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

разработки, распространения, использования и согласно уголовному законодательству Республики Беларусь является уголовно наказуемым деянием независимо от наступивших последствий. Однако количество преступлений, совершенных с использованием вредоносного программного обеспечения в общем числе преступлений в сфере противодействия киберпреступности невелико. Связано это в первую очередь с трудоемкостью изготовления качественного вредоносного программного обеспечения, а также с высоким уровнем латентности данного вида преступлений. Помимо этого, в настоящее время в процедуре проведения проверки, проводимой по сообщениям и заявлениям о преступлениях и уголовным делам, расследуемым по признакам состава преступлений, предусмотренных ст. 212 и гл. 31 Уголовного кодекса Республики Беларусь, совершение которых сопряжено с использованием вредоносного программного обеспечения, имеются отдельные правовые и процессуальные проблемы.

Латентность данного вида преступлений обусловлена в первую очередь неочевидностью наступления последствий в результате совершения преступлений с использованием вредоносного программного обеспечения. Чаще всего пострадавшие не осознают происходящего заражения устройств и утечки данных, а последующее использование похищенных данных часто не позволяет связать его с предшествующим хищением данных. Таким образом, совершенное преступление остается безнаказанным и при этом влияет на формирование волн новых преступлений других видов (мошенничеств, хищений денежных средств путем модификации компьютерной информации, вымогательств и др.). Ввиду большого количества информационных систем потенциально подверженных угрозам со стороны злоумышленника, использующего вредоносное программное обеспечение, находящихся во владении частных лиц и организаций, необходимо осуществление дополнительного контроля за соблюдением организациями, работающими с персональными данными, реквизитами банковских платежных карточек и счетов и иными критически важными данными, Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» и приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 «О технической и криптографической защите персональных данных».

Второй и наиболее важный проблемный вопрос касается процесса проведения исследований для выявления вредоносного программного обеспечения. Современная практика сложилась таким образом, что оперативный сотрудник или следователь при выбытии на место происшествия по сообщению или заявлению о преступлении производит

осмотр места происшествия и в случае выявления достаточных данных о заражении устройства осуществляет изъятие накопителей информации устройства и в последующем направление их в Государственный комитет судебных экспертиз для проведения компьютерно-технической экспертизы. При этом заключение эксперта не позволяет дать ответ на вопрос о наличии или отсутствии вредоносного программного обеспечения. Экспертиза предоставляет лишь информацию о том, определяется ли тот или иной файл, хранящийся на исследуемом объекте антивирусным программным средством как вредоносное программное обеспечение. Получение данной информации не требует специальных познаний, и она может быть получена в ходе проведения осмотра компьютерной информации. Ввиду чего полноценное исследование вредоносного программного обеспечения не производится. К тому же отсутствие программы в базе данных вирусных сигнатур может привести к отрицательному ответу при даче оценки программному продукту как вредоносному, что в последующем приведет к принятию незаконного решения по материалу проверки или уголовному делу. При проведении полного исследования вредоносного программного обеспечения, с процессом изучения его возможностей, возможно установление принципа работы исследуемого программного продукта, способа внедрения, результата работы. В случае использования программного средства с целью хищения данных возможно установление данных об узле получателя данных. Вся эта информация окажет существенную помощь в раскрытии подобного вида преступлений. Следовательно, необходимо совершенствование системы экспертного исследования вредоносного программного средства.

УДК 343.985

А.А. Петрович, Д.Н. Лахтиков

ТЕХНОЛОГИЯ BIG DATA И СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ ЕЕ ПРИМЕНЕНИЯ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

За последние несколько десятков лет объемы цифровых данных в мировой цифровой сфере растут в геометрической прогрессии. Сегодня количество информации, хранящейся на устройствах пользователей, серверах различных ресурсов и иных материальных носителях цифровой информации исчисляется в зеттабайтах. Это связано с неуклонно растущей ролью сети Интернет и цифрового пространства в