В Республике Беларусь контролирующий орган, установивший в ходе проверки факт причинения вреда в размере более 1 000 базовых величин, а также при установлении иных фактов, указывающих на признаки преступления, обязан передать материалы проверки в органы уголовного преследования в 10-дневный срок со дня вручения акта проверки проверяемому субъекту.

Материалы проверки направляются в органы уголовного преследования с сопроводительным письмом, в котором указываются наименование проверяемого субъекта, его местонахождение; выявленные нарушения, требования законодательства, которые нарушены; должности, фамилии и инициалы лиц, действия которых повлекли нарушение проверяемым субъектом законодательства.

К сопроводительному письму прилагаются копии следующих документов:

акта проверки;

документов, регламентирующих должностные обязанности лиц, действия (бездействие) которых повлекли нарушение законодательства;

возражения по акту проверки;

решения по акту проверки и требования об устранении нарушений, постановления о наложении административного взыскания в отношении проверяемого субъекта;

объяснений лиц по фактам выявленных нарушений.

К материалам проверок, передаваемым в органы уголовного преследования, могут быть приложены подлинники или копии документов бухгалтерского учета, иных документов, в том числе хранившихся в электронном виде, свидетельствующих о совершении нарушений законодательства.

По мотивированному запросу органа уголовного преследования контролирующий орган обязан в 5-дневный срок со дня поступления запроса представить копии имеющихся у него дополнительных материалов, необходимых для принятия органом уголовного преследования решения в соответствии с законодательством.

Органы уголовного преследования при получении материалов проверки регистрируют и рассматривают их, принимают решение в соответствии с уголовно-процессуальным законодательством. О принятом решении (о возбуждении уголовного дела и результатах его рассмотрения, об отказе в возбуждении уголовного дела, о прекращении возбужденного уголовного дела) в 10-дневный срок со дня его вынесения в контролирующий орган направляется соответствующая информация.

Таким образом, в Республике Беларусь на законодательном уровне определены критерии и сроки оформления результатов документальной проверки, однако следует обратить внимание и на проблемные практические вопросы, связанные с анализом и оценкой материалов документальной проверки органами уголовного преследования.

УДК 343.985

А.Г. Скоморох

ПРОЦЕСС ПОЗНАНИЯ В ОПЕРАТИВНОМ ПОИСКЕ

Преступность в современном мире характеризуется изощренностью форм и методов совершения преступлений, которые в большинстве случаев носят латентный характер. Для эффективной борьбы с ними требуется действенное средство, а именно осуществление оперативно-розыскной деятельности (ОРД), инструментом которой помимо прочего является оперативный поиск (ОП), обеспечивающий своевременное получение оперативно значимой информации, позволяющей обнаружить факты и лиц, представляющих оперативный интерес. В ходе осуществления ОП сотрудниками оперативных подразделений в той или иной мере происходит познание объективной действительности.

Способность к познанию окружающего мира является характерной особенностью человека. Процесс познания представляет собой особый вид деятельности людей и объединяет такие элементы, как субъект и объект познания. К субъектам познания относятся лица, осуществляющие процесс познания с целью достижения тех или иных целей. Объект познания – это то, на что направлена познавательная деятельность.

Согласно научным представлениям, сложившимся в современном обществе, познание является формой взаимодействия, возникающего между субъектом и объектом. Результатом такого взаимодействия будет получение истины, необходимой для удовлетворения возникших у субъекта потребностей, путем освоения изучаемого объекта. Истина в данном случае представляет собой информацию об объекте познания, получаемую посредством чувственного и рационального познания.

Рассматривая процесс познания в ОП, отметим, что субъектами познавательного процесса в данном случае выступают должностные лица, наделенные правом осуществления ОРД. Процесс познания является сложным, диалектическим и противоречивым процессом, целью которого является получение знаний об окружающей человека действительности. Исходя из изложенного, полагаем, что в основе процесса выявления и раскрытия преступлений лежит познание оперативным сотрудником окружающей объективной действительности и фактических обстоятельств совершения преступления.

Сотрудник оперативного подразделения, исследуя фактические данные, характеризующие обстоятельства совершенного или совершаемого преступления, приобретает необходимые для решения оперативно-розыскных задач знания, познает события (преступление).

Под таким углом зрения ОП выступает в качестве способа собирания информации о лицах и фактах, представляющих оперативный интерес.

