КРИМИНАЛИСТИКА

УДК 343.9

Криминалистическая классификация средств высокотехнологичных преступлений

В. В. Поляков

Алтайский государственный университет,
Российская Федерация, 656049, Барнаул, пр. Ленина, 61

Для цитирования: Поляков, Виталий В. 2024. «Криминалистическая классификация средств высокотехнологичных преступлений». *Вестник Санкт-Петербургского университета. Право* 2: 435–453. https://doi.org/10.21638/spbu14.2024.208

Становление и развитие высокотехнологичной преступности в значительной степени основывается на использовании новых компьютерно-технических средств совершения преступлений. Это обстоятельство делает важной и актуальной задачу построения практикоориентированной классификации этих средств. В работе рассматриваются общие и частные классификации средств высокотехнологичных преступлений, основанные на различных критериях. Общая классификация, применимая для всех групп средств высокотехнологичных преступлений, проведена на основе следующих критериев: содержание технической реализации средств, законность их происхождения, вклад преступников в их разработку и создание, элементы способа преступления (подготовка, непосредственное совершение, сокрытие следов). По технической реализации средства высокотехнологичных преступлений подразделены на программные, аппаратные и программно-аппаратные. По вкладу преступников в создание проведено подразделение на готовые, модифицированные в преступных целях из имеющихся и специально разработанные новые средства. Проведено подразделение средств на группы по признаку законности их создания и использования. Описана классификация на основе соответствия средства тому или иному элементу способа преступления, при этом отмечено, что уже при подготовке преступления особое внимание уделяется разработке средств сокрытия следов и преступников. Предложены частные классификации, относящиеся к группе программно-аппаратных средств совершения высокотехнологичных преступлений. В качестве дополнительных практически значимых классифицирующих признаков выделены энергозависимость, мобильность, наличие сетевого интерфейса и вид юридических правомочий на использовавшиеся средства

преступления. Разработанные классификации призваны способствовать применению более эффективных технико-криминалистических и тактико-криминалистических приемов при расследовании высокотехнологичных преступлений.

Ключевые слова: средства преступлений, способ преступления, высокотехнологичные преступления, компьютерные преступления, расследование преступлений, криминалистическая характеристика, сокрытие преступлений.

1. Введение

Развитие информационных технологий и процесса цифровизации общественных отношений создали в последние десятилетия благоприятные условия для возникновения и быстрого роста высокотехнологичной преступности. Высокая общественная опасность этого явления предопределила то внимание, которое в последние годы было уделено исследованию его характерных признаков и особенностей. В связи со сложностью и многогранностью высокотехнологичная преступность может изучаться с различных позиций. При криминалистическом подходе высокотехнологичные преступления на основе криминалистической классификации (Гавло 2004, 466; Яблоков 2015) объединяются в отдельную группу с общими криминалистически значимыми признаками и особенностями, к которым, на наш взгляд, должен быть отнесен прежде всего высокотехнологичный способ преступлений (Поляков, Слободян 2007). Роль способа для компьютерных преступлений неоднократно подчеркивалась в работах отечественных криминалистов (Ищенко 2017, 62; Россинская, Рядовский 2019, 94; Бертовский 2020, 87; и др.).

Высокотехнологичный способ предполагает использование преступниками специально созданных или модифицированных в преступных целях технических средств. Значительная роль средств преступления определяется в конечном счете феноменом, который, по выражению Л. В. Бертовского и Б. Р. Сембековой, обусловлен технологической эволюцией преступности (Бертовский, Сембекова 2020, 129). Это подтверждается анализом судебно-следственной практики и аналитических обзоров организаций, специализирующихся в сфере информационной безопасности: именно использование специфических средств совершения преступлений является принципиальным обстоятельством, позволяющим не только успешно реализовать преступный умысел, но и существенно затруднить расследование и предупреждение высокотехнологичных преступлений.

Понятие средств высокотехнологичных преступлений включает в себя широкий круг аппаратных, программно-аппаратных и программных средств, которые могут быть классифицированы по различным основаниям. В соответствии с этим могут быть построены различные взаимосвязанные классификации, исходящие из разных криминалистически значимых классификационных критериев. Высокая практическая значимость таких классификаций определяется возможностью их непосредственного использования в зависимости от той или иной конкретной ситуации, складывающейся в процессе расследования высокотехнологичного преступления. В то же время построения системы криминалистических классификаций, описывающих средства высокотехнологичных преступлений, объединяемые в классы по различным основаниям, еще не проводилось.

В криминалистической и уголовно-правовой литературе трактовки понятия «средство совершения преступления» различаются (Мещеряков 2001, 134; Ялышев,

Семенов 2008; Хлус 2018; Прудников 2018; Бычков 2020; и др.). Кроме того, полагаем, что применительно к высокотехнологичным преступлениям понятие «средство преступления» требует переосмысления. Во-первых, это обусловлено спецификой таких средств, заключающейся, согласно мнению В. А. Мещерякова, в применении «специфического орудия преступления — средств программно-математического воздействия, объектов с уникальными свойствами» (Мещеряков 2001, 134). Во-вторых, это связано с особой ролью компьютерной информации, на что обратил внимание В. Я. Колдин (Колдин 2016). Наконец, в-третьих, специфика средств высокотехнологичных преступлений определяется, как правило, дистанционным характером преступных посягательств, роль которого описана в работах А. Л. Осипенко (Осипенко 2009a; 2009b). В соответствии с указанными обстоятельствами мы предлагаем понимать под средствами высокотехнологичных преступлений следующие объекты:

— материальные объекты, включающие в себя предметы, в частности аппаратные средства компьютерной техники, различные радиоэлектронные устройства и т. д., и материальные процессы (электромагнитное излучение, звуковые волны и т. д.);

— информационные объекты, представленные обычной информацией, в том числе устной и письменной вербальной информацией, а также невербальной и компьютерной информацией, объединяющей все виды электронных документов и компьютерное программное обеспечение (в том числе вредоносные программы);

— комплексные объекты, являющиеся неразделимыми комбинациями материальных и информационных объектов, представленные программно-аппаратными средствами и телекоммуникационными сетями.

Полагаем, что такие факторы, как появление и быстрое распространение новых средств высокотехнологичных преступлений и возрастающие криминалистические сложности при их расследовании, делают актуальной криминалистическую систематизацию этих средств. В связи с этим в настоящем исследовании поставлена цель научно-практической классификации средств, применяемых при совершении высокотехнологичных преступлений. Для реализации этой цели в работе решаются задачи по выявлению особенностей, присущих рассматриваемым средствам преступления, установлению взаимосвязей между ними и построению на основе выделяемых криминалистических критериев классификационных схем, отражающих различные свойства средств преступления.

