Е. С. Шевченко*

Социально-технологические детерминанты следственных действий при расследовании киберпреступлений[1]

Аннотация. *В статье рассматриваются социально-технологические факторы производства следственных действий (допроса и очной ставки) при расследовании киберпреступлений и раскрывается зависимость выбора различных тактических приемов допроса и очной ставки киберпреступника от: уровня его технической подготовленности и пользовательских навыков; мотивов совершения киберпреступления; дифференциации мотивов в зависимости от локализации преступной деятельности; информации, размещенной преступником в социальных сетях о себе; психологического состояния и (или) информационных болезней, компьютерных фобий.*

Ключевые слова: *киберпреступления; следственные действия; тактический прием; киберпреступник; допрос; очная ставка; расследование преступлений; киберпространство.*

DOI: 10.17803/1994-1471.2016.71.10.160-169

Киберпреступность в современном мире объявлена глобальной международной проблемой, о чем свидетельствуют принятые международные договоренности, предусматривающие совместные шаги по борьбе с этими высокотехнологичными преступлениями.

Раскрытие киберпреступлений остается достаточно сложной задачей для большинства сотрудников органов предварительного расследования, что обусловлено спецификой данного рода преступлений: трудностями с обобщением материалов следственной и судебной практики по каждому виду рассматриваемых преступлений; недостаточной квалификацией следователей для работы со специфическими источниками доказательственной информации, оцифрованной в виде электронных сообщений, страниц, сайтов.

Допрос и очную ставку при расследовании киберпреступлений можно отнести к одним из самых сложных следственных действий[2].

[1] Статья подготовлена в рамках проектной части государственного задания на выполнение НИР Министерства образования и науки по проекту 942.

[2] См.: *Вехов В. Б.* Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М. : Право и закон, 1996 ; *Крылов В. В.* Информационные компьютерные преступления : учеб. и практ. пособие. М., 1997 ; *Менжега М. М.* Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ : дис. … канд. юрид. наук. Саратов, 2005 ; *Мещеряков В. А.* Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001 ; *Романенко М. А.* Расследование преступных нарушений авторских прав в сфере программного обеспечения : монография. Омск : Изд-во Омского гос. ун-та, 2008 ; *Яковлев А. Н., Олиндер Н. В.* Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем : науч.-метод. пособие. М., 2012.

* *Шевченко Елизавета Сергеевна*, младший научный сотрудник Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Essheva@mail.ru
123995, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Тактика производства допроса по уголовным делам рассматриваемой категории напрямую зависит от специфики механизма совершения киберпреступлений и иных как позитивных, так и негативных факторов.

Так, анализ практики расследования уголовных дел по киберпреступлениям и результаты проведенного опроса следователей показали, что при производстве допроса и очной ставки у следователей зачастую возникают различного рода трудности. Например, 71 % респондентов указали, что основные трудности, с которыми им приходилось сталкиваться в ходе расследования киберпреступлений, связаны с терминологией, выбором тактических приемов воздействия, установлением контакта[3].

В этой связи можно выделить следующие проблемы, которые необходимо решать при подготовке к допросу (очной ставке) и в ходе его проведения.

Во-первых, необходимость привлечения специалистов или использования специальных знаний при проведении рассматриваемых следственных действий. Так, в ходе расследования киберпреступлений необходимы знания в области телекоммуникационных систем, компьютерных технологий и компьютерной техники. Вместе с тем, как показывает практика, следователи необходимыми знаниями не всегда обладают, либо обладают в недостаточном объеме, в связи с чем для всецелого понимания ответов допрашиваемого им и нужна помощь специалиста.

Во-вторых, недостаточный уровень (либо отсутствие) специальных знаний у следователя часто обусловливает существенное «интеллектуальное» противодействие расследованию со стороны киберпреступника.

В-третьих, следователю в ходе расследования требуется изучить значительный объем данных, обнаруживаемых преимущественно в электронном виде, часть из которых будет составлять предмет следственного действия и уточняться в ходе допроса (очной ставки).

В-четвертых, необходимость применения при проведении допроса (очной ставки) знаний юридической психологии в расследовании киберпреступлений.

