Феноменология преступлений, совершенных с использованием современных информационных технологий

А.С. Шаталов

профессор кафедры уголовного права и криминалистики Национального исследовательского университета «Высшая школа экономики», доктор юридических наук. Адрес: 101000, Российская Федерация, Москва, ул. Мясницкая, 20. E-mail: asshatalov@hse.ru

Аннотация

Феноменология (греч.) в буквальном толковании — это учение о феноменах, т.е. наблюдаемых явлениях или событиях. В современной философии оно выступает как метод научного анализа сознания и имманентных, априорных структур человеческого существования. Данная статья — результат применения этого метода для постановки и осмысления оптимальных путей решения проблем, непосредственно связанных с деятельностью по предотвращению, выявлению, раскрытию и расследованию преступлений, совершенных с использованием современных информационных технологий. Прибегнув к некоторым обобщениям, автор предпринял попытку найти ответ на вопрос, почему на фоне научных достижений отечественной криминалистики, при обилии новых идей, концепций, технологий, методик, криминалистических алгоритмов и программ расследования прогресс в деле борьбы с преступностью остается малозаметным? Главная причина такого положения дел ему видится в том, что российская криминалистика долгое время развивалась в отрыве от ведущих зарубежных исследовательских школ. Вместе с тем такое ее состояние сохраняется и сейчас, несмотря на охватившие практически все страны мира глобальные интеграционные процессы. В качестве главного направления преодоления кризисных явлений автор позиционирует имплементацию в научные ресурсы отечественной криминалистики современных информационных технологий вообще, и для повышения эффективности борьбы с преступлениями, совершаемыми с использованием компьютерных и сетевых возможностей в частности. Борьбу с ними он считает проблемой международного масштаба, поскольку меры по предотвращению, выявлению, раскрытию и расследованию преступлений такого рода не могут быть результативными лишь на национальном уровне в силу транснационального и трансграничного характера сети «Интернет». С учетом непрекращающегося увеличения численности ее пользователей, закономерно порождающей их зависимость от информационного сообщества и уязвимость от разного рода киберпосягательств, произведен научный анализ современного состояния выявления и расследования преступлений такого рода и сформулированы рекомендации по повышению эффективности этой деятельности.

Ключевые слова

информационные технологии, информационные ресурсы, киберпреступность, компьютерные преступления, криминалистика, криминалистически значимая информация, криминалистическая методика, расследование преступлений, уголовное судопроизводство.

Библиографическое описание: Шаталов А.С. Феноменология преступлений, совершенных с использованием современных информационных технологий // Право. Журнал Высшей школы экономики. 2018. № 2. С. 68–83.

JEL: K 49; УДК: 343 DOI: 10.17323/2072-8166.2018.2.68.83

Современная криминалистика по своему содержанию является результатом многолетнего и целенаправленного наблюдения, с одной стороны, за совершением преступлений, а с другой — за их выявлением, раскрытием, расследованием, предотвращением, рассмотрением уголовных дел в судах. Как и всякая другая прикладная наука, она исходит из накопленного ею эмпирического материала, корни которого находятся в экономической реальности. Все, что на основе этого материала было разработано, проанализировано, внедрено, применено, накоплено и систематизировано, рано или поздно должно либо оправдать свое существование, либо отказаться от него. В качестве единственного мерила при этом всегда выступал мыслящий рассудок.

Методы и средства, которые криминалисты открыли благодаря ему, всегда требовали своего признания в качестве познавательной основы для всех практических действий в уголовном судопроизводстве. Однако ее состояние рано или поздно достигало того предела, за которым эта основа становилась односторонней, погрязшей в неразрешимых противоречиях, поскольку оказывалась неспособной видеть за отдельными событиями их взаимной связи, а также органично развиваться на фоне их возникновения и исчезновения. Причины и следствия таких событий олицетворяются в представлениях, которые имеют значение как таковые только применительно к конкретному уголовно-правовому конфликту. Но как только начинает происходить его рассмотрение в общей связи с аналогичными уголовно-правовыми конфликтами, то уже известные причины и следствия сразу же переходят в режим универсального взаимодействия, постоянно меняясь местами и трансформируясь, таким образом, в более отчетливое представление, которое с течением времени заменяется новым, еще более отчетливым.

В самом общем виде каждое такое представление является продуктом криминалистического мышления, состоящим не только в разложении воз-

никшего представления на отдельные его элементы, но и в их объединении в некоторое единство. С учетом знания и понимания закономерностей механизма преступления, возникновения информации о преступлении и его участниках, закономерностей собирания, исследования, оценки и использования доказательств объединение этих элементов становится возможным только если их единство ранее уже существовало. От того, что какие-либо сведения будут наделены статусом доказательств по уголовному делу, то или иное лицо автоматически не становится невиновным или виновным в совершении преступления. Единство элементов представления об этом, возникшее в результате доказывания, следовательно, дающее основание для принятия итогового процессуального решения по уголовному делу, как раз и есть то, что нужно доказать. Заслуга российской криминалистики состоит в том, что именно в ее рамках доказывание по уголовным делам впервые смогло предстать в виде самостоятельного, целенаправленного познавательного процесса, базирующегося не только на нормах действующего уголовно-процессуального законодательства, но и на закономерностях его продвижения, изменения, преобразования и логического завершения. Это в конечном итоге и предопределяет результативность борьбы с преступностью, позволяя, таким образом, удерживать ее на социально терпимом уровне.

