УДК 343.98

С.В. Петлицкий

ИНСТИТУТ СПЕЦИАЛЬНЫХ ЗНАНИЙ В ОРГАНИЗАЦИИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Государственный комитет судебных экспертиз Республики Беларусь (ГКСЭ) в соответствии с возложенными на него задачами проводит судебные экспертизы по материалам заявлений (сообщений) о преступлениях, уголовным делам, реализует мероприятия по поддержанию на надлежащем уровне качества и своевременности проведения экспертных исследований, ведет криминалистические учеты и коллекции, осуществляет другие функции в сфере судебно-экспертной деятельности (СЭД).

Наряду с этим, сотрудники ГКСЭ участвуют в следственных и процессуальных действиях, оперативно-розыскных мероприятиях, выполняя функции специалиста. Сегодня в Республике Беларусь технико-криминалистическая деятельность продолжает вносить огромный вклад в работу правоохранительных органов по раскрытию и расследованию преступлений. Как показывает практика, специалистам (криминалистам) приходится работать на местах происшествий по различным категориям и видам дел. Порой ими устанавливаются обстоятельства, существенно отличающиеся от первичной информации, поступившей в орган уголовного преследования. Поэтому сложно заранее предугадать, с каким преступлением, способом его совершения придется столкнуться лицу, осуществляющему экспертно-криминалистическую деятельность (ЭКД) в дежурные сутки.

Особенно, на наш взгляд, это актуально в современных условиях, когда последним приходится иметь дело с высокотехнологичной преступностью и на этом же уровне обеспечивать реализацию специальных знаний и профессиональных навыков в борьбе с ней. Осознавая всю сложность противодействия преступности в киберпространстве, ГКСЭ активно ведет подготовку и повышает на постоянной основе квалификацию судебных экспертов, основной деятельностью которых является проведение компьютерно-технических и иных экспертиз, связанных с исследованием цифровых носителей информации. Общая штатная численность таких сотрудников относительно невелика, но их значение для СЭД и правоохранительной деятельности в целом трудно переоценить.

Анализ правоприменительной деятельности по преступлениям в сфере высоких технологий показал, что в большинстве случаев использование специальных знаний и научно-технических возможностей таких экспертов осуществляется на последующем этапе их предварительного расследования. В то же время на первоначальном этапе основное внимание уделяется деятельности следователя по проведению им осмотра и изъятию цифрового носителя информации, на котором сохранились так называемые компьютерные улики. Для этих целей последние могут привлекать дежурных специалистов ГКСЭ, обладающих универсальной экспертно-криминалистической подготовкой.

Однако, даже несмотря на это, эффективность первоначального этапа, который, отметим, предопределяет результативность последующего, напрямую зависит от уровня знаний и подготовки следователя или лица, осуществляющего ЭКД, в области IT-технологий и информационной безопасности. Из-за непонимания сути происходящих процессов в цифровом пространстве реальная следовая картина преступления может быть искажена или не в полной мере отражена в протоколе следственного действия.

Как верно в своих трудах отметил А.Ф. Волынский: «цифровизация, будучи социальным явлением и длящимся во времени процессом, предполагает формирование высокотехнологичной системы реализации норм права и положений обширного круга наук. Для создания такой системы необходимы не ситуативное формальное взаимодействие между учеными-правоведами и представителями таких научных сфер, как прикладная математика, информатика, кибернетика, а их совместная деятельность, результаты которой могут использоваться в подготовке кадров для нужд правоохранительных органов страны в борьбе с киберпреступностью».

Другими словами, организация раскрытия и расследования высокотехнологичных преступлений проявляется через широкое использование цифровых средств фиксации, сохранения, автоматизированной обработки и исследования доказательственной и ориентирующей информации, а также через новые виды криминалистически значимой информации, фиксируемой в компьютерных средствах, системах, сетях. Для формирования новых инновационных профессиональных компетенций при подготовке следователей или специалистов необходима интеграция юридических знаний и знаний в области IT-технологий.

