видно из вышеизложенного, хотя и существуют широкие перспективы использования фольклора в обеспечении информационной безопасности, в этой области имеются и многочисленные проблемы, ждущие своего решения. Полагаем, что появление в перспективе возможности анализа национальных цифровых фольклорных ресурсов взаимосвязанных в рамках открытой цифровой информационной системы фольклорных ресурсов, принадлежащих другим народам, создаст условия для более широких сравнений и анализов. А это в контексте информационной безопасности еще больше расширит возможности фольклора, и какой-либо объект (текст, фото, аудио-, видеоресурс, индивидуум или тайная социальная группа), который может стать предметом киберпреступности, обретет возможность анализа на основе многочисленных фольклорных банков данных. Таким образом, анализ существующих подходов по информационной безопасности и выявлению киберпреступности дает основания утверждать, что в качестве компонента безопасности фольклор обладает уникальными и специфическими возможностями, вследствие чего существует большая потребность в проведении исследований в этой области.

Заключение

Фольклор, подпитываемый психологической действительностью и связанный с социальной средой, региональной спецификой, лингвистической типологией – местным языком и диалектом, национальным характером и стереотипом, в контексте определения национальной идентичности в качестве компонента информационной безопасности дает широкие возможности для исследования. Поэтому при исследовании различных аспектов информационной безопасности должны быть исследованы и возможности использования фольклора, изучены новые методы и подходы в этом направлении.

Анализ научной литературы по проблеме, исследуемой в статье, показывает, что в контексте информационной безопасности вопросы использования фольклора достаточно актуальны и мало изучены, а также то, что использование фольклора в информационной безопасности зависит от состояния национальных цифровых фольклорных баз данных, их адекватности для многопараметрического компьютерного анализа, наличия большого количества подобных ресурсов в Интернете и ряда других вопросов.

В статье определен ряд научных и практических проблем использования фольклора в обеспечении информационной безопасности и выявлении киберпреступности, а также внесены некоторые предложения.

Исходя из данного контекста можно сделать вывод о том, что в перспективе фольклор может играть важную ключевую роль в информационной безопасности и обнаружении киберпреступности, и в условиях возникновения мультикультурной фольклорной среды возможно широкое использование фольклора в исследовании криминальных и насильственных явлений, встречающихся в социальных сетях и форумах, в исследовании криминальных и насильственных явлений, выявлении и предотвращении криминальных социальных сетей.

Литература

1. Баева Л.В. Виртуальная сансара: трансформация модели реальности в условиях информационной культуры // Информационное общество. 2012. № 2, С. 44-51.
2. Владимирова Т.В. Информационная безопасность: к методологическим основаниям анализа вопроса // Информационное общество. 2012. № 5, С. 47-52
3. Еркин А.В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному // Информационное общество. 2012. № 1, С. 68-74
4. Арсентьев М. В. К вопросу о понятии «Информационной безопасности» // Информационное общество. 1997. № 4-6, С. 48-50

