

ВЕСТНИК КРИМИНАЛИСТИКИ № II (86), 2023



ВЕСТНИКЪ КРИМИНАЛИСТИКИ
BULLETIN OF CRIMINALISTICS
II (86) - 2023

Издается с 1999 г.

*Основатель журнала и его первый ответственный редактор
профессор А.Т. Филиппов*

Ответственный редактор Е.В. Иванова

В журнале

«ВЕСТНИКЪ КРИМИНАЛИСТИКИ ~ BULLETIN OF CRIMINALISTICS»
*публикуются статьи по криминалистике, судебной экспертизе, оперативно-
розыскной деятельности, представляющие интерес для практикующих ра-
ботников правоохранительных органов, а также адвокатов, судей, преподава-
телей и научных работников.*

ISSN 2220-847X

Адрес редакции:

author@vestcrim.ru, contact@fact-gsgu.ru

2023



СОДЕРЖАНИЕ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИКИ И СУДЕБНОЙ ЭКСПЕРТИЗЫ.. 5

ИВАНОВА Е.В. АКСЕНОВА В.И. К вопросу о понятии опасности и способах ее установления 5

ИЛЬИН Н.Н. Роль Следственного комитета Российской Федерации в защите прав, свобод и законных интересов детей 16

ОЗЕРОВ И.Н., ЖУРБЕНКО А.М. Некоторые аспекты расследования преступлений в сфере оказания медицинских услуг (ятрогении) 22

СКОБЕЛИН С.Ю. Тенденции цифровизации следственной деятельности..... 30

КРЮКОВ В.В.. Современные проблемы экспертизы дорожно-транспортных происшествий. Виды и классификация средств индивидуальной мобильности 37

ИВАНОВА Е.В. КОЛЫШЕВ В.Р. Следы от электрошоковых устройств: понятие, виды, классификации..... 48

ПОПОВ А.М., ШУРУХНОВ В.А. К вопросу о криминалистической характеристике киберпреступлений..... 57

БОНДАРЕНКО Р.В., ГУЛИНА Е.Г. Оказание помощи в подготовке специалистов правоохранительных органов иностранных государств в Московском университете МВД России им.В.Я. Кикотя 70

РАМАЛДАНОВ Х.Х. Применение цифровых технологий при расследовании преступлений, связанных с торговлей людьми..... 76

АКТУАЛЬНЫЕ ВОПРОСЫ ПОДГОТОВКИ СУДЕБНЫХ ЭКСПЕРТОВ 83

ДЬЯКОНОВА О.Г., ИВАНОВА Е.В. Подготовка по специальности 40.05.03 Судебная экспертиза в рамках юридического образования 83

ТРЕБОВАНИЯ ДЛЯ АВТОРОВ 89

К ВОПРОСУ О КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ КИБЕРПРЕСТУПЛЕНИЙ

ПОПОВ А.М., ШУРУХНОВ В.А.

Аннотация. В статье рассматриваются особенности данных составляющих криминалистическую характеристику киберпреступлений, которая, при правильном описании ее элементов и корреляционных связей имеет практическое значение на первоначальном этапе расследования преступлений данного вида. Своевременная модернизация криминалистической характеристики киберпреступлений в период активного внедрения современных компьютерно-технических технологий в преступную деятельность позволит ученым и практическим работникам реализовать комплексный подход к решению проблемы противодействия киберпреступности в нашей стране.

Ключевые слова: киберпреступность, способы совершения преступлений, противодействие расследованию, криминалистическая характеристика, корреляционные связи, расследование преступлений.

Для цитирования: Попов А.М., Шурухнов В.А. К вопросу о криминалистической характеристике киберпреступлений //Вестник криминалистики. 2023. № 2. С.57-69.

Криминалистическая характеристика отдельных видов преступлений, несмотря на неоднозначную оценку ученых и специалистов относительно ее эффективности [1, с.21; 3, с.34; 4; 2, с.224; 12], до сих пор остается достаточно работоспособным элементом криминалистической методики.

