Таким чином, перший етап переходу до змішаного документообігу, українськими підприємствами вже пройдено. Більшість з них знаходяться на другому етапі – електронні системи використовуються для реєстрації, обліку та контролю виконання документів. Для прискорення роботи активно використовуються електронні копії документів.

На наступному етапі – справжні електронні документи поступово почнуть витісняти паперові. Перш за все, це торкнеться масових внутрішніх документів підприємства, таких як службові та доповідні записки. На цьому етапі важливо грамотно відрегулювати роботу в змішаному документообігу у внутрішніх нормативних документах – зокрема, такі питання, як використання ЕЦП у документообігу підприємства.

З одного боку, необхідно подолати боязнь співробітників перед впровадженням нових технологій, з іншого – треба усвідомлювати, що у кожної технології є свої слабкі місця. До теперішнього часу не вирішені до кінця як питання законодавчого та нормативного регулювання використання електронних документів, так і питання довготривалого зберігання електронних документів, особливо підписаних ЕЦП.

Багаторічний досвід показує, що технічні проблеми переходу до змішаного документообігу, як правило, досить успішно вирішуються. Найбільші складності викликає рішення організаційних проблем, які тісно пов'язані з «людським фактором». Для успішного просування вперед до електронного документообігу дуже важливо правильно організувати підбір кадрів, виховання та навчання персоналу організації.

СПИСОК ЛІТЕРАТУРИ

1. Казиева, Н. Подготовка оперативного электронного документа к архивному хранению [Текст] / Нина Казиева // Електронний документ: актуальні завдання та практичне впровадження (життєвий цикл електронного документа) : матеріали Міжнар. наук.-практ. конф., м. Київ, 11-12 жовтня 2012 р. / Держ. архів. служба України, Укр. НДІ архів. справи та документознавства, Центр. держ. електрон. архів України, Нац. академія держ. упр. при Президентові України. – К : [б. в.], 2012 (ДЦЗД НАФ України). – С. 50–53.

2. Храмцовская, Н. Переход от бумажного к смешанному документообороту [Текст] / Н. Храмцовская // Кадровик. Кадровое делопроизводство. – 2009. – № 2. – С. 4–9. – (Система кадровой документации).

3. Тукало, С. М. Особливості автоматизації електронного документообігу в наукових установах [Електронний ресурс] / С. М. Тукало // Інформаційні технології і засоби навчання. – 2012. – №2 (28). – Режим доступу: http://archive.nbuv.gov.ua/e-journals/ITZN/2012_2/652-1986-1-RV.pdf. – Загл. з екрану.

4. Вам нужно отказаться от бумажного документооборота? [Электронный ресурс] / Удостоверяющий центр «ПНК»: [сайт]. – Режим доступа: http://pnk74.ru/index.php/2010-07-23-07-10-34/48. – Загл. з экрана.

УДК 004.89

ТЕХНОЛОГИЯ WEB MINING В АНТИТЕРРОРИСТИЧЕСКИХ ПРОГРАММНЫХ ПРОДУКТАХ

С. С. Крамаренко, М. М. Загурська

Резюме. В данной работе рассмотрены причины освоения сети Интернет террористическими группировками, проанализированы методы спецслужб по противостоянию терроризму, рассмотрены важнейшие программы США в борьбе с терроризмом, проанализированы технологии применения разных направлений Web Mining, также определены тенденции развития программных продуктов спецслужб с использованием Web Mining.

Ключевые слова: Web Mining, Web Usage Mining, сетевые структуры, террористические группировки.

Влияние информационной революции в обществе сложно переоценить. Информационные технологии получили распространение в большинстве областей

деятельности человека. Направленные на повышение эффективности различных процессов, средства Internet стали также инструментом в преступной деятельности террористических группировок. Новые преступники, особенно террористы Аль-Каиды, используют в своей деятельности технологии Web 2.0, поэтому противостояние им все сильнее затрудняется.