В качестве методологической основы привлекаются общенаучные методы познания, в частности системно-структурный подход, позволяющий рассматривать исследуемые объекты как системы, образованные взаимодействующими элементами (Ображиев 2012). При изучении эмпирических данных (судебно-следственной практики) применялись статистические методы анализа. В силу новизны исследуемого явления — высокотехнологичной преступности — возникают объективно обусловленные сложности с репрезентативностью эмпирических данных. Указанная проблема преодолевалась путем привлечения прогностических методов анализа, в том числе особое внимание уделялось методу экспертных оценок (Понкин, Лаптева 2021, 512). Для обобщения эмпирических данных, включавших в себя материалы уголовных дел, оперативно-разыскной практики и результаты анкетирования экспертов, привлекались интегративный метод, методы анализа и синтеза.

Использование сравнительно-правового метода позволило получить количественные показатели и сгруппировать средства преступления по различным юридическим основаниям. Кроме того, применялся метод контент-анализа научной литературы по рассматриваемой тематике.

2. Основное исследование

2.1. Общие классификации средств высокотехнологичных преступлений

Классификация средств высокотехнологичных преступлений может быть проведена на основе разных признаков, что приводит к различным результатам. Полагаем, что для правоохранительной практики наибольшую ценность могут представлять следующие общие признаки: содержание технической реализации средств, законность их происхождения, вклад преступников в их разработку и создание, связь с теми или иными элементами способа преступления. Рассмотрим соответствующие этим классификациям группы средств преступления.

2.1.1. Техническая реализация средств высокотехнологичных преступлений

Этот классифицирующий признак позволяет разделить средства высокотехнологичных преступлений на программные, аппаратные и программно-аппаратные.

2.1.1.1. Программные средства высокотехнологичных преступлений

Как показывает анализ имеющейся судебно-следственной практики, экспертных мнений сотрудников правоохранительных органов и специалистов, аналитических обзоров о состоянии преступности исследовательских центров и специализирующихся в сфере информационной безопасности компаний (например, аналитических обзоров компаний Group-IB[1] и Positive Technologies[2]), при совершении высокотехнологичных преступлений основную роль играют именно программные средства, фактически ставшие технической основой для наиболее опасных видов преступлений, которые совершаются организованными преступными группами путем использования дистанционных технологий, т. е. с помощью информационно-коммуникационных сетей.

В качестве программных средств чаще всего используется вредоносное программное обеспечение. Наиболее распространенное вредоносное программное средство преступления — компьютерные вирусы (например, макровирусы, загрузочные вирусы и др.), т. е. самовоспроизводящиеся вредоносные программы, несанкционированно устанавливаемые на компьютерные устройства с целью

[1] «Hi-Tech Crime Trends 2023/2024». *Group-I B*. Б. д. Дата обращения 20 мая, 2024. https://www.group-ib.com/landing/hi-tech-crime-trends-2023-2024.

[2] «Operftion TaskMaster. Кибершпионаж в эпоху цифровой экономики». *Positive Technologies*. Б. д. Дата обращения 20 мая, 2024. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Operation-Taskmasters-2019-rus.pdf.

воздействия (копирования, удаления, модифицирования, повреждения) на компьютерную информацию. К основным разновидностям компьютерных вирусов относятся компьютерные черви (самораспространяющиеся вредоносные файлы) (Пастернак, Корнеева, Дегтярева 2014), а также разнообразные троянские программы, внедряемые в компьютерные устройства, например, под видом легального программного обеспечения. Довольно распространенными программными средствами высокотехнологичных преступлений являются эксплойты, т. е. простые программы, программные коды или фрагменты программ, позволяющие эксплуатировать уязвимости в программном обеспечении объекта преступного посягательства (например, путем выполнения действий, не предусмотренных разработчиками). Пример другой разновидности программных средств, которые могут использоваться для совершения преступлений, — так называемые программы-шеллы, интерпретирующие команды пользователя по управлению компьютерной техникой.

2.1.1.2. Аппаратные средства высокотехнологичных преступлений

К аппаратным средствам совершения высокотехнологичных преступлений могут быть отнесены различные классы технических устройств, прежде всего электронные устройства с цифровыми или аналоговыми микросхемами, периферийные устройства компьютерной техники, в том числе обеспечивающие работу информационных сетей, устройства хранения и переноса компьютерной информации (например, флеш-накопители) и т. д. Аппаратные средства преступлений используются, как правило, для решения относительно узких задач, например для физического проникновения в банкоматы, размагничивания жестких дисков компьютеров и т. д. К аппаратным средствам нужно отнести также различные классы технических устройств, которые позволяют преступникам получать сведения об объекте преступного посягательства без непосредственного физического доступа к нему. Так, Н. Г. Шурухнов описывает радиоэлектронные средства связи, слежения (в том числе оптические приборы и средства с высокой разрешающей способностью), звукоулавливающую и звукозаписывающую аппаратуру (Шурухнов 2013, 128).

В ряде случаев разделение средств на аппаратные и программно-аппаратные (рассматриваемые ниже) достаточно условно, поскольку многие аппаратные средства имеют программную составляющую или используются только в сочетании с программными средствами (Ялышев, Семенов 2008).

Помимо свободно распространяемых и не ограниченных к свободному обороту аппаратных средств, в высокотехнологичных преступлениях могут использоваться собственные разработки преступников. В качестве примера можно привести аппаратные средства, специально создаваемые для хищения денег из банкоматов, в частности воздействующие на механизмы для выдачи денежных купюр (Цимбал 2013, 86).

2.1.1.3. Программно-аппаратные средства высокотехнологичных преступлений

Программно-аппаратные средства при совершении высокотехнологичных преступлений применяются значительно чаще, чем аппаратные, поскольку имеют значительно более широкие и гибкие возможности за счет использования

пользовательского и сетевого интерфейса и специализированных программ. Эти дополнительные возможности позволяют использовать их дистанционным образом. К распространенным программно-аппаратным средствам могут быть отнесены, в частности, скиммеры, шиммеры, кейлоггеры. Скиммеры (от англ. skim — «скользить») — это переносные устройства, которые крепятся к банкоматам для сбора данных с банковских карт пользователей и дальнейшего их хранения или пересылки преступникам. Как свидетельствуют изученные нами уголовные дела, использование различных видов скиммеров преступными группами в последнее десятилетие получило весьма широкое распространение[3]. Разновидностью скиммеров можно считать шиммеры (от англ. shim — «прокладка»), представляющие собой электронные устройства, помещаемые в картридер банкомата и также позволяющие собрать информацию о банковских картах, при этом в силу малого размера они практически не заметны. Кейлоггеры (от англ. keylogger; key — «клавиша», logger — «регистрирующее устройство») являются средствами, позволяющими собирать данные, вводимые пользователями (например, логин и пароль), и хранить их в собственной памяти или передавать по информационной сети.

