УДК 343.98:004

Александр Семенович ШАТАЛОВ,
профессор кафедры уголовного права и криминалистики Национального исследовательского университета «Высшая школа экономики», доктор юридических наук, профессор
asshatalov@hse.ru

РАЗРАБОТКА МЕТОДИЧЕСКИХ ОСНОВ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПОМОЩЬЮ КОМПЬЮТЕРНЫХ И СЕТЕВЫХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ И ТЕНДЕНЦИИ

WORKING OUT OF THE METHODOLOGY BASES FOR INVESTIGATION OF CRIMES COMMITTED BY COMPUTER AND NETWORK TECHNOLOGIES: ACTUAL PROBLEMS, PROSPECTS AND TRENDS

В статье предпринята попытка проанализировать киберпреступность как относительно новое и малоисследованное социально-правовое явление. Борьбу с ней автор считает задачей международного масштаба, 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. Автором произведен научный анализ современного состояния расследования преступлений такого рода и сформулированы рекомендации по повышению эффективности этой деятельности. В качестве главного направления им позиционируется имплементация современных информационных технологий в научные ресурсы отечественной криминалистики в целом и для повышения эффективности борьбы с преступлениями, совершаемыми с использованием компьютерных и сетевых возможностей, в частности.

In the given article the author tries to analyze cybercrime as a relatively new and little-investigated social and legal phenomenon. The author considers a counteraction to cybercrime to be an international challenge because measures for prevention, exposure and investigation of crimes, committed with using of modern information technologies, cannot be effective on the national level due to transnational and across-the-border character of Internet. The author conducted scientific analysis of modern cybercrime investigation and made recommendations for raising effectiveness of this activity. He suggests to apply the modern information technologies to the scientific recourses of national criminalistics, in general and to use them for improving the effectiveness in combating crimes committed with using of computer and net possibilities, in particular.

Ключевые слова: *информационные технологии; киберпреступность; компьютерные преступления; криминалистика; криминалистическая методика; расследование преступлений.*

Keywords: *information technologies, cybercrime, computer crimes, criminalistics, forensic methodology, investigation of crimes.*

Криминалисты в своих трудах правильно отмечают, что в современных условиях практически все разновидности преступлений могут быть совершены при помощи персонального компьютера, за исключением некоторых противоправных действий против жизни и здоровья граждан. [21] 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 последние годы наибольшее распространение получили следующие виды киберпреступлений: корыстные киберпреступления (в том числе 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 интернет-сайты, электронные деньги, технологии мобильной связи, интернет-имущество и т.п.). [13] 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 информационных технологий на условиях внезапности и анонимности. [17] 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.

В мае 2017 года Президент РФ В.В. Путин утвердил Стратегию развития информационного общества в Российской Федерации на 2017-2030 годы. В ней впервые было употреблено понятие «критическая информационная инфраструктура Российской Федерации» и подчеркнута важность ее защиты «с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы». Информационная безопасность Российской Федерации в этом документе трактуется как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Сама же система обеспечения информационной безопасности признана неотъемлемой частью системы обеспечения национальной безопасности Российской Федерации. [22]

Появление данной Стратегии фактически означает взятие курса на постепенный, но скорый и максимально полный отказ нашего государства от заимствования иностранных информационных технологий, за счет целенаправленного и последовательного преодоления собственного технологического отставания. С ее появлением в российском правовом поле практически ни у кого из прогрессивно мыслящих представителей юридического сообщества не осталось сомнений в том, что «только национальный проект в области информационных технологий и разработка собственных решений позволят нам сохранить цифровой суверенитет» [27] и эффективно осуществлять охрану общественного порядка.

С наступлением нового века информационные технологии превратились в неотъемлемую часть жизни общества, охватив практически все ее сферы. Для того чтобы объективно оценить их несомненную пользу, нужно отчетливо представлять масштабы вреда, который они способны причинить человечеству.

