ПРОБЛЕМЫ ОСУЩЕСТВЛЕНИЯ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СОВЕРШАЕМЫХ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Н. П. КИРИЛЛОВА,* С. П. КУШНИРЕНКО**

В статье рассмотрен комплекс проблем, определяющих уровень эффективности противодействия преступлениям, совершаемым в сфере высоких информационных технологий. Проанализированы уровень преступности в Российской Федерации и за рубежом. Приведенные в статье статистика и анализ экспертных оценок свидетельствуют о высоком уровне латентности преступности в сфере высоких информационных технологий. Анализируются причины этого явления. В статье делается вывод о том, что главной особенностью, порождающей многие проблемы в раскрытии и расследовании этих преступлений, является особая среда, в которой они совершаются. Особая среда определяет специфический механизм совершения преступления и своеобразное следообразование, вызываемое особенностями цифровой информации, обрабатываемой с помощью компьютерного оборудования и передаваемой посредством информационно-телекоммуникационных сетей. В связи с этим основное внимание уделено использованию специальных знаний в раскрытии и расследовании рассматриваемых преступлений. Анализируются уголовно-процессуальные проблемы производства отдельных следственных действий, связанных с изъятием электронных носителей информации. Дается анализ изменений уголовно-процессуального законодательства, регулирующего процедуру обыска, выемки, осмотра и иных следственных действий. Рассмотрен ряд проблем международного сотрудничества в сфере противодействия киберпреступности и возможности имплементации международно-правовых норм в российское законодательство.
КЛЮЧЕВЫЕ СЛОВА: преступления, совершаемые в сфере высоких информационно-коммуникационных технологий, анализ судебно-следственной практики, уровень латентности, изъятие электронных носителей информации, снятие информации с технических каналов связи, международное сотрудничество.

* Кириллова Наталья Павловна — доктор юридических наук, профессор кафедры уголовного процесса и криминалистики СПбГУ.
Kirillova Natalia Pavlovna — Doctor of legal sciences, professor of the Department of Criminal Procedure and Criminalistics, St. Petersburg State University.
E-mail: Kirillova59@mail.ru
** Кушниренко Светлана Петровна — кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики СПбГУ.
Kushnirenko Svetlana Petrovna — candidate of legal sciences, associate professor of the Department of Criminal Procedure and Criminalistics, St. Petersburg State University.
E-mail: fotina58@mail.ru

KIRILLOVA N. P., KUSHNIRENKO S. P. THE PROBLEMS OF THE CRIMINAL PROSECUTION IN THE SPHERE OF CYBER CRIMES
The article is devoted to a complex of problems that define the level of efficiency of the cyber crime prevention. The crime rate in the Russian Federation and in foreign countries has been analyzed. The statistics and the analysis of expert evaluations demonstrate the high level of latency in cyber crimes. The reasons for these facts are analyzed. The article contains the conclusion regarding the fact that the particular environment in which the crimes are committed is the main peculiarity that causes many problems in crime detection and investigation. The specific mechanism of commission of a crime and the original marking formation is determined by this particular environment. The marking formation is caused by the peculiarities of the digital information processed by computer equipment and transferred by information and telecommunication networks. Therefore, main attention is devoted to the use of special knowledge in crime detection and investigation. The authors analyze the problems of the investigative proceedings related to withdrawal of electronic media. They also provide the analysis of amendments in the criminal procedural law which regulate the search, seizure, examination procedure, and other investigative proceedings. The authors examine many problems in the international cooperation in the sphere of cyber crime prevention and the possibility of implementation of international legal regulations into the Russian legislation.
KEYWORDS: cyber crimes, court practice analysis, level of latency, withdrawal of electronic media, withdrawal of information from communication channels, international cooperation.

Информационные технологии органично вошли во все сферы современной жизни, став привычными и неотъемлемыми спутниками человека. По данным Минкомсвязи России, число интернет-пользователей в 2011 г. выросло на 5,4 % и достигло 70 млн чел., что позволило России обогнать по этому показателю Германию и выйти на первое место в Европе.[1] По сравнению с 2010 г. темп уменьшился, но аудитория продолжает увеличиваться; по прогнозу Минкомсвязи, в 2013 г. россиян, пользующихся глобальной сетью, станет около 90 млн. Россия уже вошла в первую десятку стран мира по развитию широкополосного доступа в Интернет (далее — ШПД). Она признана наиболее быстро растущей страной по темпам прироста пользователей: ежегодный прирост оценивается более чем в 2 млн чел. — это более чем 20-процентное увеличение в сравнении с 12-процентным приростом в мире. Темпы роста рынка ШПД в России продолжают увеличиваться: к концу 2011 г. этот показатель составил 40 линий на 100 жителей, а к 2015 г. прогнозируется увеличение до 60 линий на 100 жителей. Наибольший объем рынка занимает ШПД по кабельным линиям связи, однако в ближайшие годы наряду с ним широкое развитие получит ШПД по эфиру (радиодоступ) и с помощью спутниковых систем, работающих в Ка-диапазоне. В 2011 г. общее количество персональных компьютеров составило 74,4 млн шт., что на 20,2 % больше, чем в 2010 г. К 2013 г. оснащенность ПК должна составить 62,4 шт. на 100 чел. (всего около 89 млн шт.).

Количество киберпреступлений в России, зарегистрированных правоохранительными органами в 2012 г., выросло почти на треть (28 %) по

[1] *Число* интернет-пользователей в РФ в 2011 г. выросло до 70 млн человек // www.ria.ru/science/20111226/527204414.html.