Используемые в преступных целях программно-аппаратные средства отличаются разнообразием технического исполнения, в том числе достаточно сложного. Так, в работе Е. Р. Россинской и И. А. Рядовского при анализе технических решений, используемых в компьютерных преступлениях, описаны аппаратно-программные комплексы Black Box и бот-фермы (Россинская, Рядовский 2019, 95).

Сами информационно-телекоммуникационные сети, прежде всего интернет, для функционирования которых требуется широкий спектр различных аппаратных устройств и специализированного программного обеспечения, при их использовании современной высокотехнологичной преступностью выступают специфическими и важнейшими программно-аппаратными средствами преступлений.

2.1.2. Вклад преступников в создание средств высокотехнологичных преступлений

Важный классифицирующий признак средств высокотехнологичных преступлений — роль преступников в их разработке, использовании или модификации. При этом наиболее опасной и сложной для расследования является группа высокотехнологичных преступлений, в которых были применены новые средства, созданные преступниками, или была использована модификация уже существовавших средств. Практикоориентированность данного классификационного критерия заключается в том, что он способствует установлению действий преступников прежде всего на стадии подготовки преступления, а также установлению роли и формы вины участников преступной группы.

[3] См., напр.: Уголовное дело № 1-55/2014 (Архив Первомайского районного суда г. Владивостока); Приговоры Орджоникидзевского районного суда г. Екатеринбурга от 17.06.2014 № 1-22/2014 1-523/2013 по делу № 1-22/2014; Красногвардейского районного суда г. Санкт-Петербурга от 18.07.2017 № 1-637/2017 по делу № 1-637/2017; и др. Здесь и далее все ссылки на российские нормативно-правовые акты и судебную практику приводятся по СПС «КонсультантПлюс». Дата обращения 20 мая, 2024. http://www.consultant.ru.

2.1.2.1. Готовые средства высокотехнологичных преступлений, находящиеся в свободном обороте или исключенные из него

В преступных целях может привлекаться легально распространяемое программное обеспечение, например мессенджеры для связи, обеспечивающие законный и зачастую бесплатный мгновенный обмен текстовыми, голосовыми и видеосообщениями. Наиболее распространены в нашей стране мессенджеры WhatsApp, Telegram, Viber, Skype, обеспечивающие в большей или меньшей степени секретность передаваемой информации и анонимность пользователей. При расследовании преступлений из подобных мессенджеров может быть получена криминалистически значимая информация (Алиева, Кустов 2019). В то же время некоторые мессенджеры, например Telegram, а также сервисы в сети Darknet, практически не позволяют правоохранительным органам получать и контролировать фигурирующую в них криминалистически значимую информацию (Смушкин 2022). Кроме того, руководство компаний, которым принадлежат такие мессенджеры, как правило, не раскрывают конфиденциальную информацию клиентов даже по официальным запросам правоохранительных органов (Шатохин 2019). Фактически это означает, что преступники могут прибегать к использованию свободно распространяемого программного обеспечения, которое не контролируется правоохранительными органами и практически не оставляет доступных для сбора и использования в уголовном судопроизводстве электронно-цифровые следы (Семикаленова 2019).

Сегодня также значителен теневой рынок готовых специализированных средств, в большей степени представленный в сети Darknet (Сергеев 2017, 140). Готовые средства могут быть как узконаправленного действия, например так называемые банковские трояны, так и расширенного спектра применения, например в отношении конкретных уязвимостей какого-либо программного обеспечения, устанавливаемого на различные компьютерные системы. Зачастую преступники, использовав такие средства, затем могут продавать их как апробированные готовые продукты. Использованию в преступной деятельности готовых средств способствует, как справедливо отмечал Н. Г. Шурухнов, то, что «не представляется затруднительным приобрести наставления, нормативные документы, рекомендации по применению и использованию техники, различной аппаратуры» (Шурухнов 2013, 132).

Например, участники преступной группы, обвинявшиеся по совокупности преступлений, подпадавших под ч. 4 ст. 158, ч. 3 ст. 272, ч. 3 ст. 183 Уголовного кодекса РФ от 13.06.1996 № 63-ФЗ (УК РФ) и заключавшихся в хищении денежных средств из банкоматов, приобрели через интернет у неустановленных лиц готовое техническое устройство «скиммер», предназначенное для незаконного копирования информации с магнитных полос банковских карт и устанавливаемое на картоприемник банкомата[4].

[4] Уголовное дело № 1-329/2013 (Архив Центрального районного суда г. Барнаула).

2.1.2.2. Средства, приспособленные для совершения высокотехнологичных преступлений путем модификации

Весьма негативную роль для расследования может играть модификация преступниками уже имеющихся средств преступлений. В Рекомендательном перечне составов преступлений и административных правонарушений в сфере обеспечения информационной безопасности личности, общества и государства для государств — членов Организации Договора о коллективной безопасности (ОДКБ) справедливо указывается: «Не во всех случаях речь должна идти исключительно о разработке новых программ. Распространены случаи, когда видоизменение существующих программ наделяет их свойствами вредоносности»[5]. Полагаем, это в равной мере относится к модификации программно-аппаратных и аппаратных средств.

Так, члены упомянутой выше преступной группы изготавливали путем модификации «подручных средств»[6] технические устройства для незаконной видеофиксации введенных на клавиатуре банкомата ПИН-кодов, идентичные по форме и цвету штатным деталям банкомата. Типичными для случая программных средств могут служить действия участников преступной группы, осуществлявшей хищение денежных средств организаций, специализировавшихся на дистанционной продаже железнодорожных билетов, выражавшиеся в том, что вредоносное программное обеспечение разрабатывалось путем модификации легальной программы для удаленного администрирования компьютеров, созданной российской компанией[7].

2.1.2.3. Специально созданные для совершения высокотехнологичных преступлений новые средства

В высокотехнологичных преступлениях наряду с модификацией имеющихся средств активно происходит создание нового специализированного программного обеспечения, а также новых аппаратных и программно-аппаратных устройств. Очевидно, что именно новизна таких средств значительно усложняет противодействие высокотехнологичной преступности. Например, имеющееся антивирусное программное обеспечение может не диагностировать новые вредоносные программы. Специалисты по информационной безопасности могут испытывать значительные сложности в выявлении и понимании особенностей и принципов действия такого рода целевых атак. При этом потерпевшим, как правило, ничего не известно о новых угрозах, вследствие чего потенциальные объекты преступных посягательств остаются не защищенными должным образом. Можно утверждать,

---

[5] Рекомендательный перечень составов преступлений и административных правонарушений в сфере обеспечения информационной безопасности личности, общества и государства для государств — членов ОДКБ. Принят Постановлением Парламентской Ассамблеи Организации Договора о коллективной безопасности, Ереван, от 05.11.2019 № 12-4.2. С. 8. Дата обращения 20 мая, 2024. https://paodkb.org/uploads/document/file/111/Perechen-12-4.2.pdf.

