

Уголовный процессуальный кодекс Украины предусматривает возможность сбора доказательств путем проведения негласных следственных (розыскных) действий (НСРД). Наиболее распространенным видом НСРД, используемым при расследовании данного вида преступлений, является контроль за совершением преступления (ст. 271 УПК): контролируемая поставка, контролируемая закупка, оперативная закупка. В отличие от других НСРД, разрешение на проведение которых выносится следственным судьей апелляционного суда, согласно ч. 4 ст. 246 УПК исключительно прокурор имеет право принять решение о проведении данного НСРД.

В следственной практике возникает ряд проблемных вопросов, связанных с прогнозированием доказательственной силы результатов НСРД.

Во-первых, это связано с тем, что Закон Украины «Об оперативно-розыскной деятельности» предусматривает проведение контролируемой поставки, контролируемой и оперативной закупок товаров и веществ, в том числе запрещенных для свободного оборота (п. 2 ч. 1 ст. 8), до открытия уголовного производства, эта информация подлежит дальнейшей легализации. А такие же НСРД разрешено проводить только в рамках открытого уголовного производства после внесения информации в Единый реестр досудебных расследований (ЕРДР), результаты имеют силу доказательств. Судебная практика была неоднозначной, в некоторых случаях суды отказывались признавать в качестве доказательств результаты оперативно-розыскных действий. Точку в этом споре поставил в правовом выводе кассационный уголовный суд в составе Верховного Суда (постановление от 16 марта 2017 г. в деле № 5-364к16), согласно которому «фактические данные, полученные в результате проведения оперативной закупки до внесения сведений в ЕРДР, могут признаваться надлежащими и использоваться как доказательства, а именно как документы в уголовном судопроизводстве при условии получения их в порядке, предусмотренном УПК Украины с учетом особенностей применения Закона Украины „Об оперативно-розыскной деятельности“».

Во-вторых, нераскрытие материалов НСРД сторонами в порядке ст. 290 УПК после окончания расследования, а также дополнительных материалов, полученных до либо во время судебного рассмотрения, является основанием для признания судом сведений, имеющих в них, недопустимыми в качестве доказательств. Факт ознакомления с материалами дела после окончания расследования не является достаточным для отстаивания стороной защиты своих позиций, это свидетельствует о нарушении баланса интересов в уголовном процессе.

В-третьих, в некоторых случаях результаты незаконного допроса (разговор следователя и оперуполномоченных с подозреваемым, находящимся в следственном изоляторе, без предоставления адвоката) следственные органы пытаются представить в качестве результатов аудиовидеонаблюдения за лицом (при котором адвокат, естественно, отсутствует).

Для оценки доказательств целесообразно руководствоваться практикой Европейского суда по правам человека как источником права (ст. 17 Закона Украины «О выполнении решений и применении практики Европейского суда по правам человека»). Суд должен убедиться, что способ получения доказательств был справедливым. Европейский суд по правам человека не определяет, были ли определенные доказательства получены незаконно, а проверяет, не повлекла ли такая «незаконность» нарушение иного права, гарантированного Конвенцией о защите прав человека и основополагающих свобод.

УДК 343.985

А.В. Башан, А.Н. Тукало

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ – НОВОЕ НАПРАВЛЕНИЕ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ АКАДЕМИИ МВД

Использование компьютерных систем во всех сферах жизни современного общества, стремительное развитие сетевых технологий помимо преимуществ повлекли за собой появление ряда специфических проблем: необходимость обеспечения эффективной защиты информации, которая обусловлена ростом правонарушений, связанных с кражами и неправомерным доступом к данным, хранящимся в памяти компьютерных систем и передаваемым по линиям связи; различные виды мошенничества, совершаемого с использованием сети Интернет; хищения, осуществляемые с использованием реквизитов банковских платежных карточек, и т. д. Развитие информационно-коммуникационных технологий в Республике Беларусь позволяет прогнозировать значительный рост количества киберпреступлений в будущем.