сравнению с 2011 г. Было выявлено на 70 % больше, чем в предыдущем году, самых массовых и прибыльных видов киберпреступлений — интернет-мошенничеств и хищений денег из систем дистанционного банковского обслуживания (ДБО), а также со счетов физических лиц в банках: 3645 преступлений против 2123 в 2011 г.[2] Эксперты отмечают, что системы ДБО наиболее часто подвергаются кибератакам. Заместитель директора департамента регулирования расчетов Банка России Андрей Курило подтвердил тенденцию роста попыток мошенничества в пределах 20 % в год.[3]

Между тем законодатель отреагировал на рост мошенничества с использованием информационных технологий весьма своеобразно. Федеральный закон от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ»[4] ввел новый состав преступления — мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). При этом санкция за данный вид преступления существенно снижена. При сравнении ч. 3 ст. 159 УК РФ, предусматривающей ответственность за «простое» мошенничество, с ч. 3 ст. 159.6 УК РФ очевидно, с одной стороны, существенное снижение максимальной санкции, с другой — значительное снижение (в шесть раз) размера крупного и особого крупного размера ущерба. Кроме того, указанным Законом ст. 159.6 УК РФ отнесена к делам частно-публичного обвинения. Такая либерализация уголовного и уголовно-процессуального законодательства вряд ли будет способствовать эффективному противодействию рассматриваемым преступлениям.

По оценкам экспертов, реальное число интернет-мошенничеств в несколько раз выше, так как эти преступления характеризуются высоким уровнем латентности. Отмечается увеличение числа преступлений с использованием систем дистанционного банковского обслуживания.[5]

Компания *Symantec* опубликовала результаты опроса, проведенного в рамках ежегодного исследования *Norton Cybercrime Report*. По оценке компании, в 2012 г. от действий киберпреступников пострадали 556 млн участников «Всемирной паутины». Их совокупные потери составили 110 млрд долларов. Исследование, в ходе которого в июле 2012 г. были опрошены 13 тыс. чел. в возрасте 18–64 лет в 24 странах, показало, что жертвами киберпреступлений за истекший период оказались 46 % опрошенных, сумма индивидуальных убытков в среднем составила 197 долларов. Общее число жертв и суммарный ущерб по странам эксперты получили методом экстраполяции. По оценке *Symantec*, сумма ущерба в Китае составила 46 млрд долларов, в США — 21 млрд, в Западной Европе — 16 млрд, в том числе в Германии — 3,67 млрд, во Франции — 3,25 млрд, в Великобритании — 2,9 млрд долларов. У россиян в результате киберпреступлений похищено 2 млрд долларов, однако процент жертв в России оказался самым высоким — 92 %, что эквивалентно 30 млн чел. Высок этот показатель в Китае (84 %) и ЮАР (80 %). В Германии число

[2] *Киберпреступность* в России в 2012 г. увеличилась на треть // www.interfax.ru/russia/news.asp?id=288729.

[3] *Системы* дистанционного банковского обслуживания наиболее часто подвергаются кибератакам // www.securitylab.ru/news/441787.php.

[4] СЗ РФ. 2012. № 49. Ст. 6752.

[5] *МВД*: Интернет-мошенничество является одним из самых популярных киберпреступлений // www.osp.ru/news/2012/1002/13015095.

жертв составило 15 млн, в Великобритании — 12,5 млн, во Франции — свыше 10 млн чел.[6]

Наиболее распространены в мире киберпреступности вредоносные программы и вирусы, которые затронули 54 % опрошенных. От онлайн-мошенничества пострадали 11 %, жертвами фишинга (использования в мошеннических целях поддельных сайтов или рассылки сообщений со ссылками на такие сайты) стали 10 %, и 10 % подверглись атакам на мобильные телефоны.[7] Общие мировые затраты, связанные с киберпреступностью, превышают комбинированное воздействие на всемирную экономику контрабанды и торговли марихуаной, героином и кокаином. В докладе Пентагона, подготовленном для Конгресса США в ноябре 2011 г., приводится сумма в 1 трлн долларов — примерный ущерб, нанесенный компьютерными взломщиками оборонной промышленности США.[8] Как отмечает ведущий консультант *Norton* в области кибербезопасности А. Палмер, существует серьезная разобщенность во взглядах людей на угрозы киберпреступности. За последние 12 месяцев в три раза больше взрослых пострадали от онлайн-преступлений по сравнению с офлайн-преступностью, однако менее 1/3 респондентов считают, что в следующем году будет существовать бóльшая вероятность стать жертвой киберпреступлений, нежели столкнуться с преступлениями в повседневной жизни.[9]

Прогнозы угрожающие, но соответствуют ли они статистическим показателям выявления и расследования преступлений, совершаемых в сфере информационных технологий?

В соответствии с Алгоритмом формирования показателей по статистической форме отчетности 1-ВТ (код 615) «О преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации»[10] преступлениями, совершаемыми в сфере высоких технологий (форма 615 статистических отчетов Главного информационно-аналитического центра (ГИАЦ) МВД России), признаются преступления, совершаемые в отношении компьютерной информации (ст. 272–274 УК РФ), а также иные преступления, совершаемые с использованием информационно-коммуникационных технологий, среди которых статистическому учету и обработке подлежат преступления, предусмотренные ч. 2–3 ст. 129 УК РФ («Клевета»), ч. 2 ст. 130 («Оскорбление»), ст. 134 («Половое сношение и иные действия сексуального характера с лицом, не достигшим 16-летнего возраста»), ст. 135 («Развратные действия»), ст. 137 («Нарушение неприкосновенности частной жизни»), ч. 1–3 ст. 138 («Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»), ст. 146 («Нарушение авторских и смежных прав»), ст. 158 («Кража»), ст. 159 («Мошенничество»), ст. 160 («Присвоение или растрата»), ст. 163 («Вымогательство»), ст. 165 («Причинение имущественного ущерба путем обмана или злоупотребления доверием»), ст. 171 («Незаконное предпринимательство»), ст. 183 («Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»), ст. 187 («Изготовление

[6] *Никитина Т.* Киберпреступники украли у юзеров сто миллиардов // www.securelist.com/ru/blog/207764206.

[7] *Киберпреступность* масштабнее, чем наркоторговля // www.xakep. ru/post/56737.

[8] *Пентагон* готов ответить ударами на атаки хакеров // http://news.mail.ru/politics/7343875/?state=91&frommail=1.

[9] *Киберпреступность* масштабнее, чем наркоторговля // www.xakep. ru/post/56737.

[10] Материал для служебного пользования, не публиковался. Приводится по внутренним данным ГУВД по СПб и Ленинградской области.