[6] Уголовное дело № 1-329/2013 (Архив Центрального районного суда г. Барнаула).

[7] Приговор Смольнинского районного суда г. Санкт-Петербурга от 02.02.2016 № 1-41/2016 1-501/2015 по делу № 1-41/2016.

что непрерывная разработка и применение новых средств высокотехнологичных преступлений повышают общественную опасность этих преступных деяний.

В качестве типичного примера разработки новых программных средств преступления могут служить действия Р., выразившиеся в подыскании неустановленного разработчика вредоносного программного обеспечения на интернет-бирже программистов, передаче с использованием мер конспирации путем создания обезличенных разовых аккаунтов заказа на создание новой компьютерной программы с заданным вредоносным функционалом и последующее использование этой программы для несанкционированного копирования парольно-кодовой информации от FTP-серверов[8].

2.1.3. Законность происхождения средств высокотехнологичных преступлений

Используемые при совершении высокотехнологичных преступлений средства можно классифицировать по признаку законности их создания (модификации, оборота и использования). Данный критерий при уголовном судопроизводстве способствует решению задач доказывания, а также должен учитываться при введении данных оперативно-разыскных мероприятий в процессуальную форму.

2.1.3.1. Законные средства

К законным по происхождению относятся средства, разрешенные для свободной разработки, распространения и использования. Такие средства практически всегда используются при совершении высокотехнологичных преступлений; например, к их числу могут быть отнесены упоминавшиеся выше мессенджеры.

2.1.3.2. Незаконные средства

К незаконным средствам высокотехнологичных преступлений относятся программные, программно-аппаратные и аппаратные средства, создание и модификация которых гражданами запрещены законом.

Согласно международному праву, противозаконное использование указанных средств криминализируется в Конвенции о компьютерных преступлениях, принятой Советом Европы. Именно в ст. 6 «Противозаконное использование устройств» этой конвенции указывается, что преступлением могут считаться: «a) производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование: i) устройств, включая компьютерные программы, разработанные или адаптированные, прежде всего для целей совершения какого-либо из преступлений <…>; ii) компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их с целью совершения какого-либо из преступлений <…>; b) владение одним

[8] Уголовное дело № 1-222/2016 (Архив Советского районного суда г. Владивостока).

из предметов, упоминаемых в пунктах i) или ii), с намерением использовать его с целью совершения любого из преступлений <…>»[9].

Полагаем, что отдельного изучения заслуживает вопрос о создании и использовании в преступных целях средств, находящихся в ограниченном обороте или изъятых из оборота. Средства ограниченной оборотоспособности и изъятые из оборота зачастую используются в преступных целях для негласного получения информации, например, путем аудио- или видеозаписи. В силу особых возможностей, которые предоставляют такие средства, их применение тщательно контролируется. В соответствии со ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», разработка, производство, реализация и приобретение специальных технических средств, предназначенных для негласного получения информации, подлежат лицензированию. В силу особых возможностей таких средств они предназначены прежде всего оперативно-разыскным органам, поэтому за их изготовление, переделку (модификацию) и приспособление, сбыт и использование предусмотрена уголовная ответственность (ст. 138[1] УК РФ). Квалификация преступлений по этой статье неоднократно встречалась в исследованной нами судебно-следственной практике[10].

При анализе законности происхождения программных средств совершения высокотехнологичных преступлений нужно также учитывать наличие легитимного программного обеспечения, изначально пригодного к решению преступных задач. В эту группу средств входят, например, программы, объединяемые назначением «тестирование на проникновение» (пентест) (Киздермишов 2015; Зинкевич, Михайлов 2018). Особенностью работы таких программ является моделирование несанкционированного доступа к компьютерной системе. В силу уголовно-правовой неурегулированности статуса подобного программного обеспечения его создание и применение могут быть признаны незаконными, несмотря на то что оно фактически служит целям обеспечения информационной безопасности. Полагаем, что в силу специфики предназначения такого программного обеспечения, а также его потенциальной опасности целесообразно контролировать его использование путем определения категорией лиц, допущенных к работе с ним, и их регистрации, а также лицензирования деятельности по разработке таких программных продуктов.

2.1.4. Элементы способа высокотехнологичных преступлений

Одним из основных криминалистических понятий выступает способ преступления. По глубокой мысли Р.С. Белкина, «во всех случаях — без всяких исключений — сохраняет свое значение классификация по способу совершения преступления» (Белкин 2001, 237). В соответствии с трактовкой способа преступления, предложенной Г.Г. Зуйковым, будем исходить из понимания способа как единой

[9] The Convention on Cybercrime of the Council of Europe (CETS No. 185). Budapest, 23.11.2001. Дата обращения 20 мая, 2024. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561. Русскоязычный вариант: Конвенция о компьютерных преступлениях. Будапешт, 23.11.2001. Дата обращения 10 сентября, 2022. https://rm.coe.int/1680081580.

[10] См., напр.: Уголовное дело № 1-187/2014 (Архив Ленинского районного суда г. Барнаула); Приговор Ленинского районного суда г. Тюмени от 23.08.2016 № 1-876/2016 по делу № 1-876/2016; и др.

системы из трех элементов — действий по подготовке, непосредственному совершению и сокрытию преступления (Зуйков 1971). При этом, как подчеркивал В.К. Гавло, все эти элементы «находятся в единстве, составляют единый способ преступления в целом, так как конечные действия и результат сокрытия следов преступления обусловлены задолго до его начала единым планом и замыслом» (Гавло 1982, 153).

Анализ судебно-следственной практики свидетельствует, что высокотехнологичный способ преступлений является полноструктурным, поскольку включает стадии подготовки к преступлению, непосредственного совершения и действий по сокрытию следов-последствий и преступников. Этим определяется целесообразность классификации средств высокотехнологических преступлений по элементам способа преступлений, поскольку средства, относящиеся к разным элементам способа, как правило, ориентированы на решение разных задач преступной деятельности.

2.1.4.1. Подготовка преступления

В содержание этого элемента способа преступления обычно входят изучение обстановки на объекте посягательства, прежде всего режима его физической охраны (видеонаблюдения, сигнализации и т. п.), а также программных и программно-аппаратных средств и методов информационной безопасности (например, средств идентификации и аутентификации пользователей). В качестве средств преступления используются, в частности, специальные компьютерные программы, в том числе оценивающие объект посягательства с точки зрения защищенности. Проводится адаптация средств преступлений для достижения основной цели (например, с помощью программы-шпиона Zeus). Уже при подготовке преступления особое внимание уделяется выбору средств, направленных на сокрытие следов предстоящих преступных действий: подбирается различное оборудование (например, устройства для размагничивания жестких дисков), готовятся носители для переноса и хранения незаконно копируемой информации (флеш-диски, облачные хранилища и пр.), избираются информационные технологии, обеспечивающие анонимность преступников (TOR, VPN и др.). В силу этого, как справедливо отмечал Н.Г. Шурухнов, «нередко процесс применения технических средств, предшествующий совершению преступлений, занимает у преступников значительный промежуток времени» (Шурухнов 2013, 129). Подготовка к совершению высокотехнологичных преступлений может также включать необходимость вербовки в преступную группу специалистов с определенными знаниями и навыками в сфере компьютерных технологий.