Террористические атаки 11 сентября 2001 года привели к усилению деятельности по обеспечению национальной безопасности не только США, но и ряда других стран, стремящихся истребить проявления терроризма.

Новые террористы организованы в небольшие, но широко распространенные группы, которые координируют свою деятельность посредством сети Internet в онлайн режиме. Аль-Каида и другие группировки находят потенциальных участников в сети и инструктируют их, разрабатывают стратегии и координируют деятельность в режиме реального времени. Этот феномен получил в американской литературе название «NetWar» – «Сетевая война».

«Сетевая война» – форма правового конфликта, характеризующаяся использованием сети Internet и социальных сетей [1, 2]. Сетевые войны обычно связаны с негосударственными военизированными структурами, такими как террористические организации. Подобные структуры обладают потенциалом неограниченного роста и гибкостью; в их деятельности применяется комплексный подход и технологические инновации.

Предотвращение террористических атак стало приоритетным направлением в деятельности ряда ведущих стран мира, таких как США, Великобритания, Австралия и др. Для совместного решения проблем эти страны сотрудничают в рамках программы «Эшелон».

Основная идея антитеррористических программ сводится к мониторингу и предотвращению акций, и именно технология Web Mining стала ключевым инструментом в обеспечении деятельности таких программ национальной разведки. Технология позволяет в сети Интернет посредством интеллектуального анализа информации выявлять ранее неизвестные закономерности и делать прогнозы.

Цель данной статьи заключается в исследовании применения и выявлении основных направлений развития технологии Web Mining в программных продуктах, используемых во внешней разведке для предотвращения террористических атак.

Теме Web Mining и Text Mining во внешней разведке посвящены труды таких авторов как Alessandro Zanzi, Elovici Y., Shapira B., Last M., Kandell A., Zaafrany O. В их работах освещаются ключевые особенности террористической деятельности в Web, а также технологии, применяемые для мониторинга деятельности группировок. В то же время в данных исследованиях недостаточно полно рассмотрены тенденции и перспективы развития программных продуктов для внешней разведки с применением технологии Web Mining.

Главной особенностью Web Mining является возможность выявления разнородной информации и отслеживание активности в сети Internet. В антитеррористических программных продуктах применяются технологии Web Content Mining и Web Usage Mining. Они направлены на машинный анализ текста и выявление в нем скрытых взаимосвязей по семантическому, лексическому и статистическому признакам, позволяют извлекать веб-контент, анализировать его, выявлять закономерности и отклонения от общих тенденций; а также обнаруживать передвижения пользователей по страницам Internet, исследовать закономерности передвижения [2, 3].

В контексте национальной безопасности Web Mining является средством выявления потенциальных террористов с помощью автоматического анализа содержимого богатых онлайн-банков данных, подозрительных веб-сайтов, блогов, электронной

почты и чатов, новостных статей, а также других цифровых связей между людьми и организациями.

Технология Web Mining стала ключевой в антитеррористических программных продуктах по ряду причин:

- отслеживание текущей активности граждан позволяет прогнозировать будущие действия и передвижения по ресурсам Internet и выявлять потенциальных террористов;
- Web Mining позволяет анализировать тексты на всех известных языках, а также позволяет интерпретировать полученные выводы на удобный пользователю системы язык;
- Web Mining анализирует большие объемы текстовой и аналитический информации;
- анализу подвергаются самые последние сообщения, что позволяет оперативно реагировать на полученные сигналы;
- система позволяет анализировать не только закономерности, но и отклонения, что способствует наиболее точным выводам.

Без использования средств Web Mining сложность для разведки вызывает отслеживание всех террористических сайтов и предотвращение общения между участниками, поскольку сообщения от Аль-Каиды распространяются на более чем 4 500 сайтов по всему миру. Исходя из этого, спецслужбам целесообразно отслеживать активность на подобных сайтах, просматривать и анализировать сообщения. Инструменты Web Mining в результате мониторинга текстовой информации от террористов выявляют беспрецедентные тенденции, информацию об идеологии, мотивации и др. Расшифровка террористических сообщений позволяет понять не только планы, но и узнать базовые методики, навыки участников.