Правильное и грамотное применение и использование, основанное на качественном построении ее структуры, позволяет практическим работникам на первоначальном, самом сложном этапе расследования, определить основные пути разрешения следственных ситуаций, складывающихся в указанный период при расследовании преступлений. Своевременное принятие решения о производстве следственных и иных процессуальных действий, позволяет не только сохранить доказательства, путем грамотной их фиксации и изъятия, но и не допустить наступления негативных последствий и результатов в период всего расследования.

ПОПОВ А.М., ШУРУХНОВ В.А.

В условиях всеобщей цифровизации, широкого распространения современных цифровых технологий в криминальной среде, использование криминалистической характеристики киберпреступлений создает благоприятные условия расследования в рамках выявления, фиксации и изъятия цифровых следов на первоначальном этапе расследования преступлений данного вида. Ключевую роль в данном направлении играет наличие информационной модели преступной деятельности.

Сегодня, наше общество столкнулось с беспрецедентным скачком киберпреступности в нашей стране, которое развивается на фоне активной трансформации ее в транснациональную преступную деятельность, что негативно влияет на возможности привлечения к уголовной ответственности лиц, совершающих данный вид преступлений, находящихся за пределами государства. Активно способствует распространению киберугроз и современные проблемы с эпидемиологической обстановкой в мире.

Так по данным МВД России в январе-декабре 2019 года зарегистрировано более 294 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий или, что почти на 70% больше, чем за аналогичный период прошлого года. Половина таких преступлений совершается с использованием сети «Интернет», а более трети – средств мобильной связи. В 2020 году число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%. В 2022 году показатели киберпреступности в целом остались стабильными. С использованием высоких технологий совершается каждое четвертое преступление. Зарегистрировано на 27,6% меньше краж, на 29% – фактов мошенничества с использованием электронных средств платежа, на 22,5% – криминальных деяний в сфере компьютерной информации. Правоохранительными органами больше на 20,9% зарегистрировано фактов сбыта наркотиков. Кроме того, увеличилось количество заведомо ложных сообщений об акте терроризма, в массиве которых 92,2% совершены дистанционно¹.

Создавшееся положение требует принятия неординарных и экстренных мер, которые должны быть реализованы в рамках комплексного подхода. Ключевым

¹ Состояние преступности [Электронный ресурс] <https://xn--b1aew.xn--p1ai/reports/1/>. (Дата обращения: 28.04.2023).

элементом в таком подходе является разработка практических рекомендаций по борьбе с киберпреступностью на современном этапе, которые должны быть основаны на научных положениях, одним из которых является криминалистическая характеристика преступлений данного вида.

Традиционное описание элементного состава криминалистической характеристики, с выявлением и иллюстрацией закономерных для них корреляционных связей, позволяет создать значительную информационную базу для обеспечения условий эффективной деятельности следователя на всех этапах расследования киберпреступлений.

Раскрывая общую информационную модель киберпреступлений, необходимо отметить, что одним из ключевых элементов их криминалистической характеристики является предмет преступного посягательства, которым в полной мере является информация, при этом, в киберпреступлениях она будет являться цифровой (компьютерной). В любом варианте воздействия на такую информацию (модификация, копирование, блокирование, обмен ею, хранение и т.п.), с учетом характера выбранного способа, орудий и средств, образуется специфическая следовая картина преступной деятельности, что свидетельствует о закономерных корреляционных связях между указанными элементами. При этом любые манипуляции с подобного вида информацией, закономерно находят отражение в объективной действительности, что имеет существенное идентификационное значение.

Сама система организации, реализации и функционирования компьютерно-технических средств и технологий определяют выбор способа совершения киберпреступлений. Спектр таких способов зависит еще и от конкретных целей, которые преследуют преступники, совершая преступления данного вида. В этой связи, способ совершения киберпреступления практически всегда имеет полно структурное строение, проявляющееся, в первую очередь, в подготовке к совершению преступления. В такую деятельность обязательно входит подыскание технических средств и технологий, лиц, обладающих знаниями и навыками в рассматриваемой отрасли, а также иная, сопутствующая деятельность, по подготовке и подысканию иных средств и лиц, вовлекаемых в рассматриваемый вид преступной деятельности. Кроме этого, уже на этапе подготовки могут выполняться действия, направленные не только на сокрытие преступной деятельности, но и активное противодействие правоохранительным органам [9; 10; 11]. Сама структура и принцип работы компь-

ПОПОВ А.М., ШУРУХНОВ В.А.