В-пятых, дефицит времени и динамичность обстановки в сетевом окружении, которые определяются краткосрочностью существования и высокой изменчивостью отдельных видов доказательств, находящихся в электронной форме.

С криминалистической точки зрения допрос (очная ставка) является средством решения ряда тактических задач — изобличения во лжи лица, противодействующего следствию; проверки выдвинутых версий; распознавания прочности позиций допрашиваемых; выявления ранее неизвестных обстоятельств и т.д.[4]

Результаты проведенного анкетирования сотрудников правоохранительных органов показали, что к особенностям тактики допроса подозреваемого (обвиняемого) при расследовании киберпреступлений следователи отнесли: подготовку к следственному действию (68,4 %); изучение личности допрашиваемого (58 %); составление вопросов для допроса с участием специалиста (63,1 %); привлечение специалиста к проведению следственного действия в связи с большим количеством специальной терминологии (36,8 %).

К стадии подготовки допроса подозреваемого (обвиняемого) по киберпреступлениям необходимо отнести: информационное обеспечение допроса, изучение личности обвиняемого и планирование допроса.

Информационное обеспечение является важной составляющей стадии подготовки допроса подозреваемого (обвиняемого) по киберпреступлениям. Чем лучше информационное обеспечение у следователя, безупречнее знание и владение им всем собранным по делу материалом и вспомогательной инфор-

[3] Опрос респондентов проводился в Республике Карелия, Камчатском, Краснодарском, Ставропольском краях, Архангельской, Белгородской, Калининградской, Калужской, Ленинградской, Мурманской, Свердловской областях и некоторых других регионах. Было опрошено 78 респондентов, 22 из которых — сотрудники прокуратуры, 32 — дознаватели и 24 — следователи.

[4] *Образцов В. А., Топорков А. А.* Подготовка и производство очной ставки // Следственные действия. Криминалистические рекомендации. Типовые образцы документов. М., 2001. С. 160 ; *Еникеев М. И.* Юридическая психология. М. : Норма, 2005. С. 265.

мацией, тем более подконтрольна будет ситуация на допросе. Кроме того, информационное обеспечение необходимо для исключения ошибки при квалификации совершенного киберпреступления.

Другим условием информационного обеспечения допроса при расследовании киберпреступлений является наличие знаний компьютерных технологий, а также знаний нормативной правовой базы, регулирующей область нарушенных прав.

На этапе подготовки допроса для более глубокого понимания обстоятельств совершенного киберпреступления следователю целесообразно: ознакомиться со специальной литературой, посвященной технологиям, использованным при совершении киберпреступлений, справочниками по компьютерной терминологии и проконсультироваться со специалистом. Как верно замечает М. М. Менжега, следователю, не обладающему специальными знаниями, самостоятельно будет сложно, например, отличить сбой в работе аппаратуры или непреднамеренную ошибку от последствий действия вирусов; выявить возможные противоречия и ложь в показаниях. Кроме того, помощь специалиста позволит разграничить такие технические вопросы, как, например, производилось ли копирование или модификация информации при выполнении определенного действия и другие[5].

Фактором, положительно влияющим на выбор тактики производства допроса, является наличие определенного объема информации о преступном событии, полученного из различных источников, а также об особенностях механизма преступления, которые зависят от применяемых для его реализации орудий и средств (компьютерно-технические средства)[6].

Таким образом, отсутствие у следователя специальных знаний может вызвать трудности при решении основных задач допроса: выявление элементов состава киберпреступления, исходя из следовой информации; установление обстановки совершения киберпреступления, способа и мотивов его совершения, сопутствующих обстоятельств; выделение детальных признаков вида киберпреступления; установление способа его сокрытия и др.

Так, по рассматриваемым уголовным делам выделяют следующие способы сокрытия преступлений: шифровка (электронной почты; файлов, содержащих информацию, касающуюся совершенного киберпреступления, и прочего) — 5 %; удаление информации, находящейся в памяти компьютера и на машинных носителях — 13 %; установка пароля — 10 %; хранение информации, касающейся совершенного киберпреступления, в Облаке — 9 %; установка программ удаленного пользования, программ защиты информации от несанкционированного доступа — 8,2 %; использование вредоносных программ для удаления файлов — 8,3 %; использование ложного почтового адреса или анонимной почты — 10,7 %; использование программы смены (скрытия) IP-адреса компьютера — 5 % и другие. Поэтому при появлении новых обстоятельств, следователю необходимо пересматривать дело, с целью обнаружения новой важной информации, в связи с новыми открывшимися обстоятельствами[7].

