УДК 343.98
DOI 10.33463/1999-9917.2019.27(1-4).4.450-459

АЛЕКСАНДР СЕМЕНОВИЧ ШАТАЛОВ,
доктор юридических наук, профессор,
профессор кафедры уголовного процесса и криминалистики,
Академия ФСИН России, г. Рязань, Российская Федерация,
e-mail: asshatalov@rambler.ru;
АЛЕКСАНДР ВЛАДИМИРОВИЧ АКЧУРИН,
кандидат юридических наук, доцент,
начальник кафедры уголовного процесса и криминалистики,
Академия ФСИН России,
г. Рязань, Российская Федерация, ORCID 0000-0003-1742-1162,
e-mail: 79206310258@yandex.ru

ВОПРОСЫ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ ОСУЖДЕННЫМИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КОММУНИКАЦИИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Для цитирования
Шаталов, А. С. Вопросы выявления и расследования преступлений, совершаемых осужденными с использованием средств коммуникации и информационных технологий / А. С. Шаталов, А. В. Акчурин // Человек: преступление и наказание. – 2019. – Т. 27(1–4), № 4. – С. 450–459. – DOI : 10.33463/1999-9917.2019.27(1-4).4.450-459.

Аннотация. В статье предпринята попытка найти ответ на вопрос, почему на фоне научных достижений отечественной криминалистики, при таком обилии новых идей, концепций, технологий, криминалистических алгоритмов, программ расследования прогресс в деле борьбы с преступностью остается малозаметным. Главная причина такого положения дел видится в том, что российская криминалистика долгое время развивалась в отрыве от ведущих зарубежных исследовательских школ. Вместе с тем такое ее состояние сохраняется, несмотря на охватившие практически все страны мира глобальные интеграционные процессы. В качестве главного направления преодоления кризисных явлений позиционируется имплементация в научные ресурсы отечественной криминалистики современных информационных технологий вообще и для повышения эффективности борьбы с преступлениями, совершаемыми осужденными в местах лишения свободы, в частности. Борьбу с ними можно считать проблемой международного масштаба в силу транснационального и трансграничного характера самой 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 расследования преступлений такого рода и сформулированы рекомендации по повышению эффективности этой деятельности.

Ключевые слова: информационные технологии, киберпреступность, места лишения свободы, осужденные, компьютерные преступления, криминалистика, расследование преступлений.

Преступность, по господствующему в науке мнению, определяется как совокупность деяний, запрещенных уголовным законом. Она обладает, как минимум, двумя характерными чертами. Во-первых, состоит из отдельных преступлений, то есть 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 за собой наказание. Таким образом, преступность имеет правовой характер, географические и временные границы, она обладает приспособляемостью к социальным переменам и проявляет тенденцию к росту. Однако общедоступная информация о ней и сопровождающих ее процессах пока не дает отчетливого представления о действительных масштабах этого негативного социально-правового явления, его направленности и специфических проявлениях. Работая над этой статьей, мы пришли к выводу о том, что используемая криминалистами в своей повседневной деятельности научная база о феномене преступности нуждается в расширении за счет целенаправленного и последовательного преумножения знаний о ней на условиях решительного преодоления узкопрофессионального, ведомственного и технократического подхода к их распространению.

Очевиден тот факт, что российская преступность отличается не только значительным объемом, но и весьма широким диапазоном противоправных действий. Их предварительное расследование и объективное судебное рассмотрение немыслимо без выяснения того, где, кем и каким именно способом они были совершены. Сами сведения о способе их совершения являются наиболее ценными и представляют собой довольно внушительный массив криминалистически значимой информации. Именно он позволяет оперативным сотрудникам, дознавателям, следователям сориентироваться в сути имевшего место преступного деяния, наметить наиболее оптимальные пути его раскрытия и расследования, а значит, в полной мере проверить, оценить и использовать собранные в ходе производства по уголовному делу сведения как о самом преступном событии, так и о его участниках. Необходимость в этом объясняется тем, что способы совершения преступлений не избираются преступниками произвольно. Они детерминируются не только непосредственным объектом (предметом) преступного посягательства, но и самой обстановкой, в которой происходит его совершение.

