3. Пушкарев В.В. Понятие серии преступлений: логико-философские основания юридической терминологии // Библиотека криминалиста. Научный журнал. 2017. №5 (34). С. 163-169.

4. Пушкарев В.В. Формирование понятия и концепции уголовного преследования (обвинения) // Вестник экономической безопасности. - №3. – 2017. – С. 56-59.

5. Пушкарев В.В., Мельников С.А. Проблемы диагностики, моделирования и прогнозирования в следственной практике при расследовании серийных преступлений и направления оптимизации этой деятельности. Ч. 1 // Российский следователь. - № 11. - 2008. - С. 2-4.

6. Пушкарев В.В., Мельников С.А. Проблемы диагностики, моделирования и прогнозирования в следственной практике при расследовании серийных преступлений и направления оптимизации этой деятельности. Ч. 2 // Российский следователь. - № 12. - 2008. - С. 4-5.

7. Корнелюк В.С. Расследование хищений чужого имущества: учебное пособие. - Волгоград, 2001. -104 с.

8. Пушкарев В.В., Федяева Н.В. Особенности расследования серий квартирных краж: учебное пособие. -Волгоград, 2010. -107 с.

9. Пушкарев В.В., Скачко А.В., Хмелев С.А. Расследование вымогательств: Монография. -М., 2014. -132 с.

УДК 343.9
DOI 10.1555/2409-3203-2018-0-14-27-32

ПРОБЛЕМА РАССЛЕДОВАНИЯ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕВОГО ПРОСТРАНСТВА

Белякова Инна Михайловна
к.ю.н., доцент Департамента правового регулирования экономической деятельности
ФГБОУ ВО Финансовый университет при Правительстве Российской Федерации
Россия, г. Москва
Добрина Татьяна Борисовна
студентка 3 курса Юридического факультета
ФГБОУ ВО Финансовый университет при Правительстве Российской Федерации
Россия, г. Москва

Аннотация: Статья посвящена вопросам расследования экономических преступлений, совершенных с использованием информационных технологий и сетевого пространства. Автором проанализирована конкретная правоприменительная практика, на основе которой были выявлены недостатки и пробелы в правовой регламентации расследования киберпреступлений, в частности, возбуждения уголовного дела, процесса доказывания, применения мер уголовно-процессуального пресечения и проведения отдельных следственных действий.

Ключевые слова: уголовно-процессуальное законодательство, информационные технологии, кибепреступления, сотрудничество правоохранительных органов с международными компаниями.

THE ISSUES OF OF THE INVESTIGATION OF ECONOMIC CRIMES COMMITTED USING INFORMATION TECHNOLOGY AND NETWORK SPACE

Belyakova Inna Mikhailovna
Ph.D., Associate Professor, Department of Legal Regulation of Economic Activities
Financial University under the Government of the Russian Federation
Russia, Moscow
Dobrina Tatyana Borisovna
3-year student of the Faculty of Law
Financial University under the Government of the Russian Federation
Russia, Moscow

Abstract: The article deals with issues of the investigation of economic crimes committed using information technology and network space. It is analyzed the practice of law enforcement, identified the general problems of the investigation of high-tech crimes.

Key words: criminal procedural law, high-tech crimes, international investigation organization of cybercrime.

С начала 2000-х годов общество переживает сложный и необратимый социальный процесс – информатизацию. Ценность информации непрерывно возрастает на фоне всех остальных ресурсов. Это обусловлено в первую очередь изменением формы организации производства, которое характеризуется тем, что все данные о каком-либо процессе фиксируются в цифровой форме. В основе этого явления лежат кибернетические методы и автоматизированные средства управления. Как известно, каждое действие или явление несет в себе информационный след, а в процессе компьютеризации, – одного из значимых аспектов информатизации, - данный след обрел цифровую форму и стал доступен для восприятия посредством компьютерной обработки. Таким образом, произошел перевод некоторых повседневных процессов в виртуальную форму с целью уменьшения материальных и энергетических затрат на осуществление конкретного действия.

Внедрение компьютеров во все сферы жизни общества привело к тому, что изменился сам характер многих преступлений, появились их новые виды. Для достижения противоправных целей преступники стали активно применять компьютеры и специальную технику, создавать системы конспирации и скрытой связи в рамках системного подхода при планирования своих действий. Одновременно наблюдается резкое нарастание криминального профессионализма - количества квалифицированных по исполнению преступлений. С ростом уровня информатизации бизнеса многократно увеличивается уровень возможных финансовых потерь и рисков, а для киберпреступников растет привлекательность получения противозаконного заработка.

