Преобладающим мотивом осуществления вредоносных атак с использованием ВПО является корысть, получение финансовой выгоды.

Объектами посягательства с использованием ВПО выступают персональные компьютеры, серверное и сетевое оборудование, интернет-ресурсы, мобильные устройства, IT-устройства. Конечной целью атак с использованием ВПО на информационные системы в большинстве случаев выступает информация о персональных данных пользователей, авторизационные данные, информация, составляющая коммерческую тайну, клиентские базы данных организаций, электронная корреспонденция, а также данные платежных средств пользователей.

При этом разработчики ВПО постоянно изыскивают новые возможности для обхода существующих систем защиты программных продуктов. Для достижения поставленных целей они, как правило, используют редкие языки программирования, сигнатуры которых ввиду их незначительной распространенности пока еще не добавлены в базы существующих антивирусных программных решений, в связи с чем последние не могут обнаружить ВПО на устройстве. Некоторые злоумышленники дополняют свои инструменты функциями, позволяющими в режиме реального времени очищать следы вредоносной активности программы на устройстве жертвы.

Структурное строение способов совершения преступлений с использованием ВПО характеризуется тем, что они, как правило, относятся к разновидности полноструктурных, включающих в себя подготовку, совершение и маскировку (сокрытие) преступлений. Так, на этапе подготовки ВПО используется для собирания установочной информации о жертве, получения общих реквизитов платежных средств (номер банковской платежной карточки с маской, срок действия и имя владельца). На стадии совершения ВПО используется для получения авторизационных данных непосредственно в платежных системах либо перехвата сеансовых ключей, необходимых для удостоверения финансовых операций. Стадия маскировки (сокрытия) данных криминальных деяний характеризуется использованием средств анонимизации: VPN-сервисов, TOP-браузеров, удаленных анонимных серверов, бот-сетей и др.

Основным способом распространения ВПО является компрометация легитимных веб-ресурсов. Например, злоумышленники внедряют шпионское программное обеспечение в инструментальные средства, предназначенные для веб-разработки и устанавливаемые всеми разработчиками данной сферы. В дальнейшем это позволяет злоумышленникам удаленно собирать информацию об устройствах разработчиков и более предметно осуществлять целевые атаки. Среди способов встречаются случаи распространения ВПО посредством размещения его на крупных онлайн-площадках, предназначенных для инсталляции программного обеспечения на мобильные и десктопные устройства, например AppStore и PlayMarket.

Таким образом, ландшафт угроз в сфере использования ВПО достаточно широк. Функционал ВПО постоянно совершенствуется, а реагировать на существующие угрозы становится все сложнее. Специфика оборота ВПО, многообразие способов его создания, распространения и использования, недостаточная разработанность теоретической модели такого вида противоправных деяний создают существенные предпосылки для роста киберпреступлений в целом, в связи с чем имеется необходимость в разработке научно обоснованных практических рекомендаций по противодействию оборота ВПО.

УДК 343.985.8

С.В. Пилюшин

ОСОБЕННОСТИ АНАЛИЗА ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Деятельность оперативных подразделений органов внутренних дел по сбору, анализу, систематизации, хранению и последующему использованию оперативно-розыскной информации о лицах и фактах, представляющих оперативный интерес, рассматривается как информационное обеспечение, заключающееся в обеспечении оперативных подразделений оперативно-розыскной информацией и прикладным инструментарием для ее аналитической обработки.

Выступая в качестве одного из элементов информационного обеспечения, в теории оперативно-розыскной деятельности (ОРД) под оперативно-розыскной информацией понимают разновидность социальной информации, специфичной по цели получения, методам получения и режиму использования, обеспечивающего конспирацию и зашифровку ее источников. В ней могут находить свое отражение отношения между людьми, формирование преступного поведения, возникновение ситуаций, облегчающих или затрудняющих получение этой информации. Многообразие получаемой оперативно-розыскной информации коррелирует с многообразием обстоятельств, детерминирующих преступность и индивидуальное преступное поведение.

Оперативно-розыскная информация может быть получена из различных источников: обращения граждан; сообщения в средствах массовой информации; результаты проверок, проводимых контрольно-ревизионными органами, и др. Однако в большинстве случаев получению оперативно-розыскной информации предшествуют целенаправленные действия оперативных сотрудников по обнаружению, сбору, обработке, анализу и оценке фактических данных, содержащих сведения о замышляемых, подготавливаемых и совершенных преступлениях; лицах, представляющих оперативный интерес для органов внутренних дел; обстоятельствах, имеющих непосредственное или потенциальное значение для планирования или осуществления оперативно-розыскных мероприятий (ОРМ), проведения оперативно-аналитической работы.

По своему целевому назначению, исходя из полноты содержания, оперативно-розыскная информация может быть реализована при решении конкретной оперативно-розыскной задачи. Однако в большинстве случаев в ходе осуществления ОРД, как правило, требуется проведение ряда дополнительных операций по многим направлениям (переработка полученной информации, ее систематизация, хранение, поиск, выдача и т. д.), имеющим значение не только в настоящее время, но и в будущем. С этой целью и создаются различные по содержанию учеты.