Нередко местом криминальных проявлений становятся учреждения уголовно-исполнительной системы. Находящиеся в них осужденные совершают новые преступления разной степени тяжести, но это лишь «один из парадоксов принудительной изоляции в местах заключения» [1, с. 83]. Другой парадокс заключается в том, что, несмотря на свой невысокий образовательный уровень, осужденные быстро осваивают новые средства коммуникации и современные информационные технологии, в том числе в преступных целях [2]. Условия изоляции от внешней среды, в которых они вынуждены

находиться, не являются в этом плане непреодолимой преградой. Это означает, что все больше и больше осужденных становятся технологически просвещенными. Как следствие, они начинают мыслить и выстраивать свои противоправные действия иначе, нежели это было раньше. Реализуя свои преступные замыслы в таких условиях, они все чаще используют не только простейшие мобильные устройства, дорогостоящие гаджеты с новейшим программным обеспечением, но и самый широкий спектр интернет-ресурсов, открывающих для них неограниченные возможности для подготовки, совершения и сокрытия преступлений. Самих осужденных, совершающих преступления в период пребывания в исправительных учреждениях, криминалисты делят на три основные группы. В первую входят криминально активные лица, с устойчивой ориентацией на совершение преступлений; во вторую – лица, потенциально склонные к криминальной деятельности, но не имеющие твердой установки впредь совершать преступления; в третью – лица, случайно вовлекаемые в преступные акты в местах лишения свободы [3, с. 75].

По данным ФСИН России, в 2016 г. в исправительных учреждениях было зарегистрировано 851 преступление, совершенное осужденными, в 2017 г. – 872, а в 2018 г. – 913 (Официальный сайт ФСИН России. Характеристика лиц, содержащихся в исправительных колониях для взрослых. URL : http://fsin.su/ structure/inspector/iao/statistika/Xar-ka%20lic%20sodergahixsya%20v%20IK). Однако даже на фоне их незначительного роста может возникнуть впечатление, что для полумиллионного контингента лиц, находящихся в местах лишения свободы, общее количество совершенных ими преступлений сравнительно небольшое, хотя в действительности их совершается значительно больше. Наши многолетние наблюдения за фактическим положением дел в местах лишения свободы и данными официальной уголовной статистики о совершенных на их территории преступлениях позволяют утверждать, что ежегодно в ней учитывается не более десятой части криминальных проявлений такого рода. Более того, в публикуемых статистических данных, как правило, отсутствует дополнительная исходная информация, необходимая для полноценного научного анализа проблем, возникающих при расследовании уголовных дел о преступлениях, совершенных осужденными к лишению свободы. В частности, сведения о том, какие именно преступления они совершили, используя, например, средства традиционной телефонной коммутации, и сколько их было выявлено за тот или иной период, в официальной уголовной статистике не фиксируются. Вместе с тем масштаб их противоправного использования осужденными в преступных целях достаточно велик и в обозримом будущем будет только возрастать. Подтверждением тому могут являться не только выводы криминалистов, проводящих исследования по данной проблематике [4], но и сведения о ежегодно изымаемых у осужденных средствах связи. Отчеты о результатах оперативно-служебной деятельности отделов безопасности исправительных колоний, лечебных исправительных учреждений, лечебно-профилактических учреждений и территориальных органов уголовно-исполнительной системы свидетельствуют о том, что в 2013 г. их общее количество составило 57 012 единиц, 2014 – 62 890, 2015 – 64 175, 2016 – 63 287, в 2017 г. – 57 309 ед. (Статистические данные ФСИН России: отчеты о результатах оперативно-служебной деятельности отделов безопасности исправительных колоний, лечебных исправительных учреждений, лечебно-профилактических учреждений и территориальных органов уголовно-исполнительной системы. Форма СБ-1 за период 2013–2017 гг.). Несмотря на некоторое уменьшение числа изъятых у осужденных средств связи, их общее количество остается довольно большим, что благоприятствует «поддержанию высокой криминальной активности в местах лишения свободы» [5].

