УДК 343.985.7

И.А. Судникович, *старший следователь управления по расследованию преступлений в сфере высоких технологий и против интеллектуальной собственности главного следственного управления предварительного расследования МВД Республики Беларусь;*
Ю.М. Юбко, *кандидат юридических наук, доцент, заведующий кафедрой расследования преступлений Академии МВД Республики Беларусь*

ДЕЯТЕЛЬНОСТЬ ОРГАНОВ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ В СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА ПО ЗАЯВЛЕНИЯМ (СООБЩЕНИЯМ) О НАРУШЕНИИ ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ, КОГДА ОБЪЕКТОМ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА ЯВЛЯЕТСЯ ПРОГРАММНЫЙ ПРОДУКТ

Рассматриваются особенности деятельности сотрудников органа уголовного преследования по проверке и принятию решений по заявлениям (сообщениям) о нарушении права интеллектуальной собственности, когда объектом преступного посягательства является программный продукт. Сакцентировано внимание на проблемах, имеющих место в практической деятельности по уголовным делам рассматриваемой категории: особенностях действий оперативного работника по проверке поступившей информации, взаимодействии следователя с оперативным работником. Высказаны рекомендации для практических работников.

The article examines the peculiarities of the activities of the criminal investigation officials when checking up and making decisions when receiving the information of breaking the right of intellectual property when the object of this criminal act is a programme product. The attention is paid to the situations which take place in practice when investigating this kind of criminal cases: the peculiarities of an operative's activities when checking up the received information, the interaction of an investigator and an operative. The recommendations for the practical workers are given.

Мировое сообщество на современном этапе придает большое значение вопросу организации защиты авторских, смежных, изобретательских и патентных прав. В середине октября 2010 г. на встрече 37 стран в Токио принято решение о совместной работе над проектом торгового соглашения против подделок. Данный договор призван прекратить мировые нарушения прав по интеллектуальной собственности, а также объединить усилия по борьбе с подделками в различных отраслях мировой экономики.

Китайские власти в свою очередь с октября 2010 г. на шесть месяцев запустили широкомасштабную акцию по пресечению нарушений в области интеллектуального права, так как страна занимает второе место по объему нелегального рынка программного обеспечения среди государств Центральной и Восточной Европы, а также Ближнего Востока и Африки.

Представители стран СНГ договорились о совместном противодействии нарушениям интеллектуального права, разработав перечень мероприятий в сфере противодействия правонарушениям в области интеллектуальной собственности.

Какова ситуация на современном этапе в Республике Беларусь и какие меры принимаются органами уголовного преследования по пресечению нарушений авторских прав, когда объектом преступного посягательства является программный продукт? Анализ правоприменительной практики свидетельствует, что органы уголовного преследования нашей страны осуществляют защиту в большинстве случаев программных продуктов производителей (авторов) других государств, представительства которых базируются на территории Республики Беларусь. Наиболее ярким примером является бухгалтерская программа «1С:Предприятие», производитель которой – компания Российской Федерации – расположен в Москве. В Республике Беларусь имеется ряд ее представительств, действующих на основании доверенности. Они защищают на территории Республики Беларусь ее интересы как правообладателя. Любое физическое или юридическое лицо, желающее установить упомянутую программу («1С:Предприятие») или какую-либо другую лицензионную программу, обязано выяснить, кто является правообладателем программного продукта, и затем обратиться к нему с целью заключения договора, дающего право на установку такой программы. Если же они предпринимают попытку установки лицензионной программы без договора правопреемника, то эти действия влекут административную ответственность, а при определенных условиях подпадают под состав преступления, предусмотренного ст. 201 УК Республики Беларусь, защищающей нарушение авторских, смежных, изобретательских и патентных прав. Вместе с тем необходимо учитывать, что законодатель отнес эту норму к уголовным делам частно-публичного обвинения (ч. 4 ст. 26 УК), кото-

рые возбуждаются только по заявлению лица, пострадавшего от преступления. Часть 2 упомянутой нормы уголовного закона констатирует наличие административной преюдиции, что также следует иметь в виду при принятии решения о возбуждении уголовного дела. Как правило, представитель правообладателя программы на территории Республики Беларусь принимает меры по защите интересов стороны, которые он представляет. Для этого сотрудники представительства проводят аналитическую работу по обнаружению объявлений в интернете или средствах массовой информации о том, что такой-то гражданин или юридическое лицо устанавливает компьютерную программу (программы), владельцем которой (которых) является их правообладатель. При выявлении таких фактов они обращаются в ОВД с заявлением (сообщением) и просят провести проверку деятельности по распространению их лицензионного программного обеспечения конкретным гражданином (компанией).