2.1.4.2. Непосредственное совершение преступления

Действия преступников, относящиеся ко второму элементу способа преступлений, включают в себя применение различных программных, аппаратных и аппаратно-программных средств. Так, при неправомерном доступе к предмету преступного посягательства, которое осуществляется путем дистанционного управления автоматизированным рабочим местом пользователя, могут задействоваться

следующие средства преступления: программы, предназначенные для администрирования (TeamViewer, Radmin, TightVNC и т. п.); специализированные клиенты сетевых протоколов RDP (Remote Desktop Protocol) или VNC (Virtual Network Computing), имеющие собственный веб-интерфейс для управления ими; различные модификации вредоносного программного обеспечения, например Zeus, Carberp и т. п. При осуществлении массового заражения вирусами автоматизированных рабочих мест через веб-сервисы обычно применяются наборы эксплойтов, предназначенных для эксплуатации ошибок в веб-браузерах и всевозможных расширений к ним, например фреймворков (программных платформ) ActiveX, Adobe Flash; также используются бот-фермы, применяемые для массового распространения вредоносных программ (Россинская, Рядовский 2019, 94).

2.1.4.3. Сокрытие преступления

С целью сокрытия преступлений, прежде всего электронно-цифровых следов-последствий (Мещеряков 2013; Поляков, Слободян 2007; Семикаленова 2019; Вехов 2009; Осипенко 2009a; 2009b), могут применяться средства, различающиеся по времени их использования, характеру воздействия, специфики объекта, на который они направлены, технической реализации и т. д. Так, для сокрытия следов преступления используются ремейлеры — специализированные серверы, получающие сообщения электронной почты и переправляющие их по указанному отправителем адресу, при этом уничтожающие исходную информацию об отправителе.

Другим примером сокрытия следов являются программы, маскирующие противоправные действия путем использования специальных каналов передачи информации. Сокрытие обычно включает в себя анонимизацию преступников, для чего применяются сервисы, подменяющие реальный IP-адрес. Для этой цели активно используются VPN-сервисы, которые обеспечивают доступ к сети через цепочку промежуточных серверов (Double/Triple-VPN). Широкие возможности для анонимизации предоставляет также технология TOR и сеть Darknet.

Кроме сокрытия следов-последствий, третий элемент способа преступления может включать в себя сокрытие информации о местонахождении скрывающихся участников преступления. Особенно осложняет расследование и определение реального местонахождения преступников использование подмененных IP-адресов, относимых к другому государству.

2.2. Частные классификации для отдельных групп средств высокотехнологичных преступлений

Наряду с рассмотренными общими классификациями, применимыми ко всем группам средств высокотехнологичных преступлений, могут быть построены частные классификационные схемы, относящиеся к отдельным группам средств. Это позволяет на основе дополнительных классифицирующих признаков выделять группы (подгруппы) средств преступлений на более низких иерархических уровнях классификации.

Рассмотрим частные классификации, характеризующие группу аппаратных и программно-аппаратных средств и актуальные с позиций организации

следственных действий при предварительном расследовании. В этом случае в качестве практически значимых классифицирующих признаков, на наш взгляд, могут быть выделены следующие: энергозависимость, мобильность, наличие сетевого интерфейса.

2.2.1. Энергозависимость средств высокотехнологичных преступлений

Относящиеся к рассматриваемой группе средства высокотехнологичных преступлений могут быть подразделены на те, которым требуется постоянный источник энергии для сохранения компьютерной информации, и те, которые в таком источнике не нуждаются. В зависимости от этого выделяются энергозависимые и энергонезависимые устройства и/или элементы устройств.

На практике учет такого разделения важен, поскольку в случае, когда компьютерная информация находится в энергозависимой части устройства, она может быть безвозвратно потеряна после отключения электропитания (например, в оперативной памяти компьютера часто хранятся важные в доказательственном плане следы-последствия преступления). В энергонезависимой части устройства компьютерная информация сохраняется после отключения электропитания, например в USB-флеш-накопителе.

Проведение следственных действий, связанных с поиском, фиксацией и изъятием компьютерной информации, необходимо начинать с энергозависимой части устройств, так как всегда существует риск ее потери. Такая потеря криминалистически значимой информации может произойти в результате ошибочных действий сотрудников правоохранительных органов с компьютерной техникой, стать следствием технических сбоев в работе устройств, произойти от непреднамеренных действий со стороны третьих лиц или же преднамеренных действий преступников. Например, преднамеренные действия преступников, желающих скрыть следы-последствия преступления, могут выражаться в установке программ или устройств уничтожения информации, которые срабатывают по дистанционной команде или при определенных условиях.

2.2.2. Мобильность средств высокотехнологичных преступлений

Среди используемых в качестве средств высокотехнологичных преступлений устройств может быть выделена группа, характеризуемая свойством мобильности, т. е. возможности использования и подключения к информационным сетям при движении в пространстве. Особенностями мобильных средств являются, как правило, компактность и малый вес, обеспечивающие возможность свободного перемещения. Стационарные устройства, в отличие от мобильных, привязаны к определенному месту. В связи с этим по критерию мобильности аппаратные и программно-аппаратные средства преступлений целесообразно разделить на две группы: стационарные и мобильные.

Значимость выделения группы мобильных устройств обусловлена тем, что при их использовании могут оставаться следы, указывающие на изменение местоположения средства преступления, а также времени его использования при

смене часовых поясов. Кроме того, за счет использования мобильных средств при их передвижении увеличивается размер места происшествия, что влияет на территориальную подследственность расследуемого преступления.

Такая классификация во многом условна, поскольку современная компьютерная техника имеет тенденцию к уменьшению габаритов, вследствие чего стационарные устройства при наличии соответствующего источника электропитания могут использоваться как мобильные при их транспортировке.

2.2.3. Наличие сетевого интерфейса

Аппаратные и программно-аппаратные средства высокотехнологичных преступлений в техническом плане могут иметь сетевой интерфейс, обеспечивающий наличие такого важного свойства, как возможность выхода в информационную сеть. За счет такого выхода становятся возможными дистанционный доступ к предмету преступного посягательства и обеспечение связи между участниками группового совершения высокотехнологичных преступлений. Устройства без сетевого интерфейса также позволяют выполнять различные задачи, например осуществлять разработку вредоносных программ. В то же время в случае совершения высокотехнологичных преступлений в том или ином качестве всегда присутствуют средства, оснащенные сетевым интерфейсом для дистанционной передачи компьютерной информации.