или сбыт поддельных кредитных либо расчетных карт и иных платежных документов»), ст. 188 («Контрабанда»), ст. 242 («Незаконное распространение порнографических материалов или предметов»), ст. 242.1 («Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»), ст. 324 («Приобретение или сбыт официальных документов и государственных наград»), ст. 327 («Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков»).

Проведенный нами анализ статистических данных за 2006–2012 гг. показал, что уровень преступности в сфере высоких технологий в Санкт-Петербурге не демонстрирует тенденций к значительному росту и остается приблизительно на одном уровне. Количество зарегистрированных преступлений держится в пределах от 60 до 116 в год. Распределение зарегистрированных преступлений в сфере высоких технологий по отдельным годам можно видеть на графике 1.

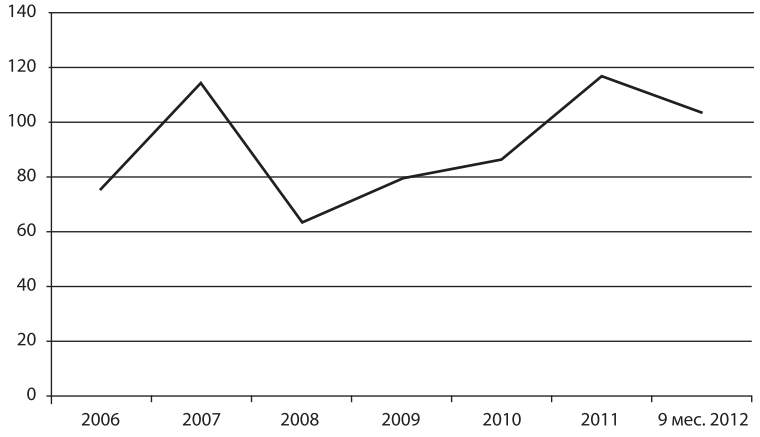

График 1. Распределение зарегистрированных преступлений в сфере высоких технологий

Эти тенденции в целом соответствуют уровню преступности в сфере высоких технологий на территории РФ, который отражен на графике 2.[11]

На фоне всероссийских показателей уровень преступности в сфере высоких технологий в Санкт-Петербурге и тем более в Ленинградской области признать высоким нельзя. Тем не менее разнообразие преступлений изучаемой группы и стабильность проявления некоторых ее видов позволяют судить о значительной общественной опасности исследуемых преступлений.

Проанализированная нами судебно-следственная практика и интервью со специалистами позволяют выразить предположение, согласно которому и общая российская статистика, и статистика по Санкт-Петербургу не отражают истинного положения дел в рассматриваемой сфере ввиду

[11] При составлении графика использованы формы Ф. 1-ВТ, 1-А, 615 ГИАЦ МВД России (материал для служебного пользования, не публиковался).

График 2. Уровень преступности
в сфере высоких информационных технологий (ВИТ)
на территории РФ (данные за 2012 и 2013 гг. отсутствуют)

высокой латентности преступлений в сфере высоких технологий. По некоторым оценкам экспертов, латентными остаются около 80 % преступлений, совершаемых в сфере высоких технологий.[12] По данным С. М. Иншакова, под руководством которого проводилось исследование латентности различных видов преступлений, за 8 лет (2002–2009 гг.) прирост зарегистрированных преступлений, предусмотренных ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), составил 156 %, прирост латентных преступлений этого вида за тот же период составил 9,6 %, коэффициент латентности — 4,8. Прирост зарегистрированных преступлений, предусмотренных ст. 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ»), за указанный период (к 2002 г.) — 553 %, прирост латентных преступлений этого вида за тот же период составил 16,2 %, коэффициент латентности — 11,8. Прирост зарегистрированных преступлений, предусмотренных ст. 274 УК РФ («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»), составил минус 37,5 %, прирост латентных преступлений этого вида — 35,5 %, коэффициент латентности — 30,0.[13]

Для того чтобы предложить совокупность адекватных мер по противодействию рассматриваемому виду преступлений, необходимо понимать их объективную распространенность, типологию, а следовательно, представлять, с какими проблемами связана столь высокая их латентность.

[12] *Сухаренко А. Н.* Транснациональные аспекты российской организованной киберпреступности // Информационное право. 2009. № 3. С. 28–31.

[13] *Теоретические* основы исследования и анализа латентной преступности / под ред. С. М. Иншакова. М., 2011. С. 481–486.

Как известно, латентность может быть естественной и искусственной. Естественная представляет собой совокупность преступлений, о факте совершения которых не известно ни правоохранительным органам, ни представителям учреждений и организаций, ни отдельным гражданам. О преступном событии осведомлены только виновные и их соучастники, т. е. лица, не заинтересованные в разглашении сведений о происшедшем и, соответственно, не желающие подвергаться уголовному преследованию. Такой вид латентности характерен для детально спланированных преступлений, при совершении которых заранее продуманы и использованы способы сокрытия, применена маскировка преступных действий под осуществление обычного процесса либо под технические сбои или неполадки.

Искусственную латентность составляют преступления, о совершении которых известно, но они не попадают в официальную статистику. Обстоятельства таких преступлений могут быть известны отдельным лицам (руководителям учреждений, организаций, гражданам), но они не заявляют об этом в правоохранительные или иные уполномоченные органы по различным мотивам: стремясь скрыть преступные факты, так как их выявление может нанести вред имиджу и престижу организации (учреждения) или ее руководителям, в том числе повлечь для них дисциплинарную, административную или уголовную ответственность за халатность; проявляя безразличие к своему гражданскому долгу; ожидая вознаграждение за недонесение; не желая тратить время и усилия на участие в предварительном следствии и судебном разбирательстве и др. Разновидностью искусственной латентности может быть невключение в статистику преступлений, о которых правоохранительным органам известно от пострадавших и очевидцев, но которые не учтены по инициативе должностных лиц. Такая ситуация может складываться по разным причинам. Во-первых, это происходит в случаях, когда уполномоченное лицо дало неправильную юридическую оценку полученной информации о событии, оценив его как некриминальное происшествие, в связи с чем оно не вошло в статистический учет. Во-вторых, может иметь место недобросовестность должностного лица правоохранительного органа, по различным мотивам умышленно сокрывшего выявленное происшествие от учета.

