В. В. Поляков
Алтайский государственный университет
(Барнаул)

СТРУКТУРА И СОДЕРЖАНИЕ СПОСОБА СОВЕРШЕНИЯ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ

В статье рассмотрена криминалистическая группа высокотехнологичных преступлений, выделяемая на основе криминалистических критериев. Обосновывается, что важнейшим идентифицирующим признаком преступных деяний этой группы выступает способ их совершения. Он всегда является полноструктурным, при этом его элементы (подготовка к преступлению, непосредственное совершение и сокрытие следов) взаимообусловлены и не всегда могут быть разделены хронологически. Проведен анализ основных признаков и особенностей, характеризующих содержание отдельных элементов способа совершения преступления. Выявлены основные задачи, решаемые при подготовке к высокотехнологичным преступлениям. Отмечено, что такая подготовка может включать в себя действия, которые в уголовно-правовом смысле представляют собой совершение отдельного преступления, при этом в криминалистическом понимании они выступают первым элементом способа совершения преступления.

Описаны важнейшие черты элемента непосредственного совершения преступления. Классифицированы способы сокрытия рассматриваемых преступлений на основе критериев, включающих в себя содержание действий при сокрытии, период их осуществления и объект воздействия. Рассмотрены приемы и средства, используемые преступниками для воспрепятствования расследованию, в том числе при инсценировке преступления. Отмечена высокая динамика совершенствования приемов, входящих в способ совершения высокотехнологичных преступлений.

Ключевые слова: *способ совершения преступлений, средства совершения преступлений, подготовка преступлений, сокрытие преступлений, компьютерные преступления, высокотехнологичные преступления*

Для цитирования

Поляков В. В. Структура и содержание способа совершения высокотехнологичных преступлений // Российское право: образование, практика, наука. 2023. № 1. С. 27–39. DOI: 10.34076/2410_2709_2023_1_27.

УДК 343.98 DOI: 10.34076/2410_2709_2023_1_27

Введение

В информационной сфере за последние десятилетия произошли и продолжают происходить важные изменения, прежде всего за счет компьютеризации и цифровизации различных областей человеческой деятельности. Преступность также стала меняться за счет активного внедрения в криминальную деятельность компьютерных технологий [Шурухнов 2013: 134], в особенности в финансовой сфере [см., например: Карагодин 1998; Сомик, Хабибулин 2020].

Одним из наиболее ярких негативных последствий этих изменений стало формирование особой группы преступлений, связанных с организацией преступных групп, применяющих передовые информационные технологии, т. е. появление высокотехнологичных преступлений. Появление таких преступлений Л. В. Бертовский и Б. Р. Сембекова справедливо связывали именно с «технологической эволюцией преступности» [Бертовский, Сембекова 2020: 129]. Среди причин роста криминального использования высоких ин-

формационных технологий Ю. А. Воронин, И. М. Беляева и Т. В. Кухтина на первое место обоснованно выдвигают расширение возможностей организованных преступных сообществ [Воронин, Беляева, Кухтина 2021: 8].

Понятия «высокотехнологичные преступления» и «высокотехнологичная преступность» характеризуют сложное и многоплановое явление, которое может рассматриваться с различных правовых позиций. В основе исследований, проводимых с криминалистических позиций, лежит криминалистическая классификация, отражающая изучаемое явление на основе представлений науки криминалистики и позволяющая выделить криминалистическую группу высокотехнологичных преступлений по достаточно четким формальным основаниям [Образцов 1982].

Полагаем, что при любом выборе таких оснований остается справедливой глубокая мысль Р. С. Белкина: «Во всех случаях – без всяких исключений – сохраняет свое значение классификация по способу совершения преступления. Это основная криминалистическая классификация преступлений и, в сущности, определяющая среди всех других подобных классификаций» [Белкин 1997: 327]. Близкой позиции по доминирующей роли способа совершения преступления придерживались А. Н. Колесниченко [Колесниченко 1976: 8], В. К. Гавло [Гавло 1980: 121] и другие отечественные криминалисты. В. А. Мещеряков вывел способ совершения преступления на первый план среди оснований криминалистической классификации компьютерных преступлений [Мещеряков 2001: 27]. Роль способа совершения для компьютерных преступлений, рассматривавшихся в криминалистическом аспекте как специфическая криминалистическая группа преступных деяний, подчеркивалась в работах Е. Р. Россинской [Россинская 2016].

