SAS Text Miner [3], так, как в ней присутствуют все необходимые нам функции (включая возможность настроек на программном уровне).

Существенный недостаток данной системы – в том, что для выделения знаний внутри текстов она использует кластер-сегментацию [3,4], хотя имеются более точные методы (например семантико-структурная сегментация [5]).

Нами было введено понятие условно бесструктурного предложения (УБП). Именно, за УБП мы принимаем предложение, на котором невозможно обнаружить дуплексные семантические структуры [5] с ключевыми терминами в вершинах. Предполагая, что мы анализируем научный или учебный текст, приходим к естественному выводу, что информация, не являющаяся знаниями, должна быть локализована в УБП, а значит, требуется их обнаружение, а затем удаление из текста.

1. Левенчук А. Онтологическая инженерия в помощь системной инженерии / А. Левенчук. [Электронный ресурс]. Режим доступа: http://ailev.livejournal.com/975466.html
2. Data Mining. [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/Data.mining
3. SAS Institute Inc. Getting Started with SAS® Text Miner 12.1. – Cary, NC: SAS Institute Inc., 2012. 93 p.
4. Щуревич Е.В. Автоматический анализ текстов на естественном языке / Е.В. Щуревич, Е.Н. Крючкова // Знания – Онтологии – Теории (ЗОНТ-09). – Барнаул: Алтайский государственный технический университет им. И.И. Ползунова, 2009.
5. Гольдштейн С.Л., Кудрявцев А.Г. Разрешение проблемных ситуаций при поддержке систем, основанных на знаниях: учеб. пособие / С.Л. Гольдштейн, А.Г. Кудрявцев. – Екатеринбург: ИД «Пироговъ», 2006. 216 с.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Камбаров А., Тулаганов Н.

Евразийский национальный университет имени Л.Н.Гумилева

Информационная безопасность включает в себя три составляющие: требования, политику и механизмы. Требования характеризуют цели защиты. Они могут отвечать на такие вопросы как, – «Что вы хотите от вашей безопасности?». Политика характеризует значение защиты. Это значение должно отвечать на вопрос, - «Какие операции должны быть осуществлены в достижении поставленных целей?». Механизмы безопасности должны предопределять ее политику. Вопрос, «задаваемый» механизмами, - «Какие устройства, процедуры и другие пути применяются, для того, чтобы политика безопасности была выполнена?» [1].

Безопасность информации на сегодняшний день стала стратегической группой, которая состоит из комплексных понятий - «международная безопасность» и «национальная безопасность». Она способна рассматриваться в нюансе общественно-финансового развития страны как стратегия, производимая для сохранения и защиты технических и языковых данных, воздействия информационных потоков на глобальное и персональное понимание, прогноз и систематизация компьютерных и сетевых угроз и предотвращения информационных войн [2]. Представление и изучение данных явлений, формирование граней противодействия – главные проблемы, решение которых обусловлено направлением всей системы национальной безопасности.

Актуальность проблемы обеспечения информационной защиты информации обусловлена в первую очередь, тем, что в современном обществе данные стали стратегическими национальными ресурсами. За минувшие годы в Республике Казахстан выполнен ряд мер по совершенствованию концепции обеспечения информационной защищенности страны. В соответствии со Стратегией национальной безопасности Республики Казахстан была разработана и установлена Концепция информационной безопасности [3], которая предусматривает реализацию комплекса законных, организационных и научно-промышленных мероприятий, направленных на мониторинг, выявление, предупреждение и предотвращение угроз в области информационной безопасности. Технический прогресс в областях микроэлектроники, аппаратных и программных средств, а так же вычислительной техники делает процесс развития информационных технологий быстрым и оказывает большое влияние на их совершенствование.

Развитие, связанное с информатизацией всех аспектов государственной и социальной жизни, объективно говорит о том, что существование современного независимого государства неразрывно связано с обеспечением информационной безопасности всех звеньев его муниципальных структур. Анализ и исследование мирового опыта показывает, что непосредственно в последние несколько лет случилось качественное изменение в процессе управления всеми уровнями: от межгосударственных образований до личных фирм и банков. В это же время одновременно развивалась и усиливалась опасность несанкционированного доступа к информации с целью получения данных и нарушения их функционирования. Подобная угроза совершенно неоспорима, потому как разрушение и расстройство информационной инфраструктуры страны соизмерима по силе воздействия с результатами реальных военных операций. Соответствующими должны быть и мероприятия по предупреждению таких последствий. Эффективно противодействовать информационным угрозам в современных условиях способна лишь хорошо организованная государственная система обеспечения информационной безопасности, осуществляемая при абсолютном взаимодействии всех государственных органов, негосударственных структур и граждан Республики Казахстан.

К внутренним атакам информационной защиты относятся:

-направленное изменение данных, целью которого является отрицательное общественное мнение и побуждение принятия необдуманного политического решения;

-невысокая техническая укомплектованность линий связи и их охрана;

-неудовлетворительная степень качества информационных, телекоммуникационных ресурсов, снижение значимости и не надлежащее обеспечение всех прав негосударственных печатных, теле- и радиокомпаний на приобретение и распространение данных;

-компьютерные правонарушения.

Основной задачей по обеспечению информационной безопасности в Казахстане, на наш взгляд, является отсутствие единой политики взаимодействия муниципальных органов с индивидуальным сектором и средствами массовой информации. К примеру, наше государство производит сравнительно небольшое количество компьютерной и другой техники, программного обеспечения, новых средств взаимосвязи. А это повышает научно-техническую малоразвитость и информационную зависимость Казахстана от других стран. В этом случае ущемляется информационная безопасность нашей страны.[4]

Подводя итог, можно сказать, что в области информационной безопасности нашей республики существует весьма немало уязвимых мест. В особенности это затрагивает государственную политику в данном направлении, когда совершаемые властью действия часто включают в себя обратный отрицательный эффект влияния информации.

1. Bishop M. What Is Computer Security? / IEEE Security & Privacy Vol. 1, No. 1; January/February 2013, pp. 67-69.
2. Gliedman C. Managing IT Risk with Portfolio Management Thinking / CIO (Analyst Corner),www.cio.com/analyst/012502_giga.html.
3. Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Материалы круглого стола «Внешнеполитические перспективы и новые концепты международной стратегии Казахстана». Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан — Лидера Нации. — 2012. — 12 марта. // iwep.kz/index
4. Информационная безопасность. Официальный сайт Комитета национальной безопасности Республики Казахстан. knb.kz/