Именно это обстоятельство по общему правилу обусловливает необходимость присутствия при производстве следственных действий (допроса, очной ставки) специалиста в сфере компьютерной информации (компьютерных технологий), который уже и на стадии подготовки к следственному действию может разъяснить следователю неясные технические термины, устройство изъятых средств, способы совершения преступлений и др.

Также одним из элементов, составляющих информационное обеспечение допроса при расследовании киберпреступлений, является изучение особенностей личности допрашиваемого.

К источникам информации о личности допрашиваемого можно отнести: изучение биографических материалов о личности; получение

---

[5] *Менжега М. М.* Указ. соч. С. 117.

[6] *Смирнова И. Г., Коломинов В. В.* Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Известия Иркутской государственной экономической академии (БГУЭП). 2015. № 3. Т. 6.

[7] *Костин П. В.* Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики : автореф. ... канд. юрид. наук. Н. Новгород, 2007. С. 6.

и сопоставление сведений о лице из различных источников; сбор и сопоставление независимых характеристик; анализ учебной и (или) трудовой деятельности лица; назначение судебно-психологических экспертиз и учет их заключений; непосредственное наблюдение за человеком (эмоции, речь и др.) и прочее[8]. Необходимо также изучить страницы преступника в социальных сетях и посетить сайты, которые наиболее часто посещал допрашиваемый.

Здесь следует особо остановиться на психологическом аспекте, который следователям необходимо учитывать как в целом при расследовании киберпреступления, так и при подготовке к допросу (очной ставке) и в ходе его проведения. Проблема получения информации о типичных характеристиках личности киберпреступника, совершающего преступления рассматриваемой категории, усугубляется отсутствием достаточного объема эмпирического материала[9].

Тем не менее Д. Айков, К. Сейгер, У. Фонсторх делят компьютерных преступников на три категории в зависимости от мотивов преступления: взломщики (основное побуждение — проникновение в систему), преступники (основное побуждение — выгода), вандалы (основное побуждение — нанесение ущерба)[10].

Психологическая характеристика отдельных киберпреступников, безусловно, важная составляющая расследования киберпреступлений, хотя и чрезвычайно объемная. Так, А. Н. Косенковым и Г. А. Чёрным представлены основные группы киберпреступников, за основу классификации которых берется вид совершенного преступления и уровень компьютерных навыков преступников[11]:

— преступники специального киберпреступного типа: данная категория преступников не только специализируется на совершении специальных киберпреступлений, но также каждый из киберпреступников данного типа совершает их самостоятельно и обладает «профессиональными» техническими знаниями, необходимыми для совершения преступлений данного рода;
— преступники общекиберпреступного типа совершают при помощи электронных устройств неспецифические для киберпространства деяния, не используя при этом специальные технические знания либо используя только поверхностные знания.

Условия киберпространства существенно отличаются от реальных, поэтому для установления процесса возникновения преступного умысла, его природы, а также степени общественной опасности данного лица возникает необходимость дифференциации киберпреступников в зависимости от локализации их преступной деятельности.

Исходя из этого критерия, можно выделить три основных группы[12]:

1. Киберпреступники, ведущие основную преступную деятельность только в киберпространстве.
2. Киберпреступники, занимающиеся преступной деятельностью в равной степени как в киберпространстве, так и реальной жизни.
3. Лица, совершившие ранее преступления, не относящиеся к киберпреступлениям, и совершающие киберпреступления в настоящее время.

Информацию о личности подозреваемого (обвиняемого) следователь может получить так же как из криминалистических учетов, так и при допросе его знакомых и родственников. При этом могут быть выяснены специальные и профессиональные навыки подозреваемого, склонность к совершению преступлений, круг общения; имеющиеся у подозреваемого средства компьютерной техники и места их хранения; вероятные цели и мотивы совершения преступления и др.

---

[8] *Питерцев С. К., Степанов А. А.* Тактика допроса. СПб. : Питер, 2001. С. 28.