Говоря о латентности преступлений в сфере высоких информационных технологий, следует акцентировать внимание на том, что для нее одинаково характерны все перечисленные разновидности. Это обстоятельство заставляет провести более глубокое исследование перечисленных проблем, выявить мотивы, по которым субъекты способствуют поддержанию столь высокого уровня искусственной латентности. Особую озабоченность вызывают мотивы, руководствуясь которыми пострадавшие от преступлений в сфере высоких информационных технологий лица не сообщают об инцидентах в правоохранительные органы. По нашим данным, такая разновидность искусственной латентности значительно преобладает над невключением в статистику информации о преступлениях, ставшей известной правоохранительным органам.

Нами установлены наиболее распространенные мотивы поведения лиц, потерпевших от совершения киберпреступлений, которые приводят к увеличению уровня латентности данных преступлений. В частности, пострадавший не обращается в правоохранительные органы, поскольку причиненный ему ущерб субъективно, по его оценке, представляется незначительным. Среди граждан распространено мнение, что обращение, как правило, не дает необходимого результата, но сопряжено с затратой значительного количества личного времени. Таким мотивом руководствуются,

например, в случае мошеннических действий в Интернете, когда при обращении к некоторым сетевым ресурсам пользователя склоняют к оплате доступа, скажем, путем оплаты через мобильную связь. Пострадавшие убеждены в невозможности раскрыть преступление и наказать виновных, а также возместить ущерб, причиненный киберпреступлением.

Мотивом отказа от обращения в правоохранительные органы может быть осознание пострадавшим того, что он сам по разным причинам не обеспечил достаточного ограничения доступа к информации.

Существенным мотивом может являться нежелание огласки обстоятельств частной жизни пострадавшего, его служебной деятельности, желание скрыть информацию компрометирующего характера, в том числе свидетельствующую о допущенных им правонарушениях, что неизбежно в случае расследования преступления.

Для руководителей коммерческих организаций мотивом, по которому скрывают от правоохранительных органов и общественности событие преступления, является боязнь огласки фактов неправомерного доступа к компьютерной информации организации в результате недостаточности мер по компьютерной безопасности и, как следствие, оттока клиентуры. Примером может служить деятельность коммерческих банков, которые предпочитают проводить собственное расследование кибератак вплоть до возмещения пострадавшим клиентам суммы ущерба, причиненного в результате мошеннических транзакций и манипуляций преступников с их счетами.

Жертвам киберпреступлений, как правило, известно, что расследование неизбежно влечет за собой ряд негативных последствий, связанных с применением мер процессуального принуждения. В частности, отрицательно могут сказаться на деятельности организации изъятие средств вычислительной техники и иных электронных носителей информации для производства экспертизы, приостановление работы на время выполнения объемных следственных действий, например, осмотров места происшествия, выемок документов и предметов. В ходе расследования могут быть выявлены налоговые, финансовые, коррупционные и иные правонарушения, допущенные потерпевшим. Кроме этого, жертвы преступлений не исключают возможности незаконной утечки конфиденциальной информации по вине сотрудников правоохранительных органов. Изложенное сдерживает пострадавшего от обращения за помощью в компетентные органы.

Поводом для возбуждения уголовного дела о преступлении в сфере высоких технологий может служить заявление не только потерпевшего, но иных лиц. Обнаружить запрещенный контент, вредоносные программы, факты нарушения авторских прав на программы для ЭВМ и базы данных, видеоролики с записями совершенных преступлений и других преступных проявлений может неопределенный круг лиц. В идеале это должно повлечь за собой многочисленные сообщения граждан в компетентные органы для принятия соответствующих мер. Однако этого не происходит в связи с тем, что в обществе, особенно среди молодежи, наблюдается героизация личности киберпреступников, приписывание им черт высокоинтеллектуальности, благородства, бесстрашия.

Общественность часто воспринимает киберпреступников как способных молодых людей, смело высказывающих свое мнение и бросающих вызов властям, отнимающих средства у тех, кто добыл их нечестным путем, современных «Робин Гудов». Фигуры некоторых киберпреступников стали знаковыми и популярными. Так, один из первых киберпреступников, совершивших банковское мошенничество в отношении американского

Сити-банка с территории России, М. Левин после осуждения в США и последующей депортации издал целый ряд книг с инструкциями по осуществлению неправомерного доступа к компьютерной информации, которые в Российской национальной библиотеке может получить и прочесть любой желающий, в том числе в открытом доступе молодежного зала.[14] Ставший героическим образ американского киберпреступника К. Митника, осужденного еще в 1999 г., до сих пор будоражит воображение его поклонников. Продолжают выходить книги и статьи о нем, а также его собственные мемуары. Последняя из таких книг была издана в России совсем недавно.[15]

По нашему убеждению, латентность киберпреступлений влечет за собой крайне негативные последствия. В частности, она значительно искажает представления о фактических размерах преступности в сфере высоких информационных технологий, ее состоянии, структуре, динамике, величине и характере ущерба, причиненного потерпевшим физическим и юридическим лицам, что затрудняет, а порой делает невозможной выработку адекватной стратегии борьбы с рассматриваемым видом преступлений.

Высокий уровень латентности уменьшает степень достоверности прогнозов преступности в сфере высоких информационных технологий и, соответственно, затрудняет разработку адекватных мер профилактики указанных преступлений, не позволяет определить комплекс эффективных мер противодействия им.

Сокрытие преступлений от учета исключает уголовное преследование и, соответственно, препятствует реализации принципа неотвратимости ответственности.