ютерно-технических средств, технологий и сопутствующих систем, позволяет эффективно применять их в преступной деятельности, при этом результативно скрывать следы такого использования.

Непосредственно реализация самого способа совершения киберпреступлений обусловлена, опять же, выбранными целями. Однако, следует признать, что большинство киберпреступлений направлено на достижение корыстных целей для личного обогащения. Кроме этого, сегодня киберпространство активно используется в целях совершения преступлений большой тяжести (такие, как убийства, террористическая и экстремистская деятельность и другие), которые могут носить бесцельный характер, для реализации своих низменных интересов и желаний, направленных на простое противопоставление себя обществу, уверовав в свою безнаказанность.

Использование различных компьютерно-технических технологий, сегодня позволяют эффективно принимать меры к сокрытию преступной деятельности, начиная от простейших технологий зашифровки данных абонентов (например, анонимный прокси-сервер, VPN, временная учетная запись, виртуальная дебетовая карта и т.п.), до использования скрытых ресурсов и анонимных сетей (Darknet, TOR (The Onion Router) и т.п.).

Для реализации того или иного способа совершения киберпреступлений, сегодня достаточно наличия, уже даже, не специального стационарного громоздкого оборудования (компьютера, ноутбука или нетбука) с проводным подключением к сети Интернет, а всего лишь мобильного смартфона, планшета и иного подобного устройств, доступ в Интернет с которого осуществляется в беспроводном режиме, посредством удаленного доступа, предоставляемого мобильным оператором подвижной сотовой связи. При этом доступ к услугам такого оператора можно получить различными путями, даже без регистрации и указания своих личных данных.

Все перечисленные обстоятельства, безусловно, по-разному влияют на процесс образования следов киберпреступлений. Как правило, даже в рассматриваемой сфере всегда речь будет идти о традиционных следах, материальных и идеальных, которые будут иметь ключевое значение в процессе доказывания преступной кибердеятельности.

Однако, сегодня ученые ведут активную полемику о существовании нового вида криминалистических следов – цифровых (компьютерных, бинарных, виртуальных и т.п.) [8]. Вероятно, в этом есть рациональное зерно, однако, представляется,

что, отображаясь в объективной действительности, указанные следы больше относятся к материальным, с той лишь разницей, что эта объективная действительность находится в некой виртуальной среде, но при этом, для их использования в процессе доказывания, необходимо их обязательное материальное отражение в уголовном деле, что ставит их в один ряд с материальными следами.

Таким образом, весь процесс формирования следов в киберпространстве отвечает существующим, давно установленным и отработанным правилам обращения с ними. Так, передача данных осуществляется путем взаимодействия первичного компьютерно-технического средства (компьютер преступника) с вторичным компьютерно-техническим средством (компьютер жертвы), посредством функционирования сложной системы компьютерно-технических средств и технологий передачи информации. Устроена она таким образом, что весь этот процесс последовательно отражается в средствах ее хранения и обработки (роутер, модем, сервер, файлообменник, wi-fi и иные, подобные сети и т.п.).

Еще одним, значимым элементом криминалистической характеристики киберпреступлений, значительно влияющим и корреляционно зависимым со всей системой ее элементов, являются данные об обстановке, в которой совершаются преступления рассматриваемого вида, то есть, те условия, в которых происходит весь процесс реализации преступной деятельности. Первым, обязательным условием является, наличие современных компьютерно-технических средств, технические возможности которых позволяют удаленно осуществлять воздействие на жертву, но и значительно ускорить такой процесс посредством высокой скорости обработки и передачи информации. Вторым условием является развитие современных технологий передачи информации на любые расстояния, что также позволяет повысить эффективность преступной деятельности и выбрать конкретный способ совершения киберпреступлений, находясь за пределами одного государства. Сюда же следует отнести существующую и постоянно модифицируемую систему денежных расчетов, реализуемую посредством виртуальных платежей, в которой на этапе передачи денежных средств от одного лица к другому, отсутствует их натуральный эквивалент (купюры, монеты и иные средства платежа).

