ISSN 2500-4255

УДК 343.9
DOI 10.17150/2500-4255.2020.14(6).882-890

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Э.В. Лантух[1], В.С. Ишигеев[2], О.П. Грибунов[3]
[1] Санкт-Петербургский университет МВД России, г. Санкт-Петербург, Российская Федерация
[2] Байкальский государственный университет, г. Иркутск, Российская Федерация
[3] Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация

Информация о статье

Дата поступления
19 октября 2020 г.

Дата принятия в печать
21 декабря 2020 г.

Дата онлайн-размещения
30 декабря 2020 г.

Ключевые слова
Предварительное расследование; компьютерные преступления; специальные знания; специалист; объекты судебной экспертизы; компьютерная экспертиза; носители информации; следственные действия

Аннотация. Статья содержит вывод о необходимости привлечения к следственным действиям специалистов в области компьютерных устройств, поскольку в процессе раскрытия и расследования компьютерных преступлений требуется изучение компьютерной информации и ее носителей. Специфика исследуемых объектов обусловливает, в свою очередь, установление особых правил их получения и фиксации, а также учет особенностей методики исследования при назначении и производстве компьютерных экспертиз. Изъятие, исследование, фиксация компьютерной информации, имеющей доказательственное значение, требуют использования специальных знаний. В связи с этим к процессу раскрытия, расследования и предупреждения компьютерных преступлений необходимо привлечение специалистов и (или) экспертов. Латентный характер компьютерных преступлений, широкое применение средств удаленного доступа, отсутствие визуального восприятия виртуальных объектов и иное затрудняют собирание компьютерной информации. Поэтому при раскрытии, расследовании и предупреждении преступлений особая роль принадлежит назначению и производству различных видов компьютерных экспертиз. Проведение современной и качественной экспертизы специалистами, имеющими специальные знания в сфере высоких технологий, по уголовным делам, связанным с преступлениями в сфере компьютерных технологий, является серьезной поддержкой, оказываемой правоохранительным органам в борьбе как с данными преступлениями, так и с целым спектром преступлений, в которых информационные технологии выступают частью базы преступной деятельности. Воздействуя таким образом на одну из составляющих основы региональной и международной преступной деятельности, правоохранительные органы повышают уровень как физической, так и информационной безопасности граждан. Авторами также подчеркивается, что чем больше общество внедряет в свою жизнедеятельность разного рода информационных технологий, тем выше уровень его уязвимости перед преступниками, использующими данные технологии в своих целях.

THE USE OF SPECIAL KNOWLEDGE IN THE INVESTIGATION OF COMPUTER CRIMES

Eduard V. Lantukh[1], Vladimir S. Ishigeev[2], Oleg P. Gribunov[3]
[1] Saint Petersburg University of the Ministry of Internal Affairs of Russia, Saint Petersburg, the Russian Federation
[2] Baikal State University, Irkutsk, the Russian Federation
[3] East-Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, the Russian Federation

Article info

Received
2020 October 19

Accepted
2020 December 21

Available online
2020 December 30

Abstract. The authors come to the conclusion that it is necessary to involve specialists in computer equipment in the process of investigation because the investigation and detection of computer crimes requires the analysis of computer information and its carriers. The characteristic features of examined objects determine, first of all, special rules for obtaining and registering them, as well as taking into consideration research methodology when ordering and conducting computer forensic examinations. Confiscation, examination, recording of computer information of evidential significance requires specialist knowledge. In this connection, it is necessary to involve specialists and (or) experts in the process of investigation, detection and prevention of computer crimes. The latent character of computer crimes, a wide use of remote assess, the absence of visual perception of virtual objects and other factors hinder the collection of computer information. Thus, ordering and conducting different types of computer forensic examination play a special role in the investigation, de-

Keywords
Preliminary investigation; computer crimes; special knowledge; specialist; objects of forensic examination; computer forensics; information storage media; investigative actions

tection and prevention of crimes. A modern and high-quality examination conducted by specialists with expert knowledge in the sphere of hi tech during the investigation of computer technology-related criminal cases offers considerable support to the law enforcement bodies in combating not only these crimes, but also a whole range of crimes where information technology acts as a partial platform for criminal activities. When law enforcement bodies thus influence one of the components of regional and international criminal activities, they raise the level of both physical and information security of citizens. The authors also stress that the more actively information technologies enter the life of a society, the more vulnerable this society is to the criminals who use these technologies for their own purposes.