5. İmamverdiyev Y.N. E-Dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli // İnformasiya cəmiyyəti problemləri. 2013. №1, s. 20-31.
6. Əliquliyev R.M., İmamverdiyev Y.N. E-Dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri. 2010. №1, s. 3-13
7. Кузнецов Н.А., Кульба В.В., Микрин Е.А. Информационная безопасность систем организационного управления. Теоретические основы. в 2 т. Москва: Наука, 2006. 495 с.
8. Blank, Trevor J. Folklore and the Internet: The Challenge of an Ephemeral Landscape. // Humanities 7. 2018. No. 2: 50. DOI: 10.3390/h7020050
9. Arklan Ü., Rençber H. İllegalitenin kaçış alanı olarak sosyal medya // Current Debates in Public Relations Cultural and Media Studies. 2017. Volume 9, pp. 31-53
10. Karahisar T. Suçu önleyici faaliyetlerde ve suç soruşturmasında sosyal medyanın rolü. 2. Uluslararası Farkındalık Kongresi Bildiri Kitabı. 2018. s. 685–697.
11. Зислин И., Архипова А.С., Радченко Д.А. «Синий Кит» и моральные паники: антрополого-психиатрический подход. «Сухаревские чтения. Суицидальное поведение детей и подростков: эффективная профилактическая среда», 14–15 ноября 2017 года, Москва. Сборник статей под общей редакцией к.м.н. М.А.Бебчук, [Электронное издание] М.: ГБУЗ «НПЦ ПЗДП им. Г.Е. Сухаревой ДЗМ», 2017. С. 51–53.
12. Архипова А., Волкова М., Кирзюк А., Малая Е., Радченко Д., Югай Е. «Группы смерти»: от игры к моральной панике. Москва: РАНХиГС, 2017, 24 с.
13. Goh, Dion Hoe-Lian; Chua, Alton Y. K.; Shi, Hanyu; Wei, Wenju; Wang, Haiyan; and Lim, Ee-peng. An analysis of rumor and counter-rumor messages in social media. // Digital libraries: Data, information, and knowledge for digital lives: 19th International Conference on Asia-Pacific Digital Libraries, ICADL 2017, Bangkok, Thailand, November 13–15, Proceedings. Springer International Publishing. pp. 256-266. https://doi.org/10.1007/978-3-319-70232-2_22
14. Berry Michael W. and Kogan J. Text mining: applications and theory. Wiley A. John Wiley and Sons, Ltd., Publication, 2010. 207 p.
15. Gupta, A., Lamba, H., Kumaraguru, P., Joshi, A. Faking sandy: characterizing and identifying fake images on Twitter during hurricane sandy. // Proceedings of the 22nd International Conference on World Wide Web, ACM Press. 2013. pp. 729-736
16. Canini, K.R., Suh, B., Pirolli, P.L. Finding credible information sources in social networks based on content and social structure. // 2011 IEEE Third International Conference on Social Computing. IEEE Press: 2011. pp. 1-8.
17. Ozturk, P., Li, H., Sakamoto, Y. Combating rumor spread on social media: the effectiveness of refutation and warning. In: Proceedings of the Hawaii International Conference on System Sciences. IEEE Press. 2015. pp. 2406–2414
18. Bernard, S., Bouza, G., Piétrus, A. An optimal control approach for E-rumor. Revista Investigacion Operacional, Volume 36 (2), 2014. pp. 108–114
19. McNeill, Lynne S. The internet is weird. Folkloristics in the digital age. Folklore Fellows' Network. № 47, December. 2015. pp. 12–13, 16–17.
20. Alıquliyev R., Niftəliyeva G. "E-dövlətin analizi texnologiyaları: text mining və sosial şəbəkələr". Ekspress informasiya. "İnformasiya texnologiyaları" seriyası. Bakı: İnformasiya Texnologiyaları nəşriyyatı, 2016, 78 s.
21. Emese Ilyefalvi. The Theoretical, Methodological and Technical Issues of Digital Folklore Databases and Computational Folkloristics // Acta Ethnographica Hungarica. 2018. 63 (1), pp. 209-258.
22. Abello J., Broadwell P., Tangherlini T.R. Computational Folkloristics // Communications of the ACM. 2012. 55 (7), pp. 60–70.
23. Tangherlini T.R. Big Folklore: A Special Issue on Computational Folkloristics // The Journal of American Folklore. 2016. vol. 129, No. 511 (Winter), pp. 5-13.
24. Broadwell P., Timothy T.R. TrollFinder: Geo-Semantic Exploration of a Very Large Corpus of Danish Folklore / In: The Third Workshop on Computational Models of Narrative, Proceedings of LREC. Istanbul, 2012, pp. 50-57
25. Alguliyev R.M., Aliguliyev R.M. and Niftaliyeva G.Y. Extracting social networks from e-government by sentiment analysis of users' comments // Electronic Government, Vol. 15, No. 1, 2019, pp. 91-106
26. Alguliyev R.M., Aliguliyev R.M. and Niftaliyeva G.Y. Filtration of Terrorism-Related Texts in the E-Government Environment // International Journal of Cyber Warfare and Terrorism. Volume 8, No. 4, 2018. pp. 35-48

OPPORTUNITIES OF USING FOLKLORE IN INFORMATION SECURITY

Aliguliyev, Rasim M.