Наиболее широко применяемыми методами познания, направленными на изучение конкретных объектов и явлений, как в научных исследованиях, так и в практической деятельности оперативных подразделений, по нашему мнению, являются: наблюдение, сравнение, измерение, моделирование, эксперимент, опрос, описание. Указанные методы познания, входя в том

или ином сочетании в ОП, раскрывают потенциальные познавательные возможности ОП, которые реализуются в практической деятельности через разработанные в теории ОРД системы тактических приемов и комбинаций. Кроме того, особое значение процесс познания имеет при его научном исследовании. Проводя подобного рода исследования на монографическом уровне, ученые анализируют проблемные вопросы использования методов познания при выявлении оперативными сотрудниками латентных преступлений. На основании проводимых исследований вырабатываются новые научные рекомендации по реализации и использованию методов познания объективной действительности при осуществлении ОП, что позволяет повысить эффективность решения задач ОРД.

Исходя из вышеизложенного, можно сделать вывод, что процесс познания, происходящий при осуществлении ОП, является чувственно-рациональным. Используя научные и общие методы познания, оперативный сотрудник приобретает необходимые ему знания, которые позволяют решать оперативно-розыскные задачи по выявлению и раскрытию латентных преступлений.

УДК 004.5 + 004.7 + 334.024 + 338.2

Е.Н. Соболевский

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Новые возможности информационных технологий создают новые угрозы для информационной безопасности любой сферы общества. Цифровой мир стремительно расширяется, становится мобильным, управляет производством и технологическими процессами, охватывает всю среду обитания человека – от бытовых приборов до умных офисов и интеллектуального транспорта. Все больше информации передается через мобильные сервисы, ранее изолированные системы начинают взаимодействовать и обмениваться информацией, лавинообразно нарастают поток данных и объемы их хранения. Внедрение новых парадигм организации распределенных крупномасштабных систем, таких как интернет вещей (Internet of Things, IoT), приведет к новым рискам информационной безопасности, когда через Сеть станут доступны практически все предметы, окружающие человека.

По мере развития технологий в окружающем человека мире появляется все больше устройств, находящихся под управлением микропроцессоров и программного обеспечения. С ростом числа внедрений решений на базе IoT, как считают эксперты, все больше атак будет направлено не только на программное обеспечение, но и на аппаратное обеспечение (сетевые карты, USB-устройства), входящее в инфраструктуру интеллектуального транспорта, умных домов, автоматизированных систем управления производством.

Возможности, которые стали доступны с возникновением сети Интернет, привели к кардинальному преобразованию общества и его экономической реальности. Интернет сегодня – это среда, используемая для всевозможных форм взаимодействия всех субъектов экономики. Высокая степень потребности в интернете как в повседневных практиках общества, так и в деятельности государства и бизнес-сообщества выдвигает его в ряд необходимых элементов социально-экономического развития общества.

Сеть Интернет позволила сформировать новый рынок цифровых услуг и оказала значительное влияние на финансовое благосостояние стран.

В современных реалиях цифровая экономика стала мощным фундаментом развития государств: страны с более развитой цифровой экономикой получают большую долю своего ВВП за счет высокотехнологичных секторов. Предполагается, что к 2025 г. цифровая экономика может достичь показателя в 50 % глобального ВВП, а в развитых странах – превысить его.

Киберугрозы сегодня нацелены на все области, использующие цифровые данные: здравоохранение, образование и науку, банковскую сферу, государственные органы, представителей бизнеса и многое другое. В большинстве случаев цель злоумышленников – хищение персональных данных (номера банковских счетов и банковских платежных карточек, паспортные данные, медицинские карты, данные об объектах интеллектуальной собственности), а также информации, относящейся к государственной, коммерческой и военной тайне.

Принято считать, что кибератакам подвержены все страны вне зависимости от уровня экономического развития.

На текущий момент основными видами атак, подпадающими под понятие киберугрозы, являются: киберфизические атаки, вредоносное программное обеспечение (включая программы-вымогатели, rootkit, backdoor, троянские программы, шпионские программы и т. д.), DDoS-атаки (потоки ложных запросов), ботнеты (компьютерные сети), социальная инженерия (в том числе фишинг) и т. д.

Данные инструменты применимы практически ко всем сферам деятельности государства, бизнесу и общественной жизни. Наиболее актуальными угрозами можно считать: социальную инженерию; DDoS-атаки или отказ от обслуживания; шифрование данных, которое в основном происходит при установке на компьютер программы-вымогателя; киберфизические атаки; атаки на IoT (интернет вещей); киберпропаганда (дезинформация) и иные.

Существующие и вновь возникающие угрозы кибербезопасности сегодня направлены на все структуры, имеющие выход в сеть Интернет: частные и государственные организации, производства, медицинские и образовательные учреждения, учреждения здравоохранения, финансовые и банковские структуры, а также многое другое.

Отсутствие необходимых знаний при разработке и внедрении сетевых технологий существенно влияет на ситуацию с киберпреступностью.

Данный период времени считается одним из наиболее тяжелых для экономики как на национальном, так и на мировом уровнях. Усложнившиеся санитарно-эпидемиологические условия позволили злоумышленникам использовать более изо-