УДК 006.322

Актаева А.У.[1], Ниязова Р.[2], Сералиева А.[1], Сарсенбаева Ж.[1], Даутов А.[1], Кусаинова У.[1], Жартанов С.[1]

[1] Кокшетауский университет имени А. Мырзахметова, г. Кокшетау, Казахстан
[2] Евразийский национальный университет им. Л. Гумилева, г. Астана, Казахстан

КОГНИТИВНЫЕ ТЕХНОЛОГИИ ОНТОЛОГИИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

Аннотация

Рассматривается структура и основные принципы технологии повышения вероятности идентификации субъектов информационных процессов открытых ресурсов сети Интернет на основе методов онтологии. На основе этой онтологии была реализована база знаний, предназначенная для создания программных систем, поддерживающих обеспечение информационной безопасности.

Разработанная онтологическая база знаний была использована при разработке программного комплекса, предназначенного для идентификации пользователя социальных сетей при обеспечении информационной безопасности, отслеживания и предотвращения угроз. Данная статья является очередной в серии статей авторов, в которых они продолжают отслеживать и анализировать современное состояние и новые тенденции в области защиты и безопасности информации.

Ключевые слова

Онтология, информационная безопасность, база знаний, идетификация пользователя, язык SPARQL, социальная сеть.

Aktayeva A.[1], Niyazova R.[2], Seraliyeva A.[1], Sarsenbayeva Zh.[1], Dautov A.[1], Kussainova U.[1], Zhartanov S.[1]

[1] Abai Myrzakhmetov Kokshetau University, Kokshetau, Kazakhstan
[2] L. Gumiyev Eurasian National University, Astana, Kazkhstan

COGNITIVE TECHNOLOGIES OF ONTOLOGY IN INFORMATION SECURITY SYSTEMS

Abstract

The structure and basic principles of technology for increasing the probability of identifying subjects of information processes of open Internet resources based on ontology methods are considered. Based on this ontology the knowledge base intended for creation of the program systems supporting ensuring information security has been realized.

The developed ontological knowledge base has been used when developing the software complex intended for identification of the user of social networks when ensuring information security, monitoring and preventing threats. This article is next in a series of articles by the authors in which they continue to monitor and analyse the current state and new tendencies in the field of information security and safety of information.

Keywords

Ontology, knowledge base, information security, Social network, SPARQL, identification.

Введение

В период бурного роста применения информационных технологий, успешное решение проблем в

* **Труды II Международной научной конференции «Конвергентные когнитивно-информационные технологии» (Convergent'2017), Москва, 24-26 ноября, 2017**

Proceedings of the II International scientific conference "Convergent cognitive information technologies" (Convergent'2017), Moscow, Russia, November 24-26, 2017

области информационной безопасности и защиты информации предполагает более эффективную деятельность в процессе обеспечения безопасности во всех сферах жизнедеятельности человека.

Транснациональный и трансграничный характер многих продуктов ИКТ и международная связанность социальных сетей используются киберпреступностью в целях совершения противоправных действий в отношении пользователей и владельцев Интернет-ресурсов, размещённых в транснациональном сегменте, а также АИСУ, взаимодействующих с Глобальной сетью. Высокая латентность и зачастую международный характер таких преступлений повышают их общественную опасность мирового сообщества. Ситуация усугубляется укоренившимися в мировом обществе стереотипами о безнаказанности так называемой «*киберпреступности*», ненужности принимаемых мер по укреплению сферы безопасного использования ИКТС (*инфокоммуникационные технологии и системы*), ограниченными возможностями общества по привлечению к ответственности виновных в совершении высокотехнологичных преступлений, несмотря на развитые правовые институты информационной безопасности в области социальных сетей [18].

Кроме того, от успешного разрешения вопросов данной области зависит обеспечение глобальной безопасности мирового сообщества. Дальнейшее становление социума, основанного на информационных технологиях, в целях обеспечения динамического равновесия общественной эволюции требует поддержания условий кибербезопасности. Кибербезопасность должна рассматривается как устойчивое состояние информационной сферы, обеспечивающее свою целостность и защиту объектов ИКТ-инфраструктуры при наличии неблагоприятных внутренних и внешних воздействий на основе осознания общества своих ценностей, жизненно важных интересов и целей развития.