Криминалисты в своих работах отмечают, что наиболее распространенными в исправительных учреждениях были и остаются противоправные действия, связанные с незаконным оборотом наркотических средств и психотропных веществ [6]. В 2017 г., например, в общем объеме пенитенциарной преступности они составляли почти четверть (23 %). Изучение возбужденных по таким фактам уголовных дел показало, что практически во всех из них зафиксированы сведения о том, как осужденные, осуществляя свои преступные намерения, активно использовали средства мобильной связи [7]. Именно с их помощью осуществлялись контакты с поставщиками наркотических средств и их сообщниками. Как это происходит в реальности, можно проиллюстрировать на следующем примере: осужденный К., отбывающий наказание в виде лишения свободы, по мобильному телефону договорился с неустановленным лицом о продаже ему наркотического средства через знакомого им обоим гражданина Т., который в темное время суток приехал к основному ограждению исправительного учреждения и после получения светового сигнала, поданного ему осужденным К. фонариком мобильного телефона, произвел выстрел стрелой из арбалета на территорию исправительного учреждения, предварительно прикрепив к ней наркотик весом 10,18 г и снабдив светодиодом для визуализации траектории ее полета (Уголовное дело № 14325. Архив ОД МО МВД России «Кирово-Чепецкий»).

Помимо приобретения наркотиков, средства мобильной связи довольно часто используются осужденными для контакта с сообщниками «на воле» и подельниками, отбывающими наказание в других исправительных учреждениях. В научных публикациях описаны случаи, когда с их помощью оплачивались разного рода «услуги», оказанные осужденным коррумпированными сотрудниками исправительных учреждений [8]. В качестве характерного примера можно привести фабулу одного из изученных нами уголовных дел: осужденный П., отбывающий наказание в виде лишения свободы, предложил сотруднику оперативного отдела И. пронести на режимную территорию исправительного учреждения два мобильных телефона, пообещав за это деньги в сумме 20 тыс. рублей. Получив телефоны в комплекте с зарядными устройствами, осужденный П., используя одно из незаконно переданных ему сотрудником исправительного учреждения средств мобильной связи, подключился к предоставляемому порталом «КИВИ Банк» сервису Visa QIWI Wallet и перевел ранее обещанную сумму на банковскую карту И. (Уголовное дело № 1-30/2015. Архив Ловозерского районного суда Мурманской области). Однако это далеко не самый вопиющий случай использования технических средств коммуникации в преступных целях, поскольку с их помощью осужденные организовывают и координируют не только собственные преступные действия, но и деятельность преступных групп или большого количества лиц, привлеченных ими к участию в противоправных деяниях. Известны случаи, когда самые примитивные мобильные телефоны играли решающую роль в формировании отрицательного общественного мнения об исправительном учреждении, в привлечении повышенного внимания правозащитных организаций и граждан к его повседневной жизни [9, 10]. Осужденный А., например, используя незаконно переданный ему мобильный телефон с выходом в Интернет, смог организовать в своем исправительном учреждении массовые беспорядки, сопровождавшиеся насилием, погромами, уничтожением имущества и оказанием вооруженного сопротивления представителям власти. В общей сложности в них участвовало около тысячи человек, среди которых были как осужденные, так и их родственники, друзья и просто знакомые. Используя средства мобильной связи, А. лично и через своих сообщников призывал их вооружаться палками, трубами, прутами, бейсбольными битами, камнями, бутылка-

ми и иными подручными предметами для силового проникновения на территорию исправительного учреждения и оказания сопротивления его персоналу (Уголовное дело № 2-39/2014. Архив Челябинского областного суда).

Используя мобильную связь и современные информационно-телекоммуникационные технологии в преступных целях, осужденные нередко проявляют изобретательность, особенно при совершении ими разного рода мошеннических действий, а сам феномен «мобильного мошенничества» не остался незамеченным в научных исследованиях криминалистической тематики [11]. Собранные нами данные свидетельствуют о том, что диапазон мошеннических действий осужденных довольно широк. Совершая их, они наиболее часто прибегали к телефонным переговорам (39, 2 %), знакомству в социальных сетях (30,9 %), размещению объявлений в средствах массовой информации (24,6 %), смс-рассылке (5,3 %). Видно, что наиболее распространенным способом достижения целей мошенничества являлись адресные и случайные телефонные звонки для ведения переговоров. Они осуществлялись осужденными посредством незаконно хранящихся у них мобильных телефонов. Осужденный К., например, отбывая наказание в исправительном учреждении, случайно узнал номер телефона гражданки А., проживавшей в другом населенном пункте. Он позвонил ей, назвался сотрудником полиции и, пообещав содействие в освобождении ее сына от ответственности за нарушение правил дорожного движения, уговорил перечислить ему деньги в сумме 85 тыс. рублей (Уголовное дело № 126334. Архив СО ОМ № 18 СУ при УВД по г. Сочи). В другом случае осужденный С., прочитав в Интернете объявление об утерянной сумке с ценными вещами и позвонив ее владельцу, путем обмана смог добиться от него перечисления немалой суммы якобы за последующий возврат его имущества (Уголовное дело № 14040603. Архив отдела дознания по обслуживанию Исакогорского и Цигломенского округов г. Архангельска ОД УМВД по Архангельской области).