Для ряда стран антитеррористическая деятельность является одной из приоритетных, поэтому происходит активная разработка программных продуктов, отслеживающих террористическую активность. Главными программными продуктам внешней разведки США являются «TDS» и «Эшелон». Применение в них технологии Web Mining свидетельствует об ее эффективности и актуальности.

Система «TDS» – Terrorist Detection System (Система Обнаружения Террористов), направлена на анализ террористических активностей, для выполнения задач используются технологии Web Usage Mining и Web Content Mining. Система функционирует в двух режимах: режиме обучения и режиме обнаружения.

Система «TDS» работает по следующему принципу: на этапе обучения происходит выявление характеристик, присущих «нормальным», безопасным группам пользователей, определение их типичного поведения путем анализа действий и передаваемого контента в Web. В режиме обнаружения террористических активностей система производит мониторинг трафика и передаваемой информации в сети Internet, отслеживает перемещения пользователей, анализирует сообщения и другую текстовую информацию, сопоставляет полученные сведения с поведением и текстами, присущими безопасным группам. При несоответствии полученных данных «норме» система выдает соответствующее сообщение [3, 4].

Другая глобальная система радиоэлектронной разведки сети и анализа сигналов Совета Национальной безопасности США – «Эшелон». Это система глобального электронного шпионажа, в которой участвуют США, Великобритания, Германия, Норвегия, Япония, Корея, Новая Зеландия, Канада, Турция и другие страны – участницы НАТО.

«Эшелон» способен перехватывать телефонные переговоры, электронные письма и другие информационные потоки путем подключения к каналам связи, таким, как спутниковая связь, оптоволоконные соединения и др. [3, 5].

Технология Web Content Mining используется системой «Эшелон» для обнаружения террористических заговоров, планов наркоторговцев, политической и дипломатической разведки.

В результате анализа принципов работы программ «Эшелон», «TDS» и определения роли Web Mining в данных программных продуктах, можно выявить тенденции использования технологии Web Mining в антитеррористических системах:

- использование компьютерных алгоритмов для прогнозирования активности террористических группировок;
- сбор и анализ информации о сомнительных личностях, проявляющих необычную активность или входящих в список потенциальных террористов;
- обнаружение авторов анонимных сообщений, распоряжений и документов;
- отслеживание финансовой активности существующих группировок;
- прогнозирование будущих террористических атак;
- предотвращение распространения наиболее
- прослушивание телефонных линий [4, 5];
- отслеживание физического местонахождения террористов как из данных, передаваемых техническими средствами (IP-адрес), так и из текстов сообщений;
- использование криптографических информационных систем для дешифровки сообщений;
- усиление мер по обеспечению секретности использования данных технологий в программах разведки

Новые террористические сетевые группировки образуются каждую неделю, а новые террористы появляются каждый день. Их имена, часто написанные на других языках, трудно проверить, проверке поддаются только те, которые уже находятся в базах данных систем разведки. Именно технология Web Mining позволяет обнаружить их имена, а также их связи с другими группами или людьми. Система обнаружения террористов является примером успешной комбинации инструментов Web Mining и техник машинного обучения на пути противодействия террористическим атакам и сетевым войнам [4, с.8-12].

В ходе данной работы были исследованы принципы работы таких аналитических антитеррористических систем как «Эшелон» и «TDS», определено место технологии Web Mining в них. Выявлено, что технология Web Mining является ключевой, поскольку решает большинство задач, поставленных перед системами обнаружения террористов. В работе выявлены основные тенденции развития систем внешней разведки с применением технологи Web Mining. Можно сказать, что использование террористами сети Internet не только не улучшило деятельность, но сделало их более уязвимыми из-за использования спецслужбами интеллектуальных технологий, позволяющих контролировать деятельность сетевых группировок и предотвращать террористические акции.