В настоящей работе высокотехнологичные преступления исследуются с криминалистических позиций. Это означает, что исходные понятия должны основываться на характерных криминалистических признаках и особенностях, отражающих изучаемое явление на основе представлений науки криминалистики. В соответствии с изложенным подходом к криминалистической классификации определим высокотехнологичные преступления как криминалистическую группу преступных деяний, объединяемых высокотехнологичным способом совершения преступлений и рядом других общих криминалистически значимых признаков и идентифицирующих особенностей [Гавло, Поляков 2007; Поляков 2019; Поляков 2022: 87 и др.].

К таким признакам могут быть отнесены наличие преступной группы, выступающей как единый групповой субъект преступления [Быков 1992: 7]; использование новых или модифицированных в преступных целях средств преступления [Ищенко 2017: 68; Поляков, Лапин 2014: 162]; применение для дистанционного доступа к объекту преступного посягательства информационно-телекоммуникационных сетей [Гавло, Поляков 2007; Осипенко 2010]; наличие противодействия расследованию. К особенностям высокотехнологичных преступлений можно отнести повышенную криминалистическую сложность расследования, понимаемую как «характеристику процесса расследования, отражающую реально необходимые силы, средства для установления истины, способы, объем и интенсивность их применения» [Зеленский 2011: 39]; «исключительно высокую латентность» [Поляков, Лапин 2014: 162]; многообъектность [Карабанова 2017: 137], т. е. посягательство одновременно на несколько видов общественных отношений.

Таким образом, основным идентифицирующим и системообразующим признаком высокотехнологичных преступлений является способ их совершения, общий для всех преступлений данной группы и являющийся важнейшим компонентом их криминалистической характеристики [Гавло, Поляков 2007: 146; Поляков, Слободян 2007].

В данной работе рассматриваются структура и содержание элементов способа совершения высокотехнологичных преступлений.

Структура способа совершения высокотехнологичных преступлений

В криминалистической литературе до сих пор не сформировалось единого общепринятого мнения о понятии способа совершения преступления, его структуре и содержании [см., например: Дудников 2012]. В связи с этим для исследования особенностей способов совершения высокотехнологичных преступлений необходимо сформулировать исходную позицию по данному вопросу. Полагаем, что за основу целесообразно взять

апробированное в криминалистических исследованиях определение, предложенное Г. Г. Зуйковым. Он понимал под способом совершения преступления «систему объединенных единым замыслом действий преступника (преступников) по подготовке, совершению и сокрытию преступления» [Зуйков 1970: 10; Зуйков 1987: 50]. Из этого определения следует важный вывод о структуре способа, включающей в себя три элемента: действия по подготовке преступления, по его непосредственному совершению и по его сокрытию, выступавшие, как отмечали Л. Я. Драпкин и М. С. Уткин, в качестве подсистем единой системы – способа совершения преступления [Драпкин, Уткин 1978: 132].

Важной особенностью взаимосвязи между элементами способа совершения преступления, характерной для высокотехнологичных преступных деяний, на наш взгляд, является то, что действия, совершаемые преступниками при подготовке, совершении и сокрытии, не всегда могут быть хронологически разделены. Так, действия по сокрытию высокотехнологичного преступления, как правило, начинаются уже при подготовке и далее продолжаются при непосредственном совершении преступного деяния. При анализе способов совершения компьютерных преступлений на это обратили внимание Е. Р. Россинская и И. А. Рядовский, отметившие, что «подготовка обычно предусматривает действия по сокрытию» [Россинская, Рядовский 2019: 96]. Другими словами, для высокотехнологичных преступлений четкие хронологические границы между действиями по подготовке, непосредственному совершению и сокрытию преступления имеют достаточно условный характер или могут оказаться в принципе не определимыми.

В криминалистической литературе при описании структурных составляющих способа совершения преступления используются разные термины, в том числе «стадия», «этап» и т. д. [см., например: Борин 2014]. Полагаем, что термины «стадия» и «этап» подразумевают хронологическую последовательность действий, каждое из которых имеет свои границы во времени. Однако наличие групп преступлений, в которых могут отсутствовать жесткие временные границы между этими действиями, ставит под сомнение корректность и точность в использовании данных терминов.

Для определения места, занимаемого высокотехнологичным способом среди различных способов совершения преступлений, воспользуемся классификацией, данной в работах М. С. Уткина [Драпкин, Уткин 1978: 133; Уткин 1975: 5]. Согласно этой классификации структура способа совершения преступлений может быть представлена четырьмя группами. В первую из них входят способы, содержащие один элемент и названные упрощенными. Способы второй и третьей групп содержат два элемента – подготовку и непосредственное совершение преступления или непосредственное совершение и сокрытие, эти способы названы усеченными. В четвертую группу входят способы, обладающие наиболее сложной структурой, включающей в себя все три элемента, такие способы были названы полноструктурными.