Ключевым фактором стремительной эволюции и развития преступности в области высоких технологий является слабая юридическая база в сфере квалификации действий и преследования хакеров в правовом поле. Недостаточное правовое урегулирование общественных отношений в области применения информационных технологий, специфичность механизма преступлений, высокая технологичность и постоянное качественное изменение способов их совершения — факторы, затрудняющие проведение

фундаментальных исследований по проблемам разработки методики расследования преступлений в сфере предоставления информационных услуг.

Судопроизводство в отношении преступлений, совершенных в виртуальной среде, разительно отличается от традиционных способов досудебного производства. Например, в рамках расследования компьютерных преступлений можно выделить такие этапы, как установление факта неправомерного доступа к информации в компьютерной системе или сети, установление места и времени несанкционированного проникновения в компьютерную систему или сеть, установление способа несанкционированного доступа. Все эти действия требуют специальной квалификации, которая в большинстве случаев отсутствует у компетентных лиц уполномоченных органов предварительного расследования, что обусловлено отсутствием обобщений материалов следственной и судебной практики, опыта работы следователей органов дознания со специфическими источниками доказательственной информации.

Целесообразно рассмотреть данную проблему на примере громкого дела о сетевом мошенничестве. Дело Братьев Попелыш стало первым в российской судебной практике делом против преступников, промышлявших фишингом — распространённым в интернете видом мошенничества. В сентябре 2012 года Чертановский суд Москвы признал виновными братьев Дмитрия и Евгения Попелыш и приговорил их к шести годам лишения свободы условно с испытательным сроком 5 лет и штрафу по 450 тысяч рублей в пользу государства с каждого. Данное дело было раскрыто лишь благодаря тому, что в процессе расследования активно принимали участие российские представители международных компаний «Лаборатория Касперского» и Group-IB, которые помогали правоохранительным органам искать преступников и доказывать их вину.

Преступную деятельность братья Попелыш начали в конце весны 2010 года. Об этом стало известно благодаря обращению представителей службы безопасности банка, клиенты которого подверглись хищению со счетов, в отдел расследования компьютерных инцидентов «Лаборатории Касперского», а также в правоохранительные органы по факту произошедших инцидентов. Практически все бремя расследования легло на представителей «Лаборатории Касперского». На все процедуры, посвященные анализу вредоносной программы и стоящей за ней инфраструктурой, а также поиску контактных данных подозреваемых ушло около двух недель. То есть тем же летом 2010 года и эксперты «Лаборатории Касперского», и правоохранительные органы знали, кто стоит за похищением денег. И на данном этапе правоохранительные органы столкнулись с формальными проблемами, решение которых из-за существующего правового вакуума в вопросе расследований компьютерных преступлений затянулось почти на 2 года.

Чтобы арестовать подозреваемого, правоохранителям нужно возбудить уголовное дело по факту совершения преступных действий. Для уголовного дела нужны основание и повод, которые четко указаны в ст. 140 УПК РФ. Технического описания мошеннической инфраструктуры и схемы действий преступников оказалось недостаточно. Чтобы подготовить материалы уголовного дела, следователи были вынуждены предоставить понятное изложение фактов и технических определений. Эта простая, на первый взгляд, задача потребовала вовлечения квалифицированных технических специалистов и их тесное взаимодействие со следствием.

На процесс составления и приобщения к делу отчетов и аналитических справок ушло почти шесть месяцев, на протяжении которых хищения продолжались, итоговый ущерб составил 13 миллионов рублей. Уголовное дело было возбуждено в январе 2011 года по признакам состава преступления, предусмотренного частью 1 статьи 273, частью 3 статьи 30 и частью 4 статьи 159 УК РФ по факту использования и распространения вредоносного программного обеспечения и дистанционного банковского обслуживания организованной группой.

С этого момента стало возможным применение меры пресечения в виде заключения под стражу. Теперь следствию предстояло подготовить все необходимые материалы для передачи дела в суд. На данном этапе технические эксперты «Лаборатории Касперского» давали разъяснения по показаниям обвиняемых, помогали переводить специфические термины на юридический язык, который бы был понятен судье. По словам криминалистов компании «Group-IB», дополнительно привлеченных в качестве экспертов, почти каждое предложение экспертных заключений требовало пошагового разбора с целью подбора наиболее четкой формулировки для «перевода» на юридический язык. На все эти процедуры ушло больше года. Первое рассмотрение дела братьев Попелыш состоялось в начале мая 2012 года в Петроградском районном суде Санкт-Петербурга. Примечательно, что, по словам экспертов, преступники не обладали высокой квалификацией в области сетевых и компьютерных технологий, а использовали уже устоявшиеся технологии кибермошенничества, что говорит о повсеместной открытости и доступности противозаконного заработка. Одновременно, если намерение совершить преступление возникнет у обученного профессионала, вероятность его раскрытия будет предельно мала.