Третьим условием, оказывающим достаточно серьезное влияние на весь характер киберпреступлений, существенно влияя на их распространение в современном мире, является отсутствие эффективной системы защиты от такой незаконной

ПОПОВ А.М., ШУРУХНОВ В.А.

деятельности, особенно это проявляется в деятельности транснациональной киберпреступности. Отсутствие своевременных и эффективных мер у правоохранительных органов, которые оказались не готовы сегодня противостоять киберпреступности, способствует активному ее распространению. Негативное влияние на деятельность правоохранительных органов в области борьбы с киберпреступностью, сегодня оказывает фактическое отсутствие качественного взаимодействия между их структурными подразделениями на международном уровне. Сегодня это стало особенно актуально в условиях формирования нестандартных ситуаций (пандемий, чрезвычайных ситуаций), а в отношении нашего государства, в условиях беспрецедентного, колоссального давления со стороны недружественных государств во всех отраслях и сферах деятельности.

Следует отметить, что только совместная правоохранительная деятельность практических органов и научного потенциала страны в значительной степени позволяет в кратчайшие сроки решать обозначенные проблемы посредством именно комплексного подхода по решению проблем в рассматриваемой сфере.

Данные о месте и времени совершения киберпреступлений, позволяет достаточно эффективно выбирать средства и технологии не только расследования преступлений данного вида, но и создавать эффективную систему противодействия рассматриваемому явлению. Существенное значение на указанные элементы, безусловно, оказывает выбранный способ, орудия и средства совершения киберпреступлений. Большое значение имеют, также знания и навыки лиц, их совершающих. Особенность технологии передачи информации компьютерно-техническими средствами, позволяет говорить о разных вариантах временного континуума совершения киберпреступлений. Как правило, в зависимости от целей преступников, преступления данного вида носят длящийся характер, направленный на извлечение значительного дохода. С другой стороны, та же специфика обуславливает особенности хранения и обработки информации компьютерно-техническими средствами, что позволяет говорить о различных периодах их нахождения в местах такого хранения и обработки. Казалось бы, говоря о виртуальном пространстве, в котором происходит весь обмен и обработка компьютерной информации колоссального объема, имеются конкретные места и средства ее хранения, длительность которых зависит от определенных обстоятельств (размеры серверного хранилища, используемые для этого средства и технологии, государственная политика в данной сфере и иные обстоятельства).

Данные о месте совершения киберпреступлений, в зависимости все от тех же перечисленных выше элементов (способ, орудия и средства и т.п.), содержат сведения о местах нахождения преступников (где они непосредственно осуществляют процесс создания и применения компьютерно-технических средств и технологий, а также обработку информации), а также последующий выход в виртуальное пространство. В данном случае, это место несет наибольшее количество следов преступной деятельности, которые имеют отношение к конкретному лицу (традиционные криминалистические следы – идеальные и материальные).

В свою очередь, как основной источник первоначальной информации о характере преступной деятельности, место нахождения компьютерно-технических средств потерпевшего (жертвы), содержит наибольшее количество следов о совершенном преступном деянии, а также особенностях его реализации именно на первоначальном этапе расследования. При этом, необходимо учитывать, что в процессе совершения киберпреступления, преступниками предпринимаются существенные меры, направленные на сокрытие преступной деятельности и противодействия правоохранительным органам. Это в полной мере позволяет говорить о существенных трудностях, которые могут возникнуть при обнаружении, фиксации и изъятия информации даже на компьютерно-технических средствах потерпевшего.

Одним из мест совершения киберпреступлений, в которых могут содержаться значительное количество следов преступной деятельности, но при этом значительно минимизирована возможность внешнего воздействия на них, будут являться технические средства и технологии, которые обеспечивают процесс обработки, передачи и хранения информации организациями, которые предоставляют услуги связи (поставщики услуг, провайдеры, а также владельцы средств ее хранения и переработки (Дата-цент ЦОД)).

Все вышеизложенное, в конечном итоге, позволяет сформировать данные о самом основном элементе криминалистической характеристики киберпреступлений, который корреляционно связан со всеми ее элементами и взаимозависимо влияет на весь процесс рассматриваемой преступной деятельности – это данные о лицах и их качествах, совершающих преступления данного вида.