В век становления компьютерных технологий, основывающегося на более широком использовании компьютеров, компьютерных систем, цифровой техники, информационных технологий, довольно востребованным становится решение проблемы по усовершенствованию законодательства в сфере борьбы с различными видами компьютерных преступлений, тактики производства отдельных следственных действий.

В последние годы категория так называемых киберпреступлений, т.е. преступлений, совершаемых с применением электронной (цифровой) информации, информационных технологий, а также информационно-телекоммуникационной сети Интернет, имеет стабильный рост. Специфика преступлений в сфере высоких технологий проявляется в многообразии и особых свойствах объектов — электронных документов, которые в процессуальном смысле приобретают характер либо вещественного доказательства, либо иного документа [1]. Компьютерные преступления вышли за пределы национальных границ и стали особым видом транснациональной преступности, требующим адекватного ответа со стороны правоохранительных органов государств.

По мнению многих криминалистов, в настоящее время наблюдается виртуализация преступности, т.е. переход общественно опасных деяний в информационную среду, исключающую физический контакт преступника и жертвы, обеспечивающую «традиционную», классическую преступность современными информационными технологиями в виде систем конспирации и скрытой связи. «Классические» преступления будут оставлять значительно больше цифровых следов и требовать от преступника технической компетентности, что, несомненно, повлияет и на механизм следообразования [2]. Кроме того, «обилие систем слежения и распознавания, работа датчиков контроля, в том числе вживленных в тело человека (бодинет, нейронет), вероятно, девальвирует… оценку некоторых юридических наук, связанных со сбором, исследованием и оценкой доказательств, в частности, криминалистику и уголовный процесс» [3].

Расследование киберпреступлений вызывает у практических работников определенные трудности, что обусловлено спецификой источников доказательственной информации, представленной в виде электронных сообщений, страниц, сайтов и др. Следует отметить, что и в зарубежной практике выделяют самостоятельный класс цифровых доказательств, обусловленных особенностями компьютерных средств и систем[1].

В связи с быстрым скачком криминогенной ситуации в стране из-за роста преступлений в сфере компьютерной информации, с возникновением все более изощренных способов их совершения проблема становления криминалистической методики и тактики раскрытия, расследования и предупреждения данных преступлений делается очень актуальной, по причине чего необходимо проводить активизацию и расширение круга научных исследований в указанной сфере с целью увеличения эффективности необходимых направлений, средств и форм организации следственной деятельности по раскрытию данных преступлений.

Низкая раскрываемость преступлений в сфере компьютерной информации обусловливает возникновение в следственной практике необходимости дополнительного комплексного исследования тактики производства отдельных следственных действий, изучения особенностей назначения и производства специальных экспертиз, разработки новых методов работы с цифровыми объектами с учетом современных достижений техники и различных наук.

[1] Guidelines for Best Practice in the Forensic Examination of Digital Technology // IOCE. 2002. May. URL: https://ru.scribd.com/document/183506063/Guidelines-for-Best-Practices-in-Examination-of-Digital-Evid.

В наше время все чаще появляется необходимость при расследовании сложных, резонансных преступлений изымать и выявлять нетрадиционные для криминалистики цифровые следы, искать вещественные доказательства, которые представлены в виде информации телекоммуникационной или вычислительной системы либо на магнитных носителях [4, с. 165–167]. В данной ситуации необходимо использовать специальные знания и умения в области новейших компьютерных технологий. Главной процессуальной формой применения такого рода специальных знаний в процессе расследования является экспертиза.

Экспертиза играет важную роль при расследовании всех без исключения преступлений в сфере компьютерной информации, которых большое разнообразие. Как об объекте исследования в криминалистике можно говорить о различных видах компьютерной информации [5, с. 72–81].

Необходимо отметить, что в настоящее время существует множество классификаций компьютерных преступлений. Общепризнанное разделение на виды предлагается в основных положениях «Конвенции Совета Европы о киберпреступности» (г. Будапешт, 23 ноября 2001 г.). В данной Конвенции все правонарушения в сфере компьютерной безопасности разделены на четыре группы. Дополнительный протокол (г. Страсбург, 28 января 2003 г.) к уже принятой Конвенции ввел еще одну группу киберпреступлений[2].

Действующие международные и региональные законодательные акты, научная практика ориентируются на представленную в Конвенции классификацию компьютерных преступлений (в ст. 2–10, а также в дополнительном Протоколе к ней), так как, по общепризнанному мнению, ее можно считать эталоном правового акта.