Для высокотехнологичных преступлений четкие хронологические границы между действиями по подготовке, непосредственному совершению и сокрытию преступления имеют достаточно условный характер

Проведенный нами анализ судебно-следственной практики приводит к важному выводу, что для высокотехнологичного способа характерно наличие наряду с действиями по непосредственному совершению преступления действий по его подготовке и сокрытию следов преступления и преступников. «С криминалистических позиций высокотехнологичный способ совершения компьютерных преступлений является полноструктурным, поскольку он включает стадии подготовки к преступлению, самого его совершения и действий по сокрытию следов» [Поляков 2012: 123].

Отметим, что значимость полноструктурности способа для близкой криминалистической группы компьютерных преступлений подчеркивалась в работе Е. Р. Россинской и И. А. Рядовского [Россинская, Рядовский 2019: 90]. В то же время значительная часть преступлений, связанных с применением информационных технологий, совершается способами, которые не являются полноструктурными. Так, Ю. В. Гаврилин показал, что преступления, посягающие на информационную безопасность в экономической сфере, со-

вершались полноструктурным способом в 34 % случаев [Гаврилин 2009: 32].

Рассмотрим криминалистически значимые особенности действий, составляющих содержание отдельных элементов способа совершения высокотехнологичных преступлений.

Подготовка к преступлению

Анализ судебно-следственной практики позволил выявить закономерности действий, осуществляемых преступниками после зарождения у них умысла на совершение высокотехнологичного преступления и до перехода к его непосредственному совершению.

Основные подготовительные действия направлены на решение следующих задач:

поиск потенциальных объектов преступлений с помощью различных приемов и средств, например путем целенаправленных атак, объектом которых являются конфиденциальные данные организаций;

разработка плана совершения преступления;

формирование преступной группы, вербовка ключевых соучастников, в первую очередь исполнителей со специальными техническими знаниями, умениями и навыками или лиц, без помощи которых совершение преступления становится трудным, например пособников-инсайдеров [Трунцевский 2014: 20]. Отметим, что в изученных нами уголовных делах инсайдеры фигурировали достаточно часто. Так, типичным являлось участие в преступных группах, занимавшихся мошенничеством с использованием платежных карт (ч. 4 ст. 159.3 УК РФ), кредитного эксперта операционного офиса коммерческого банка[1], главного специалиста отдела обслуживания банка[2] и т. п.;

приобретение, разработка или модификация (обычно в части адаптационных свойств) специальных программных, программно-аппаратных или аппаратных средств совершения преступления с необходимым функционалом [Поляков 2019] и их испытание;

применение средств совершения преступления в подготовительных целях, например путем установки на объект посягательства эксплойтов – программ, предназначенных для использования уязвимостей в программном обеспечении с целью получения данных об обстановке преступления [Поляков, Лапин 2014];

подготовка к сокрытию следов преступления и преступников, прежде всего путем использования разнообразных приемов анонимизации [Сергеев 2017].

Наибольшую опасность представляет собой тщательная подготовка высокотехнологичных преступлений организованными преступными группами, в том числе транснациональными. Для получения неправомерного дистанционного доступа к компьютерной информации ими создаются по сути дистанционные управляющие центры, разрабатываются комплексы средств преступления, объединяющих на основе новых технических решений в единое целое специализированные компьютерные устройства и вредоносные компьютерные программы [Поляков 2021: 83]. Характерным примером таких действий является тщательная подготовка так называемых APT-атак [Левцов, Демидов 2016], дистанционно осуществляемых преступными группами против компьютерных систем организаций.

Приведем достаточно типичные действия по подготовке высокотехнологичного преступления. Участниками организованной преступной группы, объединенной «целью совершения тяжких преступлений против собственности, а также преступлений в сфере компьютерной информации и в сфере экономической деятельности» (обвинение предъявлялось по ч. 4 ст. 158, ч. 3 ст. 272, ч. 3 ст. 183 УК РФ), для хищения денежных средств из банкоматов с помощью скимминговых устройств были произведены следующие подготовительные действия: приобретены техническое устройство «энкодер» и персональный компьютер со специализированным программным обеспечением, изготовлены микрокамеры для видеофиксации набираемых ПИН-кодов, приготовлены заготовки пластиковых карт, подысканы банкоматы, конструктивно подходящие для установки скиммеров, подобраны соучастники и между ними распределены обязанности и т. д.[3]

Непосредственное совершение преступления

Данный элемент структуры способа включает в себя действия по непосредственной реализации основного преступного умысла. Эти действия составляют объективную сторону

[1] Уголовное дело № 1-21/2015 // Архив Звениговского районного суда Республики Марий-Эл.