Пренебрежение политикой кибербезопасности при использовании ресурсов социальных сетей Интернета ведёт к повышенному риску для неприкосновенности частной жизни, несанкционированному использованию или модификации общедоступных персональных данных, а также разглашению персональных данных пользователей или их транснациональной доступности для преступных сообществ или разведывательных структур различных стран. Это, в свою очередь, обуславливает необходимость контроля субъектов информационных процессов для идентификации возможных направлений информационного влияния и воздействия на пользователей социальных сетей Интернета.

В связи с тем, что более 85% информации в Интернете представлено в текстовом виде, возникает необходимость в разработке средств идентификации пользователей на основе современных методов, предназначенных для обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации. В рамках этой задачи крайне важна идентификация субъектов информационных процессов, имеющих возможность легально распространять «*недостоверные или противоречивые*» сообщения [15,16].

Большое количество Интернет-ресурсов и сервисов, таких как форумы, порталы (ресурсы социальных сетей), Интернет-магазины, сталкиваются с различными проявлениями проблем манипуляции и искусственного формирования общественного мнения, путем «*организации*» целенаправленных тематических диалогов, в которых ряд пользователей имеют несколько учетных записей (аккаунтов). Возможность использования социальных порталов для распространения информации и недостаточная функциональность механизмов идентификации и аутентификации пользователей, оставляющих сообщения, определяет ряд направлений совершенствования систем защиты и систем мониторинга информационной безопасности ИКТС.

В связи с этим возникает задача повышения вероятностных показателей качества методов идентификации пользователей различных порталов сети Интернет. Отсутствие должных механизмов идентификации и аутентификации порождает ряд угроз кибербезопасности, связанных с обработкой, распространением и ознакомлением других пользователей с текстовыми сообщениями. Анонимно используя текстовые сообщения, пользователь, группы пользователей могут распространять информацию заведомо определенной направленности, нанося информационный урон экономическим, культурным, социальным, политическим объектам, представленным в социальных сетях Интернета. Одним из перспективных направлений исследований в данной области является моделирование систем кибербезопасности с использованием принципов когнитивного онтологического представления знаний с учетом спецификаций данной предметной области.

Принципы когнитивного онтологического представления знаний

Онтологии были предложены для декларативного представления знаний и определяются в общем виде как база знаний специального вида или как «*спецификация концептуализации*» любой предметной области. Это означает, что в предметной области на основе классификации базовых терминов выделяются основные понятия (концепты), и устанавливаются связи между ними – концептуализация. Затем онтология может быть представлена в графическом виде или описана на одном из формальных

языков (формальная онтология) – это процесс спецификации онтологий. Онтологическое представление знаний используется для семантической интеграции информационных ресурсов, адекватной интерпретации содержания текстовых документов, представленных на естественном языке [15,16,19].

Основой для разработки принципов когнитивного онтологического представления знаний является схема, отражающая взаимосвязи основных понятий безопасности, приведённая в Международном Стандарте по Кибербезопасности ISO/IEC 27032:2012. Сформированная на этой основе онтология отражает только понятия, описанные в данном стандарте, и лишь частично детализирует разные аспекты, которые требуется учитывать при проектировании системы обеспечения кибербезопасности объектов инфраструктуры социальных сетей Интернета [15,16,19]. Тогда, как видно из рисунка 1, для обеспечения безопасности инфраструктуры социальных сетей Интернета необходимо учитывать множество разнообразных факторов, отражающих особенности всех заинтересованных участников, их ресурсов, возможных угроз и принимать соответствующие ответные меры защиты от неблагоприятных внутренних и внешних воздействий на объекты инфраструктуры ИКТС.

Когнитивные модели используются для моделирования угроз информационной безопасности, а событийные модели для моделирования вариантов развития различных ситуаций. А когнитивное моделирование онтологии – построение когнитивных моделей (ориентированных графов), в которых вершины соответствуют факторам (концептам), а дуги – связям между факторами [15,16,19].

Событийное моделирование – построение поведенческих моделей (*поведение пользователей социальных сетей),* причем в качестве объектов моделирования могут рассматриваться как люди, так и технические объекты. Сущность событийного метода моделирования заключается в отслеживании на модели последовательности событий в том же порядке, в каком они происходили бы в реальной системе [15,16,19].

Совместное использование когнитивного и событийного моделирования позволяет получить более объективную оценку ситуации в социальных сетях. Вводятся онтологии событий, используемые для перехода от когнитивных к событийным моделям.