Несмотря на то, что описанные события произошли в промежуток с 2010 по 2012 года, существенных изменений в состоянии правовой регламентации уголовного судопроизводства в отношении дел, связанных с сетевым мошенничеством, не произошло. Это объясняется тем, что специфика данных преступлений имеет абсолютно иную природу, нежели преступления, совершенные в объективной реальности. На мой взгляд, недостаточно просто совершенствовать существующую систему противодействия преступности, необходимо создание принципиально нового механизма, который мог бы обеспечить безопасность сетевых денежных операций. На данный момент расследованием киберпреступлений занимаются квалифицированные международные компании, под вниманием которых находятся незаконные операции, связанные с хищением крупных сумм, передачей и подменой информации, шпионажем, присвоением активов и интеллектуальной собственности. Однако помимо данной категории преступлений, существует множество мелких деяний, причиняющих незначительный материальный вред отдельным индивидам. Бороться с такими «мелкими делами» нет практически никакой возможности ввиду их огромного количества, потенциальной латентности группы преступлений, связанных с сетевым мошенничеством, разнообразия способов их совершения и отсутствием необходимой базы для борьбы с такими преступлениями.

Исходя из вышесказанного, очевидна необходимость повышения эффективности работы правоохранительных органов в сфере противодействия киберпреступности. Анализ статистики информационных преступлений указывает на низкую эффективность их расследования и судебного разбирательства как по причине сложности самого процесса доказывания, так и в силу несовершенства действующего законодательства. На данный момент правоохранительные органы не обладают достаточными человеческими и техническими ресурсами, а в законодательстве отсутствует специальное регулирование, необходимое для успешного расследования дел о киберпреступлениях. Так, например, сбор и фиксация доказательств по данным делам представляет собой довольно проблемный вопрос.

Доказательство по уголовному делу всегда имеет не только фактическое содержание, но и процессуальную форму получения и сохранения необходимой информации. Так, процессуальным законодательством строго регламентируется форма, в которой могут быть получены фактические данные, а конкретно: в форме объяснений сторон, третьих лиц, показаний свидетелей, письменных доказательств, вещественных доказательств и заключений экспертов. Следовательно, для того, чтобы информация на электронных носителях обладала доказательственной силой, она должна быть получена, истребована или представлена в порядке, установленном уголовно-процессуальным

законом, и должна соответствовать признакам относимости, допустимости, достоверности и достаточности. Так, в качестве доказательств по делу могут быть использованы данные, содержащиеся на техническом носителе, но только в тех случаях, когда они преобразованы в форму, пригодную для обычного восприятия и хранения в деле. Как уже стало понятно, в УПК РФ отсутствует процедура приобщения к материалам дела электронных документов в порядке п. 2 ст. 84, также как отсутствует и практически применимая формула преобразования информационных файлов в удобную для обычного восприятия информацию.

Однако проблемы возникают еще на этапе собирания доказательств. При осмотре компьютера основной целью уполномоченного лица является не фиксация всей имеющейся на нем информации, а, в первую очередь, установление обоснованных выводов о необходимости собирания с ЭВМ той или иной информации, а также проведение следственных действий в соответствии с положениями закона и в установленном порядке. Для собирания доказательств проводится обыск и выемка части документированной информации в виде LOG-файлов. Для того, чтобы компьютерная информация соответствовала признаку допустимости, необходимо обеспечить ее сохранность в том виде, в котором она была обнаружена. В случаях работы с ЭВМ это обеспечивается посредством копирования. Но скопированная информация достаточно легко может быть фальсифицирована, причем таким образом, что обнаружить внесенные изменения практически невозможно, кроме того, информация может быть удалена из первоисточника и доказать, что именно эта информация была снята с компьютера также практически невозможно. Все эти обстоятельства показывают, что такой способ получения информации как ее копирование, повышает риск ее искажения и делают недопустимым использование ее в качестве доказательства.

Таким образом, специальные нормы, регламентирующие досудебное производство в отношении дел, связанных с преступлениями, совершенными в сетевом пространстве, видятся необходимыми в связи со спецификой места, способа и масштаба совершения информационных преступлений. Особенность противодействия киберпреступности связана также с тем, что, как правило, такие преступления носят интернациональный характер и в целом не попадают под юрисдикцию конкретного государства. Так, например, преступники редко ограничиваются территорией одного государство, используя зарубежные серверы или выбирая объект посягательства вне зависимости от территории конкретной страны. В связи с этим возникают сложности при определении территориальной подследственности, которые влияют на оперативность возбуждения уголовного дела и проведения следственных действий.