В соответствии с критерием наличия сетевого интерфейса могут быть выделены две группы средств: без сетевого интерфейса (без возможности дистанционной передачи компьютерной информации) и с сетевым интерфейсом (позволяющие дистанционно передавать или получать компьютерную информацию).

В рамках предложенного подхода могут быть рассмотрены и другие частные классификационные схемы, актуальные для конкретных ситуаций расследования высокотехнологичных преступлений. Так, для законных программно-аппаратных средств может быть предложена классификация, основанная на таком признаке, как *вид юридических правомочий* на эти средства. Законные средства, используемые в высокотехнологичной преступной деятельности, всегда находятся в чьей-либо собственности. При этом собственник может на законных основаниях разрешить владеть, пользоваться и распоряжаться компьютерными средствами (ст. 209 Гражданского кодекса РФ (часть первая) от 30.11.1994 № 51-ФЗ) другим физическим или юридическим лицам. Лицо, получившее соответствующие права, может, в свою очередь, передать средство другому лицу (например, заключив договор субаренды) (Большаков, Гаврилин 2019). Как следствие, возникают ситуации, когда компьютерные устройства передаются в многократную субаренду и впоследствии используются в преступных целях в течение относительно короткого времени. Таким образом достаточно часто используются серверы и виртуальные машины, с помощью которых происходит управление вредоносными бот-сетями, на которых хранится криминалистически значимая компьютерная информация. Собственник таких средств может быть не осведомлен об использовании его техники в преступных целях, причем в этом случае ситуация усугубляется тем, что арендатором может выступать подставное лицо.

Существуют и другие ситуации, в которых вид правомочий имеет значение для расследования. Так, в случаях использования преступниками в публичном месте общедоступной Wi-Fi-сети может потребоваться обращение к владельцу этой сети, чтобы собрать следы-последствия преступления. Полагаем, что в соответствии с данным классифицирующим критерием возможно подразделить используемые средства высокотехнологичных преступлений на следующие группы: владение средством; пользование средством; распоряжение средством.

Приведенные обстоятельства, осложняющие установление преступников, показывают, что вид правомочий на средства преступления является одним из факторов, влияющих на тактику расследования уголовных дел, и в силу этого должен приниматься во внимание субъектами расследования.

3. Выводы

Рассмотренный перечень классификационных критериев и построенных на их основе криминалистических классификаций не является исчерпывающим и при необходимости, в частности при появлении новых средств высокотехнологичных преступлений, может быть дополнен и расширен. Кроме того, предложенные классификации имеют достаточно универсальную основу и могут быть распространены на иные виды преступлений.

Проведенное классифицирование позволяет выявить содержательные особенности средств высокотехнологичных преступлений, а также предоставляет возможность установить взаимосвязи между группами этих средств. В теоретическом плане предложенные классификации расширяют и систематизируют знания о таком принципиально важном элементе криминалистической характеристики высокотехнологичных преступлений, как средства их совершения. Полученные результаты в практическом плане призваны способствовать разработке и применению более эффективных технико-криминалистических и тактико-криминалистических приемов, адаптированных к расследованию высокотехнологичных преступлений в различных криминалистических ситуациях. Это позволит следственным и оперативно-разыскным органам лучшим образом устанавливать зависимости между различными обстоятельствами преступления, выдвигать более вероятные криминалистические версии, принимать правильные тактические решения, что в итоге позитивно отразится на эффективности расследования высокотехнологичных преступлений.

Библиография

Алиева, Гюнай А., Анатолий М. Кустов. 2019. «Получение криминалистически значимой информации из мессенджера WhatsApp* в качестве источника доказательственной информации». *Проблемы получения и использования доказательственной и криминалистически значимой информации: материалы Междунар. науч.-практ. конф.*, 3–4. Симферополь: Ариал.

Белкин, Рафаил С. 2001. *Курс криминалистики*. В 3 т. Т. 3. М.: ЮНИТИ-ДАНА.

Бертовский, Лев В. 2020. «К вопросу о понятии киберпреступления». *Расследование преступлений: проблемы и пути их решения* 4 (30): 84–88.

* Продукт компании Meta, деятельность которой признана экстремистской в Российской Федерации.

Бертовский, Лев В., Бакиткул Р. Сембекова. 2020. «Высокотехнологичные преступления как угроза национальной безопасности». *Новеллы материального и процессуального права: материалы Всерос. (нац.) науч.-практ. конф.*, 127–130. Красноярск: Красноярский государственный аграрный университет.

Большаков, Никита А., Юрий В. Гаврилин. 2019. «Арендованное компьютерное оборудование и программное обеспечение как орудия и средства совершения преступлений в сфере компьютерной информации». *E-Scio* 11 (38): 384–388.

Бычков, Василий В. 2020. «Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности». *Вестник Академии Следственного комитета Российской Федерации* 3 (25): 43–46.

Вехов, Виталий Б. 2009. «Понятие и механизм образования электронно-цифровых следов». *Использование современных информационных технологий и проблемы информационной безопасности в деятельности правоохранительных органов: межвуз. тематич. сб. науч. тр.*, 62–72. Калининград: Калининград. юрид. ин-т МВД России.

Гавло, Вениамин К. 1982. «К вопросу о криминалистической характеристике преступлений». *Борьба с преступностью на современном этапе: межвуз. сб.*, 150–159. Барнаул: Алтайский государственный университет.

Гавло, Вениамин К. 2004. *Общие положения криминалистической методики расследования отдельных видов преступлений*. Под ред. Леонида Я. Драпкина, Валерия Н. Карагодина, 444–477. М.: Юридическая литература; Элит.

Зинкевич, Алексей В., Максим С. Михайлов. 2018. «Аудит информационной безопасности». *Ученые заметки Тихоокеанского государственного университета* 1 (9): 307–312.

Зуйков, Георгий Г. 1971. «Криминалистическое учение о способе совершения преступления». *Социалистическая законность* 11: 14–19.

Ищенко, Евгений П. 2017. «Криминалистические аспекты расследования киберпреступлений». *Уголовное производство: процессуальная теория и криминалистическая практика: материалы V Междунар. науч.-практ. конф.* (27–29 апреля 2017 г., г. Симферополь — Алушта), 62–65. Симферополь: Ариал.

Киздермишов, Асхад. А. 2015. «К вопросу о применении CVE-совместимых сетевых сканеров». *Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки* 1 (154): 136–140.

Колдин, Валентин Я. 2016. «Электронная информация в праве». *Вестник Московского университета. Серия 11. Право* 2: 96–110.