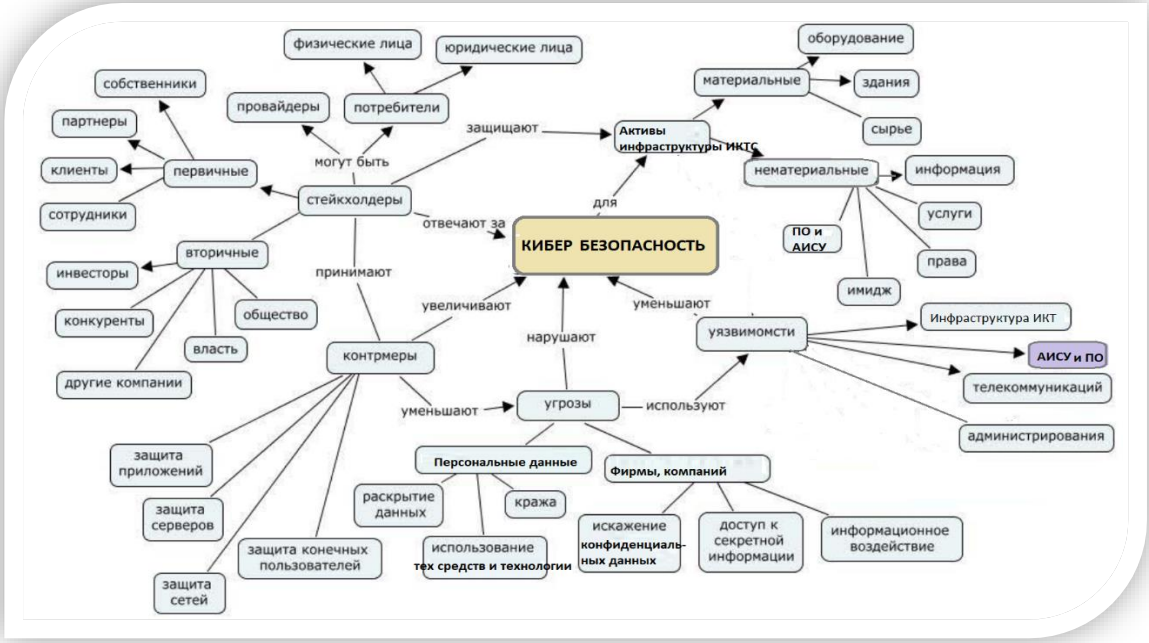

Рис.1 – Онтология кибербезопасности по ISO/IEC 27032:2012 [15,16]

При формализации задачи онтологий важно отметить, что: онтология является одним из инструментов, необходимых для моделирования предметной области; онтология содержит перечень ключевых понятий данной предметной области и спецификацию их смысла; знание о смысле ключевых понятий, представленное онтологией, должно быть очевидным для любого эксперта в данной предметной области, на основе онтологий разрабатываются базы знаний [12].

Предложенная концепция поддерживает технологию исследований направлений развития инфраструктуры социальных сетей Интернет с учетом требований информационной безопасности.

Предполагаем, что инфраструктура социальных сетей Интернет определяется как $V_{SN}=\{O, E, M_C, M_S\} \cup T_{SN}$,

где O – множество онтологий; E – множество описаний прецедентов;

M_C – множество когнитивных моделей;

M_S – множество событийных моделей;

T_{SN} - инструментальные средства поддержки ИКТ/социальной сети, включающие описание знаний, представленных в виде онтологий, описаний прецедентов, когнитивных и событийных моделей и средства оперирования ими. Формальной онтологией предметной области *S*σ называется пара *S* и σ, где σ – множество ключевых понятий предметной области, а *S* – множество аналитических предложений, описывающих смысл данных ключевых понятий [2,15,16].

Онтологии позволяют концептуализировать предметную область, формализовать накопленные знания: определить ключевые понятия предметной области, задать семантические отношения между понятиями, необходимые для постановки задач и описания процессов их решения в данной предметной области. При логической формализации, дающей возможность осуществления логического вывода, базу знаний можно мыслить, как эмпирическую теорию предметной области: теорию в логике предикатов первого порядка. Кроме того, преимуществом использования онтологий является возможность анализа, накопления и повторного применения знаний о данной предметной области, полученных из разных источников [2].