Классификация компьютерных преступлений возможна не только по материальным, уголовно-правовым критериям, но также исходя из условий производства по уголовному делу по указанным составам правонарушений. В зависимости от этого расследование компьютерных преступлений может протекать в благоприятных или неблагоприятных следственных ситуациях. При этом проведение следственных действий для установления всех необходимых обстоятельств совершения компьютерных преступлений, осуществляемое в благоприятных и неблагоприятных ситуациях, может иметь ключевое значение на первоначальном этапе расследования либо после привлечения лица (лиц) в качестве обвиняемого (обвиняемых), т.е. на последующем этапе.

При расследовании данного вида преступлений исследование компьютерной информации и компьютерной техники возможно в следующих следственно-экспертных ситуациях:

– наличие объектов преступных посягательств в виде фальсифицированных данных бухгалтерского или иного учета, наличие защитных программных средств с признаками взлома, скорректированных либо измененных персональных данных и др.;

– компьютерная информация и техника являются средствами совершения преступления либо средствами связи;

– компьютерная информация (или техника) характеризует определенный объект по уголовному делу, при этом не являясь объектом преступного воздействия или средством совершения преступления (данные с видеокамер наблюдения, информация о деятельности предприятия и др.).

Особенности преступлений в сфере компьютерной информации диктуют необходимость в исследовании их криминалистической характеристики, которая пока представляет некую научную абстракцию [6]. В качестве характерных признаков здесь следует выделить:

– информацию о предмете преступного посягательства (вид, назначение компьютерной информации, на которую направлено преступное посягательство, используемые при этом материальные носители для хранения и обработки компьютерной информации);

– информацию об обстановке или среде совершения преступления (вид информационного обеспечения компьютерной системы, в которой совершено преступление, порядок его действия, а также схема обработки и защиты информации в соответствии с назначением конкретной информационной системы);

– сведения о личности преступника, цели и мотивы преступного поведения при совершении данного вида преступлений;

– типичные способы подготовки, орудия или средства совершения преступления;

– обстоятельства совершения преступления (обстановка, время, место, вид выполняемой технологической операции при обработке информации);

[2] Конвенция о компьютерных преступлениях (ETS № 185) [рус., англ.] : заключена в г. Будапеште 23 нояб. 2001 г., с изм. от 28 янв. 2003 г. URL: http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185.

– следы совершения преступления (виртуальные либо материальные) [7];

– характеристика исходной информации на первоначальном этапе расследования компьютерных преступлений.

Л.Я. Драпкин, рассматривая информационную неопределенность, связывал ее со сложными следственными ситуациями, которые, в свою очередь, затрудняют расследование, например с отсутствием надежных источников информации и достаточного количества данных об элементах предмета доказывания, с острым противодействием следователю со стороны обвиняемых и иных конфликтующих с ним лиц, с отсутствием абсолютно надежных способов и средств достижения поставленных целей, дефицитом сил, времени и ресурсов либо их нерациональным использованием [8].

Отмечая сложную работу следователя в благоприятных и неблагоприятных следственных ситуациях, следует отметить, что успех расследования, конечно, будет зависеть от своевременного привлечения специалистов. В качестве указанных специалистов в сфере информационных технологий могут быть привлечены к участию при производстве следственных действий (например, осмотра предметов, обыска, выемки, осмотра места происшествия) эксперты экспертно-криминалистических центров МВД России, в которых в дальнейшем проводится компьютерная экспертиза; сотрудники различных организаций, обладающие профессиональными знаниями работы с компьютерной техникой и информационными технологиями, в случае наличия у них соответствующего образования, которое подтверждено дипломом [9].

Безусловно, следователь, имеющий навыки опытного пользователя персонального компьютера, вправе самостоятельно произвести осмотр персонального компьютера либо его компонентов, периферийных устройств, средств связи, сетевых технических средств, портативных систем видеонаблюдения, съемных носителей компьютерной информации и других объектов компьютерной техники, т.е. без участия специалиста, однако зачастую подозреваемый или обвиняемый, обладающий соответствующей профессиональной или специальной подготовкой, использует средства защиты информации, т.е. знания в области шифрования, парольной защиты, криптографии. Наиболее популярной программой у злоумышленников является программное обеспечение Steganos Safe[3], при помощи которого флеш-накопитель или жесткий диск превращается в защищенное зашифрованное хранилище, в котором конфиденциальная информация скрыта от посторонних глаз. Без определенных знаний и умений невозможно не только дешифровать информацию, но даже установить ее местонахождение на компьютере [10]. Также можно отметить наличие на компьютере специализированных вредоносных программ, используемых в качестве препятствия для получения скрытой информации [11].