Как нам представляется, одной из перспективных возможностей адекватного ответа правоохранительных служб на современные вызовы такой преступности является повсеместная специализация следователей, оперативных сотрудников и, конечно же, судебных экспертов, выполняющих в дежурные сутки функции специалиста. Внедрение такой специализации в работу отечественных субъектов раскрытия и расследования преступлений должно сопровождаться, во-первых, со-

ответствующей правовой регламентацией, во-вторых предусматривать первоначальную профильную подготовку.

В этой связи представляется интересной позиция Е.Р. Россинской, которая в курс такой подготовки современного следователя или специалиста включает изучение следующих базовых направлений: 1) общие принципы работы компьютерных устройств, осведомленность об основных компонентах и их функциях; наиболее распространенные виды вычислительных устройств: компьютеры, мобильные и игровые устройства, «умные» вещи (IoT), серверы; 2) общие принципы устройства электронных носителей информации, их виды, а также осведомленность о способах хранения информации, например, на сервере в RAID-массиве, на «облаках» и пр.; 3) общее понятие о файловой системе как средстве для хранения и поиска данных; 4) принципы построения локальных сетей, понимание того, как устроена сеть Интернет (на аппаратном уровне передачи сетевого трафика и общее понимание сетевых протоколов); 5) общее понимание задач информационной безопасности как состояния защищенности компьютерной информации, таких ее свойств, как конфиденциальность, целостность, доступность, подлинность, подотчетность, безотказность и достоверность способов, методов ее обеспечения.

Исходя из вышеизложенного, на наш взгляд, заслуживает внимания опыт Следственного комитета Российской Федерации, где сохранился институт следователей-криминалистов и их специализированная подготовка. Находясь непосредственно в штатной численности следственных подразделений, они обеспечивают комплексное, системное технико-криминалистическое сопровождение расследования преступлений. При этом такие участники уголовного процесса не озадачены проведением каких-либо экспертиз, что позволяет использовать их потенциал в организации раскрытия и расследования сложных «цифровых преступлений». Несмотря на то что их деятельность, пока не нашла своего детального отражения в Уголовно-процессуальном кодексе Российской Федерации, их навыки могут положительно использоваться в отечественной следственно-экспертной практике по организации борьбы с киберпреступностью.

В заключение подчеркнем, что СЭД и ЭКД – как автономные, но взаимосвязанные виды деятельности во многом определяют эффективность всей организации раскрытия и расследования преступлений. Их развитие и совершенствование – задача государственной важности, а потому качественное ее решение не может быть обеспечено на узковедомственном (моносистемном) уровне.

УДК 343.985

А.А. Петрович

ПОВЫШЕННАЯ ЛАТЕНТНОСТЬ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

С каждым днем растет количество разнообразной информации о лицах, организациях и событиях, распространение которой третьим лицам, в зависимости от ее использования, может повлечь негативные последствия, в том числе общественно опасные последствия, предусмотренные Уголовным кодексом Республики Беларусь.

В результате развития информационной сферы любого государства, в том числе и Республики Беларусь, количество преступлений, совершенных в сфере информационной безопасности, растет волнообразно. Данное явление обусловлено самим процессом развития, в результате которого введение новых информационных технологий, переход тех или иных правоотношений в информационное пространство порождает возможность использования благ в корыстных, преступных и иных целях. Снижение же роста преступлений в данной сфере обусловлено совершенствованием введенных информационных технологий, организационными мероприятиями, снижающими виктимность пользователей, а также профилактическими мероприятиями.

При этом все больше электронных устройств, имеющих в своей структуре накопители информации и управляемые операционными системами различных видов, задействованы в общественных отношениях и хранят данные ограниченного распространения (персональные данные, сведения, относящиеся к коммерческой тайне, результаты работы специалистов в сфере проектирования, разработки в различных сферах, сведения о банковских реквизитах, контактных данных организаций и лиц и др.). Помимо этого, для повышения эффективности работы юридического лица указанные устройства часто подключены к локальным сетям, а они в последующем подключены к сети Интернет. Данный фактор существенно ускоряет обмен информацией и в целом повышает эффективность работы, но и порождает риски хищения информации или иных противоправных действий. Описанные выше устройства чаще всего становятся целью злоумышленников, так как главная цель злоумышленника – это завладение данными для последующего их использования или сбыта.

Одним из способов атаки подобных устройств является применение вредоносного программного обеспечения. При этом даже сам факт