[9] *Маслакова Е. А.* Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Политика и право. 2014. № 1. С. 114—115.

[10] *Айков Д., Сейгер К., Фонсторх У.* Компьютерные преступления : Руководство по борьбе с компьютерными преступлениями : пер. с англ. М. : Мир, 1999. С. 90.

[11] *Косенков А. Н., Чёрный Г. А.* Общая характеристика психологии киберпреступника // Криминологический журнал БГУЭП. 2012. № 3 (21). С. 92.

[12] *Косенков А. Н., Чёрный Г. А.* Указ. соч. С. 92.

Особенно важными источниками для данной категории дел будут являться анализ учебной и (или) трудовой деятельности лица; назначение судебно-психологических или судебно-психиатрических экспертиз и учет их заключений; непосредственное наблюдение за человеком. Результаты анализа различной информации о допрашиваемом при подготовке к допросу по данной категории дел помогут следователю узнать, каким уровнем знаний в области информационных технологий обладает преступник, с чем было сопряжено преступление, могло ли допрашиваемое лицо совершить расследуемое киберпреступление или нет.

Информацию можно получить в результате изучения данных пользователя социальной сети — информации, которую необходимо указать при регистрации в социальной сети, а также сведений о личной жизни пользователя, размещенных им добровольно в процессе пользования сайтами. Это фамилия, имя, пол, средние и высшие учебные заведения, год их окончания, дата и место рождения, семейное положение (при этом, если близкие родственники зарегистрированы в той же социальной сети, автоматически появляются ссылки на их персональные странички), место работы, контактная информация, данные, характеризующие личность.

В дальнейшем человек сам наполняет свою страницу информацией, при анализе которой можно прямо либо косвенно его характеризовать. Например, круг общения можно установить, изучив список друзей, круг личных интересов — через группы, в которых пользователь состоит. Отношение к тем или иным социальным явлениям и наиболее обсуждаемым в обществе событиям можно предположить в ходе анализа комментариев на стене пользователя[13]. Также в случае, если номер мобильного телефона не указан в контактах на странице, следователь может его выяснить, так как при регистрации в социальной сети необходимо указать номер своего мобильного телефона для завершения регистрации[14].

Назначение судебно-психологических или судебно-психиатрических, ситуационных экспертиз и учет их заключений следователю необходимо как источник информации о личности (вместе с тем по данной категории уголовных дел такие экспертизы назначаются редко: судебно-психологическая — 8,5 % случаях, судебно-психиатрическая — 5,5 % случаях).

Наиболее тяжкие и изощренные киберпреступления совершают лица, имеющие техническое образование и продолжительный опыт работы в области информационных технологий. Это программисты, операторы терминалов, системные администраторы и другие. Однако основную часть раскрытых киберпреступлений совершают специалисты низкой квалификации. Не исключено, что это может быть связано с их невысокими навыками уничтожать следы своей противоправной деятельности в компьютерных системах.

Допрос (очная ставка) подозреваемого (обвиняемого) по киберпреступлениям является важным этапом расследования по сбору и проверке не только доказательственной, но и ориентирующей информации, которую следователь получает с помощью вербальных и невербальных коммуникаций[15].

При производстве допроса (очной ставки) при расследовании киберпреступлений основной целью является выявление (выяснение) информации, связанной с виртуальными следами, а также иной, имеющей отношение к расследуемому виду киберпреступления.

При проведении допроса (очной ставки) следователю нужно учитывать, что киберпространство существенно меняет восприятие человеком действительности. В условиях киберпространства меняется психологическое содержание взаимосвязей «преступник — предмет преступления (потерпевший)», которые

---

[13] Стена — способ публикации открытых записей личного и общего характера временной значимости, отсортированных в обратном хронологическом порядке, то есть последняя запись находится сверху. В сети «ВКонтакте» стену имеют каждый пользователь и каждая группа. См.: URL: http://www.sarafannoeradio. org/novosti/201-perviy-slovar-sotsialnih-setey.html.

[14] URL: http://hr-portal.ru/blog/yuristy-nastoyatelno-rekomenduyut-polzovatelyam- interneta-ne-ostavlyat-v-socialnyh-setyah-svoi/ (дата обращения: 01.05.2016).

