2. Ендольцева А.В. Поручение следователя органу дознания: проблемные вопросы в теории и практике // Вестн. Моск. ун-та МВД России. 2020. № 1. С. 91–96.

3. Есина А.С. К вопросу об исполнении поручений следователя на производство следственных действий // Вестн. Моск. ун-та МВД России. 2011. № 3. С. 128–130.

4. Паутова Т.А. Взаимодействие следователей органов внутренних дел с органами дознания при возбуждении и расследовании уголовных дел : дис. … канд. юрид. наук. Тюмень, 2005.

5. Равинский В.В. Поручение следователя органу дознания как процессуальная форма взаимодействия в свете принятия нового УПК РФ // Правовые проблемы укрепления российской государственности : сб. ст. / под ред. Ю.К. Якимовича. Томск, 2002. С. 147–150.

6. Седельников П.В. Поручение следователя органу дознания // Законодательство и практика. 2017. № 1. С. 24–28.

УДК 343.534

В.В. Кузнецов

О ПРОБЛЕМАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

С каждым годом компьютеры и телекоммуникационные системы используются все чаще и шире во всех сферах жизнедеятельности человека и государства – от решения проблем национальной безопасности, здравоохранения и управления транспортом до торговли, финансов и простого межличностного общения.

Доступность технических средств связи и возможность неограниченного допуска к сети Интернет создают устойчивые предпосылки для роста преступлений, совершаемых с использованием информационно-коммуникационных технологий, огромное количество которых остается латентным. В настоящее время достижения технического прогресса все чаще используются для совершения таких преступлений, как кибермошенничество, экономический шпионаж, хищения результатов интеллектуальной деятельности, находящихся под правовой охраной, которые приводят к негативным последствиям и потерям ресурсов общества.

Термин «киберпреступность» впервые появился в американской и западноевропейской литературе в начале 60-х гг. прошлого столетия, когда стали выявляться первые случаи совершения подобных преступлений. Согласно данным энциклопедии Britannica, первый зарегистрированный случай злоупотребления использования компьютера относится к 1958 г.

На территории бывшего СССР первое подобное преступление зарегистрировано в 1979 г. в Вильнюсе. Оператор почтовой связи Н. путем мошенничества с использованием автоматизированного программно-технического комплекса «Онега» в течение двух лет совершала хищения денежных средств, направляемых соответствующими государственными органами гражданам в качестве пенсий и пособий по старости. Одновременно с компьютерным велся обычный (ручной) учет и обработка бумажных (дублирующих) бухгалтерских документов. Несовершенство программного обеспечения «Онеги» и наличие двойной бухгалтерии, которая велась на различных (по форме представления информации) материальных носителях, позволили преступнице длительное время создавать излишки подотчетных денежных средств, изымать их из кассы и присваивать, а также уходить от ответственности. Общий ущерб, по оценке суда, составил 78 584 р.

Еще одним громким для того времени преступлением в сфере высоких технологий стало умышленное повреждение программным способом оборудования известного государственного промышленного предприятия в 1983 г. «Системный программист Волжского автозавода, занимаясь с коллегами автоматической системой для подачи механических узлов на конвейер, произвел модификацию программного обеспечения АСУ ТП главного конвейера, в результате чего произошла его остановка на трое суток. Двести автомобилей не сошли с конвейера ВАЗа, пока программисты искали источник сбоев. Ущерб исчислялся миллионами рублей в ценах 1983 г. Виновное лицо привлечено к уголовной ответственности по ч. 2 ст. 98 УК РСФСР», – написали в «Известиях» по поводу происшедшего.

В современном мире существуют различные виды киберпреступлений: экономические, против личных прав и неприкосновенности частной сферы, против общественных и государственных интересов. Все большую актуальность приобретают вопросы кибермошенничества и шантажа, информационных блокад и других методов компьютерного давления, шпионажа и передачи компьютерной информации лицам, не имеющим к ней доступа. Эти правонарушения приводят к тяжелым последствиям и потерям ресурсов общества, негативным воздействиям на информационно-вычислительные системы и линии телекоммуникаций, вызывающим их повреждения.

Киберпреступления, хотя и имеют незначительный удельный вес в общей структуре преступности, однако проявляют стойкую тенденцию к ежегодному росту. Так, количество таких преступлений в России увеличилось с 10 698 в 2014 г. до 174 674 в 2018 г. (более чем в 16 раз). По данным Генеральной прокуратуры Российской Федерации, в 2018 г.