Doctor of technical sciences, professor
Institute of Information Technologies of ANAS
Baku, Azerbaijan
r.alguliev@gmail.com

Guliyev, Hikmat V.

PhD in Philology, associate professor
Institute of Folklore of ANAS
Baku, Azerbaijan
quliyevh@mail.ru

Abstract

The article examines the possibilities of using folklore in solving information security problems. It is noted that at present, the rapid growth of the role of the Internet in everyday life, in addition to advantages, has such negative aspects as the emergence of cybercrimes and cyber violence, hidden social networks and criminal processes, which has led to the actualization of the information security problem. Currently, various methods and approaches have been proposed to identify and prevent negative social processes taking place in the virtual environment, in particular, propaganda of crimes and violent acts. The article analyzes the issues of identifying adequate methods and means of detecting secrecy focused on negative actions, hidden criminal virtual social networks and groups using the unique capabilities of folklore in the context of information security; proposals are put forward for carrying out activities in this direction in the future.

Keywords

information security, cybercrime, disinformation, Internet folklore, folkloric fact, the multicultural folklore environment, national identity

References

1. Baeva L.V. Virtual'naja sansara: transformacija modeli real'nosti v uslovijah informacionnoj kul'tury // Information Society Journal. 2012. № 2, pp. 44-51.
2. Vladimirova T.V. Informacionnaja bezopasnost': k metodologicheskim osnovanijam analiza voprosa // Information Society Journal. 2012. № 5, pp. 47-52.
3. Erkin A.V. Ponjatija «informacija» i «informacionnaja bezopasnost'»: ot industrial'nogo obshhestva k informacionnomu // Information Society Journal. 2012. № 1, pp. 68-74.
4. Arsent'ev M. V. K voprosu o ponjatii «Informacionnoj bezopasnosti» // Information Society Journal. 1997. № 4-6, pp. 48-50.
5. Imamverdiyev Y.N. Conceptual model of e-government information security management // Problems of Information Society. 2013. №1, pp. 20-31 (in Azerbaijanian).
6. Alguliev R.M., Imamverdiyev Y.N. E-Government Information Security Management Research // Challenges Problems of Information Society. 2010. №1, pp. 3-13 (in Azerbaijanian).
7. Kuznecov N.A., Kul'ba V.V., Mikrin E.A. Informacionnaja bezopasnost' sistem organizacionnogo upravlenija. Teoreticheskie osnovy. v 2 t. Moskva: Nauka, 2006. 495 p.
8. Blank, Trevor J. Folklore and the Internet: The Challenge of an Ephemeral Landscape // Humanities 7, 2018. No. 2: 50. DOI: 10.3390/h7020050.
9. Arklan Ü., Rençber H. Social media as the escape area for illegality // Current Debates in Public Relations Cultural and Media Studies. 2017. Volume 9, pp. 31-53 (in Turkish).
10. Karahisar T. The role of social media in activities on crime prevention and criminal investigation // II. İnternatioan Conference on Awareness // Proceedings. 2018. pp. 685–697 (in Turkish).
11. Zislin I., Arhipova A.S., Radchenko D.A. «Sinij Kit» i moral'nye paniki: antropologo-psihiatricheskij podhod. «Suharevskie chtenija. Suicidal'noe povedenie detej i podrostkov: jeffektivnaja profilakticheskaja sreda», 14–15 nojabrja 2017 goda, Moskva. Sbornik statej pod obshhej redakciej k.m.n. M.A.Bebchuk, [Jelektronnoe izdanie] M.: GBUZ «Sukhareva Scientific-practical Children's Mental Health Centre», 2017. pp. 51–53.