Преступность, по ныне господствующему в науке мнению, определяется как совокупность деяний, запрещенных уголовным законом. Принято выделять две характерные черты преступности. Во-первых, она состоит из отдельных преступлений, т.е. деяний, наказуемых именно и только действующим уголовным законодательством. Во-вторых, в нее входят все преступления, совершенные в той или иной стране или гражданами этой страны за определенный промежуток времени независимо от того, выявлены ли они и повлекли ли они наказание[1]. Таким образом, преступность как социально-правовое явление имеет противоправный характер, географические и временны*е* границы. Она обладает приспособляемостью к социальным переменам, проявляя тенденцию к постоянному преумножению не только количественного и видового разнообразия самих преступных актов, но и способов их подготовки, совершения и сокрытия.

В последние годы сформировалась устойчивая причинно-следственная связь между количественным разнообразием современных информационных технологий и качественными изменениями в структуре российской преступности. Повсеместное распространение и довольно быстрое развитие технологий такого рода формирует практически безграничные возможности для подготовки, совершения и сокрытия преступлений абсолютно новыми способами и средствами. В не меньшей мере они позволяют формировать и совершенствовать методические основы выявления, раскрытия

[1] *Жалинский А.Э.* Избранные труды. Т.1. М., 2014. С. 146.

и расследования преступлений, совершаемых с помощью разнообразных компьютерных и сетевых технологий. Однако по различным причинам это происходит очень медленно и бессистемно. Значительно быстрее приходит понимание того, что преступность все больше и больше «уходит» в цифровую среду. Соответственно, правоохранительным органам государства необходимы новые научные методы борьбы с ней в киберпространстве и своевременного предотвращения тех или иных ее проявлений. Следовательно, задача их разработки и повсеместного внедрения в следственную практику весьма остро стоит перед российской криминалистикой как самостоятельной отраслью научного знания.

Все это не дает оснований для вывода о скорой и полной победе над киберпреступностью. Причин для этого немало.

За почти два века отечественная криминалистика накопила довольно большой массив высококлассной научной информации. Она содержится в многочисленных диссертациях, монографиях, статьях, тезисах и отдельных практических рекомендациях, призванных оптимизировать предотвращение, выявление, раскрытие, расследование преступлений и судебное рассмотрение уголовных дел. На фоне таких вполне очевидных научных достижений кажется нелепым вопрос — почему при таком обилии новых идей, концепций, технологий, криминалистических алгоритмов, программ расследования прогресс в деле борьбы с преступностью остается незаметным? Более того, следственная и судебная практика нередко игнорирует то, что ей предлагает отечественная криминалистическая наука, а ее достижения подвергаются справедливой критике за их явное отставание от нужд правоохранительных органов. Несомненным признанием бессилия науки, возникшего на данном этапе ее развития, являются публикации самих ученых-криминалистов, в которых анализируются кризисные явления в отечественной криминалистике и формулируются заслуживающие внимания предложения об их преодолении[2].

Ничего удивительного в такой постановке вопроса нет, поскольку российская криминалистика довольно долго «варится лишь в собственном соку» в отрыве от ведущих зарубежных исследовательских школ. Она уже перестала быть дидактическим эталоном не только в странах, некогда строивших социализм, но и во многих государствах, отпочковавшихся от Советского Союза. Если российские криминалисты и дальше будут видеть свои научные интересы только лишь в национальных границах либо в пределах русскоговорящих пространств, игнорируя, таким образом, свободный обмен научной информацией с коллегами из других стран мира, то наука, которую им выпала честь представлять, рискует рано или поздно остаться на

[2] См., напр.: *Эксархопуло А.А.* Предмет и система криминалистики. Проблемы развития на рубеже XIX — XX вв. Курс лекций. СПб., 2004. 112 с.; *Сокол В.Ю.* Кризис отечественной криминалистики. Краснодар, 2017. 332 с. и др.

обочине глобальных интеграционных процессов и превратиться в невостребованный конгломерат наукообразного типа.

При этом значительная часть российских криминалистов не признает кризисного состояния своей науки и соответственно противится не только переосмыслению надуманных теоретических конструкций криминалистики, но и их целенаправленному осовремениванию. Оговоримся, что мы не настаиваем на том, чтобы огульно отвергать прошлые достижения отечественной криминалистики. Необходима их систематизация и переоценка с учетом реалий сегодняшнего дня, выделение в них знания действительно ценного и ожидающего своего дальнейшего поступательного развития. Особую и ярко выраженную актуальность эти задачи приобретают в деле имплементации в научные ресурсы отечественной криминалистики современных информационных технологий.