Ни для кого не секрет, что многие россияне, включая незаконопослушную их часть, являются в значительной степени интернет-зависимыми. По имеющимся у нас данным, не менее 87% пользователей компьютеров

выходят в Интернет ежедневно. Неуклонный рост их числа и стремительное распространение новых информационных технологий не дают возможности полно, объективно, а главное, своевременно осмысливать криминальные новшества в киберпространстве и сопряженные с ними риски. Это не только новые вирусы, уязвимости и закладки, но и реальная угроза несанкционированного доступа, отсутствие приватности, утечка персональных данных пользователей сети, тотальный контроль российского рынка иностранными производителями и т.д., и т.п. Оценивая реальные и потенциальные риски нужно понимать, что все современные девайсы – интернет-сервисы, теле– и радиоприспособления, транспорт, связь, промышленные комплексы – прочно связаны с Интернетом и обновляются извне. Это значит, что и управляются они таким же путем.

Наблюдается 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 нисколько не меньшей мере они позволяют разрабатывать и совершенствовать методические основы выявления, раскрытия и расследования преступлений, совершаемых с помощью разнообразных компьютерных и сетевых технологий. Однако по разным причинам это происходит очень медленно. Значительно быстрее пришло осознание 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 ожидаемых ее проявлений. Именно эта задача сейчас остро стоит перед российской криминалистикой как самостоятельной отраслью научного знания.

Подчеркивая неуклонно возрастающую актуальность этой задачи, важно отметить, что за почти два века существования в отечественной криминалистике был накоплен 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 застойных процессов в науке, возникших на данном этапе ее развития, являются публикации самих ученых-криминалистов (в том числе наши работы), в которых анализируются кризисные явления в отечественной криминалистике и формулируются заслуживающие внимания предложения по их преодолению. [31, 25, 29, 20]

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 неким 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 евроазиатских 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 обочине глобальных интеграционных процессов и превратиться в маловостребованный конгломерат наукообразного типа. При всем этом значительная часть российских криминалистов не признают кризис-

ного состояния своей науки и, соответственно, противятся 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. Необходимы их систематизация и переоценка с учетом реалий сегодняшнего дня, выделение знания, действительно ценного и ожидающего своего дальнейшего поступательного развития. Особую актуальность эти задачи приобретают в деле имплементации в научные ресурсы отечественной криминалистики новых сведений, основанных на использовании современных компьютерных и сетевых технологий.

Прежде чем перейти к обоснованию этой мысли, следует отметить, что сейчас технологии такого рода занимают в экономике страны особое место, а их эффективное функционирование является одним из важнейших факторов, способствующих решению ключевых задач государственной политики. В Российской Федерации они являются наиболее зависимыми от использования импортного программного обеспечения (до 90% операционных систем и систем управления базами данных). С учетом этого факта технологическая независимость Российской Федерации в сфере информационных технологий провозглашена основой не только информационной безопасности, но и безопасности государства в целом, в том числе от преступных посягательств. [14]

Помимо прочего, информационные технологии должны сыграть важную роль в обеспечении дальнейшего поступательного развития отечественной криминалистики. Сейчас стало очевидно, что в ней назрел ряд вопросов, ожидающих комплексного решения. Выше уже говорилось, что необходимо, в частности, как можно скорее 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 и разного рода компьютерной информации, нарушение правил эксплуатации автоматизированных электронных систем – вот далеко не полный перечень преступлений, совершаемых с помощью информационных технологий. Данное явление в научных публикациях принято именовать по-разному: киберпреступностью, компьютерными преступлениями, преступлениями в сфере компьютерных технологий, преступлениями в сфере компьютерной информации и др. В юридической литературе, изданной за последнее десятилетие, наиболее 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, сокрытия, 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 некоего криминального бизнеса прежде всего является его невероятная прибыльность, а сам процесс получения доходов, которые могут превышать миллионы долларов, обычно не отождествляется с риском разоблачения и наказания в широком их понимании. Поэтому сама 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 национальном уровне, 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 использования современных информационных технологий. Соответственно, возникла необходимость во все бóльшем внимании к подготовке специалистов для борьбы с такими престу-

плениями, переподготовке действующих кадров, с тем чтобы эффективно разоблачать преступников посредством обнаружения, фиксации, изъятия и использования разного рода «электронных» доказательств.