Однако обнаружение эпизодов преступной деятельности того или иного лица возможно и оперативным путем. И если оперативные работники выявляют такие эпизоды, то они обязаны согласовать свои действия в дальнейшем с представителями правообладателя и выяснить, желает ли он привлечь гражданина к уголовной ответственности. Вместе с тем уголовно-процессуальный закон Республики Беларусь констатирует, что по таким преступлениям уголовное дело может быть возбуждено прокурором и при отсутствии заявления лица, пострадавшего от преступления, если имеется ряд условий, предусмотренных в ч. 5 ст. 26 УПК.

С момента поступления заявления (сообщения) оперативный работник приступает к проверке отраженной в нем информации и начинает собирать доказательства в соответствии с требованиями ч. 2 ст. 173 УПК Республики Беларусь, подтверждающие наличие оснований к возбуждению уголовного дела. При этом возникают две ситуации. Первая – когда в заявлении представитель правообладателя указывает не только лицо, устанавливающее контрафактные программы, но и приводит перечень предприятий и организаций, где такие программы установлены. Во втором случае в заявлении или сообщении речь идет только о распространителе контрафактного программного продукта. С учетом данных ситуаций и должна проводиться проверка заявления (сообщения) оперативным работником.

В рамках первой ситуации в отношении установленного лица проводятся оперативно-розыскные мероприятия в соответствии с законом Республики Беларусь «Об оперативно-розыскной деятельности», а также процессуальные действия по проверке конкретных учреждений или организаций для подтверждения фактов установки конкретным лицом контрафактного программного продукта.

Во второй ситуации проводятся оперативно-розыскные мероприятия по установлению и документированию эпизодов преступной деятельности.

Как в первой, так и во второй ситуации деятельность в рамках предварительной проверки направлена на собирание доказательственной информации, указывающей на признаки преступления, предусмотренного ст. 201 УК Республики Беларусь. При этом наиболее важным моментом являются способы собирания доказательственной информации на конкретных предприятиях и организациях, на компьютерах которых, по имеющейся информации, инсталлированы контрафактные программы.

В связи с тем, что ч. 1 ст. 103 УПК констатирует возможность собирания доказательств в процессе разрешения заявлений и сообщений о преступлении, оперативный работник в рамках доследственной проверки вправе получить объяснения у сотрудников предприятия или организации о том, имеются ли документы на приобретение данной программы, а также электронный ключ защиты от несанкционированного использования программы (такой ключ в виде USB-flash прилагается к лицензионной программе, которая без него не запускается и не работает). Как свидетельствует анализ практики, у владельца контрафактной программы отсутствует электронный ключ защиты, с помощью которой она запускается. Те, кто устанавливает контрафактную программу заказчику с помощью вирусных программ, самостоятельно вносят изменения в лицензионную программу (эти изменения связаны со взломом ее ключа или его обходом) или же приобретают готовую контрафактную программу. При получении объяснения необходимо выяснить, кто и когда устанавливал контрафактную программу? Каким образом проводился расчет? Руководствуясь ч. 2 ст. 103 и ч. 2 ст. 173 УПК, следует истребовать документы, подтверждающие приобретение установленной программы (договор, акт выполненных

работ), и документы, свидетельствующие об оплате услуг за ее установку (платежные бухгалтерские документы).

Наряду с истребованием документов и получением объяснений в соответствии с ч. 1 ст. 103 УПК собирание доказательственной информации производится и в процессе проведения осмотра. Чтобы результаты осмотра отвечали требованиям ст. 105 УПК, оперативный работник обязан провести осмотр места происшествия, руководствуясь требованиями ч. 2 ст. 173, ст. 203, 204 УПК, в рамках которого необходимо осмотреть конкретную компьютерную технику и убедиться, что программы, установленные на ней, являются нелицензионными. Наряду с требованиями процессуального закона следует также учитывать и тактический аспект производства данного следственного действия, а именно:

необходимо провести осмотр помещения, где находится (находятся) компьютер (компьютеры);

осуществить последовательно осмотр каждого компьютера.