Прежде чем перейти к обоснованию этой мысли, следует отметить, что сейчас они занимают в экономике страны особенное место, а их эффективное функционирование является одним из важнейших факторов, способствующих решению ключевых задач государственной политики. Важно отметить, что в России они являются наиболее зависимыми от использования импортного программного обеспечения (до 90% операционных систем и систем управления базами данных). Вместе с тем технологическая независимость России в сфере информационных технологий провозглашена основой не только информационной безопасности, но и безопасности государства в целом, в том числе от преступных посягательств[3]. Помимо прочего, информационные технологии должны сыграть важную роль в дальнейшем поступательном развитии отечественной криминалистики. Стало очевидно, что в ней назрел ряд вопросов, ожидающих комплексного решения. Необходимо, в частности, реализовать меры, направленные на разработку и внедрение новых способов выявления, раскрытия и расследования преступлений, совершаемых в киберпространстве.

Распространение компьютерных вирусов, мошенничества с платежными картами, хищения денежных средств с банковских счетов, компьютерной информации, нарушение правил эксплуатации разного рода автоматизированных электронных систем — далеко не полный перечень преступлений, совершаемых с их помощью. Данное явление принято называть по-разному: киберпреступностью, компьютерными преступлениями, преступлениями в сфере компьютерных технологий, преступлениями в сфере компьютерной информации и т.д. В литературе, изданной за последнее десятилетие, наибо-

[3] Постановление Совета Федерации от 20.04. 2016 № 154-СФ «О развитии информационных технологий в Российской Федерации и мерах поддержки отечественной ИТ-отрасли» // СПС КонсультантПлюс.

лее часто встречаются два термина: «*киберпреступления*» и «*компьютерные преступления*». Их можно считать равнозначными, поскольку они используются для обозначения группы одних и тех же общественно-опасных деяний. В криминалистическом аспекте киберпреступления (или компьютерные преступления) — это общественно опасные деяния, для подготовки, совершения, а, соответственно, выявления, раскрытия и расследования которых применяются разного рода компьютерные технологии и (или) используется информационно-телекоммуникационная сеть «Интернет».

Причиной популярности и стремительного роста киберпреступности как криминального бизнеса прежде всего является его невероятная прибыльность, а процесс получения доходов, которые могут превышать миллионы долларов, обычно не отождествляется с риском разоблачения и наказания в широком их понимании. Поэтому киберпреступность наряду с экологией, коррупцией и незаконным оборотом наркотиков фактически стала важнейшей проблемой геополитического масштаба. С наступлением нового века ее решению стало уделяться много внимания как на национальных уровнях, так и в рамках реализации программ международного сотрудничества государственных правоохранительных органов.

Главная криминалистическая особенность киберпреступлений заключается в том, что их предотвращение, выявление, раскрытие и расследование невозможно без современных информационных технологий. Соответственно возникла необходимость во все большем внимании к подготовке специалистов для борьбы с такими преступлениями, переподготовке действующих кадров с тем, чтобы разоблачать преступников посредством обнаружения, фиксации, изъятия и использования разного рода «электронных» доказательств.

Однако существующая система противодействия преступным посягательствам, совершенным с использованием современных информационных технологий, заметно отстает в своем развитии. Трудности обусловлены спецификой совершения преступлений данной разновидности, которая, на наш взгляд, заключается в следующем: в доступности самым широким слоям населения (т.е. повсеместной распространенности и относительной дешевизне) компьютерной техники; в весьма «большой» и фактически трансграничной географии совершения преступлений; в однозначной досягаемости объекта преступного посягательства (т.е. фактическое расстояние до него не имеет значения); в комфортности условий, сопутствующих подготовке и совершению преступлений в киберпространстве (т.е. их подготовка и совершение могут осуществляться практически с любого персонального компьютера, имеющего выход во Всемирную паутину).

Сам процесс выявления, раскрытия и предварительного расследования преступлений, совершенных с использованием современных информаци-

онных технологий, имеет ряд существенных особенностей. Ошибки, допускаемые при этом следователями и дознавателями, в своем большинстве являются следствием их неудовлетворительной профессиональной подготовки именно к этому сегменту криминалистической деятельности. Одной из наиболее существенных причин низкого качества предварительного расследования преступлений, совершаемых в киберпространстве, в научных публикациях справедливо признается отсутствие качественных методических разработок, в реализации которых были бы в полной мере использованы современные информационные технологии. В таких условиях объективные сложности обнаружения, фиксации и изъятия криминалистически значимой информации с целью ее дальнейшего использования в качестве доказательств по уголовному делу нередко становятся непреодолимыми. Более того, здесь как нигде высока вероятность того, что доказательства, которые все же были обнаружены, могут быть непреднамеренно изменены и даже утрачены как в результате ошибок при их фиксации или изъятии, так и в ходе их исследования. Подготовка в ходе досудебного производства по уголовному делу доказательств такого рода для дальнейшего представления их в суде обязательно требует не только основательной профессиональной подготовки, но и регулярного обновления имеющихся знаний у следователей, дознавателей, оперативных работников, и, разумеется, у специалистов и экспертов.