[15] Тактика следственных действий : учеб. пособие / под ред. В. И. Комиссарова. Саратов, 2000. С. 90.

превращаются во взаимосвязь «преступник — электронное устройство (сети) — потерпевший (предмет преступления)»[16]. Также киберпространство создает у преступника впечатление возможности уклонения от уголовной ответственности. Это впечатление складывается благодаря анонимности и «эффекту онлайн-дезингибиции»[17]. Анонимность дает преступнику возможность создать образ личности, не соответствующий реальности; быть некоторое время неидентифицированным.

В связи с этим у киберпреступников могут встречаться такие психические отклонения, как интернет-зависимость, тревожные расстройства, диссоциативные расстройства личности.

Близко к рассматриваемой выше группе преступников можно отнести еще одну, вторую группу, в которую входят лица, страдающие новым видом психических заболеваний — информационными болезнями, или компьютерными фобиями. Киберпреступления могут совершаться лицами, страдающими указанным видом заболеваний.

Успешность в расследовании киберпреступлений во многом зависит от умений следователя находить новые тактические ходы, их комбинации на основе знания психологических закономерностей поведения допрашиваемого, и применять традиционные приемы, но с учетом индивидуальных особенностей конкретного обвиняемого по конкретному делу.

Немаловажным для следователя при выборе тактики проведения допроса является то, что лица, совершившие киберпреступления, не имеют, как правило, антисоциальной установки. Поэтому в допросе при расследовании киберпреступлений в сложных ситуациях применяются тактические приемы, наиболее эффективным из которых будет убеждение[18].

С учетом названного критерия следственные ситуации, складывающиеся в ходе допроса, могут быть условно разделены на бесконфликтные (простые), когда следователь располагает доказательствами, фактическими данными, и конфликтные (сложные), когда он не обладает ими и ведет допрос с надеждой на их получение.

Как показывает практика, в большинстве случаев допросы подозреваемого (обвиняемого) по делам о киберпреступлениях проходят в конфликтных ситуациях. Допрашиваемые отказываются от дачи показаний или дают ложные показания, принижая свою вину либо вообще отрицая участие в преступлении.

Особенностью характера киберпреступлений в основном является их тщательная спланированность, а также осведомленность преступника об информации, которая имеется у следователя. Соответственно, преступник четко продумывает правдоподобную ложную версию. Помимо этого, преступник перегружает ложную версию специальными терминами, что еще более осложняет работу следователя по выявлению лжи.

Поэтому следователю нужно предварительно тщательно продумать тактику, применяемую во время допроса (очной ставки), и особенности фиксации данного следственного действия.

---

[16] См. подробнее: Стенограмма Национальной конференции США по киберэтике // URL: http://connect.marymount.edu/ethics/cyberethics/sessions/gensession3.pdf. С. 23.

[17] См. подробнее: *Suler J.* The Psychology of Cyberspace // URL: http://users.rider.edu/suler/psycyber/psycyber.html.
Основу этого эффекта составляют: диссоциативная анонимность («ты меня не знаешь»), сущность которой состоит в том, что в условиях анонимности люди могут отделить свои действия в киберпространстве от реального мира и реальной личности, в таком случае человек полагает, что может не брать на себя ответственность за свои действия ; невидимость («ты меня не видишь») позволяет избегать установления психологического контакта ; асинхронность («увидимся позже») — возможность общаться в отдельных случаях без необходимости немедленной реакции на слова или действия собеседника, что является немаловажным дезингибирующим фактором; солиптическая интроекция («это всё в моей голове») — при онлайн-общении может возникнуть ощущение, что все происходит исключительно в нашем собственном воображении; минимизация власти («мы равны») возникает из-за опосредованного восприятия атрибутов более высокого социального положения, а также возможности их игнорировать.

[18] *Доспулов Г. Г.* Психология допроса на предварительном следствии. М., 1976. С. 16—17.

При проведении допроса подозреваемому (обвиняемому) сначала задаются общие вопросы (навык и уровень работы с компьютером, место работы, что входит в обязанности допрашиваемого на работе (если преступление связано с рабочей деятельностью), каковы цели и мотивы и пр.). Потом следователь ставит конкретные вопросы, затрагивающие непосредственно совершенное киберпреступление.

