да программ-вымогателей может выступать как устройство в целом, так и отдельное программное обеспечение, например, веб-браузер.

Программа-шифровальщик – тип программ-вымогателей, которая модифицирует пользовательские данные, путем использования различных алгоритмов и техник шифрования. После кодирования информации вредоносное программное обеспечение инициирует подключение к удаленному рабочему столу и пересылает информацию об идентификаторе зашифрованного устройства, для последующего восстановления модифицированной компьютерной информации.

Указанные типы вредоносного программного обеспечения могут распространяться по следующим векторам: перенаправление трафика; вложения электронной почты; ботнеты.

Перенаправление трафика. Данный вектор является наиболее распространенным способом побудить пользователя перейти по ссылке на вредоносную рекламу или перенаправить веб-трафик пользователя на другой интернет-ресурс, на котором размещено вредоносное программное обеспечение в виде набора различных эксплоитов. Чаще всего это встречается на интернет-ресурсах с порнографическим содержимым, пользователя с указанных сайтов перенаправляют на портал, предлагающий бесплатные игры или обновления для пользовательских приложений. При загрузке указанного контента вредоносное программное обеспечение использует уязвимости устройства пользователя, что приводит к блокировке либо шифрованию пользовательской информации.

Вложения электронной почты. Электронные письма с вложениями или ссылками побуждают пользователей открывать и получать доступ к веб-ресурсам, содержащим программу-вымогатель. На первый взгляд жертве кажется, что электронное письмо отправлено подлинным корреспондентом, так как вложения могут содержать электронный счет за потребляемую электроэнергию, налоговую или юридическую документацию, или даже содержат информацию от лиц, ищущих работу с просьбой открыть вложение или перейти по ссылке, чтобы актуализировать информацию о пользователе.

Ботнеты. В последние годы особую популярность приобрел данный вид вредоносного программного обеспечения, так злоумышленники стремятся взять под контроль миллионы устройств по всему миру и таким образом управлять огромной сетью устройств, которые можно использовать для осуществления атак типа «отказ в обслуживании» (DDoS), тем самым блокируют доступ к информационным системам. Распространяется данный вид вредоносного программного обеспечения при помощи загрузчиков путем компрометации пользовательских компьютерных систем и сетей, после чего загружается вредоносное программное обеспечение в качестве второго шага. Загрузчики пред-

ставляют собой легальное программное обеспечение, такое как бесплатные игры и инструменты, которые не содержат вредоносного кода, а загружает его позже.

В данной ситуации для получения необходимой информации о распространителе вредоносного программного обеспечения важно проанализировать данные, хранящиеся в журналах обращений к сетевому оборудованию, либо оперативного взаимодействия с организациями, представляющими услуги в качестве хостинг- и интернет-провайдера.

Данный перечень угроз не является исчерпывающим. Преступность не ограничивается существующими решениями, а постоянно совершенствует инструменты для проведения кибератак с целью компрометации компьютерных систем и сетей.

Подводя итог изложенному, важно особо отметить необходимость в разработке научно-методических и научно-практических рекомендаций для сотрудников правоохранительных органов по грамотному и эффективному извлечению следов активности программ-вымогателей, и сохранению данных следов для последующего изучения и использования в суде в качестве доказательства.

УДК 343.985.8

С.В. Пилюшин

О НЕКОТОРЫХ ПРОБЛЕМАХ МЕТОДОЛОГИИ КАТЕГОРИАЛЬНО ПОНЯТИЙНОГО АППАРАТА АНАЛИТИКИ В СИСТЕМЕ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Изменения, происшедшие за последние годы в социальной, экономической жизни общества, законодательстве, возникновение новых форм проявления преступности, в том числе основывающихся на использовании информационных технологий, оказывают существенное влияние на процессы принятия управленческих решений, постоянное усложнение которых объективно требует максимального включения в оперативно-розыскную практику современного аналитического инструментария, формирования и развития аналитических компетенций.

Очевидно, что в сложившихся условиях борьбы с преступностью назрела необходимость глубокого понимания и осмысления сущностного содержания аналитики как особого вида деятельности, обоснования используемой в процессе выявления и раскрытия преступлений ее определенной модели конкретными оперативными подразделениями.