Следует отметить, что в последние годы МВД Республики Беларусь системно совершенствует информационно-аналитическое обеспечение оперативно-служебной деятельности органов внутренних дел. Проведена большая работа по внедрению в эту деятельность различных совре-

менных автоматизированных информационных систем и программно-технических комплексов: внедрены типовые программные решения по интеграции данных; предприняты шаги по организации единого информационного пространства в системе МВД; категорированы основные подходы и определены уровни формирования информационных массивов на республиканском, областном и районном уровнях. Это позволило упорядочить и системно организовать основные связи между подразделениями, оптимизировать уровни доступа и порядок сбора, хранения и использования информации (учетов), определить рациональный состав оборудования, информационных, технико-технологических и других ресурсов.

В настоящее время сотрудники оперативных подразделений ОВД получают большой массив оперативно значимой информации посредством изучения открытых информационных ресурсов сети Интернет (в том числе в ее теневом сегменте).

В этой связи с целью повышения эффективности работы по предупреждению, выявлению, пресечению преступлений, совершаемых с использованием высоких технологий, по инициативе Академии в МВД Республики Беларусь проработан вопрос о подготовке специалистов по соответствующему профилю на базе ведомственного учебного заведения по учебным дисциплинам кафедр оперативно-розыскной деятельности факультета милиции и правовой информатики.

С целью реализации указанной задачи проведен комплекс правовых и организационно-практических мероприятий:

разработана образовательная программа высшего образования I ступени по специальности «Правоведение» специализации «Оперативно-розыскная деятельность» (направление оперативно-служебной деятельности «Противодействие киберпреступности и компьютерная разведка»);

подготовлены и согласованы с заинтересованными подразделениями заказчиков кадров изменения и дополнения в тематику дипломных и курсовых работ для обучающихся по указанному направлению оперативно-служебной деятельности;

изменены Нормы времени в части установления объема часов на проведение профессионально-образовательной стажировки, а также разработку учебно-программной документации и методического обеспечения по вновь вводимым учебным дисциплинам;

разработана программа преддипломной практики по специальности «Правоведение» специализации «Оперативно-розыскная деятельность» (направление оперативно-служебной деятельности «Противодействие киберпреступности и компьютерная разведка»);

введены в учебный план Академии новые учебные дисциплины по кафедре правовой информатики («Комплексная защита информации и противодействие киберпреступности») и оперативно-розыскной деятельности факультета милиции («Противодействие киберпреступности и компьютерная разведка»), разработана новая образовательная программа по учебной дисциплине кафедры правовой информатики «Информационное обеспечение служебной деятельности»;

сформирована учебная группа из числа курсантов третьего курса, склонных к данному направлению оперативно-служебной деятельности и имеющих навыки работы со средствами компьютерной техники;

профессорско-преподавательским составом кафедры оперативно-розыскной деятельности факультета милиции осуществлена стажировка в заинтересованных подразделениях заказчиков кадров (главное управление по наркоконтролю и противодействию торговле людьми криминальной милиции МВД Республики Беларусь (ГУНиПТЛ), управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь (УРПСВТ), а также соответствующих структурных подразделениях ГУВД Мингорисполкома);

профессорско-преподавательским составом кафедры правовой информатики пройдена стажировка в подразделениях центрального аппарата Следственного комитета Республики Беларусь;

внесены соответствующие изменения и дополнения в нормативные правовые акты, регламентирующие порядок использования сети Интернет в подразделениях органов внутренних дел, с целью реализации возможности отработки обучающимися навыков проведения поисково-аналитической работы в сети Интернет;

согласована с заинтересованными субъектами возможность использования в образовательных целях учебных аккаунтов в социальных сетях, а также осуществления компьютерной разведки с использованием средств анонимизации и деанонимизации в сети Интернет (в том числе в ее теневом сегменте);

для материально-технического обеспечения образовательного процесса произведена закупка необходимых товарно-материальных ценностей (материальные носители информации, модемы и т. д.), а также заключены договоры на получение интернет-услуг;

заинтересованными подразделениями заказчиков кадров обеспечено предоставление имеющейся информационно-справочной документации, доступа к специализированному программному обеспечению, согласован график их участия в образовательном процессе.

Начать подготовку курсантов по направлению оперативно-служебной деятельности «Противодействие киберпреступности и компьютерная

разведка» планируется с 1 сентября 2019 г. Несомненно, оценку качеству подготовки выпускников Академии по данному направлению оперативно-служебной деятельности даст время и руководители структурных подразделений, однако очевидно, что в специалистах такого уровня заинтересованы не только ГУНиПТЛ, УРПСВТ, но и другие оперативные подразделения МВД Республики Беларусь.