Как свидетельствуют результаты исследования практики, научной литературы, общие вопросы при расследовании любого киберпреступления будут типичными. Однако уточняющие вопросы должны быть составлены следователем с привлечением специалиста, в каждом отдельном случае индивидуально, с учетом особенностей совершенного киберпреступления.

Как отмечалось ранее, допрос свидетелей, потерпевших имеет тактические особенности, которые зависят не только от механизма совершения киберпреступлений, но и от криминалистического типа потерпевших или свидетелей. Необходимо выделить точку зрения В. М. Быкова, который считает, что тактика допроса должна строиться с учетом соответствующего криминалистического типа допрашиваемых. Исходя из занятой допрашиваемыми позиции в ходе предварительного следствия, ученым были выделены следующие типы: активные и неактивные, добросовестные потерпевшие, неустойчивые, недобросовестные потерпевшие[19]. Данную типизацию можно применить и к свидетелям.

Такая типизация может быть использована и взята за основу при подготовке к допросу потерпевших и свидетелей. Так, например, допрашивая потерпевших (свидетелей), необходимо выяснить следующую информацию: какие компьютерно-технические средства использовались потерпевшим или свидетелем; какими знаниями о компьютерно-технических средствах, их характеристиках обладают допрашиваемые; какими навыками работы на компьютере или технически сложном устройстве владеют и другое. В процессе их допроса необходимо установить: местонахождение юридического лица, вид деятельности и форму организации; режим деятельности юридического лица; содержание и объем информации, хранящейся в компьютере; кто из сотрудников и каким образом вступал в контакт с предполагаемыми преступниками и другое. Данный перечень зависит от конкретной типичной исходной следственной ситуации и не является исчерпывающим.

Таким образом, тактически значимая информация о личности киберпреступников при производстве допроса (очной ставки) должна включать сведения об уровне их технической подготовленности и компьютерных навыков; о мотивах совершения киберпреступления; об их дифференциации в зависимости от локализации их преступной деятельности; об информации, размещенной в социальных сетях о самом себе; о психологическом состоянии или информационных болезнях (зависимостях, фобиях).

Тактика производства допроса (очной ставки) по уголовным делам этой категории напрямую зависит от специфики механизма совершения киберпреступлений и иных как позитивных, так и негативных факторов.

Выбор тактических приемов допроса (очной ставки) киберпреступника зависит: от уровня его технической подготовленности и пользовательских навыков; мотивов совершения киберпреступления; дифференциации мотивов в зависимости от локализации преступной деятельности; информации, размещенной преступником в социальных сетях о себе; психологического состояния и (или) информационных болезней, компьютерных фобий.

---

[19] *Быков В. М.* Допрос потерпевшего // Законность. 2014. № 6. С. 27—32.

[20] The article was prepared within the framework of the project of the State job on the execution of the Scientific and Research Work of the Ministry of Education and Science, project 942.