Находясь в местах лишения свободы, осужденные не только отслеживают, но и самостоятельно размещают на наиболее посещаемых сайтах объявления о покупке или продаже дорогостоящих вещей с целью установления контактов с доверчивыми людьми, обладающими более или менее значительными денежными средствами. Например, осужденный С., отбывающий наказание в виде лишения свободы, используя похищенное у другого осужденного средство мобильной связи, размещал объявления в сети Интернет о продаже автомобилей. По мере вхождения в доверие к гражданам он добивался от них перечисления на свой счет денежного задатка, после чего прекращал с ними общение, а полученные обманным путем деньги использовал по своему усмотрению (Уголовное дело № 20249. Архив СО № 2 СУ УМВД РФ по Республике Дагестан). В другом случае осужденный к лишению свободы, имея доступ в Интернет, организовал массовую рассылку смс-сообщений, в которых получателям сообщалось о якобы выигранном ими дорогом автомобиле, передача которого должна состояться сразу после оплаты небольшой денежной пошлины в конкретный электронный кошелек. Желающих ее оплатить нашлось немало, вследствие чего общая сумма, попавшая обманным путем к осужденному, оказалась довольно внушительной (Уголовное дело № 28-1-0642-2013. Архив ОВД СЧ по РОПД СУ УМВД России по Тульской области). Приведенные примеры из рассмотренных судами уголовных дел не только являются характерными, но и однозначно свидетельствуют о том, что подготовка и совершение осужденными преступлений, сокрытие их следов с использованием средств коммуникации и информационных технологий – это далеко не разовые случаи, а в полной мере

проявившая себя тенденция расширения и усиления возможностей современной преступности вообще и пенитенциарной в частности.

Прежде чем перейти к рассмотрению наиболее общих тенденций и конкретных проблем, возникающих в связи с выявлением и расследованием преступлений, совершаемых с использованием средств коммуникации и информационных технологий, необходимо отметить, что их совершают не только осужденные, которые отбывают наказание и имеют определенный преступный опыт, но и другие граждане, в том числе ранее несудимые. Рано или поздно они могут оказаться в местах принудительного содержания и поделиться своими навыками, умениями и знаниями с другими осужденными, усилив таким образом их противоправный потенциал. Изложенные в трудах криминалистов обобщенные научные данные о механизме преступлений такого рода, об обстановке, в которой они совершаются, об особенностях личности современного технически и технологически вооруженного преступника позволят должностным лицам, занимающимся их выявлением и предварительным расследованием, правильно организовать свою работу, четко знать основные и дополнительные источники получения криминалистически значимой информации и особенности ее использования в доказывании по уголовному делу.

В отечественной криминалистике уже сформировался весьма значительный объем высококлассной научной информации, которую можно найти в успешно защищенных диссертационных исследованиях, монографических работах, научных статьях, тезисах, практических и методических рекомендациях. Данные материалы направлены на совершенствование процесса предотвращения, выявления, раскрытия, расследования преступлений. На фоне таких вполне очевидных научных достижений кажется нелепым вопрос о том, 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. При всем этом значительная часть российских криминалистов не признает кризисного состояния своей науки и соответственно противится не только переосмыслению надуманных теоретических конструкций, но и их целенаправленному осовремениванию. Считаем, что 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, занимающих в экономике страны особое место, а их эффективное функционирование является одним из важнейших факторов, способствующих решению ключевых задач государственной политики. Кроме того, информационные технологии должны сыграть важную роль в обеспечении дальнейшего поступательного развития отечественной криминалистики. Сейчас все больше становится очевидно, что в ней назрел ряд вопросов, ожидающих своего комплексного решения. Необходимо, в частности, реализовать меры, направленные на разработку и внедрение новых способов выявления, раскрытия и расследования преступлений, совершаемых в киберпространстве. В их числе: распространение компьютерных вирусов, мошенничество с платежными картами, неправомерное изъятие денежных средств с банковских счетов, хищение компьютерной информации, нарушение правил эксплуатации разного рода автоматизированных

электронных систем и др. Все это 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, наиболее часто встречаются термины «киберпреступление» и «компьютерное преступление». 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 средства коммуникации, информационные технологии и самый широкий спектр интернет-ресурсов.