В контексте затронутой проблемы важно отметить, что исследования, посвященные именно получению, обработке, использованию и хранению информации, стали проводиться с середины XX века, т.е. сравнительно недавно. Понадобилось еще примерно 50 лет для того, чтобы информационные технологии получили повсеместное распространение и стали доступными практически всем. В начале 1960-х годов в американской юридической печати появился и стал активно использоваться термин «компьютерная преступность». Примерно в это же время западные социологи и социальные философы (Д. Белл, Д. Рисман, А. Турень и др.) стали обсуждать вопрос о вступлении в качественно иную стадию социального развития, охарактеризованную ими как «постиндустриальное», или «информационное» общество. В последующие годы развитие информационных технологий привело к появлению преступлений новых видов и, как следствие, к значительному увеличению научных исследований. Постепенно стало понятно, что практически все они носят междисциплинарный характер и используют достижения многих наук и в первую очередь криминалистики.

Из общего массива работ, посвященных данной проблематике, можно выделить диссертационные исследования А.В. Касаткина[4] и С.В. Киселе-

[4] *Касаткин А.В.* Тактика собирания и использования компьютерной информации при расследовании преступлений: автореф. дис. … к. ю. н. М., 1997. 23 с.

ва[5], имевшие место в конце 90-х годов прошлого века, а также диссертации А.А. Шаевича[6], Ю.А. Куриленко[7], А.В. Нарижного[8], С.А. Ковалева[9], А.А. Косынкина[10], К.В. Костомарова[11] и В.О. Давыдова[12], защищенные в период с 2007 по 2013 гг. Обращает на себя внимание то обстоятельство, что диссертационные исследования названных авторов (за одним только исключением) проводились не в столичных городах (Москве или Санкт-Петербурге), а в региональных центрах. Причем последнее из них (диссертационное исследование В.О. Давыдова) было защищено в 2013 году, т.е. около пяти лет тому назад. «Застой» отчасти был компенсирован монографическими работами профессоров Е.П. Ищенко[13], В.Б. Вехова[14] и некоторых других российских криминалистов, проявивших интерес к данной проблематике. Однако этого оказалось явно недостаточно.

В науке уголовного права и криминологии наблюдается примерно такая же картина. Вывод неутешительный: отсутствие системного и институционального характера в исследовательской работе на этом направлении ощутимо затрудняет борьбу с преступлениями, совершаемыми с использованием постоянно совершенствующихся информационных технологий. Сама информация выступает объектом преступного посягательства в этой сфере. Ее хищение, изменение, неправомерное использование так или иначе вносят диссонанс в функционирование экономических систем. Более того,

---

[5] *Киселев С. В.* Проблемы расследования компьютерных преступлений: автореф. дис. … к. ю. н. СПб., 1998. 23 с.

[6] *Шаевич А.А.* Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений: автореф. дис. … к. ю. н. Иркутск, 2007. 24 с.

[7] *Куриленко Ю.А.* Компьютерные технологии как средство повышения эффективности организации правоохранительной деятельности (применительно к деятельности ОВД по расследованию преступлений): автореф. дис. … к. ю. н. Саратов, 2008. 23 с.

[8] *Нарижный А.В.* Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: автореф. дис. … к. ю. н. Краснодар, 2009. 22 с.

[9] *Ковалев С.А.* Основы компьютерного моделирования при расследовании преступлений в сфере компьютерной информации: автореф. дис. … к. ю. н. Воронеж, 2011. 22 с.

[10] *Косынкин А.А.* Преодоление противодействия расследованию преступлений в сфере компьютерной информации: автореф. дис. … к. ю. н. Саратов, 2012. 24 с.

[11] *Костомаров К.В.* Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков: автореф. дис. … к. ю. н. Челябинск, 2012. 30 с.

[12] *Давыдов В.О.* Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: автореф. дис. … к. ю. н. Ростов-на-Дону, 2013. 26 с.

[13] См., напр.: *Ищенко Е.П.* Виртуальный криминал. М., 2015. 232 с.

[14] См., напр.: *Вехов В.Б.* Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев. Судебная экспертиза. М., 2016. С. 10–19.

в отличие от организованной преступности, коррупции, терроризма и экстремизма деятельность киберпреступников не согласуется с известными и привычными в обществе моделями поведения. По сути это означает, что она индивидуальна, иррациональна, анонимна и интернациональна, а каждый человек в современном мире, от обывателя до крупной компании, банка и государства, рискует в любой момент стать жертвой злоумышленников в киберпространстве, постоянно изобретающих новые и разнообразные схемы мошеннических операций. Положение осложняется тем, что даже если факт совершения киберпреступления стал известен пострадавшим от него лицам, то по причине примененных преступниками высокоразвитых технологий, новых тактик и схем суть имевшего место события не может быть во всей полноте объяснена ими с использованием специальных терминов и понятий. В связи с этим у сотрудников правоохранительных органов, осуществляющих проверку информации, возникают неопределенность и разумные сомнения как относительно наличия самого киберпреступления, так и предусмотренного законом основания для возбуждения уголовного дела.

