В указанной ситуации оперативному сотруднику необходимо обратить внимание на пояснения руководителя проверяемого предприятия, а также на заключение налоговой инспекции или решение экономического суда по существу этих возражений. Кроме того, целесообразно запросить сведения об интересующих субъектах хозяйствования и их контрагентах в Департаменте финансового мониторинга Комитета государственного контроля Республики Беларусь.

После получения вышеуказанной информации правоохранительными органами осуществляется выдвижение оперативных версий: налоговое преступление совершено при обстоятельствах, имеющихся в материалах налоговых проверок; преступные посягательства в сфере налогообложения отсутствуют, однако имеются признаки других наказуемых деяний.

С целью проверки выдвигаемых версий о совершенном налоговом преступлении необходимо истребовать документы: отражающие учет операций по расчетным счетам в банковских учреждениях, из вышестоящей организации и обслуживающей аудиторской организации, с предприятий, с которыми осуществлялись финансово-хозяйственные сделки. В налоговом органе могут быть получены документы, в которые внесены искаженные данные, повлекшие уклонение от уплаты сумм налогов, сборов. Кроме того, к материалам проверки должны быть приобщены копии приказов о назначении должностных лиц на должность, выписки из инструкций (нормативных правовых актов), касающихся их обязанностей.

Второй вид оперативно-розыскной ситуации: поступает оперативная информация о совершаемом либо совершенном преступлении.

Выявление налоговых преступлений оперативным путем предполагает предварительный сбор, накопление и систематизацию сведений о лицах, представляющих оперативный интерес, и фактических сведений, указывающих на различные признаки скрытой противоправной деятельности. Оперативными сотрудниками выделяются следующие признаки, свидетельствующие о совершении юридическими лицами преступных посягательств в сфере налогооблажения: отсутствие персонала или средств для осуществления хозяйственных операций, а также экономического смысла при их проведении; использование без явной необходимости посредников при осуществлении хозяйственных операций; несоответствие заработной платы сотрудников их квалификации; уменьшение налоговой нагрузки при одновременном увеличении выручки; положительная разница между заемными средствами и выручкой.

На этапе проверки первичной информации необходимо: установить достоверность первичной информации, т. е. выявить дополнительную



информацию, которая подтверждает факт незаконных действий руководителей организации в сфере налогообложения; осуществить сбор информации, характеризующей личность руководителей, сотрудников бухгалтерии; выявить лиц из числа сотрудников организации, обладающих возможностью доступа к информации о преступной деятельности проверяемых лиц; установить лиц из числа сотрудников организации, осведомленных о совершении налоговых преступлений; выявить и задокументировать конкретную схему уклонения от уплаты налогов; определить роль каждого участника преступления. С целью реализации указанных задач проводятся такие оперативно-розыскные мероприятия, как оперативный опрос, наведение справок, сбор образцов, исследование предметов и документов. В ходе проведения ОРМ необходимо опрашивать плательщиков налогов, получать сведения, связанные с их профессиональной деятельностью, а также проверять их посредством использования информационных учетов.

При подтверждении первичной оперативной информации заводится дело оперативного учета, в рамках которого осуществляется документирование уклонения от уплаты налогов.

После того как будут собраны достаточные данные, необходимые для возбуждения уголовного дела, целесообразно планировать и проводить задержание всех соучастников преступления.

Знание типичных оперативно-розыскных ситуаций, а также порядка действий оперативного сотрудника в них позволяет наиболее эффективно выявлять преступления в сфере налогообложения.

УДК 343.985

***Е.И. Давидович***

## ПРЕПЯТСТВИЯ, ВОЗНИКАЮЩИЕ ПРИ РАСКРЫТИИ КИБЕРПРЕСТУПЛЕНИЙ

Число киберпреступлений, как и их изощренность и влияние, продолжает расти. Преступники не только создают или разрабатывают свои собственные инструменты, но и используют законное или общедоступное программное обеспечение. В настоящее время существуют проблемы, связанные с масштабом и объемом киберпреступлений, технической сложностью идентификации преступников, а также с необходимостью действовать на международном уровне для привлечения виновных к установленной законом ответственности.