Приведенная нами выше статистика расследованных и рассмотренных судами уголовных дел о киберпреступлениях свидетельствует о наличии лишь небольшого эмпирического материала, недостаточного для разработки полноценных методик расследования. Сегодня ученые-криминалисты предлагают только ряд частных методик расследования некоторых разновидностей преступлений в сфере высоких технологий,[16] что является

[14] См., напр.: *Левин М. Д.* 1) Руководство для хакеров (Сер. «Карманный атрибут компьютерщика»). Красноярск, 2000; 2) Как стать хакером. Самоучитель. М., 2002; 3) Как стать хакером. Интеллектуальное руководство по хакингу и фрикингу. М., 2005; 4) Как стать хакером. Войдите в мир хакеров (Компьютер без проблем). М., 2005; 5) Методы хакерских атак (Хитрости и тонкости). М., 2001; 6) Хакинг с самого начала: методы и секреты (Руководство по работе: советы, хитрости, трюки и секреты). М., 2001; 7) E-mail «безопасная»: взлом, «спам» и «хакерские» атаки на системы электронной почты Internet (Сер. «Мой компьютер»). М., 2002; 8) Библия хакера (Сер. «Популярный компьютер»). М., 2002; и др.

[15] *Митник К., Саймон У. Л.* Призрак в сети: мемуары величайшего хакера. М., 2012.

[16] См., напр.: *Андреев Б. В., Пак П. Н., Хорст В. П.* Расследование преступлений в сфере компьютерной информации (Библиотека криминалиста). М., 2001; *Вехов В. Б., Попова В. В., Илюшин Д. А.* Тактические особенности расследования преступлений в сфере компьютерной информации. Науч.-практ. пособие. 2-е изд., доп. и испр. М., 2004; *Вехов В. Б.* Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов. Монография. Волгоград, 2005; *Кушниренко С. П., Щепельков В. Ф.* Нарушение авторских прав на программы для ЭВМ и базы данных. Квалификация, расследование, доказывание. Учеб. пособие. СПб., 2008; *Мещеряков В. А.* Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002; *Рогозин В. Ю.* Особенности расследования и предупреждения преступлений в сфере компьютерной информации. Учеб. пособие. Волгоград, 2000; *Соловьев Л. Н.* Вредоносные программы: расследование и предупреждение преступлений. М., 2004; и др.

первым шагом к созданию родовой методики, необходимость которой назрела.

Не затрагивая в данной статье вопрос о структуре родовой методики, отметим наиболее важную особенность таковой применительно к группе преступлений, совершаемых в сфере высоких информационных технологий. Главной особенностью, порождающей многие проблемы в раскрытии и расследовании этих преступлений, является особая среда, в которой они совершаются, обусловливающая специфический механизм совершения преступления и своеобразное следообразование, вызываемое особенностями цифровой информации, обрабатываемой с помощью компьютерного оборудования и передаваемой посредством информационно-телекоммуникационных сетей.

В связи с изложенным особую актуальность в процессе расследования приобретает использование специальных знаний. Они требуются на всех этапах расследования, поскольку криминалистическая характеристика рассматриваемой группы преступлений обусловливается фактором постоянного поступательного движения в развитии информационных технологий, коммуникационных систем, компьютерных средств и электронного оборудования.

Одним из способов использования специальных знаний в уголовном процессе является привлечение специалиста к производству следственных действий для оказания помощи следователю при обнаружении, изъятии, фиксации следов преступления. Несмотря на рекомендации, разработанные криминалистами, следователи зачастую осуществляли изъятие компьютерной информации без участия специалиста, изымали носители с информацией, не имеющей отношения к предмету доказывания. Продолжительные сроки расследования, длительное производство компьютерно-технических экспертиз влекли за собой негативные последствия для владельцев изъятых носителей компьютерной информации. В частности, изъятие компьютерного оборудования у юридических лиц на неопределенный период значительно затрудняло или даже приостанавливало их деятельность, причиняя неоправданный ущерб.

Следственной практике известны случаи, когда обладатели информации не могли получить даже сведений о месте нахождения изъятых у них объектов по причине соединения уголовных дел, перенаправления материалов дел по подследственности и по иным причинам. В результате изъятые объекты либо возвращались частично, либо вообще не возвращались. Безусловно, такая ситуация существенно нарушала права участников уголовного процесса.

Факт изъятия компьютерной информации без участия специалиста использовался защитой для оспаривания полученных доказательств. Обосновывая свою позицию относительно признания доказательств недопустимыми, сторона защиты нередко ссылалась на то, что в ходе изъятия носителей компьютерной информации в нее были внесены изменения и, таким образом, сфальсифицированы доказательства. Обобщение судебно-следственной практики показало, что суды в ряде случаев соглашались с позицией защиты и признавали значимые для дела доказательства недопустимыми.

Ученые-криминалисты в своих рекомендациях по методике расследования предлагали использовать помощь специалистов при производстве следственных действий, связанных с изъятием информации на электронных носителях, в тех случаях, если имеется техническая возможность внесения в нее изменений, а также для изучения этой информации с точки зрения ее относимости к предмету доказывания. Например, с участием

специалиста рекомендуется изымать встроенные и выносные накопители на жестком магнитном диске, флэш-память и другие аналогичные носители. В то же время изъятие электронных носителей информации может быть осуществлено без риска неправильного обращения с объектом, а значит, и без участия специалиста. Например, по делам о преступлениях, предусмотренных ст. 146 УК РФ («Нарушение авторских и смежных прав»), следователь изымает «пиратские» диски. Разумеется, правовой вопрос о том, является ли продукция контрафактной, решается только после экспертного исследования. Аналогичным может быть подход к изъятию CD и DVD с порнографическими изображениями при расследовании преступлений, предусмотренных ст. 242 УК РФ («Незаконные изготовление и оборот порнографических материалов или предметов»).

Однако если в ходе следственного действия следователь установит наличие носителя, в информацию на котором могут быть внесены изменения, помощь специалиста необходима. В случае его отсутствия следователю целесообразно приостановить следственное действие и обеспечить участие специалиста.

Оценивая содержание ст. 182–183 УПК РФ, можно сделать вывод о том, что законодатель не различает электронные носители информации, в которые могут быть внесены изменения (а значит, их осмотр требует участия специалиста), и те, которые могут быть осмотрены и изъяты следователем самостоятельно.