Такой подход позволяет повысить качество процессов идентификации, рассматриваемой в теории ОРД как деятельность, осуществляемую в ходе выявления, раскрытия преступлений, заключающуюся в сопоставлении на основе характерных устойчивых признаков идентифицируемых объектов, отображаемых в виде следов, добытых в ходе проведения поисковых мероприятий, с данными, содержащимися в информационных массивах. В такой интерпретации оперативно-розыскная идентификация выступает в роли связующего звена в процессах по сбору оперативно-розыскной информации и ее накоплении, обнаружении связей между людьми и событиями преступлений.

Развитие информационных технологий позволило пересмотреть устоявшиеся подходы по накоплению и анализу оперативно-розыскной информации. В 70–80-х гг. прошлого века стали разрабатываться концептуальные положения использования ЭВМ в целях совершенствования информационного обеспечения ОРД. Предусматривалась автоматизация трудоемких процессов сбора, обработки и поиска оперативно-розыскной информации, объединение разрозненных по территориальным оперативным подразделениям массивов оперативных данных и др.

Это способствовало внедрению в практическую деятельность оперативных подразделений органов внутренних дел автоматизированных информационных систем (АИС) с использованием баз данных с разграничением доступа различных категорий (уровней) пользователей. В итоге существенно повысилось качество информационных процессов, возросла эффективность осуществления ОРД в целом.

В последнее десятилетие с предоставлением доступа к АИС, ведение которых осуществляется государственными органами и учреждениями, информативные возможности информационного обеспечения оперативных подразделений органов внутренних дел существенно расширились, в том числе стало возможным получать и более детально анализировать данные, предоставляемые операторами сотовой подвижной электросвязи. С введением в действие республиканской системы мониторинга общественной безопасности появился доступ к данным фотовидеофиксации.

Используемый в настоящее время в деятельности оперативных подразделений современный информационно-аналитический инструментарий позволяет оперативно собирать и обрабатывать разрозненные массивы данных, извлекать из них оперативно значимую информацию, принимать оптимальные решения.

Вместе с тем развитие информационных технологий, внедрение новейших технических средств в процессы оборота информации во все сферы жизнедеятельности современного общества привело к необходимости ее сбора и аналитической обработки в масштабах и объемах несравнимо больших, чем в недавнем прошлом. В то же время существует вероятность того, что оперативные подразделения органов внутренних дел могут столкнуться с реальной проблемой существенного отставания в овладении существующими современными технологиями. Данное обстоятельство требует уже сегодня разработки мер, предусматривающих подготовку специалистов соответствующего уровня, обладающих навыками использования новейших технологий в аналитической деятельности в процессе работы с большими объемами информации, в том числе с цифровыми данными.

По нашему мнению, решение этой проблемы лежит в плоскости не только разработки и внедрения соответствующих программно-технических средств сбора информации, ее хранения и обработки, но и в развитии методического сопровождения данных процессов. Методическое сопровождение информационного обеспечения ОРД является одной из составляющих эффективной деятельности оперативных подразделений. Оно позволяет оптимизировать процессы выявления и расследования противоправных деяний, имеющих свое отражение в различных процессах противоправной деятельности.

УДК 343

А.А. Помелов

ИСПОЛЬЗОВАНИЕ В СУДОПРОИЗВОДСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Одним из возможных и, наверное, самых действенных решений для изобличения виновных лиц, опровержения выдвинутых подозреваемыми версий, оправдывающих преступное поведение последних, а также для эффективной защиты гражданина и государства от преступных посягательств является использование результатов оперативно-розыскной деятельности (ОРД) в качестве доказательств в ходе уголовного судопроизводства.

В ряде случаев признание некоторых результатов оперативно-розыскных мероприятий иными документами предусмотрено ст. 84 УПК РФ. Данный вид доказательства весьма специфичен, так как позволяет переносить непроцессуальную информацию в уголовный процесс с сохранением своего «внешнего вида». Как отмечает А.Г. Маркелов, иные документы – это широкоуниверсальное средство сообщения системы доказательств с системами иных сфер правоохранительной деятельности, которые могут убедить приведенными доводами в истинности того или иного сообщения.

Как видно из анализа изученных приговоров и архивных уголовных дел по экономическим преступлениям, в основной своей массе признание доказательствами результатов оперативно-розыскной деятельности строится на вовлечении их в уголовный процесс с помощью показаний свидетеля, вещественных доказательств и иных документов, так как иных возможностей привлечения и использования сил и средств ОРД в выявлении обстоятельств совершенного преступления нет. При этом привлечение результатов ОРД в качестве доказательств на основании ст. 84 УПК РФ, в частности по п. 3, который говорит о приобщении документов к материалам уголовного дела и хранении их в течение всего срока его хранения, влечет расширительный подход к такому виду доказательств, как иные документы, и позволяет непосредственно использовать результаты ОРД в качестве доказательств, что, на наш взгляд, недопустимо. Отсутствие в данном случае процедуры осмотра и приобщения к материалам уголовного дела результатов ОРД на основании процессуального решения, в отличие от