Однако существующая система противодействия преступным посягательствам, совершенным с использованием современных информационных технологий, пока заметно отстает в своем развитии. Сложности обусловлены спецификой совершения преступлений данной разновидности, которая, на наш взгляд, заключается в следующем:

в доступности (т.е. повсеместной распространенности и относительной дешевизне) компьютерной техники для самых широких слоев населения;

в весьма обширной и фактически трансграничной географии совершения преступлений;

в однозначной досягаемости объекта преступного посягательства (т.е. фактическое расстояние до него не имеет никакого значения);

в комфортности условий, сопутствующих подготовке и совершению преступлений (т.е. их подготовка и совершение реально могут осуществляться практически с любого персонального компьютера, имеющего выход во Всемирную паутину).

Сам процесс выявления, раскрытия и предварительного расследования преступлений, совершенных с использованием современных информационных технологий, также имеет ряд существенных особенностей. Ошибки, допускаемые при этом следователями и дознавателями, в большинстве являются следствием их неудовлетворительной профессиональной подготовки именно для этого сегмента 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 задействованы 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 те доказательства, что все же были обнаружены, могут быть непреднамеренно изменены и даже утрачены как в результате допущенных ошибок при их фиксации или, например, изъятии, так и в ходе их исследования. Подготовка в ходе досудебного производства по уголовному делу доказательств такого рода для дальнейшего представления их в суде требует обязательного наличия 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 развитие информационных технологий привело не только к появлению преступлений новых видов, но и к резкому увеличению научных исследований соответствующей тематики. 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 [5] и С.В. Киселева [6], имевшие место в конце 90-х годов прошлого века, а также диссертации А.А. Шаевича [28], Ю.А. Куриленко [10], А.В. Нарижного [12], С.А. Ковалева [7], А.А. Косынкина [9], К.В. Костомарова [8] и В.О. Давыдова [2], защищенные в период с 2007 г. по 2013 г. 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, то есть около пяти лет тому назад. Возникшее застойное явление отчасти было компенсировано монографическими работами Е.П. Ищенко [3], В.Б. Вехова [1] и некоторых других российских

криминалистов, проявивших интерес к данной проблематике. Однако этого оказалось явно недостаточно.

В науках 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 компьютерных и сетевых технологий. Сама же информация выступает объектом преступной деятельности в этой сфере. Ее хищение, изменение, неправомерное использование так или иначе вносят диссонанс в функционирование экономических систем. Более того, в отличие от организованной преступности, коррупции, многих проявлений 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 простого обывателя до крупной компании, банка и государства, рискует в любой момент стать жертвой злоумышленников в киберпространстве, постоянно изобретающих новые, сложные и разнообразные схемы мошеннических операций.

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. общее количество увеличилось втрое (10,4 тыс.). В последующие годы стал наблюдаться некоторый количественный спад. В 2015 г., например, было зафиксировано 2382 таких преступления [11], за совершение которых были осуждены лишь 235 человек (!). В 2016 г., по данным Судебного департамента при ВС РФ, эта цифра сократилась до 185 чел. [16]

Причины таких несколько странных количественных расхождений различны, но нам они видятся в том, что абсолютное большинство преступлений в сфере компьютерной информации – латентные. Специалисты правильно утверждают, что до 90% криминальных актов данной разновидности не находят отражения в официальной уголовной статистике. [23] Наиболее распространенная причина такого положения дел нам видится в нежелании практически всех коммерческих предприятий (в том числе банков) предавать гласности сведения о похищении у них компьютерной информации и денежных средств путем виртуальных взломов систем их защиты. Объяснение этому простое – все они предпочитают дорожить репутацией и боятся потерять клиентов, а доказывание фактов совершения таких преступлений – довольно сложное и затратное занятие.

