Одним из наиболее сложных ОРМ при реализации в киберпространстве является оперативный эксперимент. Международной практике известны примеры осуществления оперативного эксперимента, которые связаны с созданием в сетевом пространстве негласно контролируемых объектов, представляющих интерес для преступников.

Ограниченное применение возможно и для контроля почтовых отправлений. Такие действия в конкретных ситуациях позволяют не только получать важные фактические данные, но и создавать препятствия обмену информацией между изучаемыми лицами.

Рост количества торговых операций, которые реализуются через сеть Интернет, заставляет расширять практику использования и ОРМ «проверочная закупка» и «контролируемая поставка» в целях выявления преступлений в сфере торговли и в сфере распространения запрещенных к обороту объектов. К примеру, в практике известно успешное применение проверочной закупки в ходе реализации контролируемых поставок наркотических средств.

Решение задач по поиску, отбору и систематизации оперативной информации предполагает применение информационных систем, позволяющих существенно расширить круг информации, необходимой для аналитической работы, и распространяется в нескольких направлениях.

Важной стороной информационного обеспечения деятельности оперативного сотрудника является организация содействия в анализировании имеющейся информации для формирования решений. Экспертные системы, применяющиеся в оперативной работе, занимают особое место среди информационного обеспечения.

Существует несколько видов экспертных систем раскрытия и расследования преступлений: выявления скрытых преступлений, прогнозирования преступлений, поиска и установления личности преступника.

В деятельности подразделений ОВД используется специализированное программное обеспечение, которое ориентировано на непосредственное применение при осуществлении ОРМ в направлении борьбы с информационной преступностью.

Следовательно, в информационном пространстве (при учете его социальной составляющей) на сегодняшний день может осуществляться практически любое из предусмотренных законом оперативно-розыскное мероприятие. В то же время при подготовке и проведении таких мероприятий оперативный сотрудник обязан учитывать специфику сетевого информационного пространства и сформировавшейся в нем криминогенной среды.

УДК 004.056

М.К. Новиков, Т.Ф. Старовойтова

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ЕДИНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТАМОЖЕННЫХ ОРГАНОВ РЕСПУБЛИКИ БЕЛАРУСЬ

В середине 2016 г. Государственным таможенным комитетом Республики Беларусь была введена единая автоматизированная информационная система таможенных органов (ЕАИС ТО) Республики Беларусь. Данная система включает в себя 40 информационных систем. Основные из них:

автоматизированная подсистема «Транзит Таможенного союза»;

Национальная автоматизированная система электронного декларирования;

автоматизированная информационная система автоматизации операций таможенного оформления и контроля, ведения базы данных таможенной информации на уровне пунктов таможенного оформления и таможни;

автоматизированная система управления рисками;

автоматизированная подсистема «Модуль автоматической рассылки сообщений».

Система защиты информации (СЗИ) ЕАИС ТО Республики Беларусь предназначена для обеспечения конфиденциальности, целостности и доступности информации ограниченного распространения и другой критичной информации, обрабатывающейся в ЕАИС ТО, а также для обеспечения защиты информации при взаимодействии ЕАИС ТО с внешними информационными системами.

СЗИ ЕАИС ТО включает в себя следующие подсистемы: управления пользователями и разграничения доступа, аудита событий, защиты каналов связи, криптографической защиты информации, антивирусной защиты, резервного копирования и восстановления работоспособности.

В конце 2016 г. система защиты информации ЕАИС ТО Республики Беларусь была аттестована. Это означает, что система защиты информации ЕАИС ТО Республики Беларусь класса Б2 (по СТБ 34.101.30-2007) соответствует всем требованиям законодательства Республики Беларусь в области защиты информации, а именно: Закону Республики Беларусь «Об информации, информатизации и защите информации», приказу Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации».

Но, несмотря на все принимаемые меры по защите информации, найти в огромном массиве данных конфиденциальную информацию и выявить факт записи ее на внешнее запоминающее устройство или передачи по сети, электронной почте очень сложно. DLP-система (систе-

ма предотвращения утечки информации) поможет автоматизировать этот процесс.