СПИСОК ЛИТЕРАТУРЫ

1. Elovici Y., Shapira B. Using data mining techniques for detecting terror-related activities on the web [Text] / Elovici Y. // Journal of Information Warfare. – 2010. – pp.17–28.
2. Berry M., Browne M.-mail surveillance using nonnegative matrix factorization [Text] / Berry M. // Computational & Mathematical Organization Theory. – 2011. – pp. 249–264.
3. Zanasi A. Virtual weapons for real wars: text mining for national security [Text] / Zanasi A //

Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems. Advances in Soft Computing. – 2010. – pp.53–60.

4. Alguliev R., Classification of textual e-mail spam using data mining techniques [Text] / Alguliev R. // Applied Computational Intelligence and Soft Computing. – 2011. – Article 416308, 8 p.

5. European Parliament. European Parliament report on ECHELON [Electronic resource].– Mode of access: http://www.fas.org/irp/program/process/ rapport_echelon_en.pdf. – 2011.

УДК 004.418

ИСПОЛЬЗОВАНИЕ РЕИНЖИНИРИНГА БИЗНЕС-ПРОЦЕССОВ В КРУПНОЙ ОРГАНИЗАЦИИ

И. В. Куракина, И. К. Сапицкая

Резюме. В статье охарактеризованы возможности бизнес-аналитики как составной части процесса реинжиниринга, определены ключевые бизнес-процессы ООО «Донбасс Арена», приведено программное обеспечение ИС для выполнения бизнес-процессов, разработаны рекомендации по совершенствованию бизнес-процессов.

Ключевые слова: реинжиниринг, стратегическая карта, бизнес-процесс, бизнес-аналитика, программное обеспечение.

Современным предприятиям в условиях постоянных внешних перемен и возрастающей неопределенности, требуется вносить изменения в структуру и принципы работы, внедрять информационные системы (ИС) и технологии (ИТ), т.к. данный фактор является ключевым при обеспечении стабильной работы субъекта хозяйствования. Этим обуславливается необходимость использования реинжиниринга как способа обеспечения конкурентоспособности организации путем реализации процессного подхода (определение текущих бизнес-процессов субъекта и замена их на более эффективные) и внедрения информационных систем управления [1]. Инструменты бизнес-аналитики рассматриваются как составная часть процесса реинжиниринга. Они позволяют с помощью специализированного программного обеспечения (ПО) выполнять анализ больших объемов данных и формировать отчеты, выводы и прогнозы, тем самым способствовать повышению эффективности работы организации.

Теорию и практику бизнес-анализа рассматривали такие ученые, как Паклин Н., Орешков В. [3], Барсегян А. [4], Кацко И., Косоруков О. [5]. Основоположниками реинжининга являются Хаммер М. и Чампи Дж., которые в своей работе определяют реинжиниринг как "фундаментальное переосмысление и радикальное перепроектирование бизнес-процессов компаний для достижения коренных улучшений в основных показателях их деятельности: стоимость, качество, услуги и темпы". [2]

Объект исследования: ООО «Донбасс Арена»

«Донбасс Арена» — первый в Украине и Восточной Европе стадион категории «Элит», спроектированный и построенный в соответствии со стандартами УЕФА.

Общее число сотрудников ООО «Донбасс Арена» по полной занятости – 436 чел., по частичной занятости (только в матчевые дни) – около 2000 чел.

Цель статьи –исследование основных бизнес-процессов организации с использованием инструментов бизнес-аналитики.

Проведенный сбор и анализ информации о деятельности ООО «Донбасс Арена» позволил сформировать стратегическую карту организации, представленную на рис.1.

Возможности бизнес-аналитики по основной деятельности организации представлены на рис.2. Конкретные пакеты прикладных программ (ПП) по этому направлению предлагают различный набор возможностей. Наиболее функциональными