В США и многих странах европейского континента уже отработана технология поиска киберпреступников. Расходы на розыск каждого из них в среднем составляют немногим более 300 долларов. [Цит. по: 26] Борьба с киберпреступлениями российских правоохранительных органов оставляет желать лучшего. А если выразиться более категорично, то пока им особенно 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». [30] Здесь есть над чем работать!

Звучит весьма вызывающе и несколько странно, но гораздо эффективнее борьбу с высокотехнологичными преступлениями в России пока осуществляют несколько частных агентств, специализирующихся на их инициативном расследовании. Они действуют не только в силу собственной заинтересованности в извлечении прибыли, но и по причине наличия у них больших возможностей, знаний и технологического потенциала. Компания «Group-IB», например, за полтора десятилетия своего существования расследовала около тысячи киберпреступлений, немалая часть которых являлись особо сложными. [19] Агентство финансовой и правовой безопасности также достигло определенных успехов на этом поприще в основном за счет использования в работе сотрудников не только новейших информационных технологий, но и аккаунтов в социальных сетях (анализи-

руя списки друзей на наличие общих признаков). [4]

Согласно данным, полученным компанией «Juniper Research», при сохранении текущего уровня кибератак в ближайшие годы общие убытки мировой экономики от их осуществления к 2019 г. составят 2,1 трлн долл. [15] Что касается именно России, то ущерб от имевших место на ее территории кибератак в 2015 г., например, составил сумму, равную половине затрат российского бюджета на здравоохранение (приблизительно 1 трлн 423 млрд рублей!). [24]

Таким образом, большинство изменений, возникших по причине развития информационных технологий, принесли пользу обществу прежде всего в медицине, инженерии, управлении ресурсами (в том числе финансовыми). Однако они же предопределили появление новых возможностей для 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 бы вообще не существовало 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. [37, p. 14; 33, p. 3] Второй подход более широкий. В его рамках киберпреступление рассматривается как любое преступление, совершаемое с использованием компьютеров и сетей. Также считается, что при совершении киберпреступления могут быть задействованы не только компьютеры, но и любые технические устройства. [35, p. 3; 38, p. 81; 32, p. 28] 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 сторонниками отрицается необходимость отграничения понятия «киберпреступление» от других понятий, используемых для описания схожих феноменов (например, компьютерное преступление, высокотехнологичное преступление, цифровой инцидент и т.д.). [36, p. 7] Следовательно, главными характеристиками, определяющими то или иное противоправное деяние как киберпреступление, правильнее всего считать его совершение с помощью компьютерных и сетевых технологий.

Борьба с киберпреступностью является проблемой международного масштаба, 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 в обществе растет вероятность стать очередной жертвой киберпреступности. [18] Именно поэтому одним из принципов Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы провозглашено обеспечение государственной защиты интересов российских граждан в информационной сфере. [22]