В более сложном случае онтология задается в виде множества формальных определений, сформулированном на некотором языке представления знаний, допускающем логический вывод. В настоящее время актуальной является задача разработки онтологий с помощью различных средств, основанных на логиках описаний.

В результате анализа состояния предметной области идентификации пользователей социальных сети Интернет необходимо выделить следующее:

- в связи с широкими возможностями по обеспечению анонимности пользователей социальных сети Интернет, особую важность приобретают методы идентификации. Но этот метод не учитывает изменения технических характеристик устройства;
- методы определения авторства текста, применяемые классическими лингвистами, показывают хорошие результаты для больших объемов текста, подвергшихся коррекции, но требуют основательной адаптации для обработки коротких сообщений;
- в целях повышения качественных показателей методов идентификации пользователей социальных сети Интернет необходимо разработать кортеж лингвистических признаков короткого сообщения, позволяющего учитывать особенности построения идентификаторов.

На сегодняшний день большую популярность получили методы идентификации, использующие технические характеристики, в первую очередь, такие как:

- HTTP Cookie;
- IP-адрес;
- MAC-адрес;
- геолокационные данные;
- данные об используемой ОС, браузере, параметрах оборудования *(разрешение и размер экрана, центральный процессор* и т.д.).

Методы идентификации, использующие технические характеристики ИКТС эффективны для поиска «*троллей-одиночек*» или недобросовестных пользователей, но малоэффективны для борьбы и идентификации организованного *астротурфинга (*AstroTurf), проводимого специальными организациями, которые могут обеспечить изменение данных характеристик [2,4,5,12].

Все эти особенности необходимо учитывать в процессе идентификации для повышения качества получаемых результатов. Таким образом, на основе полученной модели текстового сообщения, содержащей информацию о лексической, графематической и синтаксической составляющих, становится возможным определение профиля для каждого пользователя портала сети Интернет.

Профиль пользователя – это совокупность данных и настроек окружения пользователя. Построение профиля пользователя возможно на основе ряда технических характеристик и статистических данных. Такой подход к созданию профиля не всегда может дать достоверный результат. Предлагаемый профиль пользователя особо важен в случаях, когда возможна подмена, клонирование ряда технических характеристик устройств, т.е. практически однозначная идентификация пользователя невозможна [2,4,5,12].

Метод создания профиля пользователя сети Интернет предполагает реализацию ряда шагов:

- обработка пользовательских сообщений в рамках Интернет портала;
- разбор сообщений по частям речи с последующим применением шаблонов для выделения наиболее распространенных конструкций;
- лексикографический анализ сообщения и выделение конструкций в соответствии с описанными шаблонами и сбор статистики об использовании знаков препинания и специальных символов;
- выделение лексических конструкций на основе слов и словоформ языка, а также выявление

тематических специальных слов и выражений, характерных для аудитории конкретного форума.

Реализация предлагаемого метода построения профиля пользователя портала сети Интернет направлена на решение обозначенных задач в случаях, когда одним и тем же ПК пользуются несколько человек или же сообщения оставляются пользователями, находящимися в одной локальной подсети. В таблице 1 приведён процесс создания профиля пользователя, использующего лингвистические характеристики [2,4,5,12].

Таблица 1 – Основные методы идентификации автора сообщений

<table>
<tr><th colspan="5">Методы идентификации</th></tr>
<tr><th colspan="2">Статистический анализ</th><th>Машинное обучение</th><th colspan="2">Лингвистический анализ</th></tr>
<tr><td>Одномерный</td><td>Многомерный</td><td>Метод Байеса</td><td rowspan="9">Статистический</td><td rowspan="9">Аналитический</td></tr>
<tr><td>Критерий Стьюдента</td><td>Энтропийный подход</td><td>Деревья решений</td></tr>
<tr><td>Двусторонний критерий Фишера</td><td>Критерий Колмогорова-Смирнова</td><td>Генетические алгоритмы</td></tr>
<tr><td>QSUM</td><td>Сложностный подход</td><td>Нейронные сети</td></tr>
<tr><td rowspan="5">χ^2 -пирсона (Критерий согласия Пирсона)</td><td>χ^2 -пирсона для распределений</td><td>Машина опорных векторов</td></tr>
<tr><td>Статистический кластерный анализ</td><td rowspan="4">Метод ближайших соседей</td></tr>
<tr><td>Линейный дискретный анализ</td></tr>
<tr><td>Метод главных компонентов</td></tr>
<tr><td>Марковские цепи</td></tr>
</table>