Федеральным законом от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в УПК РФ»[17] введено обязательное участие специалиста в изъятии электронных носителей информации при обыске и выемке, а также предусмотрены дополнительные гарантии прав законных владельцев информации. Положения ч. 4 ст. 81 и п. 5 ст. 82 УПК РФ обеспечивают возврат изъятых в ходе досудебного производства, но не признанных вещественными доказательствами электронных носителей информации. Следует приветствовать обеспечение прав законных владельцев средств вычислительной техники возможностью требовать копирования компьютерной информации после производства неотложных следственных действий в случае невозможности возврата изъятых электронных носителей информации их владельцу (ч. 2-1 ст. 82 УПК РФ).

В соответствии с ч. 9-1 ст. 182 и ч. 3-1 ст. 183 УПК РФ при производстве обыска и выемки электронные носители информации изымаются с участием специалиста. Хотя законодатель не определил характер специальных знаний, которыми должен обладать такой участник, из контекста статьи следует, что таковым должно быть лицо, сведущее в обращении с электронными носителями информации, которые отныне должны изыматься только с его участием.

По ходатайству законного владельца изымаемых электронных носителей информации специалистом, участвующим в обыске или выемке, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации на другие электронные носители, предоставленные их законным владельцем. Владельцу передается копия, о чем в протоколе делается запись. При производстве обыска или выемки не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации.

[17] СЗ РФ. 2012. № 31. Ст. 4332.

Учитывая приведенные выше аргументы ученых-криминалистов, можно высказать предположение о том, что необходимость привлечения специалиста возникает не во всех случаях. Представляется, что законодателю было бы целесообразно оставить вопрос о привлечении специалиста на усмотрение следователя, уточнить редакцию ст. 182–183 УПК РФ, конкретизировав случаи обязательного участия специалиста.

Кроме того, остается неясным, почему законодатель включил норму об участии специалиста в статьи, регламентирующие только обыск и выемку. В следственной практике изъятие электронных носителей информации осуществляется, помимо этих следственных действий, в ходе осмотра места происшествия (ст. 176 УПК РФ), проверки показаний на месте (ст. 194 УПК РФ), личного обыска (ст. 184 УПК РФ). Буквальное толкование приведенных норм позволяет сделать вывод о том, что при изъятии электронных носителей информации в ходе этих следственных действий специалист не требуется. Соответственно, в этих случаях не будут обеспечены права владельцев электронных носителей информации.

Интервьюирование следователей, специализирующихся на расследовании преступлений в сфере высоких информационных технологий, показало, что вступление в силу Федерального закона от 28 июля 2012 г. № 143-ФЗ не повлияло на следственную практику, по крайней мере в течение трех месяцев его действия. Следователи продолжали изымать соответствующие объекты без участия специалистов, когда отсутствовали технические возможности внесения изменений в информацию. Дополнительным мотивом прямого нарушения уголовно-процессуального закона являлось отсутствие достаточного количества специалистов нужного профиля.

В этом вопросе следователей поддерживали и государственные обвинители, которые, как следует из их интервью, готовы были отстаивать в суде доказательства, полученные без участия специалиста. Например, если накопитель на жестком магнитном диске был изъят следователем без предварительного осмотра информации, упакован и опечатан надлежащим образом, что исключало внесение в него изменений, то, с точки зрения государственного обвинителя, такой объект может быть признан допустимым доказательством.

Таким образом, можно сделать вывод о том, что несовершенство уголовно-процессуального закона в некоторых случаях влечет за собой его нарушение на практике.

Большинство специалистов констатирует отставание процессуальных норм от условий информационного общества, в обстановке которого совершаются преступления и протекает процесс расследования.[18]

Важно не только адаптировать уже имеющиеся следственные действия к современным условиям, но и ввести дополнительные, необходимые для поиска, резервирования, фиксации и изъятия цифровых данных, например, арест электронно-почтовой корреспонденции.

Положения ст. 185 УПК РФ, регламентирующей наложение ареста на почтово-телеграфные отправления, нельзя применить к корреспонденции, передаваемой по электронной почте. Обмен письмами и телеграфными

[18] См., напр.: *Волеводз А. Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002; *Осипенко А. Л.* Особенности расследования сетевых преступлений // СПС «КонсультантПлюс»; *Усов А. И.* Концептуальные основы судебной компьютерно-технической экспертизы. Автореф. дис. … д. ю. н. М., 2002. С. 14; и др.

сообщениями между гражданами в значительной мере заменила возможность обмена информацией посредством таких сервисов, как электронная почта, *ICQ*, *Skype* и др. Для ареста подобной информации должны быть разработаны и приняты соответствующие нормы, позволяющие следствию получать не только доказательства факта соединений между абонентами, но и содержание сообщений, имеющих значение для дела.

Анализ нормативных правовых актов позволяет сделать однозначный вывод о том, что технические возможности для реализации подобной нормы уже разработаны и применяются, правда, для решения задач оперативно-розыскной деятельности. Например, организации связи предоставляют уполномоченным органам, осуществляющим оперативно-розыскную деятельность, комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий (далее — ОРМ) в сетях телефонной, подвижной и беспроводной связи и радиосвязи.[19]

Имеются технические возможности и для наложения ареста на электронно-почтовую корреспонденцию. В соответствии с законодательством[20] сети передачи данных обеспечивают техническую возможность передачи на пункт управления ОРМ информации различного характера: о выделенных абоненту (пользователю) сетевых адресах (IP-адресах) до реализации функции преобразования (трансляции) сетевых адресов и до начала передачи первого информационного пакета, а также информации о завершении контролируемого соединения; о передаваемой в контролируемом соединении и сообщении электросвязи информации, включая связанную с обеспечением процесса оказания услуг связи в том виде и последовательности, в которых такая информация поступала с пользовательского оборудования или из присоединенной сети связи; о местоположении пользовательского оборудования, используемого для передачи или приема информации контролируемого соединения или сообщения электросвязи. Такие возможности имеются и у владельцев электронных почтовых сервисов.