Мещеряков, Владимир А. 2001. *Преступления в сфере компьютерной информации: правовой и криминалистический анализ*. Воронеж: Воронежский государственный университет.

Мещеряков, Владимир А. 2013. «Следы преступлений в сфере высоких технологий». *Библиотека криминалиста. Научный журнал* 5 (10): 265–270.

Ображиев, Константин В. 2012. «Системный подход в юриспруденции: теоретико-методологические основы». *Вестник Ленинградского государственного университета им. А. С. Пушкина* 1 (2): 89–96.

Осипенко, Анатолий Л. 2009a. «Проблемы вовлечения электронно-цифровых следов в уголовный процесс». *Научный вестник Омской академии МВД России* 4 (35): 31–34.

Осипенко, Анатолий Л. 2009b. *Сетевая компьютерная преступность: теория и практика борьбы*. Омск: Омская академия МВД России.

Пастернак, Юрий Г., Наталья Н. Корнеева, Ксения В. Дегтярева. 2014. «К вопросу моделирования процесса реализации атак посредством компьютерных червей». *Информация и безопасность* 2 (17): 330–331.

Поляков, Виталий В., Степан М. Слободян. 2007. «Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации». *Известия Томского политехнического университета* 1 (310): 212–216.

Понкин, Игорь В., Алена И. Лаптева. 2021. *Методология научных исследований и прикладной аналитики*. М.: Буки Веди.

Прудников, Ярослав В. 2018. «Понятия та види засобів вчинення злочину». *Проблеми законності* 142: 189–199.

Россинская, Елена Р., Игорь А. Рядовский. 2019. «Современные способы компьютерных преступлений и закономерности их реализации». *Lex russica* 3 (148): 87–99.
Семикаленова, Анастасия И. 2019. «Цифровые следы: назначение и производство экспертиз». *Вестник Университета им. О. Е. Кутафина* 5 (57): 115–120.
Сергеев, Сергей М. 2017. «Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет». *Вестник Санкт-Петербургского университета МВД России* 1 (73): 137–140.
Смушкин, Александр Б. 2022. «Криминалистические аспекты исследования даркнета в целях расследования преступлений». *Актуальные проблемы российского права* 3 (17): 102–111.
Хлус, Александр М. 2018. «Средства совершения преступлений как элемент их криминалистической структуры». *Российское право: образование, практика, наука* 1 (103): 24–33.
Цимбал, Виталий Н. 2013. «Проблемы учета криминалистически значимой информации о способах хищений денежных средств из банкоматов». *Вестник Калининградского филиала Санкт-Петербургского университета МВД России* 4 (34): 85–88.
Шатохин, Сергей А. 2019. «Меры государственного противодействия распространению информации экстремистского характера в сети "Интернет" на примере блокировки интернет-мессенджера "Telegram"». *Ученые записки Крымского федерального университета им. В. И. Вернадского. Юридические науки* 3 (71): 210–216.
Шурухнов, Николай Г. 2013. «Современная преступность (истоки, направленность, техническая оснащенность, способы совершения, сокрытия): содержание рекомендаций по раскрытию и расследованию». *Известия Тульского государственного университета. Экономические и юридические науки* 4–2: 123–136.
Яблоков, Николай П. 2015. «Криминалистическая классификация преступлений в методике расследования и ее виды». *Вестник Московского университета. Серия 11. Право* 5: 40–51.
Ялышев, Станислав А., Николай В. Семенов. 2008. «Высокотехнологичные компьютерные изделия и некоторые проблемы их экспертного исследования». *Эксперт-криминалист* 2: 41–42.

Статья поступила в редакцию 11 сентября 2022 г.;
рекомендована к печати 19 января 2024 г.

Контактная информация:

Поляков Виталий Викторович — канд. юрид. наук; agupolyakov@gmail.com

Criminalistic classification of the means of high-tech crimes

V. V. Polyakov

Altai State University,
61, pr. Lenina, Barnaul, 656049, Russian Federation

For citation: Polyakov, Vitaly V. 2024. "Criminalistic classification of the means of high-tech crimes". *Vestnik of Saint Petersburg University. Law* 2: 435–453. https://doi.org/10.21638/spbu14.2024.208 (In Russian)

The formation of high-tech crime is largely based on the use of new means of committing crimes. This circumstance makes the task of constructing a practice-oriented classification of these tools important and relevant. The paper considers classifications for the means of high-tech crimes, based on various criteria. The general classification applicable to all groups of high-tech crimes is based on the following criteria: the content of the technical implementation of the funds, the legality of their origin, the contribution of criminals to the development and creation of the means, the elements of the crime method. According to the technical implementation, the means of high-tech crimes are divided into software, hardware and

software and hardware. According to the contribution of criminals to the creation, a division was made into ready-made funds modified for criminal purposes and specially designed new ones. Private classifications related to the group of software and hardware tools for committing high-tech crimes are proposed. Energy dependence, mobility and the presence of a network interface and the type of legal authority for the means of crime used were identified as additional practically significant classifying features. The developed classifications are designed to promote the use of more effective technical forensic and tactical forensic techniques in the investigation of high-tech crimes.

Keywords: means of crimes, method of crime, high-tech crimes, computer crimes, crime investigation, criminalistic characterization, concealment of crime.

References

Alieva, Giunai A., Anatolii M. Kustov. 2019. "Obtaining forensic information from the WhatsApp messenger as a source of evidentiary information". *Problemy polucheniia i ispol'zovaniia dokazatel'stvennoi i kriminalisticheski znachimoi informatsii: materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii*, 3–4. Simferopol, Arial Publ. (In Russian)

Belkin, Rafail S. 2001. *Course of criminology.* In 3 vols, vol. 3. Moscow, IuNITI-DANA Publ. (In Russian)

Bertovskii, Lev V. 2020. "To the question about the concept of cybercrime". *Rassledovanie prestuplenii: problemy i puti ikh resheniia* 4 (30): 84–88. (In Russian)

Bertovskii, Lev V., Bakitkul R. Sembekova. 2020. "High-tech crimes as a threat to national security". *Novelly material'nogo i protsessual'nogo prava: materialy Vserossiiskoi (natsional'noi) nauchno-prakticheskoi konferentsii*, 127–130. Krasnoyarsk, Krasnoiarskii gosudarstvennyi agrarnyi universitet Publ. (In Russian)

Bolshakov, Nikita A., Yuri V. Gavrilin. 2019. "Rented computer equipment and software as tools and means of committing crimes in the field of computer information". *E-Scio* 11 (38): 384–388. (In Russian)

Bychkov, Vasilii V. 2020. "Information and telecommunication networks as a means of committing extremist crimes". *Vestnik Akademii General'noi prokuratury Rossiiskoi Federatsii* 3 (25): 43–46. (In Russian)