Применения онтологического представления знаний для построения профиля пользователя портала сети Интернет

Онтологический подход к представлению знаний позволяет применять существующие и прошедшие апробацию алгоритмы выполнения аналитических запросов расширенного профиля для каждого пользователя портала сети Интернет. Выполнение аналитических запросов к данным обеспечивается в процессе взаимодействия конечного пользователя системы с программной реализацией модели, описывающей область знания. Для применения онтологического представления знаний для построения профиля пользователя портала сети Интернет и составления когнитивной модели предметной области необходимо:

1. выделить значимые факторы;
2. построить матрицу взаимовлияний;
3. определить начальные тенденции изменения факторов.

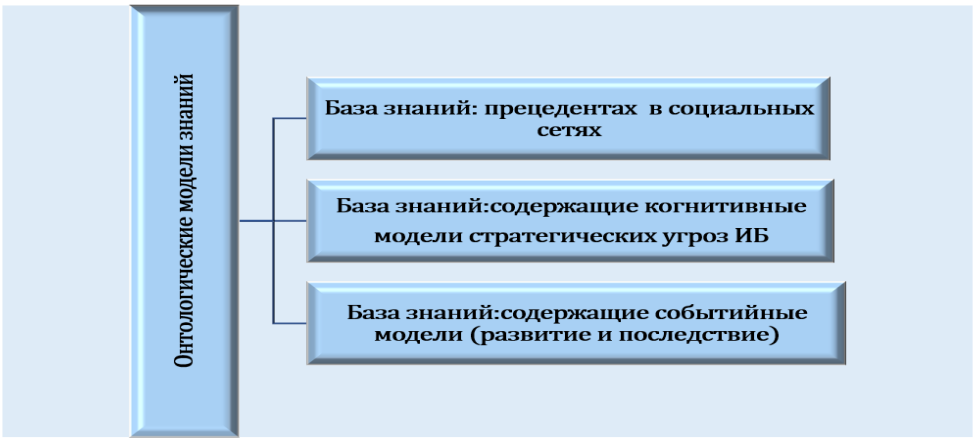

Рис. 2 – Онтологические модели знаний в области информационной безопасности: инфраструктура социальных сетей Интернет

Таким образом, инфраструктура социальных сетей Интернет включает пространство знаний, интегрирующее: онтологические модели знаний в области исследований ИБ, базу знаний о прецедентах в социальных сетях и базы знаний, содержащие когнитивные модели стратегических угроз ИБ и событийные модели развития и последствий событий в социальных сетях, а также инструментальные средства описания знаний (см.рис.2).

Выделение информации традиционно имеет целью найти сведения, которые описывают некоторую область знаний, заданную структурой данных. Онтологии же как раз и представляют собой формальную модель предметной области, выраженную, например, в виде графа понятий и связей, что обобщает иерархическую структуру данных, обычно используемую для заполнения в задаче выделения информации и включает в себя этапы (см.рис.3).

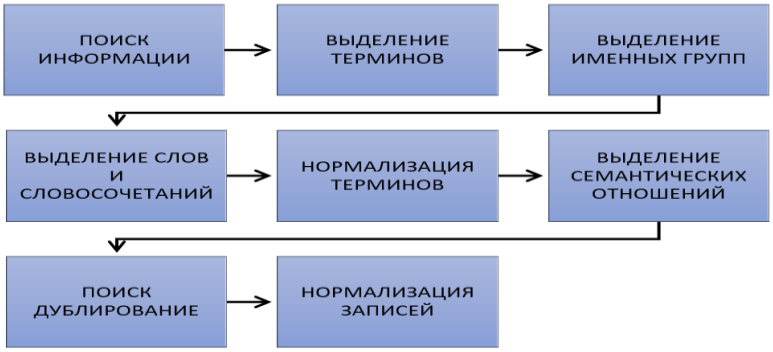

Рис.3 – Онтологический подход к представлению знаний: выделение информации

Показатели эффективности алгоритмов выделения информации делятся на два класса, а именно – показатели корректности, например, точность, корректность выделенной информации, полнота: *количество выделенной информации по отношению к объему всей доступной информации* и мера избыточности, а также оценки вычислительных ресурсов, таких как время и память.