При расследовании компьютерных преступлений в рамках проводимых следователем следственных действий требуется привлечение специалистов соответствующего профиля и использование в определенной следственно-экспертной ситуации их профессиональных компетенций [12, с. 14].

По свидетельству практических работников, в ходе расследования уголовных дел о компьютерных преступлениях нередко возникают объективные сложности либо использовать помощь специалистов при назначении компьютерных экспертиз невозможно. В итоге остаются неустановленными либо не подтвержденными проводимыми впоследствии экспертными исследованиями ключевые обстоятельства по уголовным делам данной категории.

Еще раз подчеркнем, что для проведения исследования средств компьютерной техники и информации необходимо привлекать грамотных специалистов, которые имеют определенные знания и умения в данной области. Такие специалисты, обладающие высоким профессионализмом, смогут найти способы дешифрования информации, скрытой на электронных носителях, которая в дальнейшем повлияет на раскрытие и расследование киберпреступлений.

Важной формой применения специальных знаний при расследовании преступлений в сфере компьютерной информации является привлечение к участию в следственных действиях специалистов. Следственные действия могут проводиться как с работающей, так и с неработающей техникой, например при задержании подозреваемого лица с поличным можно проводить осмотр с работающий техникой, а с неработающей — уже непосредственно в момент фиксации доказательственной информации.

[3] URL: https://www.steganos.com/de/steganos-safe-18.

В подавляющем большинстве случаев применение специальных познаний специалиста требуется при производстве осмотра места происшествия и иных видов осмотра [13]. Так, деятельность специалиста при осмотре складывается из следующих последовательных действий:

– установление наличия и выполнения соответствующей компьютерной программы (при включенном компьютере);

– подробное изучение изображения на мониторе компьютера и его описание;

– фото- либо видеофиксация изображения, фиксация всех действий специалиста при производстве следственного действия;

– завершение работы компьютерной программы. Письменное закрепление хода и результатов осмотра в протоколе;

– фиксация наличия у компьютера внешних и периферийных устройств (магнитные и виртуальные диски, флеш-накопители и иное);

– по окончании процессуальных действий разъединение сетевого кабеля при включенном сетевом питании [14];

– копирование всей информации, которая необходима для расследования преступления, со всех файлов, хранящихся на виртуальных дисках и магнитных носителях;

– упаковывание каждого устройства, а также соединительных проводов и кабелей, обеспечивающих их сохранность.

Необходимо помнить о том, что при обысках и осмотрах могут быть обнаружены отпечатки скрытых следов пальцев рук, находящиеся на клавиатуре, на сетевых кабелях, на выключателях и других объектах.

В процессе осмотра места происшествия данной группы преступлений могут быть обнаружены и зафиксированы важные документы, которые в дальнейшем станут вещественными доказательствами по делу:

1. Документы, которые сохраняют в себе следы совершенного преступления, различные рукописные тексты, записи, пароли или коды, телефонные счета, номера телефонов и банковских счетов, которые могут выявить связь с другими участниками, сведения о совершенных процедурах на компьютере или в сети Интернет и др.

2. Документы со следами печати, которые необходимо искать в периферийных устройствах, например в принтерах, сканерах, факсах. Также необходимо обратить внимание на бумажные носители информации, которые могли остаться внутри этих устройств.

3. Личные документы (информация о подозреваемом).

4. Правила пользования компьютером, нормативные правовые акты, инструкции, которые регламентируют правила работы с компьютером, сетью, доказывающие, что преступник умышленно совершил преступление.

5. Документы, которые содержат в себе инструкцию либо описание аппаратуры или какого-либо устройства, доказывают нелегальное приобретение [15].

Поиск информации и элементов программного обеспечения в большинстве случаев требует специальных познаний, так как является сложной процедурой. В оперативном запоминающем устройстве может находиться информация о программах, которые запускались на компьютере, также эта информация может находиться в оперативном запоминающем устройстве периферийных и различных накопительных устройств (жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, CD- и DVD-диски, USB-флеш-накопители, карты памяти и др.). Самым эффективным способом фиксации данных является информация (появляющаяся на экране монитора), которая распечатана на бумаге.

При неработающем компьютере информация может находиться в ящиках электронной почты, на других электронных носителях и технических устройствах либо в компьютерной сети. Более детальному осмотру они подлежат в лаборатории либо на рабочем месте следователя при участии специалиста. Лучше всего изучать копии, изъятые из электронных устройств, которые изготовлены с помощью данных операций, а не сам подлинник. Для того чтобы получить более точную информацию, необходимо обращать внимание на скрытые файлы (папки), в которых может храниться важная информация, зашифрованная паролями и кодами; если такие имеются, то их нужно отправлять специалистам на декодирование и расшифровку.