БИБЛИОГРАФИЯ

1. *Антонян Ю. М., Еникеев М. И., Эминов В. Е.* Психология преступника и расследования преступлений. — М. : Юристъ, 2008. — 336 с.
2. *Быков В. М.* Допрос потерпевшего // Законность. — 2014. — № 6. — С. 27—32.
3. *Быстряков Е. Н., Иванов А. Н., Климов В. А.* Расследование компьютерных преступлений. — 2-е изд. — Саратов, СГАП, 2001. — 112 с.
4. *Васильев В. Л.* Юридическая психология. — СПб. : Питер, 2009. — 608 с.
5. *Вехов В. Б.* Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. — М. : Право и закон, 1996 — 182 с.
6. Всемирная организация здравоохранения. 2007. Вып. 85 // URL: http://www.who.int/entity/bulletin/volumes/85/1/en/index.html.
7. *Доспулов Г. Г.* Психология допроса на предварительном следствии. — М., 1976. — 112 с.
8. *Ефимичев П. С., Ефимичев С. П.* Расследование преступлений: теория, практика, обеспечение прав личности. — М. : Юстицинформ, 2008. — 315 с.
9. *Китаев Н. Н.* Очная ставка — эффективное следственное действие в арсенале настоящих профессионалов // Российская юстиция. — 2008. — № 4.
10. *Коновалова В. Е.* Тактика производства очной ставки. — Харьков, 1955.
11. *Косенков А. Н., Чёрный Г. А.* Общая характеристика психологии киберпреступника // Криминологический журнал БГУЭП. — 2012. — № 3 (21). — С. 87—94.
12. *Костин П. В.* Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики : автореф. … канд. юрид. наук. — Н. Новгород, 2007. — 30 с.
13. *Крылов В. В.* Информационные компьютерные преступления : учебное и практическое пособие. — М. : Инфра-М, Норма, 1997. — 285 с.
14. *Малютин М. П.* Формирование психологического контакта как тактическая цель допроса // Юридический вестник КубГУ. — 2010. — № 1 (2). — С. 73—74.
15. *Маслакова Е. А.* Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Политика и право. — 2014. — № 1.
16. *Менжега М. М.* Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ : дис. … канд. юрид. наук. — Саратов, 2005. — 238 с.
17. *Мещеряков В. А.* Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. — Воронеж, 2001. — 387 с.
18. *Осипенко А. Л.* Борьба с преступностью в глобальных компьютерных сетях : Международный опыт : монография. — М. : Норма, 2004. — 432 с.
19. *Питерцев С. К., Степанов А. А.* Тактика допроса. — СПб. : Питер, 2001. — 160 с.
20. *Романенко М. А.* Расследование преступных нарушений авторских прав в сфере программного обеспечения : монография. — Омск : Изд-во Омск. гос. ун-та, 2008. — 232 с.
21. *Смирнова И. Г., Коломинов В. В.* Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Известия Иркутской государственной экономической академии (БГУЭП). — 2015. — № 3. — Т. 6.
22. Стенограмма Национальной конференции США по киберэтике. — С. 23 // URL: http://connect.marymount.edu/ethics/cyberethics/sessions/gensession3.pdf.
23. Тактика следственных действий : учебное пособие / под ред. В. И. Комиссарова. — Саратов : СГАП, 2000. — 202 с.
24. *Чуфаровский Ю. В.* Психология оперативно-розыскной и следственной деятельности : учебное пособие. — М. : Проспект, 2010. — 207 с.
25. *Яковлев А. Н., Олиндер Н. В.* Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем : научно-методическое пособие. — М., 2012. — 182 с.

Материал поступил в редакцию 1 мая 2016 г.

SOCIAL AND TECHNOLOGICAL DETERMINANTS OF INVESTIGATIVE ACTIVITIES IN INVESTIGATING CYBER CRIMES20

SHEVCHENKO Elizaveta Sergeevna — Junior Researcher at the Kutafin Moscow State Law University (MSAL)
Essheva@mail.ru
123995, Russia, Moscow, Sadovaya-Kudrinskaya Street, 9

Review. *This article considers the socio-technological factors in the production of investigative activities (interrogation and confrontation) in investigation of cyber crimes and reveals the dependence of choosing different tactical methods of questioning and confrontation of the cyber criminal on: its level of technical competencies and custom skills; motives for cybercrime; differentiation of motives depending on the location of the crime; offender information posted on social networks about himself; psychological state and (or) disease information, computer phobias.*

Keywords: *cybercrime; investigative activities; tactic; cyber criminal; interrogation; confrontation; investigation of crimes; cyberspace.*

REFERENCES (TRANSLITERATION)