Обращает на себя внимание тот факт, что с начала XXI века и до настоящего времени количество выявленных преступлений в сфере компьютерной информации (ст. 272–274 УК РФ) изменялось практически постоянно. Если в 2001 г. их было зафиксировано около 3,7 тыс., то к 2003 г. их общее количество увеличилось втрое (до 10,4 тыс.). В последующие годы стал наблюдаться некоторый количественный спад. В 2015 г., например, было зафиксировано 2382 таких преступления[15], за совершение которых было осуждено лишь 235 чел. (!). В 2016 г., по данным Судебного департамента при Верховном Суде России, количество осужденных сократилась до 185 чел.[16]

Причины таких несколько странных статистических расхождений различны, но нам они видятся в том, что абсолютное большинство преступлений в сфере компьютерной информации латентны. Специалисты подсчитали, что до 90% данных криминальных актов не находят отражения в официальной уголовной статистике[17]. Наиболее распространенная причина такого положения дел заключается в нежелании практически всех коммерческих предприятий (в том числе банков) предавать гласности сведения о похищении у них компьютерной информации и денежных средств путем

[15] *Михайлова Б.П., Хазова Е.Н.* Особенности противодействия киберпреступности подразделениями уголовного розыска / Состояние преступности в России (за январь — декабрь 2010 г., 2011 г., 2012 г., 2013 г., 2014 г.) [Электронный ресурс]: // URL: http://www.mvd.ru (дата обращения: 28.02.2018)

[16] [Электронный ресурс]: // URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 31.03.2018)

[17] См., напр.: *Тарасов А.М.* Электронное правительство и информационная безопасность. СПб., 2011. 647 с.

виртуальных взломов систем их защиты. Объяснение этому простое — все они предпочитают дорожить репутацией и опасаются потерять клиентов, а доказывание фактов совершения таких преступлений — довольно обременительное и дорогостоящее занятие. Криминалисты правильно отмечают, что в современных условиях многие организации стремятся разрешить подобные ситуации своими силами, поскольку убытки от их расследования неминуемо окажутся значительно выше суммы причиненного ущерба[18].

К категории латентных, несомненно, должна быть также отнесена совокупность преступлений, о факте совершения которых ничего не известно ни правоохранительным органам, ни представителям компаний, ни отдельным лицам. К латентным следует относить и такие киберпреступления, информация о которых известна правоохранительным органам, но проверяющие ее сотрудники, не обладая необходимыми навыками их раскрытия и расследования, не в состоянии дать верную юридическую оценку обстоятельствам совершенных деяний. Таким образом, они остаются за рамками официальной отчетности или умышленно укрываются от учета.

В США и многих странах Европейского континента к настоящему времени технология поиска киберпреступников отработана. Расходы на розыск каждого из них в среднем составляют немногим более 300 долл.[19] Борьба с киберпреступлениями российских правоохранительных органов оставляет желать лучшего. Если выразиться яснее, то киберпреступности некому противостоять. Только 4,5% следователей обладают более или менее удовлетворительными знаниями по специальности «Информатика и вычислительная техника». Около 72% из них оценивают свой уровень владения персональным компьютером «как у среднего пользователя»[20]. Здесь есть над чем работать.

Звучит весьма вызывающе и несколько странно, но гораздо эффективнее борьбу с киберпреступлениями в России пока осуществляет несколько агентств, специализирующихся на инициативном расследовании высокотехнологичных преступлений. Они действуют не только в силу собственной заинтересованности в извлечении прибыли, но и по причине у их бо́льших возможностей, знаний и технологического потенциала. Компания «Group-IB», например, за полтора десятилетия своего существования расследовала

---

[18] См., напр.: *Коликов Н.Л.* Причины и условия профессиональной компьютерной преступности // Вестник ЮУрГУ. Серия: Право. 2011. № 19 [Электронный ресурс]: // URL: http://cyberleninka.ru/article/n/prichiny-i-usloviya-professionalnoy-kompyuternoy-prestupnosti (дата обращения: 31.03.2018)

[19] [Электронный ресурс]: // URL: http://itua.info/software/28662.html (дата обращения: 31.03.2018)

[20] *Шевченко Е.С.* Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист. 2015. № 3. С. 29–30.

около тысячи высокотехнологичных преступлений, немалая часть которых являлись особенно сложными[21]. Агентство финансовой и правовой безопасности также на этом поприще достигло успехов, в основном, за счет использования в работе своих сотрудников не только новейших информационных технологий, но и аккаунтов в социальных сетях (анализируя списки «друзей» на наличие общих признаков)[22]. Согласно данным, полученным компанией «Juniper Research», при сохранении текущего уровня кибератак в ближайшие годы общие убытки мировой экономики от них к 2019 г. составят 2,1 трлн. долл.[23] Что касается России, то ущерб от кибератак имевших место на ее территории в 2015 г., например, составил сумму, равную половине затрат российского бюджета на здравоохранение (приблизительно 1 трлн. 423 млрд. руб.!)[24].