Gavlo, Veniamin K. 1982. "On the question of the forensic characterization of crimes". *Bor'ba s prestupnost'iu na sovremennom etape: mezhvuzovskii sbornik*, 150–159. Barnaul, Altaiskii gosudarstvennyi universitet Publ. (In Russian)

Gavlo, Veniamin K. 2004. *General provisions of the criminal investigation methodology for certain types of crimes*. Eds Leonid Ia. Drapkin, Valerii N. Karagodin, 444–477. Moscow, Iuridicheskaia literatura Publ.; Elit Publ. (In Russian)

Iablokov, Nikolai P. 2015. "Forensic classification of crimes in the investigation method and its types". *Vestnik Moskovskogo universiteta. Seriia 11. Pravo* 5: 40–51. (In Russian)

Ialyshev, Stanislav A., Nikolai V. Semenov. 2008. "High-tech computer products and some problems of their expert research". *Ekspert-kriminalist* 2: 41–42. (In Russian)

Ishchenko, Evgenii P. 2017. "Forensic aspects of cybercrime investigation". *Ugolovnoe proizvodstvo: protsessual'naia teoriia i kriminalisticheskaia praktika: materialy V Mezhdunarodnoi nauchno-prakticheskoi konferentsii (27–29 aprelia 2017 g., g. Simferopol — Alushta)*, 62–65. Simferopol, Arial Publ. (In Russian)

Khlus, Aleksandr M. 2018. "Means of committing crimes as an element of their criminal structure". *Rossiiskoe pravo: obrazovanie, praktika, nauka* 1 (103): 24–33. (In Russian)

Kizdermishov, Askhad. A. 2015. "On the issue of CVE-compatible network scanners". *Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriia 4: Estestvenno-matematicheskie i tekhnicheskie nauki* 1 (154): 136–140. (In Russian)

Koldin, Valentin Ia. 2016. "Electronic information in law". *Vestnik Moskovskogo universiteta. Seriia 11. Pravo* 2: 96–110. (In Russian)

Meshcheriakov, Vladimir A. 2001. *Computer-related crime: Legal and forensic analysis.* Voronezh, Voronezhskii gosudarstvennyi universitet Publ. (In Russian)

Meshcheriakov, Vladimir A. 2013. "Traces of crimes in the high-tech sphere". *Biblioteka kriminalista. Nauchnyi zhurnal* 5 (10): 265–270. (In Russian)

Obrazhiev, Konstantin V. 2012. "System approach in jurisprudence: theoretical and methodological bases". *Vestnik Leningradskogo gosudarstvennogo universiteta imeni A. S. Pushkina* 1 (2): 89–96. (In Russian)
Osipenko, Anatolii L. 2009a. "Problems of involving electronic and digital footprints in criminal proceedings". *Nauchnyi vestnik Omskoi akademii Ministerstva vnutrennikh del Rossii* 4 (35): 31–34. (In Russian)
Osipenko, Anatolii L. 2009b. *Online computer crime: Theory and practice of struggle*. Omsk, Omskaia akademiia Ministerstva vnutrennikh del Rossii Publ. (In Russian)
Pasternak, Iurii G., Natal'ia N. Korneeva, Kseniia V. Degtiareva. 2014. "To the issue of modeling the process of implementing attacks through computer worms". *Informatsiia i bezopasnost'* 2 (17): 330–331. (In Russian)
Polyakov, Vitaly V., Stepan M. Slobodian. 2007. "Analysis of high-tech ways of inappropriate remote access to computer information". *Izvestiia Tomskogo politekhnicheskogo universiteta* 1 (310): 212–216. (In Russian)
Ponkin, Igor' V., Alena I. Lapteva. 2021. *Methodology of scientific research and applied analytics*. Moscow, Buki Vedi Publ. (In Russian)
Prudnikov, Iaroslav V. 2018. "Concept and ways of approaches of crime". *Problemi zakonnosti* 142: 189–199. (In Ukrainian)
Rossinskaia, Elena R., Igor' A. Riadovskii. 2019. "Modern methods of computer crimes and regularities of their implementation". *Lex russica* 3 (148): 87–99. (In Russian)
Semikalenova, Anastasiia I. 2019. "Digital footprints: purpose and production of expertise". *Vestnik Universiteta imeni O. E. Kutafina* 5 (57): 115–120. (In Russian)
Sergeev, Sergei M. 2017. "Some problems of counteracting the use of means of ensuring anonymization of the user in the Internet". *Vestnik Sankt-Peterburgskogo universiteta Ministerstva vnutrennikh del Rossii* 1 (73): 137–140. (In Russian)
Shatokhin, Sergei A. 2019. "Measures of state action against dissemination of extremist information in the network 'Internet' on the example of blocking the Internet messenger 'Teelegram'". *Uchenye zapiski Krymskogo federal'nogo universiteta imeni V. I. Vernadskogo. Iuridicheskie nauki* 3 (71): 210–216. (In Russian)
Shurukhnov, Nikolai G. 2013. "Modern crime (sources, direction, technical equipment, methods of commission, concealment): content of recommendations for disclosure and investigation". *Izvestiia Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i iuridicheskie nauki* 4–2: 123–136. (In Russian)
Smushkin, Aleksandr B. 2022. "Forensic aspects of darknet research for the purpose of crime investigation". *Aktual'nye problemy rossiiskogo prava* 3 (17): 102–111. (In Russian)
Tsimbal, Vitalii N. 2013. "Problems of accounting forensically significant information about methods of theft of money from ATMs". *Vestnik Kaliningradskogo filiala Sankt-Peterburgskogo universiteta Ministerstva vnutrennikh del Rossii* 4 (34): 85–88. (In Russian)
Vekhov, Vitalii B. 2009. "Concept and mechanism of formation of electronic-digital footprints". *Ispol'zovanie sovremennykh informatsionnykh tekhnologii i problemy informatsionnoi bezopasnosti v deiatel'nosti pravookhranitel'nykh organov: mezhvuzovskii tematicheskii sbornik nauchnykh trudov*, 62–72. Kaliningrad, Kaliningradskii Iuridicheskii institut Ministerstva vnutrennikh del Rossii Publ. (In Russian)
Zinkevich, Aleksei V., Maksim S. Mikhailov. 2018. "Information security audit". *Uchenye zametki Tikhookeanskogo gosudarstvennogo universiteta* 1 (9): 307–312. (In Russian)
Zuikov, Georgii G. 1971. "Forensic Doctrine on the Method of Committing Crime". *Sotsialisticheskaia zakonnost'* 11: 14–19. (In Russian)

Received: September 11, 2022
Accepted: January 19, 2024

Author's information:

Vitaly V. Polyakov — PhD in Law; agupolyakov@gmail.com