Запрос при использовании онтологий может выполняться автоматически с помощью механизмов логического вывода. В качестве языка запросов к онтологиям можно использовать язык SPARQL. Выбор именно этого языка обусловлен высоким уровнем его развития, зрелости и хорошем потенциалом, что подтверждают следующие факты:

•в 2008 году язык SPARQL получил статус официальной рекомендации консорциума W3C2;

•язык SPARQL не привязан к конкретному программному комплексу, в отличие от других языков запросов к онтологиям;

•для языка SPARQL существует большое число программных реализаций и приложений [4,5,12].

Ниже приведены примеры использования языка SPARQL в научном исследовании:

Пример 1. Перечень тем участников портала, которые активно исследуются в рамках интересующей тематики. Интерпретация запроса: «*выдать все результаты, за последний (2016) год и отсортировать их по убыванию встречаемости в этих результатах*». Формализуем его на языке SPARQL. Сначала сформируем множество ***Terms***, содержащее все термины с/без повторения), сопоставленные результатам деятельности за год.

```
SELECT ?term
WHERE {
?term a cs:term .
?res a swrc:Result .
?res swrc:isAbout ?term . ?res swrc:year 2016. }
```

Полученное множество терминов ***Terms***, необходимо отсортировать по убыванию количества повторений каждого уникального элемента. Термины, расположенные в начале отсортированного списка, и определяют направления, которые активно исследуются в рамках интересующей области знания.

Пример 2. Список пользователей на интересующем направлении. Интерпретация запроса на языке SPARQL следующим образом: «*выдать список пользователей, результатов поиска которых связаны с терминами заданного направления*

$T = \{t_1, \ldots, t_n\}$». Сформулируем этот запрос на языке SPARQL.

```
SELECT DISTINCT ?person
WHERE {
?person a swrc:Person .
?res a swrc:Result .
?res dc:creator ?person .
```

{ ?res swrc:isAbout t_1 }
UNION { ?res swrc:isAbout t_2 } ...
UNION { ?res swrc:isAbout t_n } . }
Пример 3. Список публикаций, похожих на заданную.

Интерпретация запроса на языке SPARQL следующим образом «*выдать список запрос, связанных с терминами, которые характеризуют заданный поиск*». Формальная запись этого запроса на языке SPARQL представлена ниже.

SELECT DISTINCT ?
WHERE {
?p a swrc:Publication . ?term a cs:term .
?p swrc:isAbout ?term . Pub swrc:isAbout ?term . }
Пример 4. Перечень форумов, посвященных интересующему направлению.

Перепишем этот запрос следующим образом: «*выдать список форумов, связанных с терминами заданного направления* $T = \{t_1, \ldots, t_n\}$». Интерпретация запроса на языке SPARQL:

SELECT DISTINCT ?forum
WHERE {
? forum a swrc: Forums .
{ ? forum swrc:isAbout t_1 }
UNION { ?forum swrc:isAbout t_2 } ...
UNION { ?forum swrc:isAbout t_n } . }

Связь между запросами, формальной моделью разрабатываемой системы и кодом запросов на языке SPARQL позволяет контролировать влияние:

•модификаций множества принятых в системе запросов и используемых онтологий на программный код системы;

•модификаций программного кода системы на используемые онтологии и рассматриваемые запросы предметной области ИБ.

И создает дополнительные возможности для эффективной верификации ПО на всех этапах её жизненного цикла [4,5,12].

Заключение

В результате теоретических исследований и их практической реализации была разработана онтология предметной области информационной безопасности в социальных сетях, частности разработан метод идентификации профиля пользователя сети Интернет. На основе исследования предметной области построены модели и алгоритмы, разработаны опирающиеся на онтологии архитектурные и технологические решения для создания системы пополнения и хранения, анализа и выдачи по запросу информации, характеризующей результаты деятельности *Пользователя* Информация на Web-страницах в социальных сетях.

Онтология реализована вместе с базой знаний – с использованием онтологий и языка SPARQL, где формальное описание запросов к системе, создающее гарантии их вычисления и дополнительные возможности дает эффективную верификацию кода системы на всех этапах ее жизненного цикла. Такая структура является отличительной чертой разработанной онтологии и базы знаний. Она позволяет боле эффективно обрабатывать запросы пользователей.