Таким образом, большинство изменений, возникших по причине развития информационных технологий, принесли пользу обществу, прежде всего в науке в целом, а практически — в медицине, инженерии, управлении ресурсами (в том числе финансовыми). Однако они же предопределили появление новых возможностей причинения вреда интересам общества и государства, поскольку с появлением технологических новаций возникли основывающиеся на них новые разновидности преступлений, такие, например, как хакерский взлом, внедрение шпионских программ и др. Если бы не технологический прорыв в области информационно-коммуникационных технологий, то, наверное, их не существовало бы в природе.

В иностранной литературе описаны три основных подхода к определению понятия «киберпреступление». В рамках первого из них оно понимается как преступление, совершение которого связано с сетевыми технологиями[25]. Второй подход более широк. В его рамках киберпреступление рассматривается как любое преступление, совершаемое с использованием компьютеров

---

[21] *Сачков И.* Технологии позволяют бороться с киберпреступностью — этот бизнес становится неэффективным [Электронный ресурс]: // URL: http://sk.ru/news/b/press/archive/2017/12/20/ilya-sachkov-tehnologii-pozvolyayut-borotsya-s-kiberprestupnostyu-_1320_-etot-biznes-stanovitsya-neeffektivnym.aspx (дата обращения: 31.03.2018)

[22] Как современные Шерлоки Холмсы находят интернет-мошенников // Статус. 2012. № 8 (19). С. 7.

[23] Общемировые убытки от киберпреступности составят $ 2,1 трлн до 2019 года [Электронный ресурс]: // URL: http://www.securitylab.ru/news/472924.php. (дата обращения: 31.03.2018)

[24] *Трунцевский Ю.В.* Состояние и тенденции преступности в Российской Федерации и прогнозы ее развития // Российская юстиция. 2016. № 8. С. 29–31.

[25] *Viano E.* Cybercrime: a new frontier in criminology // International Annals in Criminology. 2006. Vol. 44. P. 14; *Stephenson P., Gilbert K.* Investigating computer-related crime. 2013 [Электронный ресурс]: // URL: https://books.google.ru/books?id=2c0nAAAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false (дата обращения: 28.02.2018); *Finklea K., Theohary C.* Cybercrime: conceptual issues for congress and U. S. law enforcement. Congressional Research Service, 2015. P. 3.

и сетей. Также считается, что при совершении киберпреступления могут быть использованы не только компьютеры, но и любые технические устройства[26]. Третий подход к толкованию этого понятия основывается на том, что преступления такого рода также совершаются при помощи сетевых и компьютерных технологий. Вместе с тем его сторонники отрицают необходимость разграничения понятия «киберпреступление» от других понятий, используемых для описания схожих феноменов (например, компьютерное преступление, высокотехнологичное преступление, цифровой инцидент и т.д.)[27]. Следовательно, главными характеристиками, определяющими то или иное противоправное деяние как киберпреступление, правильнее всего считать его совершение с помощью компьютерных и сетевых технологий.

Криминалисты отмечают, что в современных условиях практически все разновидности преступлений могут быть совершены при помощи персонального компьютера, исключая, пожалуй, некоторые преступления против жизни и здоровья граждан[28]. При совершении киберпреступлений нередко осуществляются прямые атаки на компьютеры или другие устройства с целью вывода их из строя. Иногда атакованные компьютеры используются для распространения вредоносных программ, незаконной информации, разного рода изображений (например, детской порнографии) и других материалов.

В новейшей юридической литературе выделяются следующие виды киберпреступлений: корыстные киберпреступления (фишинг, кибервымогательство, финансовое мошенничество и др.), хищение персональных данных, кибершпионаж, кибербуллинг, нарушение авторских прав и некоторые другие. Рассматривая их, нужно учитывать, что в современных условиях в легальный экономический оборот активно поступают «нетрадиционные» виды имущества (в том числе веб-сайты, криптовалюты, технологии мобильной связи, интернет-имущество и т.п.)[29]. Поскольку они обладают способностью приносить высокие доходы, на них соответствующим образом реагирует криминальная среда. В результате появляются все новые виды преступных посягательств, предполагающие использование современных

---

[26] *Thomas D., Loader B.* Cybercrime: law enforcement, security and surveillance in the information age. London: England: Routledge, 2000. P. 3; *Casey E.* Digital evidence and computer crime. Elsevier: Academic Press, 2004. P. 28; *Wall D.* Cybercrime as a conduit for criminal activity // Information, Technology and the Criminal Justice System. Beverly Hills, CA: Sage Publications, 2005. P. 81; *Kirwan G., Power A.* The psychology of cyber crime: concepts and principles. Hershey, PA: Information Science Reference, 2012. P. 15.

[27] *Viano C.* Cybercrime, organized crime, and societal responses: international approaches. Dordrecht: Springer International Publishing, 2017. P. 7.

[28] См., напр.: *Степанов-Егиянц В.Г.* Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М., 2016. 190 с.