Библиографический список

1. Вехов, В.Б. Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. – 2016. – № 2. – С.10-19.
2. Давыдов, В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей : автореф. дис. … канд. юрид. наук / В.О. Давыдов. – Ростов-на-Дону, 2013. – 26 с.
3. Ищенко, Е.П. Виртуальный криминал / Е.П. Ищенко. – М.: Проспект, 2015. – 232 с.
4. Как современные Шерлоки Холмсы находят интернет-мошенников // Статус : правовая газета. – 2012. – №8.1 (19).
5. Касаткин, А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений : автореф. дис. … канд. юрид. наук / А.В. Касаткин. – М., 1997. – 23 с.
6. Киселев, С.В. Проблемы расследования компьютерных преступлений : автореф. дис. … канд. юрид. наук / С.В. Киселев. – СПб., 1998. – 23 с.
7. Ковалев, С.А. Основы компьютерного моделирования при расследовании преступлений в сфере компьютерной информации : автореф. дис. … канд. юрид. наук / С.А. Ковалев. – Воронеж, 2011. – 22 с.
8. Костомаров, К.В. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков : автореф. дис. … канд. юрид. наук. – Челябинск, 2012. – 30 с.
9. Косынкин, А.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации : автореф. дис. … канд. юрид. наук. – Саратов, 2012. – 24 с.
10. Куриленко, Ю.А. Компьютерные технологии как средство повышения эффективности организации правоохранительной деятельности (применительно к деятельности ОВД по расследованию преступлений) : автореф. дис. … канд. юрид. наук / Ю.А. Куриленко. – Саратов., 2008. – 23 с.
11. Михайлова, Б.П. Особенности противодействия киберпреступности подразделениями уголовного розыска / Б.П. Михайлова, Е.Н. Хазова // Состояние преступности в России (за январь-декабрь 2010 г., 2011 г., 2012 г., 2013 г., 2014 г.). – М.: ФГУ ГИАЦ МВД РФ. – URL: www.mvd.ru.
12. Нарижный, А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий : автореф. дис. … канд. юрид. наук. – Краснодар, 2009. – 22 с.
13. Некрасов, В.Н. Актуальные вопросы уголовно-правовой охраны информационной деятельности в России / В.Н. Некрасов // Актуальные проблемы российского права. – 2017. – №7. С.108-114.
14. О развитии информационных технологий в Российской Федерации и мерах поддержки отечественной ИТ-отрасли : постановление Совета Федерации Федерального Собрания РФ от 20 апреля 2016 г. №154-СФ // СПС КонсультантПлюс.
15. Общемировые убытки от киберпреступности составят $ 2,1 трлн до 2019 года. – URL: http://www.securitylab.ru/news/472924.php.
16. Официальный сайт Судебного департамента при ВС РФ. – URL: http://www.cdep.ru/index.php?id=79.
17. Рассолов, И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. – 2008. – №2. – С. 44-46.
18. Русскевич, Е.А. Уголовное право и информатизация / Е.А. Русскевич // Журнал российского права. – 2017. – №8. – С. 73-80.
19. Сачков, И. Технологии позволяют бороться с киберпреступностью – этот бизнес становит-

ся неэффективным / И. Сачков // Sk.ru. – URL: http://sk.ru/news/b/press/archive/2017/12/20/ilya-sachkov-tehnologii-pozvolyayut-borotsya-s-kiberprestupnostyu-_1320_-etot-biznes-stanovitsya-neeffektivnym.aspx.

20. Сокол, В.Ю. Кризис отечественной криминалистики : монография / В.Ю. Сокол. – Краснодар, 2017. – 332 с.

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

22. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы : утв. Указом Президента РФ от 9 мая 2017 г. №203 // СПС КонсультантПлюс.

23. Тарасов, А.М. Электронное правительство и информационная безопасность / А.М. Тарасов. – СПб., 2011. – 647 с.

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

25. Федотов, Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. – М.: Юридический Мир, 2007. – 432 с.

26. 80% пользователей не верят, что интернет-преступников можно наказать // ITUA.info. – URL: http://itua.info/software/28662.html.

27. Шадрина, Т. Обогнать, не догоняя / Т. Шадрина // Российская газета. – 2018. – 5 марта. – №47 (7510).

28. Шаевич, А.А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений : автореф. дис. … канд. юрид. наук / А.А. Шаевич. – Иркутск, 2007. – 24 с.

29. Шаталов, А.С. Криминалистические методики расследования преступлений: в ожидании перемен / А.С. Шаталов // Вестник криминалистики. – 2014. – №4 (52). – С.8-23.

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

31. Эксархопуло, А.А. Предмет и система криминалистики. Проблемы развития на рубеже XX – XIX вв. : курс лекций / А.А. Эксархопуло. – СПб.: Изд-во СПбГУ, 2004. – 112 с.

32. Casey, E. Digital evidence and computer crime / E. Casey. – 2nd ed. – Elsevier: Academic Press, 2004.

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

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

35. Thomas, D. Cybercrime: law enforcement, security and surveillance in the information age / D. Thomas, B. Loader. – London: Routledge, 2000.

36. Viano, C. Cybercrime, organized crime, and societal responses: international approaches / C. Viano. – Springer International Publishing, 2017.

37. Viano, E. Cybercrime: a new frontier in criminology / E. Viano // International Annals in Criminology. – 2006. – Vol. 44.

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