Основываясь на всех, ранее рассмотренных элементах, существует возможность создания абстрактного портрета лица, его личностных качествах и его определенных особенностях, совершающего киберпреступления. Первым ключевым элементом данного описания, безусловно, является наличие значительных (выше

ПОПОВ А.М., ШУРУХНОВ В.А.

уровня простого пользователя (юзера)) знаний и навыков работы с компьютерно-техническими средствами и технологиями. При этом следует учитывать, что в некоторых случаях, когда указанные средства и технологии используются только в целях создания условий совершения иного преступления (доведение до самоубийства [6, с.62], мошенничества [5; 7], распространение порнографии и т.п.), преступник может обладать всего лишь уровнем уверенного пользователя, которых будет достаточно для использования компьютерно-технических средств и простейших технологий передачи информации.

Достаточно сложно себе представить совершение киберпреступления без наличия самих компьютерно-технических средств и технологий, знания о специфических особенностях, которых на момент совершения преступления, могли бы отсутствовать у преступника. Осведомленность о возможностях удаленного доступа к средствам передачи информации, их хранения и обработки, являются существенным, при создании условий совершения киберпреступлений. В большинстве случаев, о чем свидетельствует судебно-следственная практика, особенно при совершении преступлений группами лиц или преступными формированиями, в рассматриваемую деятельность вовлекаются только такие лица, которые имеют значительные познания и навыки работы и обращения с компьютерно-техническими средствами и технологиями. При этом, наличие знаний и навыков противодействия установлению обстоятельств совершения киберпреступлений, в таких случаях имеет ключевое значение (так называемые хакеры).

Специалисты в области IT-технологий говорят о наличии у каждого конкретного лица, совершающего киберпреступления, собственного почерка его реализации, который особенно проявляются в ходе создания вредоносных программ. При этом, как показывает анализ судебно-следственной практики, возраст лица не имеет устойчивого значения. В последнее время, особенно в условиях вынужденной изоляции, в преступную сферу киберпреступности было вовлечено большое количество несовершеннолетних, которые находились на дистанционном обучении.

Таким образом, наличие разработанной, обоснованной, отвечающей всем требованиям криминалистической науки, системы данных о киберпреступлениях, в виде информационной модели, именуемой криминалистической характеристикой имеет большое практическое значение, для раскрытия и расследования преступлений данного вида на всех этапах деятельности правоохранительных органов.

Обусловлено это описанием основных элементов преступной деятельности, с отражением всех значимых признаков, которые позволяют уже на этапе получения сведений о преступлении, выдвинуть обоснованные версии и предположить характер складывающихся следственных ситуаций, что обеспечивает возможность выбора наиболее эффективных средств по их разрешению.

Библиографический список:

1. Баев, О.Я. И все же: реальность или иллюзия (еще раз о криминалистической характеристике преступлений) // О.Я. Баев // Вестник криминалистики. – 2000. – № 1(3) – С.21.
2. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. – М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА • М), 2001. С.220-224
3. Бессонов, А.А. История развития криминалистической характеристики преступлений / А.А. Бессонов // Проблемы уголовного процесса, криминалистики и судебной экспертизы. – 2018. – № 1(11). – С. 34.
4. Гавло, В.К. К вопросу о криминалистической характеристике преступлений (статья вторая) / В.К. Гавло // Избранные труды. – Барнаул: Алтайский государственный университет, 2011. – С. 207-216.
5. Журбенко, А. М. Теоретические аспекты типичных следственных ситуаций на первоначальном этапе расследования мошенничества, совершенного с использованием платежных карт / А. М. Журбенко, И. Н. Озеров, А. В. Черникова // Теория и практика расследования преступлений: Материалы X Международной научно-практической конференции, Краснодар, 14 апреля 2022 года / Редколлегия: Э.С. Данильян, И.Г. Башинская, М.Ю. Лакомская [и др.]. – Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации», 2022. – С. 164-167.
6. Ильин Н. Н. Особенности расследования доведения до самоубийства: учебное пособие. – М.: Проспект, 2021. С. 62.
7. Милованова, М. М. О способах мошенничества в сети «интернет» / М. М. Милованова, В. А. Шурухнов // Имущественные отношения в Российской Федерации. – 2021. – № 10(241). – С. 86-92.

