Несмотря на тот факт, что удаление времени с графика позволяет более внимательно изучить различные свойства шаблонов комментариев, оно также маскирует изменение шаблонов с течением времени. Для визуализации изменений предпочтений пользователя с течением времени используется другой тип графика – график истории.

Карма (общая длина и количество комментариев) для каждого сабреддита представлена отдельным слоем. Изменение соотношения толщины слоев наиболее наглядно показывает изменения предпочтений пользователей с течением времени.

Следующий график визуализирует количество комментариев в день. Этот график позволяет выявлять события, вызвавшие наибольшую дискуссию в сообществе.

Наблюдение за изменением графика по мере загрузки старых комментариев (Reddit отправляет максимум 100 комментариев за раз) или медленного увеличения минимальной длины комментария путем удерживания кнопки приводит к информативной анимации. Рисование графика занимает всего несколько миллисекунд, поэтому повторное рисование графика с разными параметрами создает видимость движения.

Еще одним направлением аналитики профилей пользователей является выявление связанных логинов, используемых одним пользователем. Аналитика комментариев напрямую не раскрывается Reddit, поэтому отслеживать разных комментаторов на Reddit непросто. Определенные результаты могут быть достигнуты с использованием плагинов Reddit Enhancement Suite.

В заключении отметим, что формирование специальных компетенций в сфере анализа контента социальных сетей в процессе подготовки кадров для правоохранительных органов способно стать перспективным направлением совершенствования служебной деятельности.

УДК 343.985

Н.В. Якимович

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ-МОНИТОРИНГА ПРИ ВЫЯВЛЕНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В современном мире информационные технологии развиваются постоянно и динамично, выходя на новый качественный уровень, в связи с чем появляются новые и модернизируются уже известные способы и средства обработки информации. Для пользователей сети Интернет воз-

растает угроза стать жертвами усовершенствованных противоправных деяний, в процессе совершения которых возможности сети Интернет используются и как средство, и как орудие, а также могут являться местом их совершения. Внедрение информационных технологий во все сферы жизнедеятельности общества является объективной реальностью, а использование возможностей информационных технологий, в том числе сети Интернет, в противоправных целях – одним из серьезнейших вызовов, стоящих перед правоохранительными органами. В связи с тем, что количество пользователей сети Интернет с каждым годом возрастает, а социальные сети и различные мессенджеры прочно вошли в повседневную жизнь человека, в сети Интернет может быть обнаружена информация, представляющая интерес для правоохранительных органов.

В Республике Беларусь в целях выявления преступлений, совершенных с использованием информационных технологий, широко применяется интернет-разведка, в структуре правоохранительных органов созданы и успешно функционируют специальные подразделения «аналитической разведки». Ввиду того, что киберпространство может являться криминогенной средой, проведение мероприятий по поиску значимой информации можно называть оперативным поиском. Полагаем, что мониторинг сети Интернет или интернет-мониторинг является одним из перспективных направлений оперативного поиска.

Мониторинг в широком смысле означает систематическое наблюдение за состоянием объектов, явлений, процессов в целях их оценки, контроля или прогноза. Под интернет-мониторингом понимается комплекс мероприятий по сбору, обработке и анализу информации о преступных деяниях в сети Интернет. Данное определение позволяет выделить три этапа в процессе поиска криминалистически значимой информации: обнаружение сведений, их фиксация и анализ. Бывают случаи, когда анализ предшествует фиксации, например, если есть уверенность в том, что обнаруженная информация не будет удалена или повреждена в процессе ее анализа, тогда фиксируется только та информация, которая представляет интерес.

Объектом интернет-мониторинга являются все информационные ресурсы сети Интернет. Можно выделить следующие основные источники информации: поисковые системы, официальные сайты государственных органов и различных общественных и политических организаций, сайты-энциклопедии и сайты-справочники, социальные сети и блоги, специализированные сайты и форумы преступных сообществ, сайты знакомств, сообщества и чаты, в том числе в различных мессенджерах.

Чтобы найти необходимую информацию в поисковой системе нужно создать запрос, который может включать в себя: фамилии, псевдо-

нимы интересующих лиц, названия организаций (при этом необходимо предусмотреть вариации в написании этих слов), ключевые слова, которыми пользуются в преступном сообществе, различные изображения (например, по фотографии лица через общедоступные ресурсы можно найти его учетные записи в социальных сетях). Социальные сети и мессенджеры, как известно, позволяют обмениваться не только текстовыми сообщениями, но и звуковыми, а также фотографиями и видеозаписями. Такая информация накапливается и хранится долгое время, поэтому сотрудники правоохранительных органов имеют возможность ее анализировать и использовать в целях выявления преступлений. Специализированные форумы помогают сотрудникам правоохранительных органов ознакомиться с открытой перепиской участников сообществ, ориентироваться в новых способах и методах совершения преступлений, на основании чего возможно предупреждение данных преступлений.

Некоторые ресурсы могут быть недоступны для просмотра, так как доступ к ним можно получить при наличии прямой ссылки. Эти ресурсы находятся в «Глубоком интернете» или Deepweb – сегменте сети Интернет, страницы и порталы которого не определяются поисковыми системами. Частью Deepweb является Darknet («Теневой интернет») – скрытый из общего доступа сегмент сети Интернет, доступ к которому возможен только при наличии специального программного обеспечения. С учетом изложенного можно говорить об интернет-мониторинге в зависимости от доступности его проведения: в открытом пространстве и в Deepweb. При этом интернет-мониторинг в Darknet будет являться подвидом интернет-мониторинга в Deepweb.

С целью повышения эффективности интернет-мониторинга могут применяться средства OSINT – технологии, позволяющие собирать и анализировать информацию на всем пространстве сети Интернет. Применяя различные фильтры можно получить необходимую информацию, в том числе о совершенных преступлениях с использованием информационных технологий. OSINT представляет собой поисковую программу с открытым исходным кодом. Таких программ в настоящее время существует огромное множество. Чтобы найти информацию о лицах и компаниях можно использовать приложение Maltego, так как оно осуществляет поиск в записях социальных сетей, DNS и Whois, анализирует информацию и создает ее графическое отображение (диаграммы, графики). Платформа Cobwebs работает по принципам искусственного интеллекта, не требует участия сотрудника, обрабатывает значительные объемы данных и выявляет киберугрозы в режиме реального времени, позволяет работать как в открытом сегменте сети Интернет, так и в Darknet. Возможности данной платформы имеют значение при выявле-

нии мошенничеств, совершенных с использованием информационных технологий. Для поиска и анализа значимой информации в Deepweb используются возможности программы Dark Owl Vision с использованием множества фильтров и ключевых слов. Также среди средств OSINT можно выделить сервис PhoneInfoga, с помощью которого можно анализировать абонентские номера и их группы, а также собирать статистическую информацию. Преимуществами средств OSINT является доступность и объем источников информации, простота ознакомления и дальнейшего использования полученной информации, а также отсутствие затрат на получение значимой информации.

Таким образом, действенным инструментом при выявлении преступлений, совершенных с использованием информационных технологий, является интернет-мониторинг, который представляет собой комплекс мероприятий по сбору, обработке и анализу информации о преступных деяниях в сети Интернет. Интернет-мониторинг может проводиться в открытых ресурсах сети Интернет и в Deepweb. Подвидом интернет-мониторинга в Deepweb является интернет-мониторинг в Darknet. С целью повышения эффективности интернет-мониторинга необходимо использовать технологии, позволяющие собирать и анализировать информацию на всем пространстве сети Интернет.