Онтология по информационной безопасности и база прецедентов были использованы при разработке программного комплекса, предназначенного для управления рисками при обеспечении безопасности сетей, отслеживания и предотвращения угроз. Предложенный метод идентификации пользователя сети Интернет позволяет достичь около 70% вероятность для систем мониторинга состояния ресурсов социальных сетей.

Литература

1. Васенин В. А. К созданию международной системы мониторинга и анализа информационного пространства для предотвращения и прекращения киберконфликтов // Информационные технологии, 2012, № 9, 2–10 с.
2. Мирзагитов А. А., и др. Методы разработки онтологии по информационной безопасности, основанные на прецедентном подходе // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии, 2013, Т.11, вып. 3, 37–46 с.
3. Домарев В. В. Безопасность информационных технологий. Системный подход. К.: ДиаСофт, 2004. 992 с.
4. Aktayeva Al. & etc. – Technique of identification of users of social networks over ontologies // International scientific journal «Modern IT and IT – education». vol.12, №2, 2016, 26 – 34 pp.
5. Aktayeva Al & etc. – Cognitive Ontology of information security priorities in social networks// International Scientific and Practical Conference Open Semantic Technologies for Intelligent Systems – OSTIS-2017, 365-376 pp., http://proc.ostis.net/eng/ main.html
6. Schumacher M. Security Engeneering with Patterns, LNSC 2754. Springer-Verlang Berlin Heidelberg, 2003, 87–96 pp.
7. Jutla D. N., Bodorik P., Gao D. Management of Private Data: Web Services Addressing User Privacy and Economic, Social, and Ethical Concerns, in Secure Data Management. Toronto, Canada, 2004, 100–117 pp.
8. Undercoffer J. Modeling Computer Attacks: An Ontology for Intrusion Detection. University of Maryland, Baltimore, 2004.

9. Степанов П. А. Автоматизация обработки текстов естественного языка // Вестник НГУ, Серия: Информационные технологии, 2013, Т.11, вып. 2. 109–115 с.
10. Пальчунов Д. Е., Степанов П. А. Применение теоретико-модельных методов извлечения онтологических знаний в предметной области информационной безопасности // Программная инженерия, 2013, № 11
11. Пальчунов Д. Е., Яхъяева Г. Э., Хамутская А. А. Программная система управления информационными рисками RiskPanel // Программная инженерия, 2011, № 7, 29–36 с.
12. Голомазов, Д.Д. Выделение терминов из коллекции текстов с заданным тематическим делением / Д.Д. Голомазов // Информационные технологии, 2010, № 2, 8–13 с.
13. Колин К.К. Философия информации: структура реальности и феномен информации // Метафизика, 2013, № 4, 61–84 с.
14. Урсул А.Д. Природа информации: философский очерк. – 2-е изд. – Челябинск, 2010, 231 с.
15. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity
16. http://www.ontology-of-designing.ru/article/2014_4%2814%29/7_Vorozhtsova.pdf
17. https://core.ac.uk/download/pdf/53068632.pdf (дата обращения 01.09.2017)
18. https://online.zakon.kz/m/Document/?doc_id=39754354
19. http://www.lib.tpu.ru/fulltext/v/Bulletin_TPU/2014/v324/i5/08.pdf (дата обращения 01.09.2017)