Процесс выявления, раскрытия и предварительного расследования преступлений, совершенных с использованием современных информационных технологий, имеет ряд существенных особенностей. Ошибки, допускаемые при этом следователями и дознавателями, являются следствием их неудовлетворительной профессиональной подготовки именно для этого сегмента криминалистической деятельности. Доминирующим фактором, влияющим на снижение качества предварительного расследования преступлений, совершаемых в киберпространстве, является отсутствие или низкое качество методических разработок, позволяющих выстроить алгоритм противодействия противоправной деятельности киберпреступников. Объективные условия, создающие сложность в расследовании подобных преступлений, – особенности обнаружения, фиксации и изъятия криминалистически значимой информации по преступлениям в сфере информационных технологий. Более того, здесь как нигде высока вероятность того, что те доказательства, которые все же были обнаружены, могут быть непреднамеренно изменены и даже утрачены в результате ошибок, допущенных при их изъятии или исследовании. Подготовка в ходе досудебного производства по уголовному делу доказательств такого рода для дальнейшего представления их в суде требует обязательного наличия основательной профессиональной подготовки, а также 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 в., то есть сравнительно недавно. Понадобилось еще примерно пятьдесят 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 философы (Д. Белл, Д. Рисман, А. Турен и др.) обсуждали 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 резкому увеличению числа 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 и С. В. Киселева, имевшие место в конце 1990-х годов, а также диссертации А. А. Шаевича, Ю. А. Куриленко, А. В. Нарижного, С. А. Ковалева, А. А. Косынкина, К. В. Костомарова и В. О. Давыдо-

ва, защищенные в период с 2007 по 2013 год. 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 г., то есть более пяти лет тому назад. «Застой» отчасти был компенсирован монографическими работами профессоров Е. П. Ищенко, В. Б. Вехова и некоторых других российских криминалистов, проявивших интерес к данной проблематике. Однако этого оказалось явно недостаточно.

Обращает на себя внимание тот факт, что с начала XXI в. 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 (10,4 тыс.). В последующие годы стал наблюдаться их некоторый количественный спад. В 2015 г., например, было зафиксировано 2382 таких преступления [12], за совершение которых было осуждено лишь 235 человек. Данные Судебного департамента при Верховном Суде Российской Федерации свидетельствуют о том, что в 2016 г. эта цифра сократилась до 185 человек (Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL : http://www.cdep.ru/index.php?id=79). Причины таких несколько странных расхождений различны, но нам они видятся в том, что абсолютное большинство преступлений в сфере компьютерной информации – латентные. Среди специалистов бытует устоявшееся мнение относительно таких преступлений, что девять из десяти подобных противоправных деяний не отражаются в официальной статистике [13].

В Северной Америке и во многих странах европейского континента уже отработана технология поиска киберпреступников. Расходы на розыск каждого из них в среднем составляют немногим более 300 долл. США (http://itua.info/software/28662.html). Борьба с киберпреступностью российскими правоохранительными органами оставляет желать лучшего. Если выразиться более категорично, то пока ей 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» [14].

Эффективную борьбу с киберпреступлениями в России осуществляет несколько агентств, специализирующихся на инициативном расследовании высокотехнологичных преступлений. 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 высокотехнологичных преступлений, немалая часть которых являлись особо сложными [15]. Агентство финансовой и правовой безопасности также на этом поприще достигло определенных успехов в основном за счет использования в работе своих сотрудников как новейших информационных технологий, так и аккаунтов в социальных сетях [16].

Согласно данным, полученным компанией «Juniper Research», при сохранении текущего уровня кибератак в ближайшие годы общие убытки мировой экономики от их осуществления в 2019 г. составят 2,1 трлн долларов США [17]. Что касается 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!) [18].