предварительно расследовано 43 362 уголовных дел, направлено в суд – 36 767, при этом до 72 % дел прекращаются либо приостанавливаются производством. Уровень раскрываемости таких киберпреступлений ниже в сравнении с общей раскрываемостью почти в два раза (21 % против 39,5 %).

Ущерб российской экономике от киберпреступлений превышает триллионы рублей и продолжает увеличиваться. Как правило, эти преступления совершаются в финансовой сфере. В то же время наблюдается значительное расширение использования информационно-коммуникационных технологий при совершении ряда иных уголовно наказуемых деяний, в том числе террористического и экстремистского характера, коррупционной направленности, преступлений против личности, половой неприкосновенности, иных охраняемых законом прав и законных интересов.

В основном органами Следственного комитета Российской Федерации осуществляется уголовное преследование по фактам совершения преступлений с использованием информационных технологий: против установленного порядка проведения азартных игр; в сфере незаконного оборота наркотических средств; связанных с изготовлением и распространением порнографических материалов; против половой неприкосновенности и половой свободы личности; экстремистской направленности.

Как показывает практика, киберпреступления часто носят транснациональный и трансграничный характер. Жертва и злоумышленник могут находиться на территории разных государств или даже континентов, а технологии позволяют им условно быть рядом.

Независимо от вида преступлений в качестве инструментов для их совершения используются ресурсы, размещенные на серверах в странах со сложным правовым порядком обмена информацией между правоохранительными органами. При этом для российских органов правоохраны по-прежнему основными инструментами получения данных из иных стран являются международная правовая взаимопомощь и каналы обмена информацией Национального центрального бюро Интерпола. Сроки получения ответов на запросы составляют от 6 до 24 месяцев, тогда как сроки хранения информации у большинства компаний, предоставляющих ресурсы для ее размещения на сервере, постоянно находящемся в сети (услуги хостинга), не превышают 6 месяцев. Таким образом, большинство запросов изначально не результативны.

К основным проблемам, связанным с оперативностью и качественными показателями расследования киберпреступлений, относятся:

разработка законодательства с учетом бумажного документооборота, а не высокоскоростного и трансграничного обмена данными;

различный подход государств к вопросам обмена данными, отсутствие единых стандартов, протоколов и т. д.;

монопольное владение основными ресурсами сети Интернет (социальные сети, корневые узлы сети, хостинг серверов) крупными корпорациями, находящимися в иной юрисдикции;

высокая латентность выявления и регистрации киберпреступлений;

низкие объемы и скорость обмена данными между правоохранительными органами и недостаточная их цифровизация;

отсутствие достаточного количества компетентных образовательных учреждений в сфере противодействия кибератакам и борьбе с киберпреступностью;

катастрофическая нехватка компетентных в раскрытии и расследовании киберпреступлений сотрудников правоохранительных органов;

высокая по скорости и существенная по содержанию мутация моделей угроз, способов использования технологий в противоправных целях;

рост количества квалифицированных высокоорганизованных преступных кибергрупп и сообществ, в том числе кибердиверсионных и террористических (занимаются телефонными минированиями, ложными новостями, направленными на подрыв доверия к власти и свержение государственного строя, и др.).

Неоспоримым фактором в решении этих проблем является формирование единого правового поля, которое будет содержать единый понятийный аппарат и подходы к сбору, фиксации, анализу и представлению цифровых доказательств, чтобы эффективно и максимально быстро взаимодействовать правоохранительным органам различных государств.

УДК 343.98

С.В. Кузьмина

ПРОБЛЕМЫ НАЗНАЧЕНИЯ И ПРОИЗВОДСТВА СУДЕБНЫХ ЭКСПЕРТИЗ ПО ДЕЛАМ О МОШЕННИЧЕСТВАХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

В условиях цифровизации практически любые виды преступлений, в том числе мошенничества, могут совершаться с помощью телекоммуникационных средств и систем. В связи с широким использованием информационно-телекоммуникационных технологий при совершении мошенничеств существенно изменились способы осуществления указанной преступной деятельности, а также следы, образующиеся в результате подготовки, совершения и сокрытия преступления. Указанные