Перечисленные технические возможности активно используются при осуществлении таких ОРМ, как контроль почтовых отправлений, телеграфных и иных сообщений и снятие информации с технических каналов связи. Иными сообщениями в соответствии ч. 2 ст. 8 и ч. 1 ст. 9 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[21] являются сообщения, передаваемые по сетям электрической связи. В соответствии со ст. 2 Федерального закона от 7 июля

[19] *Федеральный* закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. Ст. 2895; *Приказ* Министерства связи и массовых коммуникаций РФ от 11 июля 2011 г. № 174 «Об утверждении правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть 1. Правила применения оборудования оконечно-транзитных узлов связи сетей подвижной радиотелефонной связи, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий» (зарегистрирован в Минюсте РФ 3 августа 2011 г. № 21543) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2011. 5 сент.

[20] *Приказ* Министерства связи и массовых коммуникаций от 27 мая 2010 г. № 73 «Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть 2. Требования к сетям передачи данных» (зарегистрирован в Минюсте РФ 7 июля 2010 г. № 17748) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2010. 26 июля.

[21] СЗ РФ. 1995. № 33. Ст. 3349.

2003 г. № 126-ФЗ «О связи» под электрической связью понимаются любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Термин «технические каналы связи» не встречается в законодательных актах, кроме Федерального закона «Об оперативно-розыскной деятельности», и требует конкретизации. В ведомственной инструкции, утв. Приказом МВД России от 10 июня 1994 г., в настоящее время утратившей действие в соответствии с Приказом МВД РФ от 31 декабря 2008 г. № 1200 (ред. от 6 августа 2009 г.) «О признании утратившими силу нормативных правовых актов МВД России»,[22] к техническим каналам отнесены телексные, факсимильные, селекторные, радиорелейные каналы передачи данных, линии абонентского телеграфирования и т. п. В эту группу можно отнести компьютерные сети и различные радиопереговорные устройства, основанные на использовании радиоволн.[23]

Таким образом, технические возможности, имеющиеся для проведения ОРМ, могут быть использованы и для производства следственных действий.

Если содержание некоторых видов сообщений, например, *SMS*, *MMS*, *Skype*, можно получить для использования в доказывании в рамках следственного действия «Контроль и запись переговоров» (ст. 186 УПК РФ), то для сообщений, полученных по электронной почте, такая возможность отсутствует. В связи с этим представляется необходимым ввести следственное действие, которое позволит следователю непосредственно использовать в качестве доказательства содержание сообщений, получаемых и отправляемых по электронной почте, а также различных приложений к ним: фото- и видеоизображений, документов, созданных в различных форматах, компьютерных программ и иных приложений. Таким следственным действием могли бы стать наложение ареста, консервация, выемка и осмотр корреспонденции, получаемой по электронной почте. Нормы ст. 185 («Наложение ареста на почтово-телеграфную корреспонденцию, их осмотр и выемка»), 186 («Контроль и запись переговоров»), 186.1 («Получение информации о соединениях между абонентами и/или абонентскими устройствами») УПК РФ не позволяют налагать арест на сообщения, передаваемые по электронной почте.

Проведенное нами интервьюирование следователей, надзирающих прокуроров и государственных обвинителей показывает, что единственным средством использования в доказывании содержания электронных почтовых отправлений является их выемка у владельца электронного почтового сервиса. В настоящее время практические работники рассматривают это действие как вид выемки документов (электронных документов). В то же время они не имеют возможности изъять удаленные почтовые сообщения и, соответственно, использовать их в процессе доказывания. Указанная конструкция не позволяет просматривать всю корреспонденцию и выявить отправления, имеющие отношение к делу. Эту проблему можно было бы решить, предусмотрев использование такой меры процессуального принуждения, как наложение ареста на электронную корреспонденцию.

[22] Официально опубликован не был, доступен в СПС «КонсультантПлюс».

[23] *Киселев А. П., Васильев О. А.* Комментарий к Федеральному закону от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс».

Предлагаемое следственное действие должно включать не только наложение ареста, выемку и осмотр корреспонденции, но и ее консервирование. Под консервированием понимается накопление и сохранение путем копирования информации владельцем электронного почтового сервиса в течение определенного срока. Введение консервирования данных позволит использовать в процессе доказывания всю передаваемую по электронной почте информацию, включая удаленную впоследствии респондентом. Поскольку такое следственное действие будет ограничивать конституционные права граждан, законодателю необходимо предусмотреть судебный порядок получения разрешения на его проведение и установить соответствующие процессуальные сроки.

В настоящее время отсутствие такого следственного действия практические работники пытаются компенсировать использованием в процессе доказывания результатов ОРМ «снятия информации с технических каналов связи». Обобщение судебно-следственной практики показало, что это происходит крайне редко. По-прежнему суды с большой осторожностью относятся к доказательствам, добытым на основе оперативно-розыскной деятельности, предпочитая опираться в своих выводах на протоколы следственных действий.

Целесообразность включения в уголовно-процессуальное законодательство таких следственных действий, как наложение ареста, консервация, выемка и осмотр электронной корреспонденции, поддерживает абсолютное большинство опрошенных нами следственных и прокурорских работников.

Безусловно, введение предлагаемого следственного действия не решит всех имеющихся проблем. Известно, что преступники находят всё новые способы сокрытия следов преступления. Понимая, что органы расследования будут иметь возможность доступа к их электронной корреспонденции через владельца электронного почтового сервиса, не исключено, что они будут регистрировать почтовые ящики у иностранных владельцев. Это осложнит процесс доказывания, поскольку в таких случаях доступ к информации будет возможен только в рамках оказания международной правовой помощи, а для выполнения международных поручений требуется продолжительное время. Двусторонние международные договоры о правовой помощи заключены Россией не со всеми государствами. В основном запросы о правовой помощи направляются запрашиваемым сторонам в соответствии с Европейской конвенцией о взаимной правовой помощи по уголовным делам (Страсбург, 20 апреля 1959 г.) ETS № 030 и Дополнительным протоколом к ней (Страсбург, 17 марта 1978 г.) ETS № 099. Для получения помощи от стран СНГ Россия пользуется возможностями, предоставляемыми Конвенцией о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (Минск, 22 января 1993 г.). Однако взаимодействие государств по вопросам правовой помощи в рамках названных конвенций удовлетворяет стороны не в полной мере, поскольку предусмотренные ими виды помощи не соответствуют реалиям информационного общества. Особенно это касается получения электронных доказательств за рубежом.