References

1. Vasenin VA To the creation of an international system for monitoring and analyzing the information space for the prevention and cessation of cyber conflicts // Information Technologies, 2012, № 9, 2-10 pp.
2. Mirzagitov AA, et al. Methods of developing an ontology for information security, based on the precedent approach, Vestn. Novosib. state. un-ta. Series: Information technology, 2013, Vol. 11, № 3, 37-46 pp.
3. Domarev V. V. The security of information technology. Systems approach. K: DiaSoft, 2004. 992 pp.
4. Aktayeva Al. & etc. – Technique of identification of users of social networks on ontologies // International scientific journal "Modern IT and IT – education". vol.12, №2, 2016, 26-34 pp.
5. Aktayeva Al & etc. – Cognitive Ontology of information security priorities in social networks // International Scientific and Practical Conference Open Semantic Technologies for Intelligent Systems – OSTIS-2017, 365-376 pp., http://proc.ostis.net/eng/ main.html
6. Schumacher M. Security Engeneering with Patterns, LNSC 2754. Springer-Verlang Berlin Heidelberg, 2003, 87-96 pp.
7. Jutla D. N., Bodorik P., Gao D. Management of Private Data: Web Services Addressing User Privacy and Economic, Social, and Ethical Concerns, in Secure Data Management. Toronto, Canada, 2004, 100-117 pp.
8. Undercoffer J. Modeling Computer Attacks: An Ontology for Intrusion Detection. University of Maryland, Baltimore, 2004
9. Stepanov PA Automation of the processing of natural language texts / / Vestnik NSU, Serie: Information Technology, 2013, Vol. 11, № 2, 109-115 pp.
10. Palchunov DE, Stepanov PA Application of model-theoretic methods for extracting ontological knowledge in the domain of information security // Program Engineering, 2013, № 11
11. Palchunov D. Ye., Yakhyayeva G. E., Hamutskaya A. A. The program system of information risk management RiskPanel // Program Engineering, 2011, №7, 29-36 pp.
12. Golomazov, D.D. Selection of terms from the collection of texts with a specified thematic division / D.D. Golomazov // Information Technologies, 2010, №2, 8-13 pp.
13. Kolin K.K. Philosophy of information: the structure of reality and the phenomenon of information // Metaphysics, 2013, №4, 61-84 pp.
14. Ursul A.D. Nature of information: a philosophical essay. – 2 nd ed. – Chelyabinsk, 2010, 231 pp.
15. ISO / IEC 27032: 2012. Information technology. Security techniques. Guidelines for cybersecurity
16. http://www.ontology-of-designing.ru/article/2014_4%2814%29/7_Vorozhtsova.pdf
17. https://core.ac.uk/download/pdf/53068632.pdf (дата обращения 01.09.2017)
18. https://online.zakon.kz/m/Document/?doc_id=39754354
19. http://www.lib.tpu.ru/fulltext/v/Bulletin_TPU/2014/v324/i5/08.pdf (дата обращения 01.09.2017)

Об авторах:

Актаева Алкена, доктор Ph.D, доцент, Кокшетауский университет им. А. Мырзахметова, Алматинский технологический университет, Казахстан, aaktaewa@list.ru

Ниязова Розамгуль, кандидат технических наук, доцент, Евразийский национальный университет им. Л.Гумилева, Казахстан, rozamgul@list.ru

Сералиева Айдын, магистр технологии ИС, преподаватель «ИСИ», Кокшетауский университет им. А. Мырзахметова, Казахстан, seralieva_a_a@mail.ru

Сарсенбаева Жаныл, магистр технологии ИС, преподаватель «ИСИ», Кокшетауский университет им. А. Мырзахметова, Казахстан, doza20102014@mail.ru

Даутов Айбек, магистр математики, преподаватель «ИСИ», Кокшетауский университет им. А. Мырзахметова, Казахстан, d.abeke@mail.ru

Кусаинова Улжан, магистр технологии ИС, преподаватель «ИСИ», Кокшетауский университет им. А. Мырзахметова, Казахстан, ulzhan-92-92@mail.ru

Жартанов Сейлхан, магистр технологии ИС, преподаватель «ИСИ», Кокшетауский университет им. А. Мырзахметова, Казахстан, s_xah@mail.ru

Note on the authors:

Aktayeva Alkena, doctor Ph.D, associate professor, A. Myrzakhmetov Kokshetau University, and Almaty Technological University, Kazakhstan, aaktaewa@list.ru

Niyazova Rosamgul, Candidate of technical sciences, associate professor, L.Gumilyov Eurasian National University, Kazakhstan, rozamgul@list.ru

Seraliyeva Aydin, MSc of IS Technology, teacher at the department ISI, A. Myrzakhmetov Kokshetau University, Kazakhstan, seralieva_a_a@mail.ru
Sarsenbayeva Zhanyl, MSc of IS technology, teacher at the department ISI, A.Myrzakhmetov Kokshetau University, Kazakhstan, doza20102014@mail.ru
Dautov Aibek, MSc of mathematics, dozent at the department ISI, A. Myrzakhmetov Kokshetau University, Kazakhstan, d.abeke @mail.ru
Kussainova Ulzhan, MSc of IS Technology, teacher at the department ISI, A. Myrzakhmetov Kokshetau University, Kazakhstan, ulzhan-92-92@mail.ru
Zhartanov Salehan, MSc of IS technology, teacher at the department ISI, A.Myrzakhmetov Kokshetau University, Kazakhstan, s_xah@mail.ru