Стоит отметить, что на данный момент существует несколько активных крупных группировок, которые осуществляют хищения у физических и юридических лиц в крупных размерах, а также несколько неактивных группировок, члены которой так и не были установлены и привлечены к уголовной ответственности. Но даже с учетом успешной поимки и задержания преступников обосновать их вину и доказать причастность к преступлению в рамках правового механизма привлечения к ответственности в силу уже упомянутых обстоятельств будет довольно сложно.

Из заявления Генерального прокурора России Юрия Чайки на Третьей встрече руководителей прокурорских служб стран БРИКС в Бразилии стало известно, что ущерб от киберпреступлений в России только за первое полугодие 2017 года превысил 18 миллионов долларов. На данный момент правоохранительные органы и прокуроры ориентированы на ведение мониторинга ситуации, складывающейся в интернет-пространстве, постоянное повышение квалификации сотрудников, методическое обеспечение их деятельности. Кроме того, для защиты баз данных надзорного ведомства от кибератак в прокуратуре России создано специальное подразделение - Управлению «К» МВД РФ, в задачу которого входит обнаружение вредоносного программного

обеспечения, установление и устранение причин возникновения угроз целостности, доступности и неизменности хранимой информации. На данный момент данное подразделение работает совместно со специализированными организациями, созданных целью предотвращения и расследования киберпреступлений и мошенничеств с использованием высоких технологий.

Подводя итог вышесказанному можно сделать вывод о том, что выявление, раскрытие и расследование преступлений в сфере компьютерной информации и высоких технологий по-прежнему остается одной из труднейших задач для уголовного розыска и органов предварительного расследования. Это связано с целым рядом проблем, среди которых выделяются такие, как отсутствие должного мониторинга следственной и судебной практики в области киберпреступлений, в целом незначительный опыт работы отечественных специалистов в данной сфере, некачественная подготовка следователей и сотрудников уголовного розыска, и, наконец, общая нехватка научно обоснованных и апробированных на практике методических рекомендаций по тактике и методике расследования преступлений в сфере компьютерной информации и высоких технологий.

Список литературы:

1. Пушкарев В.В. Кардинг - системообразующий фактор экономической преступности: секреты механизма и проблемы уголовного преследования // Библиотека криминалиста. Научный журнал. -2017. -№ 4(33). -С. 197-204.

2. Пушкарев В.В. Проблемы уголовного преследования при расследовании киберпреступлений, посягающих на системы и ресурсы банковского сектора // Криминалистика как наука и учебная дисциплина: история, настоящее и перспективы развития: Сборник докладов Международной научно-практической конференции, посвященной 35-летию кафедры криминалистики Института права БашГУ // Под общ. ред. И.А. Макаренко. – Уфа: РИЦ БашГУ, 2017. - С. 104-111.

3. Пушкарев В.В. Актуальные проблемы расследования кардинга // Право и экономика: междисциплинарные подходы в науке и образовании. IV Московский юридический форум. IIX Международная научно-практическая конференция (Кутафинские чтения. 6 апреля 2017 года). - Часть 3. - Москва, 2017. - С. 230-239.

4. Group-IB//[Электронный ресурс]. URL: https://www.group-ib.ru/

5. Куфтерин А.Н., Пушкарев В.В. Расследование преступлений экономической направленности и коррупционных преступлений: учебное пособие. Рязань, 2016. 75 с.

6. Тришкина Е.А. Правовое регулирование института специальных знаний, используемых в процессе уголовного судопроизводства по делам об экономических преступлениях (настольная книга юриста). -Волгоград, 2007. -386с.

7. Макаренко М.М., Пушкарев В.В. Проблемные вопросы возбуждения уголовных дел о преступлениях в сфере оборонно-промышленного комплекса // Организационно-управленческие механизмы антикоррупционной деятельности (российский и зарубежный опыт): сборник тезисов докладов и статей V международной научно-практической конференции российских и зарубежных университетов и РЭУ им. Г.В. Плеханова при участии представителей государственных и муниципальных органов власти 25.09.2017 / кол. авторов ; сост. Е.Ю. Халатенкова. — Москва : РУСАЙНС, 2017. — С. 128-131.

8. Уголовное дело № 1-486/2012//Архив Чертановского районного суда г. Москвы.

9. Тришкина Е.А., Пушкарев В.В. Некоторые типичные способы хищений товарно-материальных ценностей и денежных средств в бюджетных учреждениях // В сборнике: актуальные проблемы современной юриспруденции: Электронный сборник материалов Международной научно-практической конференции магистрантов, аспирантов, студентов и молодых ученых. - Липецк: Институт права и экономики, 2017. - С. 229-232.