Решить названные проблемы могли бы Конвенция Совета Европы о киберпреступности (Будапешт, 23 ноября 2001 г.) ETS № 185[24] и Дополнительный протокол к ней (Страсбург, 28 января 2003 г.) ETS № 189. Российской Федерацией было продемонстрировано желание ратифицировать Конвен-

[24] Вступила в силу с 1 июля 2004 г.

цию. В частности, 15 ноября 2005 г. Президент РФ издал Распоряжение № 557-рп «О подписании Конвенции о киберпреступности».[25] Однако подписания и ратификации указанной Конвенции не последовало. 22 марта 2008 г. Президент РФ отменил свое предыдущее решение Распоряжением № 144-рп «О признании утратившим силу Распоряжения Президента РФ от 15 ноября 2005 г. № 557-рп "О подписании Конвенции о киберпреступности"».[26] Причиной этого стало несогласие с положениями п. «b» ст. 32 «Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным», в соответствии с которым сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получать их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему. По мнению представителей РФ, данное положение может нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц.

Поскольку авторы настоящей статьи являются сторонниками ратификации Конвенции о киберпреступности, стоит привести некоторые аргументы в пользу ее ратификации. Она охватывает три основных направления: согласование национальных норм, определяющих составы преступлений; определение порядка расследования по преступлениям в глобальных компьютерных сетях; создание оперативной и действенной системы международного сотрудничества по борьбе с киберпреступностью.

В ней закреплены основные нормы, облегчающие расследование компьютерных преступлений с использованием новых форм взаимопомощи. Они предусматривают защиту хранящихся в компьютерах данных, хранение и оперативное представление данных об интернет-трафике, поиск и арест систем, используемых преступниками, динамическую фиксацию трафика и перехват сетевого контента. В интересах соблюдения прав человека и принципа соразмерности действие этих норм ограничивается условиями и гарантиями, предусмотренными национальными законодательствами государств-участников. Так, следственные действия могут быть начаты лишь с санкции суда или иного независимого органа.

Помимо традиционных форм международного сотрудничества, регулируемого такими правовыми актами, как Европейская конвенция о выдаче (экстрадиции) и Европейская конвенция о взаимной правовой помощи по уголовным делам, в Конвенции о киберпреступности предусматривается возможность правоохранительных органов одних государств собирать хранимую в компьютерах информацию и доказательства для правоохранительных органов других государств, не проводя при этом специальных трансграничных расследований. Собираемая таким образом информация должна оперативно передаваться по назначению. Для оказания содействия в текущих расследованиях уже создана постоянно действующая круглосуточная система связи в виде центров G 24/7.

Конвенция в качестве нового метода расследования предусматривает «поиск и конфискацию сохраненных компьютерных данных». Эта норма позволяет стороне добиться сохранения важной информации, необходимой для расследования преступления, находящейся в юрисдикции другой стороны.

[25] СЗ РФ. 2005. № 47. Ст. 4929.
[26] Официально опубликовано не было, доступно в СПС «КонсультантПлюс».

Провайдеры услуг Интернет, как правило, располагают данными об информационном обмене сообщениями в прошлом, которые можно получить с помощью оборудования, регистрирующего конкретные аспекты информационного обмена, включая время, продолжительность и дату любого сообщения. Такие данные хранятся обычно ограниченное время, которое зависит от коммерческих потребностей оператора или поставщика услуг, а также от юридических требований, касающихся неразглашения частной информации.

Национальное законодательство многих стран разрешает правоохранительным или судебным органам издавать распоряжение, касающееся сбора данных информационного обмена. В то же время в тех случаях, когда данные информационного обмена являются частью сообщения (например «заголовок» сообщений, передаваемых по электронной почте), их сбор может рассматриваться как перехват самого сообщения и по этой причине подпадать под юридические ограничения. Именно такая практика распространена в России.

Значимым в рассматриваемом контексте является положение Конвенции, которое дает возможность принимать законодательные и другие меры, уполномочивающие ее компетентные власти арестовать или подобным образом обезопасить от уничтожения данные, имеющиеся у провайдера и необходимые для расследования. Положения статей Конвенции «Быстрая консервация данных, сохраненных в компьютерной системе» и «Быстрая консервация и раскрытие данных трафика» дают возможность правоохранительным органам проводить расследование таких преступлений или предпринимать действия для сохранения данных, которые могут быть уничтожены по истечении определенного времени, что, безусловно, позволит получить важные доказательства. Именно такие возможности мы подразумевали, предлагая введение следственного действия по аресту электронной корреспонденции.

Несомненное значение имеют и общие принципы, касающиеся международного сотрудничества, приведенные в Конвенции. Это вопросы выдачи киберпреступников и предоставления друг другу широкой взаимопомощи для расследования уголовных дел, связанных с компьютерными системами и данными, и для сбора электронных доказательств. С учетом специфики социального феномена киберпреступности, масштабов информатизации и развития глобальной сети Интернет становится все менее вероятным, что преступления такого вида будут ограничены территорией отдельного государства. В процессе проведения расследований правоохранительные органы различных государств должны сотрудничать, используя такие структуры, как Интерпол и пр.

В связи с правовой помощью при расследовании киберпреступлений неизбежно будут возникать и другие проблемы. Если внутренним правом одной из сторон не предусмотрены конкретные полномочия на поиск доказательств в электронной среде, такая сторона не в состоянии будет адекватно реагировать на просьбу об оказании помощи. В случае ратификации Конвенции Российская Федерация должна будет пересмотреть и по-новому урегулировать правила сбора, поиска, изъятия электронных доказательств с учетом глобальной природы сети Интернет.

Таким образом, совершенствование отечественного законодательства, в том числе в направлении его соответствия нормам международного права, является важным инструментом повышения эффективности уголовного преследования по делам о преступлениях в сфере высоких информационных технологий.