[29] *Некрасов В.Н.* Актуальные вопросы уголовно-правовой охраны информационной деятельности в России // Актуальные проблемы российского права. 2017. № 7. С. 108–114.

информационных технологий на условиях внезапности и анонимности[30]. Практически все названные противоправные деяния значительно опаснее иных преступлений, совершаемых вне киберпространства, поскольку обладают способностью причинять ущерб всем охраняемым законом интересам. Их диапазон варьируется от частных неимущественных интересов отдельных граждан до интересов безопасности государства.

Изучение следственной практики показывает, что перед совершением преступлений данной категории злоумышленники нередко проводят масштабные организационные и технические подготовительные мероприятия. Они изучают характеристики программно-аппаратных средств, определяют уровень защиты информации, оптимальные пути доступа к ней, принимают иные меры. Факты осуществления таких действий могут при определенных условиях фиксироваться. Из их числа криминалисты выделяют технологии, позволяющие обнаруживать попытки проникновения в компьютерные системы, а также процедуры регистрации программных операций и действий персонала[31].

Сведения, изложенные, проанализированные и систематизированные в данной статье, несомненно, подтверждают правильность позиции, доминирующей среди российских криминалистов, что борьба с киберпреступностью является проблемой международного масштаба. Действительно, поскольку меры по предотвращению, выявлению, раскрытию и расследованию преступлений, совершаемых с использованием современных информационных технологий, не могут быть результативными лишь на национальном уровне в силу транснационального и трансграничного характера самой сети «Интернет». Более того, непрекращающееся увеличение численности ее пользователей закономерно порождает их зависимость от информационного сообщества и уязвимость от разного рода киберпосягательств. Одновременно растет вероятность стать очередной жертвой киберпреступности[32]. Именно поэтому одним из принципов Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. провозглашено обеспечение государственной защиты интересов российских граждан в информационной сфере. Необходимость в этом вызвана множеством факторов, из которых следует выделить: увеличение объемов информации, обрабатываемой и хранимой в киберпространстве; ее «привлекательность» для преступников; повышенную скрытность совершения преступлений и отсутствие их связи

[30] *Рассолов И.М.* Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2. С. 44–46.

[31] *Степанов В.В.* Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий. М., 2014. С. 167–169.

[32] *Русскевич Е.А.* Уголовное право и информатизация // Журнал российского права. 2017. № 8. С. 73–80.

с определенной территориальной локацией; существование объективных сложностей их выявления, раскрытия и расследования; нестандартность, сложность и постоянное обновление способов совершения преступлений; длительную неосведомленность потерпевших о факте их совершения; отсутствие возможности «предотвращения и пресечения преступлений данного вида традиционными средствами»[33].

Библиография

Батоев В.Б., Семенчук В.В. Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии управления МВД России. 2017. № 2. С. 9–15.

Бондаренко Д.Д. Виртуальные валюты: сущность и борьба с их использованием в преступных целях (на примере США) // Международное уголовное право и международная юстиция. 2015. № 6. С. 23–25.

Вехов В.Б. Электронные следы в системе криминалистики / Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Судебная экспертиза. М.: Юрлитинформ, 2016. С. 10–19.

Некрасов В.Н. Актуальные вопросы уголовно-правовой охраны информационной деятельности в России // Актуальные проблемы российского права. 2017. № 7. С. 108–114.

Русскевич Е.А. Уголовное право и информатизация // Журнал российского права. 2017. № 8. С. 73–80.

Сокол В.Ю. Кризис отечественной криминалистики: монография. Краснодар: КрУ МВД России. 2017. 332 с.

Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016. 190 с.

Трунцевский Ю.В. Состояние и тенденции преступности в Российской Федерации и прогнозы ее развития // Российская юстиция. 2016. № 8. С. 29–31.

Шевченко Е.С. Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист. 2015. № 3. С. 29–30.

Casey E. Digital evidence and computer crime. Elsevier: Academic Press, 2004. 690 p.

Finklea K., Theohary C. Cybercrime: conceptual issues for congress and U. S. law enforcement. Congressional Research Service, 2015. 27 p.

Kirwan G., Power A. The psychology of cyber crime: concepts and principles. Hershey, PA: Information Science Reference, 2012. 372 p.

Viano C. Cybercrime, organized crime, and societal responses: international approaches. Dordrecht: Springer International Publishing, 2017. 378 p.

Wall D. Cybercrime as a conduit for criminal activity // Information, Technology and the Criminal Justice System, Beverly Hills CA: Sage Publications, 2005. P. 77–98.

Young J., Foster K., Garfinkel S., Fairbanks K. *Distinct sector hashes for target file detection* // Computer. 2012. N 45. P. 28–3

[33] *Осипенко А.Л.* Сетевая компьютерная преступность. Омск, 2009. С. 109–110.