ПОПОВ А.М., ШУРУХНОВ В.А.

8. Озеров, И. Н. Некоторые проблемы использования цифровой информации при раскрытии и расследовании преступлений в особых условиях / И. Н. Озеров, А. Р. Махмутов, А. М. Журбенко // Актуальные вопросы обеспечения национальной безопасности: Материалы международной научно-практической конференции, Москва, 30 ноября 2022 года / Санкт-Петербургская академия Следственного комитета Российской Федерации; Московская академия Следственного комитета Российской Федерации. – Москва: Московская академия Следственного комитета Российской Федерации, 2023. – С. 76-82.

9. Попов, А. М. Противодействие расследованию: теория и практика / А. М. Попов, В. А. Шурухнов. – Москва: Московская академия Следственного комитета Российской Федерации, 2022. – 53 с.

10. Противодействие расследованию преступлений и меры по его преодолению: Учебник для вузов / С. В. Валов, А. Ф. Волынский, А. В. Воронцов [и др.]. – Москва: Общество с ограниченной ответственностью «Издательство ЮРАЙТ», 2020. – 205 с. – (Высшее образование).

11. Шурухнов, В. А. Современные проблемы противодействия преступлениям, совершаемым с применением информационных технологий / В. А. Шурухнов // Проблемы борьбы с преступностью в условиях цифровизации: сборник статей XIX Международной научно-практической конференции, Барнаул, 29 мая 2021 года. Том Вып. XVII. – Барнаул: Алтайский государственный университет, 2021. – С. 480-486.

12. Шурухнов, Н.Г. Виды криминалистических методик: их система, взаимосвязь, роль в научных исследованиях и расследовании преступлений / Н.Г. Шурухнов, Н.Е. Мерецкий // Актуальные проблемы организации правоохранительной и правозащитной деятельности: Материалы Всероссийской научно-практической конференции, Тула, 25 января 2020 года / Отв. редактор В.Н. Яшин. – Тула: Тульский государственный университет, 2020. – С. 205-219.

References:

1. Baev, O.Ya. And yet: reality or illusion (once again about the criminalistic characteristics of crimes) // O.Ya. Bayev // Bulletin of Criminalistics. – 2000. – № 1(3) – P.21. (In Russ).

ВЕСТНИК КРИМИНАЛИСТИКИ № II (86), 2023

2. Belkin R.S. Criminalistics: problems of today. Topical issues of Russian criminalistics. – M.: Publishing house NORMA (Publishing group NORMA-INFRA • M), 2001. pp. 220-224. (In Russ).

3. Bessonov, A.A. The history of the development of criminalistic characteristics of crimes / A.A. Bessonov // Problems of criminal process, criminalistics and forensic examination. – 2018. – № 1(11). – P. 34. (In Russ).

4. Gavlo, V.K. On the question of criminalistic characteristics of crimes (article two) / V.K. Gavlo // Selected works. – Barnaul: Altai State University, 2011. – pp. 207-216. (In Russ).

5. Zhurbenko, A.M. Theoretical aspects of typical investigative situations at the initial stage of investigation of fraud committed using payment cards / A.M. Zhurbenko, I. N. Ozerov, A.V. Chernikova // Theory and practice of crime investigation: Materials of the X International Scientific and Practical Conference, Krasnodar, April 14, 2022 / Editorial Board: E.S. Danilyan, I.G. Bashinskaya, M.Y. Lakomskaya [et al.]. – Krasnodar: Federal State State Educational Institution of Higher Professional Education "Krasnodar University of the Ministry of Internal Affairs of the Russian Federation", 2022. – pp. 164-167.

6. Ilyin N. N. Features of the investigation of suicide: textbook. – M.: Prospect, 2021. P. 62. (In Russ).

7. Milovanova, M. M. On the methods of fraud on the Internet / M. M. Milovanova, V. A. Shurukhnov // Property relations in the Russian Federation. – 2021. – № 10(241). – Pp. 86-92. (In Russ).