При визуальном осмотре конкретного компьютера фиксируются: форма, размер, материал корпуса, цвет, название, фирма-изготовитель, серийный номер, объем памяти и другие технические данные, наличие на мониторе ярлыка или файла запуска искомой программы. Если искомая программа запускается, то отмечается отсутствие электронного ключа защиты в USB-разъемах системного блока, что свидетельствует о явном признаке ее контрафактности. В ходе дальнейшего осмотра компьютерной техники на признак контрафактности установленной программы указывает также наличие нелицензионного драйвера ключа защиты. Отмеченные признаки являются несомненным основанием для изъятия винчестера осматриваемого компьютера с целью его детального последующего осмотра в органе уголовного преследования.

В ходе осмотра компьютерной техники могут возникнуть ситуации, когда у предприятия или организации имеется договор с аттестованным на территории Республики Беларусь продавцом лицензионного программного продукта, а также приобретенный диск с лицензионной программой и электронный ключ защиты для ее запуска, однако наряду с лицензионной программой на рабочих компьютерах установлена и контрафактная, что объясняется необходимостью использования конкретной программы данным учреждением на нескольких машинных носителях в различных структурных подразделениях. Как правило, версия лицензионной программы рассчитана на установку на один или несколько компьютеров, при этом стоимость в одном и другом случае значительно отличается, поэтому компании не хотят нести затраты, но, желая обезопасить себя, закупают одну однопользовательскую версию и устанавливают ее на один компьютер, а на остальные компьютеры устанавливают контрафактные программы.

После завершения осмотра винчестер компьютера, на котором установлена программа, имеющая признаки контрафакта, изымается, о чем делается отметка в протоколе. Всегда ли необходимо изымать винчестер? Представляется, что при проведении осмотра места происшествия оперативный работник обязан изымать винчестер с установленной программой, имеющей признаки контрафакта. Как следует поступать в случаях, когда нелицензионные программы установлены на машинных носителях нескольких предприятий? Следственная практика знает прецеденты, когда в поле зрения органов уголовного преследования Республики Беларусь попадали до 40 учреждений и организаций, на компьютерной технике которых был установлен контрафактный программный продукт, и в ходе производства расследования в дальнейшем по уголовному делу эти эпизоды были доказаны. В отдельных литературных источниках имеются рекомендации о целесообразности создания копии (образца) машинного носителя в тех ситуациях, когда нет реальной возможности изъятия компьютерной техники из-за технологического процесса организации [1, с. 165]. Целесообразно ли в ходе проверки по заявлению или сообщению о распространении контрафактного программного продукта создавать копии винчестеров (БЭКАП) и на отдельных предприятиях их не изымать вообще? Представляется, что такое решение может быть принято только следователем при производстве расследования по конкретному уголовному делу в соответствии с требованиями ст. 96, 97 УПК. Оперативный работник обязан собрать доказательства, указывающие на признаки преступления, предусмотренного ч. 2 или 3 ст. 201 УК, и представить подлинные источники доказательств следователю для принятия решения о возбуждении уголовного дела.

Если имеется информация о наличии нелицензионных программ на машинных носителях ряда предприятий, то оперативный работник обязан осуществить осмотры и изъятие винчестеров с учетом складывающейся ситуации в ходе проведения проверки, чтобы не допустить их уничтожения сотрудниками этих учреждений.

После изъятия винчестера сотрудник органа уголовного преследования обязан незамедлительно назначить экспертизу, чтобы эксперт установил, действительно ли на нем имеется программа, обладающая признаками контрафактности. В этой связи закономерно возникает вопрос: кому поручить производство компьютерно-технической экспертизы? Согласно требованиям ст. 230, 231 УПК она может быть проведена как в экспертном, так и вне экспертного учреждения. Анализ практики свидетельствует, что оперативные работники назначают экспертизы всегда в ГЭКЦ МВД. Вместе с тем представляется, что согласно букве закона данная экспертиза может быть проведена вне экспертного учреждения компетентным специалистом в области программного обеспечения.

Может ли данная экспертиза проводиться специалистами представительства правообладателя, которое обратилось с заявлением о распространении контрафактных программ, или другого представительства, так как у них имеются копии лицензионных программ и их сотрудники имеют реальную возможность установления идентификационного тождества или отсутствия такового между программными продуктами? Представляется, что с просьбой о производстве экспертизы в данные представительства обращаться не следует, так как в ходе производства предварительного следствия защитник, представляющий интересы обвиняемого, будет заявлять ходатайства, констатируя заинтересованность должностных лиц данного представительства, предприняв попытку поставить под сомнение заключение эксперта.