DLP-система создает защищенный цифровой контур вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию. Контролируемым является информационный поток, состоящий из документов, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываются на принтере, отправляются по сети и по почте и т. д.

Все DLP-системы по способности блокирования конфиденциальной информации можно разделить на активные и пассивные. Первые умеют блокировать передаваемую информацию, вторые, соответственно, такой способностью не обладают. Первые системы гораздо лучше борются со случайными утечками данных, но при этом способны допустить нечаянную остановку передачи важного документа в организации, вторые же безопасны, но подходят только для борьбы с систематическими утечками.

Как правило, по сетевой архитектуре DLP-системы используют совместно шлюзовые и хостовые компоненты (серверная часть и агенты, работающие на рабочих станциях сотрудников). Агенты только передают всю информацию серверной части. Поступившая от агентов информация анализируется ресурсами сервера.

Таким образом, внедрение DLP-системы в таможенные органы Республики Беларусь позволит отследить и проанализировать основные каналы передачи конфиденциальной информации и выявить факты нарушения информационной безопасности.

УДК 004.832+351.759.6

Ю.Б. Савва

МЕТОДИКА ВЫЯВЛЕНИЯ СРЕДСТВАМИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ УЧАСТНИКАМИ ВИРТУАЛЬНЫХ СОЦИАЛЬНЫХ СЕТЕЙ

В виртуальных социальных сетях (ВСС), завоевавших пользователей интернета в последнее десятилетие, нашли свое отражение как положительные, так и негативные черты современного общества. К числу последних относятся: пропаганда терроризма и экстремизма, привлечение к употреблению наркотических и психотропных веществ, вовлечение в секты, понуждение к суициду и другие противоправные действия, направленные на деструктивное воздействие на участников ВСС. В связи с этим перед органами правопорядка встала задача выявления и пресечения противоправного поведения и деструктивной деятельно-

сти в ВСС, эффективно решить которую возможно только посредством использования средств современных информационных технологий по соответствующим методикам.

Для решения данной задачи нами разработана автоматизированная система мониторинга и анализа сообщений участников ВСС, структура которой приведена на рис. 1. Методика выявления противоправных действий участников ВСС средствами информационных технологий основывается на лингвистическом анализе текстов сообщений, как размещаемых ими на «стенах», так и тех сообщений, которыми они обмениваются между собой в личной переписке.

При сканировании ВСС с использованием специально разработанной программы «Краулер» модель ВСС представляется в виде графа $G = (V, E)$, где V – это множество узлов, представляющих участников ВСС, а E – множество дуг, обозначающих отношения между этими участниками.

Сканирование графа ВСС начинается с одного или нескольких узлов (система позволяет вести сканирование параллельно как в одной ВСС, так и в нескольких сетях одновременно). При посещении одного узла осуществляется сбор отправленных с него текстовых сообщений на «стену». Эти сообщения собираются в пакеты, которые подвергаются компьютерному лингвистическому анализу. При этом формируется список соседей этого узла с целью выявления его контактов, что позволяет получать тексты сообщений между участниками ВСС при их прямом общении. Эти сообщения также собираются в пакеты для последующего компьютерного лингвистического анализа.

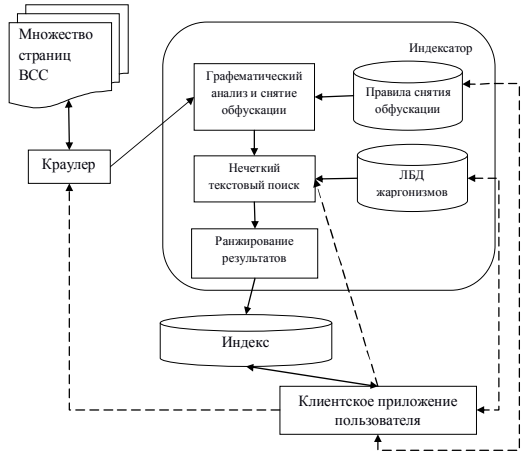

Рис. 1. Структура автоматизированной системы мониторинга и анализа сообщений участников виртуальных социальных сетей