Применительно к деятельности оперативных подразделений органов внутренних дел категория «аналитика» характеризуется следующими понятиями и терминами: «аналитическая работа»; «аналитическая деятельность»; «информационно-аналитическая деятельность»; «инициативная аналитика»; «оперативно-розыскная аналитика»; «аналитическая разведка»; «аналитический поиск»; «оперативно-розыскной мониторинг»; «управленческое решение»; «аналитическое решение» и др.

Наиболее распространенными являются представления об аналитике как об элементе получения знания, как творческой деятельности, как виде специфической деятельности. В основном в научных публикациях аналитика отождествляется с категориями «информационно-аналитическая деятельность» или «аналитическая работа», которыми принято определять разновидность деятельности сотрудников оперативных подразделений, направленной на получение нового знания об объектах, представляющих оперативный интерес, путем анализа разобщенных сведений.

Несмотря на то что основные концептуальные положения аналитической работы (информационно-аналитической деятельности) в сфере оперативно-розыскной деятельности принято считать устоявшимися, проведенный анализ содержания научных трудов, показал разобщенность трактовок отдельных категорий и понятийных характеристик, используемых при описании аналитических процессов, связанных с получением, анализом, накоплением оперативно-розыскной информации, принятием на ее основе управленческих решений.

Так, например, деятельность сотрудников оперативных подразделений, связанная с поиском и предварительной аналитической обработкой добытой информации, в научной литературе определяется терминами «аналитический поиск» либо «аналитическая разведка». Вместе с тем в одних случаях «разведка» отождествляется с «поиском», в других – рассматривается в качестве его разновидности. Однако веских аргументов, на основании которых представляется возможным сделать однозначные выводы о синонимичности данных терминов либо усмотреть в их содержании наличие существенных различий, в большинстве случаев не приводится.

В том числе, результаты научных исследований практики применения сотрудниками оперативных подразделений методик сбора и аналитической обработки информации, с использованием возможностей информационных технологий, показывают, что «аналитическая разведка», в свою очередь, дублируется целым рядом сходных по содержанию терминов. Фактически речь идет о «компьютерной разведке», «компьютерном поиске», «компьютерном мониторинге», «киберразведке», а также «аналитической разведке средствами Интернет», «оперативно-розыскном мониторинге информационных ресурсах глобальных компьютерных сетей», «информационно-аналитической работе в Интернете» и др.

Безусловно, введенные в научный оборот новые понятия и термины расширяют теоретические представления о рассматриваемом виде деятельности, отражают уровень знания об объектах и явлениях объективной реальности, выступают средством их дальнейшего углубленного познания. Вместе с тем их избыточность, собственно говоря, интерпретация однотипных по содержанию действий, не только не способствует формализации знаний, но и может ввести в заблуждение относительно верного восприятия содержания тех или иных процессов.

Таким образом, категория «аналитика» в деятельности оперативных подразделений характеризуется достаточно широким перечнем понятий и терминов, преимущественно определяющих ее как специфический вид проводимой работы, сопряженной с процессами поиска и обработки добытых сведений, извлечением новых знаний, принятием на их основе оптимальных управленческих решений.

В разрезе существующих в настоящее время научных представлений о сущности и содержании аналитических процессов, полагаем, что ряд разработанных научных понятий и терминов требует более тщательной научной разработки, апробирования, что позволит их отличать друг от друга, исключить дублирование, разобщенность трактовок.

УДК 343.985

Ю.В. Полковниченко

О СЛЕДОВОЙ КАРТИНЕ В ХОДЕ ОСМОТРА КОМПЬЮТЕРНОЙ ТЕХНИКИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ ОБ УБИЙСТВАХ

Одним из первых табу во всех источниках моральных норм человека является запрет на убийство человека. Во всех странах мира убийство законодательно признано наиболее тяжким преступлением, в связи с чем охрана права человека на жизнь является одной из важнейших норм уголовного законодательства и одной из важнейших задач правоохранительного блока любого государства. Процесс сбора доказательств по рассматриваемой категории преступлений, по своей сути, является классическим и представляет собой совокупность материальных следов, зафиксированных, в первую очередь, в ходе осмотра места происшествия, а в дальнейшем – при проведении проверок показаний на месте и иных процессуальных действий. Идеальными же следами считаются показания участников процесса, так называемые отпечатки событий в сознании памяти преступника, потерпевшего, свидетелей и других людей.