1. *Antonjan Ju. M., Enikeev M. I., Jeminov V. E.* Psihologija prestupnika i rassledovanija prestuplenij. — M. : Jurist#, 2008. — 336 s.
2. *Bykov V. M.* Dopros poterpevshego // Zakonnost'. — 2014. — № 6. — S. 27—32.
3. *Bystrjakov E. N., Ivanov A. N., Klimov V. A.* Rassledovanie komp'juternyh prestuplenij. — 2-e izd. — Saratov, SGAP, 2001. — 112 s.
4. *Vasil'ev V. L.* Juridicheskaja psihologija. — SPb. : Piter, 2009. — 608 s.
5. *Vehov V. B.* Komp'juternye prestuplenija: sposoby sovershenija i raskrytija / pod red. B. P. Smagorinskogo. — M. : Pravo i zakon, 1996 — 182 s.
6. Vsemirnaja organizacija zdravoohranenija. 2007. Vyp. 85 // URL: http://www.who.int/entity/bulletin/volumes/85/1/en/index.html.
7. *Dospulov G. G.* Psihologija doprosa na predvaritel'nom sledstvii. — M., 1976. — 112 s.
8. *Efimichev P. S., Efimichev S. P.* Rassledovanie prestuplenij: teorija, praktika, obespechenie prav lichnosti. — M. : Justicinform, 2008. — 315 s.
9. *Kitaev N. N.* Ochnaja stavka — jeffektivnoe sledstvennoe dejstvie v arsenale nastojashhih professionalov // Rossijskaja justicija. — 2008. — № 4.
10. *Konovalova V. E.* Taktika proizvodstva ochnoj stavki. — Har'kov, 1955.
11. *Kosenkov A. N., Chjornyj G. A.* Obshhaja harakteristika psihologii kiberprestupnika // Kriminologicheskij zhurnal BGUJeP. — 2012. — № 3 (21). — S. 87—94.
12. *Kostin P. V.* Issledovanie mashinnyh nositelej informacii, ispol'zuemyh pri sovershenii prestuplenij v sfere jekonomiki : avtoref. … kand. jurid. nauk. — N. Novgorod, 2007. — 30 s.
13. *Krylov V. V.* Informacionnye komp'juternye prestuplenija : uchebnoe i prakticheskoe posobie. — M. : Infra-M, Norma, 1997. — 285 s.
14. *Maljutin M. P.* Formirovanie psihologicheskogo kontakta kak takticheskaja cel' doprosa // Juridicheskij vestnik KubGU. — 2010. — № 1 (2). — S. 73—74.
15. *Maslakova E. A.* Lica, sovershajushhie prestuplenija v sfere informacionnyh tehnologij: kriminologicheskaja harakteristika // Politika i pravo. — 2014. — № 1.
16. *Menzhega M. M.* Kriminalisticheskie problemy rassledovanija sozdanija, ispol'zovanija i rasprostranenija vredonosnyh programm dlja JeVM : dis. … kand. jurid. nauk. — Saratov, 2005. — 238 s.
17. *Meshherjakov V. A.* Osnovy metodiki rassledovanija prestuplenij v sfere komp'juternoj informacii : dis. … d-ra jurid. nauk. — Voronezh, 2001. — 387 s.
18. *Osipenko A. L.* Bor'ba s prestupnost'ju v global'nyh komp'juternyh setjah : Mezhdunarodnyj opyt : monografija. — M. : Norma, 2004. — 432 s.

19. *Pitercev S. K., Stepanov A. A.* Taktika doprosa. — SPb. : Piter, 2001. — 160 s.
20. *Romanenko M. A.* Rassledovanie prestupnyh narushenij avtorskih prav v sfere programmnogo obespechenija : monografija. — Omsk : Izd-vo Omsk. gos. un-ta, 2008. — 232 s.
21. *Smirnova I. G., Kolominov V. V.* Takticheskie osobennosti proizvodstva doprosa po delam o prestuplenijah v sfere komp'juternoj informacii // Izvestija Irkutskoj gosudarstvennoj jekonomicheskoj akademii (BGUJeP). — 2015. — № 3. — T. 6.
22. Stenogramma Nacional'noj konferencii SShA po kiberjetike. — S. 23 // URL: http://connect.marymount.edu/ethics/cyberethics/sessions/gensession3.pdf.
23. Taktika sledstvennyh dejstvij : uchebnoe posobie / pod red. V. I. Komissarova. — Saratov : SGAP, 2000. — 202 s.
24. *Chufarovskij Ju. V.* Psihologija operativno-rozysknoj i sledstvennoj dejatel'nosti : uchebnoe posobie. — M. : Prospekt, 2010. — 207 s.
25. *Jakovlev A. N., Olinder N. V.* Osobennosti rassledovanija prestuplenij, sovershennyh s ispol'zovaniem jelektronnyh platezhnyh sredstv i sistem : nauchno-metodicheskoe posobie. — M., 2012. — 182 s.