УДК 343.985

С.И. Бординович, Д.В. Ковалевич

**НЕКОТОРЫЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЯ
НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ВОПРОСОВ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
ОТДЕЛЬНЫХ КАТЕГОРИЙ ЗАЩИЩАЕМЫХ ЛИЦ
В УГОЛОВНОМ ПРОЦЕССЕ**

В соответствии с ч. 1 ст. 10 Уголовно-процессуального кодекса Республики Беларусь на орган уголовного преследования возлагается обязанность обеспечивать защиту прав и свобод лиц, участвующих в уголовном процессе, создавать предусмотренные законом условия для ее осуществления, своевременно принимать меры по удовлетворению законных требований участников уголовного процесса. Руководствуясь указанной нормой закона и требованиями ст. 67 УПК, орган, ведущий уголовный процесс, при наличии достаточных данных, указывающих на то, что имеется реальная угроза убийства, применения насилия, уничтожения или повреждения имущества, осуществления других противоправных действий в отношении участника уголовного процесса, а также членов его семьи и близких в связи с его участием в уголовном процессе, обязан принять предусмотренные законом меры по обеспечению безопасности этих лиц и их имущества.

Статья 66 УПК содержит перечень процессуальных и иных мер безопасности, применяемых в отношении участников уголовного процесса, их близких родственников и членов их семей либо иных лиц, которых они обоснованно считают близкими, а также в отношении их имущества.

Процессуальные меры безопасности (неразглашение сведений о личности; освобождение от явки в судебное заседание; закрытое судебное заседание) принимает и самостоятельно обеспечивает орган, ведущий уголовный процесс. Применение иных мер безопасности (использование технических средств контроля; прослушивание перегово-

ров, ведущихся с использованием технических средств связи, и иных переговоров; личная охрана, охрана жилища и имущества; изменение паспортных данных и замена документов; запрет на выдачу сведений) на основании мотивированного постановления (определения) органа, ведущего уголовный процесс, обеспечивается органом внутренних дел или государственной безопасности по месту жительства, работы или учебы защищаемого лица.

В свою очередь, обеспечивающему безопасность органу внутренних дел или государственной безопасности с учетом характера и степени опасности для жизни, здоровья, имущественных и иных прав защищаемых лиц в соответствии с ч. 3 ст. 66 УПК предоставлено право применить в отношении участников уголовного процесса и другие меры безопасности (выдача специальных средств индивидуальной защиты и оповещения об опасности; временное помещение в безопасное место; перевод на другую работу (службу), изменение места работы (службы) или учебы; переселение на другое место жительства; перевод из одного места содержания под стражей или отбывания наказания в другое). Реализация указанных мер осуществляется органами, обеспечивающими безопасность, в соответствии с актами законодательства, регламентирующими оперативно-розыскную деятельность.

Закон Республики Беларусь «Об оперативно-розыскной деятельности» (далее – Закон об ОРД) возлагает на органы, осуществляющие ОРД, обязанность обеспечивать защиту должностных лиц органов, осуществляющих ОРД, а также граждан, оказывающих или оказывавших содействие этим органам на конфиденциальной основе, и их близких от преступных посягательств.

Закон Республики Беларусь «О государственной защите судей, должностных лиц правоохранительных и контролирующих (надзорных) органов, сотрудников органа государственной охраны» (далее – Закон о госзащите) устанавливает систему мер государственной защиты жизни, здоровья и имущества судей, должностных лиц правоохранительных и контролирующих (надзорных) органов, сотрудников органа государственной охраны, осуществляющих служебную деятельность, выполнение которой может быть сопряжено с посягательством на безопасность указанных лиц, их близких.

В Республике Беларусь установлен единый порядок применения мер безопасности и мер по обеспечению безопасности в отношении всех вышеперечисленных категорий защищаемых лиц, который закреплен в соответствующем положении, утвержденном постановлением Совета Министров Республики Беларусь от 21 января 2016 г. № 44. Тем не менее действующее нормативно-правовое регулирование в указанной сфе-