При проведении оперативно-розыскных мероприятий по установлению лица, совершившего киберпреступление, могут возникнуть несколько препятствий.

Анонимность – одно из таких препятствий. Она позволяет людям участвовать в деятельности, не раскрывая себя и (или) свои действия другим. Анонимность предоставляют пользователям информационные и коммуникационные технологии. Есть несколько способов анонимизации, один из которых основан на использований прокси-сервера. Прокси-сервер – промежуточный сервер, поскольку он используется для подключения к серверу клиента, т. е. его компьютера, который запрашивает ресурсы. Анонимайзеры, или анонимные прокси-серверы, скрывают идентификационную информацию пользователей, маскируя их IP-адреса и заменяя их другим IP-адресом. Киберпреступники также могут использовать анонимные сети для шифрования трафика и сокрытия адреса интернет-протокола или IP-адреса (уникального идентификатора), присвоенного интернет-провайдером компьютеру или другому цифровому устройству, подключенному к сети. В этих анонимных сетях не только маскируются данные о пользователях, но и размещаются вебсайты, доступные только пользователям этих сетей.

Атрибуция – еще одно препятствие, с которым сталкиваются сотрудники правоохранительных органов при раскрытии киберпреступлений. Она закрепляется в определении, кто или что несет ответственность за совершение киберпреступления. Однако киберпреступность пытается этот процесс подменить, приписав конкретному цифровому устройству, пользователю устройства или другим лицам ответственность за совершение киберпреступления. Использование инструментов анонимности может затруднить идентификацию устройств и лиц, совершивших киберпреступление. Атрибуция дополнительно осложняется использованием зараженных вредоносным программным обеспечением бот-компьютеров или бот-сетей либо цифровых устройств, управляемых без ведома пользователя инструментами удаленного доступа, для совершения киберпреступлений.

Третьим препятствием раскрытию киберпреступлений является обратное отслеживание – процесс отслеживания незаконных действий до их источника, т. е. преступника или цифрового устройства. Отслеживание проводится после того, как киберпреступление произошло либо было обнаружено, для выявления информации путем изучения всех обстоятельств происшедшего, а также компьютерных устройств, которые могут раскрыть информацию о киберпреступлении. Например, изучаются журналы событий операционной системы Windows, которые автоматически записывают события, происходящие на компьютере, чтобы



в дальнейшем данные сведения можно использовать для мониторинга, понимания и диагностики действий и проблем в компьютерной системе. Такими являются журналы приложений, которые записывают события, регистрируемые программами (приложениями), и журналы безопасности, в которых записываются все попытки входа в систему, как действительные, так и недействительные, а также создание, открытие или удаление файлов, программ или других объектов. Время, необходимое для завершения процесса обратного отслеживания, зависит от знаний, навыков и возможностей киберпреступников, а также от тактики, которую они используют для участия в противоправной деятельности.

Таким образом, в настоящее время правоохранительные органы многих стран, в том числе и Республики Беларусь, сталкиваются с серьезными проблемами при раскрытии киберпреступлений. Для устранения описанных препятствий при раскрытии киберпреступлений необходимо активно применять профилактические меры по отношению к пользователям компьютерных сетей, использовать новейшее специализированное программное обеспечение для анализа полученной информации, а также регулярно повышать квалификации сотрудников правоохранительных органов, занимающихся раскрытием киберпреступлений.

УДК 343.985

***Е.И. Давидович, Д.А. Новаш***

## СВЯЗЬ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ СО СМЕЖНЫМИ СОСТАВАМИ ПРЕСТУПЛЕНИЯ

В конце XX в. большая часть информации была размещена в цифровом пространстве. В условиях активного развития информационных технологий большинство преступлений видоизменились и противоправные замыслы стали реализовываться с помощью компьютерных систем, в результате чего возникла проблема корректной реализации норм права и правильной квалификации преступлений, связанных с несанкционированным доступом к компьютерной информации. Решение данной проблемы должно способствовать реализации принципа законности и правильной квалификации преступлений.

Несанкционированный доступ к компьютерной информации – неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающееся нарушением систем защиты лицом, которое не имеет на это права. Уголов-