При назначении экспертизы оперативный работник в постановлении формулирует ряд вопросов, разрешение которых экспертом позволит определить, установлена ли на изъятом и представленном на исследование винчестере контрафактная программа. При подготовке постановления о назначении экспертизы он должен сформулировать следующие вопросы:

1. Имеются ли на представленном на исследование носителе информации (винчестере) воспроизведенные и инсталлированные (установленные) компьютерные программы комплекса «1С:Предприятие»? Какие версии компьютерной программы комплекса «1С:Предприятие» установлены на представленном на исследование носителе, работоспособны ли они?

2. Какая информация о времени установки и использования компьютерной программы комплекса «1С:Предприятие» имеется на представленном на исследование носителе?

3. Имеются ли на носителе информации программы, предназначенные для удаления и блокирования средств защиты компьютерной программы комплекса «1С:Предприятие» от несанкционированного использования и копирования. Если да, то каков механизм их действия и последствия применения?

4. Имеются ли следы использования программ для удаления, блокирования и модификации компьютерной программы комплекса «1С:Предприятие» на представленном на исследование носителе информации, а также какие изменения были произведены в компьютерной программе?

Следующее обстоятельство, на которое обязан обратить внимание при производстве проверки сотрудник органа уголовного преследования, связано с размером дохода, полученного лицом в результате совершения преступных действий по распространению контрафактного программного продукта. В соответствии с требованиями уголовного законодательства Республики Беларусь доход должен быть получен в крупном размере. Доход в нашем случае состоит из двух элементов: во-первых, это фактический доход, а именно та сумма денежных средств, которую затратило предприятие на установку и обслуживание данной программы. В нашем примере по установке программы «1С:Предприятие» предприятие за установку перечисляет лицу на расчетный счет в соответствии с договором определенную сумму денежных средств (безналичный расчет) (возможен и наличный расчет), значит граждан получил доход от преступной деятельности. Во-вторых, это стоимость самого продукта, т. е. лицо установило программу с определенной конфигурацией, однако данная программа оценивается правообладателем в определенную денежную сумму и соответственно реализуется по какой-то конкретной цене. Гражданин за установку программы получил деньги у предприятия, но он не затратил

денежных средств на ее приобретение у правообладателя, поэтому размер дохода будет складываться из стоимости за ее установку и реальной цены правообладателя. Действующий уголовный закон предусматривает также причинение ущерба в крупном размере, поэтому когда в ходе производства проверки выясняется, что гражданин инсталлировал (установил) 30 программ, оперативный работник обязан выяснить их стоимость у правообладателя и если данная стоимость подпадает под критерий «ущерб в крупном размере», то в действиях распространителя контрафактной программной продукции будут усматриваться признаки преступления ч. 3 ст. 201 УК Республики Беларусь.

Собрав доказательственную информацию о преступных действиях конкретного лица по распространению контрафактного программного продукта, оперативный работник передает материалы проверки следователю, который при наличии в них признаков преступления, предусмотренного ч. 2, 3 ст. 201 УК Республики Беларусь, принимает решение о возбуждении уголовного дела или требует провести дополнительные процессуальные действия для выяснения отдельных неустановленных обстоятельств.

В случае принятия решения о возбуждении уголовного дела следователь и оперативный работник обязаны незамедлительно запланировать и провести задержание и допрос подозреваемого, а также обыск по месту жительства и работы с целью получения доказательств о его причастности к распространению контрафактной программной продукции.

При проведении проверочных действий по заявлению (сообщению) о преступлении, предусмотренном ст. 201 УК Республики Беларусь, сотрудник органа уголовного преследования обязан выяснить, на каких предприятих установлен контрафактный программный продукт; произвести осмотр компьютерной техники и изъятие носителей информации (винчестеров) с имеющимся на них программным продуктом, обладающим признаками контрафакции; назначить компьютерно-техническую экспертизу изъятых винчестеров; получить объяснения у сотрудников предприятий и организаций о фактах установления контрафактного программного продукта; истребовать у должностных лиц указанных учреждений документы, подтверждающие обстоятельства установления контрафактного программного продукта и порядок расчета с лицом, его установившим; выяснить размер дохода и ущерба в соответствии с требованиями ч. 2, 3 ст. 201 УК Республики Беларусь. После возбуждения уголовного дела следователь и оперативный работник обязаны незамедлительно провести обыски по месту жительства и работы подозреваемого, его задержание и допрос.

Библиографические ссылки

1. Лепехин А.Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты : монография. Минск : Тесей, 2008.

: 12.10.10