Среди следственных действий при расследовании преступлений в сфере компьютерной информации большое значение имеет допрос. К особенностям допроса относится то, что для начала необходимо собрать все важные данные о лице (место работы, жительства, учебы, формы проведения досуга). Источником информации являются родственники, соседи, коллеги (одноклассники), сотрудники полиции, различных инспекций, инстанций, в которые лицо предположительно могло обращаться, личное

дело на работе (учебе), информация в социальных сетях. В ходе изучения данной информации можно определить его навыки и умения работы с компьютером и в системах.

Главной задачей является то, что необходимо установить обстоятельства, цель, время, место, способ совершения преступления и какие последствия оно принесло. Одной из проблем фиксации данных показаний выступает специфическая терминология и определения, которые необходимо подробно описывать в протоколе. При описании движения информации и структуры систем их необходимо отобразить на схеме с описанием и приложить к протоколу досмотра.

Особенности тактики допроса также зависят от следственной ситуации, целей, способов совершения преступления, связей между лицами. Важно обратить внимание на личность допрашиваемого, изучить его навыки владения компьютером, сетевыми программами, установить цель проникновения в систему, уничтожения программ, внедрения вирусных вредоносных программ, завладения различной информацией и т.д. Необходимо определить, какой реальный ущерб нанес допрашиваемый компьютерной системе в результате своих несанкционированных действий и есть ли возможность снизить или устранить причиненный вред и каким способом.

Как отмечалось выше, для грамотного применения компьютерных данных, документов, электронной информации, которая содержится на компьютере или электронном носителе, необходимы специальные знания, а не базовые знания следователя. Даже в случае если следователь прошел подготовку по данному направлению (кибернетика), его знания могут быть недостаточными, и вывод будет непонятен участникам процесса или суду.

После проведения осмотра и фиксации его в необходимых процессуальных документах следователь назначает необходимую экспертизу, определяет, какие виды исследований необходимо провести, выбирает экспертное учреждение и эксперта, выделяет необходимые объекты, которые предоставляются на экспертизу, а также формулирует вопросы эксперту [16].

Объекты, отправленные на компьютерную экспертизу, могут быть в виде текста (текстов), который сохранен на электронном носителе либо предоставлен на бумаге. Не стоит забывать о том, что носителем информации является ПК, локальная сеть и само место происшествия.

Важно помнить о назначении и традиционных видов экспертиз, таких как дактилоскопия (следы рук, которые могут быть как на самой поверхности компьютера, так и на его периферийных устройствах), техническая экспертиза документов (выявление подделки оттисков печатей и штампов, денежных знаков, ценных бумаг, установление времени изготовления и способа, обнаружение подчистки и допечатки), почерковедческая экспертиза (исследование подписей в документах и ценных бумагах). В рамках производства компьютерных экспертиз они назначаются экспертно-криминалистическими подразделениями МВД России чаще всего в соответствии со следующими статьями УК РФ: ст. 159 «Мошенничество», ст. 172 «Незаконная банковская деятельность», ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» и др. Например, в экспертно-криминалистический центр МВД по г. Санкт-Петербургу и Ленинградской области на исследование поступают различные объекты, а именно специализированные программно-аппаратные комплексы, имеющие в своем составе устройства для работы с информацией на представленных носителях, а также имеющие возможность блокировать запись информации на указанных носителях, копировать информацию с одного носителя на другой, вычислять хеш-функции файлов, восстанавливать и удалять информацию, манипулировать информацией и т.д. [17].

Анализируя возможности современных программных продуктов, следует обратить внимание, что в скором времени на исследование, возможно, будут поступать объекты, которые управляются с помощью функции smart house (умный дом), поскольку вероятность использования данного программного продукта в преступных целях велика. Примером тому могут служить современные автомобильные сигнализации, которые с легкостью вскрываются при совершении угонов автомашин. Также на исследование поступает большое количество радиотехнических устройств, в основном это прослушивающие устройства, заглушки, различные объекты, с помощью которых информация добывается незаконным путем.

На сегодняшний день довольно часто объектами экспертизы видео- и звукозаписи становятся цифровые фонограммы либо видеофонограммы, у которых звуковой сигнал подвергся сжатию. При этом главной целью сжатия является то, что в каналах связи сокращается голосовой трафик либо становится меньше объем хра-

нимой информации. Программы и устройства, которые осуществляют режим сжатия указанной информации, называются кодеками.