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.) [19]. Поскольку они обладают способностью приносить высокие доходы, на них соответствующим образом реагирует криминальная среда. В результате появляются новые виды преступных посягательств, предполагающие использование современных информационных технологий на условиях внезапности и анонимности [20]. Практически все названные противоправные деяния значительно опаснее иных преступлений, совершаемых вне киберпространства, поскольку обладают способностью причинять ущерб всем охраняемым законом интересам, диапазон которых варьируется от частных неимущественных интересов отдельных граждан до интересов безопасности государства.

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 растет вероятность стать очередной жертвой киберпреступности [21]. Именно поэтому одним из принципов Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, провозглашено обеспечение государственной защиты интересов российских граждан в информационной сфере.

Изменения, произошедшие в обществе, его экономических, социальных, правовых отношениях, требуют поиска решений создавшихся кризисных явлений, коснувшихся многих юридических наук, в том числе криминалистики. Стремительное использование в противоправных целях новейших достижений науки и техники, изобретение преступниками новых способов подготовки, совершения и сокрытия преступлений заставляют криминалистов искать адекватные меры реагирования. В связи с этим очевидна потребность перехода криминалистической науки к такому этапу ее развития, где по-новому должны быть пересмотрены подходы как к теоретическим ее основам, так и к практическому применению полученных результатов.

Библиографический список

1. Антонян Ю. М., Колышницына Е. Н. Мотивация поведения осужденных : монография. М., 2009. 144 с.

2. Шурухнов Н. Г. Информационные технологии : современное состояние и отдельные данные их использования в совершении преступлений лицами, отбывающими наказание в учреждениях уголовно-исполнительной системы // Международный пенитенциарный журнал. 2015. № 2. С. 96–99.

3. Шурухнов Н. Г. Личность пенитенциарного преступника // Социологические исследования. 1993. № 3. С. 74–83.

4. Жарко Н. В., Новикова Л. В. Субъективные и объективные факторы как особенности расследования пенитенциарных преступлений // Евразийский юридический журнал. 2016. № 8(99). С. 219–221.

5. Шиханов В. А. Особенности правового регулирования оборота средств мобильной сотовой связи в исправительных учреждениях уголовно-исполнительной системы // Человек: преступление и наказание. 2016. № 2(93). С. 96–101.

6. Егорова Т. И. Противодействие незаконному обороту наркотиков в местах лишения свободы // Наркоконтроль. 2017. № 1. С. 33–35.

7. Морозов Р. М. Факторы, влияющие на производство расследования уголовных дел о незаконном обороте наркотических средств в исправительных учреждениях // Уголовное наказание в России и за рубежом: проблемы назначения и исполнения (к 10-летию принятия Европейских пенитенциарных правил) : сб. материалов Междунар. науч.-практ. конф. Вологда, 2017. С. 109–113.

8. Филиппов М. Н. Методика расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов // Ведомости уголовно-исполнительной системы. 2015. № 5(156). С. 26–30.

9. Беляков А. В. Использование средств массовой информации при подготовке к дезорганизации деятельности учреждений, обеспечивающих изоляцию от общества // Юрист Поволжья. 2008. № 3–4.

10. Тищенко Ю. Ю., Масленников Е. Е. Оперативно-розыскные аспекты пресечения групповых неповиновений осужденных // Групповые неповиновения и массовые беспорядки в учреждениях УИС : материалы круглого стола / под общ. ред. С. В. Гарника. М. : НИИ ФСИН России, 2018. С. 39–394.

11. Фомин Ю. С. Особенности получения информации из систем мобильной связи при расследовании преступлений, совершенных в исправительных учреждениях // Вестник Владимирского юридического института. 2011. № 3. С. 65–67.

12. 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.). М. : ГИАЦ МВД России. URL : www.mvd.ru (дата обращения: 28.09.2019).

13. Тарасов А. М. Электронное правительство и информационная безопасность. СПб., 2011. 647 с.

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

15. Сачков И. Технологии позволяют бороться с киберпреступностью – этот бизнес становится неэффективным // 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 (дата обращения: 28.09.2019).

16. Как современные Шерлоки Холмсы находят интернет-мошенников // Статус. 2012. № 8.1(19). С. 7.

17. Общемировые убытки от киберпреступности составят $ 2,1 трлн до 2019 года. URL : http://www.securitylab.ru/news/472924.php (дата обращения: 28.09.2019).

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

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

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

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