12. Arhipova A., Volkova M., Kirzjuk A., Malaja E., Radchenko D., Jugaj E. «Gruppy smerti»: ot igry k moral'noj panike. Moskva: RANEPA, 2017, 24 p.
13. Goh, Dion Hoe-Lian; Chua, Alton Y. K.; Shi, Hanyu; Wei, Wenju; Wang, Haiyan; and Lim, Ee-peng. An analysis of rumor and counter-rumor messages in social media. // Digital libraries: Data, information, and knowledge for digital lives: 19th International Conference on Asia-Pacific Digital Libraries, ICADL 2017, Bangkok, Thailand, November 13–15, Proceedings. Springer International Publishing. pp. 256-266. https://doi.org/10.1007/978-3-319-70232-2_22.
14. Berry Michael W. and Kogan J. Text mining: applications and theory. Wiley A. John Wiley and Sons, Ltd., Publication, 2010. 207 p.
15. Gupta, A., Lamba, H., Kumaraguru, P., Joshi, A. Faking sandy: characterizing and identifying fake images on Twitter during hurricane sandy. // Proceedings of the 22nd International Conference on World Wide Web, ACM Press. 2013. pp. 729-736.
16. Canini, K.R., Suh, B., Pirolli, P.L. Finding credible information sources in social networks based on content and social structure. // 2011 IEEE Third International Conference on Social Computing. IEEE Press: 2011. pp. 1-8.
17. Ozturk, P., Li, H., Sakamoto, Y. Combating rumor spread on social media: the effectiveness of refutation and warning. In: Proceedings of the Hawaii International Conference on System Sciences. IEEE Press. 2015. pp. 2406–2414.
18. Bernard, S., Bouza, G., Piétrus, A. An optimal control approach for E-rumor. Revista Investigacion Operacional, Volume 36 (2), 2014. pp. 108–114.
19. McNeill, Lynne S. The internet is weird. Folkloristics in the digital age. Folklore Fellows' Network. № 47, December. 2015. pp. 12–13, 16–17.
20. Aliguliyev R., Niftaliyeva G, "E-government analysis technologies: text mining and social networks". Express information. "Information technology" series. Baku, "Information Technologies" publishing house, 2016, 78 p (in Azerbaijanian).
21. Emese Ilyefalvi. The Theoretical, Methodological and Technical Issues of Digital Folklore Databases and Computational Folkloristics // Acta Ethnographica Hungarica. 2018. 63 (1), pp. 209-258.
22. Abello J., Broadwell P., Tangherlini T.R. Computational Folkloristics // Communications of the ACM. 2012. 55 (7), pp. 60–70.
23. Tangherlini T.R. Big Folklore: A Special Issue on Computational Folkloristics // The Journal of American Folklore. 2016. vol. 129, No. 511 (Winter), pp. 5-13.
24. Broadwell P., Timothy T.R. TrollFinder: Geo-Semantic Exploration of a Very Large Corpus of Danish Folklore / In: The Third Workshop on Computational Models of Narrative, Proceedings of LREC. Istanbul, 2012, pp. 50-57.
25. Alguliyev R.M., Aliguliyev R.M. and Niftaliyeva G.Y. Extracting social networks from e-government by sentiment analysis of users' comments // Electronic Government, Vol. 15, No. 1, 2019, pp. 91-106.
26. Alguliyev R.M., Aliguliyev R.M. and Niftaliyeva G.Y. Filtration of Terrorism-Related Texts in the E-Government Environment // International Journal of Cyber Warfare and Terrorism. Volume 8, No. 4, 2018. pp. 35-48.