Перечисленные свойства таких цифровых данных обусловливают необходимость соблюдения определенных правил при фиксации и изъятии цифровых доказательств, а также их судебно-экспертном исследовании [18, с. 322].

В ходе расследования компьютерных преступлений определяющей экспертизой является компьютерная, в рамках которой проводятся следующие виды исследований: в целях исследования технических (аппаратных) средств компьютерной системы, а именно исследования закономерностей эксплуатации аппаратных средств компьютерной системы, назначается и проводится судебная аппаратно-компьютерная экспертиза; в рамках исследования функционального предназначения программного обеспечения компьютерной системы, его характеристик и реализуемых к нему требований, его алгоритма и структурных особенностей, текущего состояния — судебная программно-компьютерная экспертиза; в целях поиска, обнаружения, анализа и оценки информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе, — судебная информационно-компьютерная экспертиза (данных); в рамках исследования функционального предназначения компьютерных средств, реализующих какую-либо сетевую информационную технологию, — судебная компьютерно-сетевая экспертиза. Данные виды судебных экспертиз в достаточной степени аргументированы и исследованы Е.Р. Россинской [19].

На основании изложенного следует констатировать, что не только проведение экспертизы специалистами, имеющими специальные знания в сфере высоких технологий, по уголовным делам, связанным с преступлениями в сфере компьютерных технологий, является серьезной поддержкой, оказываемой правоохранительным органам в борьбе как с данными преступлениями, так и с целым спектром преступлений, в которых информационные технологии выступают частью базы преступной деятельности, но и участие специалиста на всех этапах расследования данных преступлений, а также при проведении всех следственных действий становится залогом успешного раскрытия, расследования и предупреждения данного вида преступлений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Бархатова Е.Н. Особенности квалификации преступлений, связанных с мошенничеством в сфере высоких технологий : учеб. пособие / Е.Н. Бархатова, В.С. Ишигеев, О.В. Радченко. — Иркутск : Изд-во ВСИ МВД России, 2018. — 111 с.

2. Грибунов О.П. Криминалистическая теория причинности в контексте установления механизма следообразования: философские и теоретические аспекты / О.П. Грибунов // Вестник Томского государственного университета. — 2019. — № 446. — С. 207–211.

3. Жмуров Д.В. Эра милосердия. Пути развития преступности / Д.В. Жмуров, А.А. Протасевич, А.С. Костромина // Baikal Research Journal. — 2019. — Т. 10, № 2. — URL: http://brj-bguep.ru/reader/article.aspx?id=23010.

4. Ткачев А.В. Возможности исследования компьютерных средств / А.В. Ткачев // Вещественные доказательства: собирание и возможности исследования / отв. ред. Н.Н. Егоров. — Москва : Юрлитинформ, 2017. — С. 165–187.

5. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки / В.Б. Вехов. — Волгоград : Изд-во Волгогр. акад. МВД России, 2008. — 407 с.

6. Мещеряков В.А. Состав, структура и особенности криминалистической характеристики преступлений в сфере компьютерной информации / В.А. Мещеряков // Воронежские криминалистические чтения / под ред. О.Я. Баева. — Воронеж : Изд-во Воронеж. гос. ун-та, 2001. — Вып. 2. — С. 137–154.

7. Степаненко Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко, В.В. Коломинов // ГлаголЪ правосудия. — 2018. — № 3 (17). — С. 38–43.

8. Криминалистика : учебник / под ред. Л.Я. Драпкина. — Москва : Юрайт, 2013. — 831 с.

9. Баев О.Я. Тактика следственных действий / О.Я. Баев. — Москва : Юрлитинформ, 2013. — 224 с.

10. Лантух Э.В. Выявление сокрытия преступлений с использованием криминалистических средств / Э.В. Лантух // Криминалистика — наука без границ: традиции и новации : материалы Всерос. науч.-практ. конф., Санкт-Петербург, 2 нояб. 2018 г. — Санкт-Петербург, 2019. — С. 126–128.

11. Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений / Л.Н. Соловьев. — Москва : Собр., 2004. — 221 с.

12. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний / С.В. Воронцова // Российская юстиция. — 2011. — № 2. — С. 14–16.

13. Коломинов В.В. Осмотр места происшествия по делам в сфере компьютерной информации / В.В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. — 2017. — № 3. — С. 145–149.

14. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. — 2012. — № 1. — С. 9–22.

15. Еникеев М.И. Следственные действия: психология, тактика, технология : учеб. пособие / М.И. Еникеев, В.А. Образцов, В.Е. Эминов. — Москва : Проспект, 2011. — 216 с.

16. Криминалистика : учебник / ред. Е.П. Ищенко. — Москва : Проспект, 2020. — 560 с.

17. Лантух Э.В. Роль специальных знаний в информационном сопровождении раскрытия и расследования преступлений / Э.В. Лантух // Деятельность правоохранительных органов в современных условиях : материалы 23-й междунар. науч.-практ. конф., Иркутск, 24–25 мая 2018 г. В 2 т. Т. 2. — Иркутск, 2018. — С. 84–87.

18. Россинская Е.Р. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники / Е.Р. Россинская, Г.П. Шамаев // Уголовно-процессуальные и криминалистические средства обеспечения уголовного судопроизводства : материалы междунар. науч.-практ. конф., Иркутск, 25–26 сент. 2014 г. — Иркутск, 2014. — С. 317–325.

19. Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е.Р. Россинская // Вестник университета им. О.Е. Кутафина. — 2019. — № 5 (57). — С. 31–44.

REFERENCES

1. Barkhatova E.N., Ishigeev V.S., Radchenko O.V. *Osobennosti kvalifikatsii prestuplenii, svyazannykh s moshennichestvom v sfere vysokikh tekhnologii* [Specifics of the qualification of crimes connected with fraud in the sphere of high technologies]. Irkutsk, East Siberian Institute of the Ministry of the Interior of Russia Publ., 2018. 111 p.

2. Gribunov O.P. The Forensic Theory of Causality in the Establishment of the Trace Creation Mechanism: Philosophical and Theoretical Aspects. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal*, 2019, no. 446, pp. 207–211. (In Russian).

3. Zhmurov D.V., Protasevich A.A., Kostromina A.S. The Era of Mercy. Ways of Criminality Development. *Baikal Research Journal*, 2019, vol. 10, no. 2. Available at: http://brj-bguep.ru/reader/article.aspx?id=23010. (In Russian).

4. Tkachev A.V. Possibilities of Computer Tools Research. In Egorov N.N. (ed.). *Veshchestvennye dokazatel'stva: sobiranie i vozmozhnosti issledovaniya* [Material Evidence: Collecting and Research Opportunities]. Moscow, Yurlitinform Publ., 2017, pp. 165–187. (In Russian).

5. Vekhov V.B. *Osnovy kriminalisticheskogo ucheniya ob issledovanii i ispol'zovanii komp'yuternoi informatsii i sredstv ee obrabotki* [Fundamentals of Forensic Science on the Study and Use of Computer Information and its Processing Tools]. Volgograd Academy of the Ministry of Internal Affairs of Russia Publ., 2008. 407 p.

6. Meshcheryakov V.A. Composition, Structure and Features of Criminalistic Characteristics of Crimes in the Field of Computer Information. In Baev O.Ya. (ed.). *Voronezhskie kriminalisticheskie chteniya* [Voronezh Criminalistic Readings]. Voronezh State University Publ., iss. 2, pp. 137–154. (In Russian).

7. Stepanenko D.A., Kolominov V.V. Digital Reality and Criminalistics. *Glagol pravosudiya = The Verb of Justice*, 2018, no. 3 (17), pp. 38–43. (In Russian).

8. Drapkin L.Ya. (ed.). *Kriminalistika* [Criminalistics]. Moscow, Yurait Publ., 2013. 831 p.

9. Baev O.Ya. *Taktika sledstvennykh deistvii* [Tactics of Investigation Activities]. Moscow, Yurlitinform Publ., 2013. 224 p.

10. Lantukh E.V. Identification of crime concealment with the use of criminalistic means. *Kriminalistika — nauka bez granits: traditsii i novatsii. Materialy Vserossiiskoi nauchno-prakticheskoi konferentsii, Sankt-Peterburg, 2 noyabrya 2018 g.* [Criminalistics — Science without Borders: Traditions and Innovations. Materials of All-Russian Research Conference, Saint Petersburg, November 2, 2018]. Saint Petersburg, 2019, pp. 126–128. (In Russian).

11. Soloviev L.N. *Vredonosnye programmy: rassledovanie i preduprezhdenie prestuplenii* [Malicious Program: Investigation and Prevention of Crimes]. Moscow, Sobranie Publ., 2004. 221 p.