Phenomenology of the Computer-Oriented Crimes

Alexander S. Shatalov

Professor, Department of Criminal Law and Criminal Science, National Research University Higher School of Economics, Doctor of Juridical Sciences. Address**:** National Research University Higher School of Economics. Address: 20 Myasnitskaya Str., Moscow 101000, Russian Federation. E-mail: asshatalov@rambler.ru**,** asshatalov@hse.ru

Abstract

Phenomenology in its Greek literal interpretation is the doctrine of phenomena, i.e. phenomena or events under observation. In modern philosophy, it acts as a method of scientific analysis of consciousness and immanent, a priori structures of human existence. This article is the result of applying this method to setting and understanding the best ways to solve the problems directly related to the investigation of computer oriented crimes. Having resorted to historical generalizations, the author made an attempt to find an answer to the question why against the backdrop of the doctrinal achievements of domestic criminalistics with so many new ideas, concepts, technologies, forensic algorithms and investigation programs, the progress in combating crime remains underestimated? The main cause of this situation is seen in the fact that Russian criminalistics for a long time developed apart from the leading foreign research schools. In turn, this situation is still preserved despite the global integration processes that have taken hold practically all the countries of the world. As the main direction of overcoming the crisis phenomena, the author positions the implementation in the scientific resources of domestic criminalistics of modern information technologies in general, and, to increase the effectiveness of combating crimes committed using computer and network capabilities, in particular. He considers the fight against them to make an international problem, since the measures to prevent, detect, uncover and investigate crimes committed using modern information technologies cannot be effective only at the national level, because of the transnational and transborder nature of the Internet itself. Given the continuing increase in the number of its users, which naturally causes their dependence on the information community and the vulnerability of all kinds of cyberattacks, a scientific analysis of the current state of investigation of crimes of this kind is made and recommendations are formulated to raise the effectiveness of this activity.

Keywords

information technologies; cybercrime; computer crimes; criminalistics; forensic methodology; investigation of crimes; forensic methodology; informational resources; criminal proceedings; forensic information.

Citation: Shatalov A.S. (2018) Phenomenology of the Computer-Oriented Crimes. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 2, pp. 68–83 (in Russian)

DOI: 10.17323/2072-8166.2018.2.68.83

References

Batoev V.B., Semenchuk V.V. (2017) Ispol'zovanie kriptovalyuty v prestupnoy deyatel'nosti: problemy protivodeystviya [Using cryptocurrency in crimes: issues of counteracting]. *Trudy Akademii upravleniya MVD Rossii*, no 2, pp. 9–15.

Bondarenko D.D. (2015) Virtual'nye valyuty: sushchnost' i bor'ba s ikh ispol'zovaniem v prestupnykh tselyakh [Virtual currencies and tackling their use for criminal purposes]. *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yustitsiya*, no 6, pp. 23–25.

Casey E. (2004) *Digital evidence and computer crime*. Elsevier: Academic Press, 690 p.

Finklea K., Theohary C. (2015) *Cybercrime: conceptual issues for congress and US. law enforcement*. Washington, D.C.: Congressional Research Service, 27 p.

Kirwan G., Power A. (2012) *The psychology of cyber crime: concepts and principles*. Hershey, PA: Information Science Reference, 372 p.

Nekrasov V.N. (2017) Aktual'nye voprosy ugolovno-pravovoy okhrany informatsionnoy deyatel'nosti v Rossii [Criminal law protection of information activity in Russia]. *Aktual'nye problemy rossiyskogo prava*, no 7, pp. 108–114.

Russkevich E.A. (2017) Ugolovnoe pravo i informatizatsiya [Criminal law and information technologies]. *Zhurnal rossiyskogo prava*, no 8, pp. 73–80.

Shevchenko E.S. (2015) Aktual'nye problemy rassledovaniya kiberprestupleniy [Issues of investigating cybercrimes]. *Ekspert-kriminalist*, no 3, pp. 29–30.

Stepanov-Egiyants V.G. (2016) *Otvetstvennost' za prestupleniya protiv komp'yuternoy informatsii po ugolovnomu zakonodatel'stvu Rossiyskoy Federatsii* [Liability for a crime against computer information under RF criminal law]. Moscow: Statut, 190 p. (in Russian)

Sokol V. Yu. (2017) *Krizis otechestvennoy kriminalistiki* [Crisis of Russian criminal science]. Krasnodar: MVD Rossii, 332 p. (in Russian)

Truntsevskiy Yu.V. (2016) Sostoyanie i tendentsii prestupnosti v Rossiyskoy Federatsii i prognozy ee razvitiya [State and Trends in crime in Russia and forecasts]. *Rossiyskaya yustitsiya*, no 8, pp. 29–31.

Vekhov V.B. (2016) Elektronnye sledy v sisteme kriminalistiki [Electronic signs in criminal science]. *Sudebnaya ekspertiza*. Moscow: Yurlitinform, pp. 10–19.

Viano C. (2017) *Cybercrime, organized crime, and societal responses: international approaches*. Dordrecht: Springer International Publishing, 378 p.

Wall D. (2005) *Cybercrime as a conduit for criminal activity. Information, Technology and the Criminal Justice System*. Beverly Hills, CA: Sage Publications, pp. 77–98.

Young J. et al. (2012) Distinct sector hashes for target file detection. *Computer*, no 45, pp. 28–35.