8. Ozerov, I. N. Some problems of using digital information in the disclosure and investigation of crimes in special conditions / I. N. Ozerov, A. R. Makhmutov, A.M. Zhurbenko // Topical issues of ensuring national security: Materials of the International scientific and practical conference, Moscow, November 30, 2022 / St. Petersburg Academy of the Investigative Committee of the Russian Federation; Moscow Academy of the Investigative Committee of the Russian Federation. – Moscow: Moscow Academy of the Investigative Committee of the Russian Federation, 2023. – pp. 76-82. (In Russ).

9. Popov, A.M. Counteraction to investigation: theory and practice / A.M. Popov, V. A. Shurukhnov. – Moscow: Moscow Academy of the Investigative Committee of the Russian Federation, 2022. – 53 p. (In Russ).

10. Countering the investigation of crimes and measures to overcome it: Textbook for universities / S. V. Valov, A. F. Volynsky, A.V. Vorontsov [et al.]. – Moscow: Limited

ПОПОВ А.М., ШУРУХНОВ В.А.

Liability Company "YURAYT Publishing House", 2020. – 205 p. – (Higher education). (In Russ).

11. Shurukhnov, V. A. Modern problems of countering crimes committed with the use of information technologies / V. A. Shurukhnov // Problems of combating crime in the conditions of digitalization: collection of articles of the XIX International Scientific and Practical Conference, Barnaul, May 29, 2021. Volume Issue XVII. – Barnaul: Altai State University, 2021. – pp. 480-486. (In Russ).

12. Shurukhnov, N.G. Types of criminalistic techniques: their system, interrelation, role in scientific research and investigation of crimes / N.G. Shurukhnov, N.E. Meretsky // Actual problems of organization of law enforcement and human rights activities: Materials of the All-Russian Scientific and Practical Conference, Tula, January 25, 2020 / Editor V.N. Yashin. – Tula: Tula State University, 2020. – pp. 205-219. (In Russ).

ALEXEY M. POPOV VLADIMIR AL. SHURUKHNOV

**ON THE QUESTION OF THE CRIMINALISTIC CHARACTERIZATION OF
CYBERCRIMES**

Abstract: the article discusses the features of the data that make up the criminalistic characteristics of cybercrime, which, if properly described, its elements and correlations are of practical importance at the initial stage of the investigation of crimes of this type. Timely modernization of the criminalistic characteristics of cybercrimes during the period of active introduction of modern computer and technical technologies into criminal activity will allow scientists and practitioners to implement a comprehensive approach to solving the problem of countering cybercrime in our country.

Keywords: cybercrime, methods of committing crimes, counteraction to investigation; criminalistic characteristics, correlations, investigation of crimes.

Сведения об авторах:

Попов Алексей Михайлович – кандидат юридических наук, доцент, декан факультета подготовки следователей, федеральное государственное казенное образовательное учреждение высшего образования «Московская академия Следственного комитета Российской Федерации».

Адрес электронной почты: ramtambov@yandex.ru

ВЕСТНИК КРИМИНАЛИСТИКИ № II (86), 2023

Шурухнов Владимир Александрович – кандидат юридических наук, доцент, доцент кафедры судебно-экспертной и оперативно-розыскной деятельности, федеральное государственное казенное образовательное учреждение высшего образования «Московская академия Следственного комитета Российской Федерации».

Адрес электронной почты: shuruhnov74@mail.ru

About the authors:

Alexey M. Popov– Candidate of Sciences (Law), Associate Professor, Dean of the Faculty of Investigator Training, Federal State state Educational Institution of Higher Education "Moscow Academy of the Investigative Committee of the Russian Federation".

E-mail: pamtambov@yandex.ru

Vladimir AI. Shurukhnov– Candidate of Sciences (Law), Associate Professor, Associate Professor of the Department of Forensic Expert and Operational Investigative Activities, Federal State state Educational Institution of Higher Education "Moscow Academy of the Investigative Committee of the Russian Federation".

E-mail: shuruhnov74@mail.ru

© Попов А.М., Шурухнов В.А., 2023