12. Vorontsova S.V. Cybercrime: Problems of Qualification of Criminal Acts. *Rossiiskaya yustitsiya = Russian Justice*, 2011, no. 2, pp. 14–16. (In Russian).

13. Kolominov V.V. The Inspection of the Scene of Affairs in the Sphere of Computer Information. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Process and Criminalistic Readings*, 2017, no. 3, pp. 145–149. (In Russian).

14. Chekunov I.G. Modern Cyber Threats. Criminal Law and Criminological Classification. *Pravo i kiberbezopasnost' = Law and Cyber Security*, 2012, no. 1, pp. 9–22. (In Russian).

15. Enikeev M.I., Obraztsov V.A., Eminov V.E. *Sledstvennye deistviya: psikhologiya, taktika, tekhnologiya* [Investigative Actions: Psychology, Tactics, Technology]. Moscow, Prospekt Publ., 2011. 216 p.

16. Ishchenko E.P. (ed.). *Kriminalistika* [Criminalistics]. Moscow, Prospekt Publ., 2020. 560 p.

17. Lantukh E.V. The Role of Special Knowledge in Information Support of Crime Detection and Investigation. *Deyatel'nost' pravookhranitel'nykh organov v sovremennykh usloviyakh. Materialy 23-i mezhdunarodnoi nauchno-prakticheskoi konferentsii, Irkutsk, 24–25 maya 2018 g.* [Activities of Law Enforcement Agencies in Modern Conditions. Materials of the 23rd International Scientific and Practical Conference, Irkutsk, May 24–25, 2018]. Irkutsk, 2018, vol. 2, pp. 84–87. (In Russian).

18. Rossinskaya E.R., Shamayev G.P. Criminalistic Research of Computer Tools and Systems as a New Partition of Forensic Technology. *Ugolovno-protsessual'nye i kriminalisticheskie sredstva obespecheniya ugolovnogo sudoproizvodstva. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii, Irkutsk, 25–26 sentyabrya 2014 g.* [Criminal Process and Criminalistic Means of Ensuring Criminal Proceedings. Materials of International Scientific and Practical Conference, Irkutsk, September 25–26, 2014]. Irkutsk, 2014, pp. 317–325. (In Russian).

19. Rossinskaya E.R. Problems the Use of Special Knowledge for the Judicial Investigation of Computer Crimes in the Conditions of Digitalization. *Vestnik Universiteta imeni O.E. Kutafina = Courier of the Kutafin Moscow State Law University*, 2019, no. 5 (57), pp. 31–44. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Лантух Эдуард Владимирович — начальник кафедры криминалистики Санкт-Петербургского универ-

INFORMATION ABOUT THE AUTHORS

Lantukh, Eduard V. — Head, Chair of Criminalistics, Saint Petersburg University of the Ministry of Internal Affairs of

ситета МВД России, кандидат юридических наук, доцент, г. Санкт-Петербург, Российская Федерация; e-mail: lantuh71@mail.ru.

Ишигеев Владимир Степанович — профессор кафедры уголовного права, криминологии и уголовного процесса, Институт государства и права, Байкальский государственный университет, доктор юридических наук, профессор, г. Иркутск, Российская Федерация; e-mail: Vladimir.ishigeev@mail.ru.

Грибунов Олег Павлович — заместитель начальника Восточно-Сибирского института МВД России (по научной работе), доктор юридических наук, профессор, г. Иркутск, Российская Федерация; e-mail: gribunov@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Лантух Э.В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э.В. Лантух, В.С. Ишигеев, О.П. Грибунов. — DOI: 10.17150/2500-4255.2020.14(6).882-890 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 6. — С. 882–890.

Russia, Ph.D. in Law, Ass. Professor, Saint Petersburg, the Russian Federation; e-mail: lantuh71@mail.ru.

Ishigeev, Vladimir S. — Professor, Chair of Criminal Law, Criminology and Criminal Process, Institute of State and Law, Baikal State University, Doctor of Law, Professor, Irkutsk, the Russian Federation; e-mail: Vladimir.ishigeev@mail.ru.

Gribunov, Oleg P. — Deputy Head for Research, East-Siberian Institute of the Ministry of Internal Affairs of Russia, Doctor of Law, Professor, Irkutsk, the Russian Federation; e-mail: gribunov@mail.ru.

FOR CITATION

Lantukh E.V., Ishigeev V.S., Gribunov O.P. The use of special knowledge in the investigation of computer crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 6, pp. 882–890. DOI: 10.17150/2500-4255.2020.14(6).882-890. (In Russian).