[2] Уголовное дело № 1-12/2016 // Архив Железнодорожного районного суда г. Хабаровска.

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

преступления и соответствуют тем или иным составам преступления, предусмотренным Уголовным кодексом РФ. В зависимости от цели, средств и иных обстоятельств избираются конкретные приемы непосредственного совершения преступления.

Важной общей чертой рассматриваемого элемента является использование для совершения преступлений специальных средств [Поляков, Лапин 2014]. В отличие от средств, обычно применяемых в преступлениях в сфере компьютерной информации, при совершении высокотехнологичных преступлений требуются более сложные технологические решения. Обычно разрабатываются новые или модифицируются имеющиеся программные, программно-аппаратные и аппаратные средства. Данное обстоятельство, на наш взгляд, требует от правоохранительных органов большего внимания к контролю за созданием и модификацией средств, которые могут найти применение при совершении высокотехнологичных преступлений. Полагаем, что деятельность в этой области, например создание, модификация и использование программ, относящихся к роду «пентест» (тестирование на проникновение), может подлежать лицензированию, а сами объекты – отдельной регистрации и учету (в том числе криминалистическому).

Другой важной чертой непосредственного совершения высокотехнологичных преступлений является использование информационных сетей для получения дистанционного доступа к предмету преступного посягательства [Осипенко 2010]. Приемы получения дистанционного доступа становятся все более изощренными. Например, преступники могут на кратковременной основе арендовать компьютерную технику с сетевым интерфейсом, используемую как «виртуальная машина», позволяющая дистанционно выполнять преступные задачи, в то время как находящаяся в распоряжении преступников компьютерная техника предоставляет лишь посреднический доступ. В результате таких действий электронно-цифровые следы, как правило, существуют недолго и быстро удаляются, в частности затираясь новой компьютерной информацией. В связи с этим установление причинно-следственных связей событий преступления и их доказывание вызывают особые криминалистические сложности.

Необходимо подчеркнуть такую опасную особенность рассматриваемых элементов способа совершения высокотехнологичных преступлений, как высокая динамика в развитии и совершенствовании средств и приемов, используемых преступниками. Например, технологии, связанные с использованием организованными преступными группами «программ-вымогателей», осуществляющих шифрование данных на компьютерах потерпевших для последующего выкупа за возвращение информации, усовершенствовались и стали значительно более опасными буквально в течение одного года с внедрением тактики прерывистого шифрования [Milenkoski, Walter 2022]. Показавшие свою эффективность программные средства затем продаются их разработчиками в сети *Darknet* по бизнес-модели *RaaS* (англ. *Ransomware as a Service* – «программа-вымогатель» как услуга)[1], которая, на наш взгляд, может рассматриваться как новая реализация концепции «преступность как услуга» [см., например: Jirovský, Pastorek, Mühlhäuser et. al. 2020].

Сокрытие преступления

В структуре способа совершения преступлений этот элемент является заключительным. Согласно определению Р. С. Белкина, «сокрытие преступления – деятельность (элемент преступной деятельности), направленная на воспрепятствование расследованию путем утаивания, уничтожения, маскировки или фальсификации следов преступления и преступника и их носителей» [Белкин 1997: 364]. При совершении высокотехнологичных преступлений всегда предпринимаются действия по сокрытию следов преступления, отдельных преступников и места их нахождения.

Приведем примеры наиболее распространенных приемов и средств, используемых при сокрытии и существенно затрудняющих расследование. Для повышения анонимности преступники используют технологию TOR, VPN-сервисы, особые прокси-серверы, *dedicated*-серверы, SSH-туннели; анонимные сети, «виртуальные машины» («гипервизоры») и иные анонимайзеры [Поляков, Лапин 2014; Сергеев 2017: 138]. При совершении преступлений широко применяются подменные сетевые IP-адреса, относящиеся к дру-

[1] *Безмалый В.* Что такое программа-вымогатель как услуга (RaaS)? 2021 // URL: https://ib-bank.ru/bisjournal/news/15767 (дата обращения: 11.11.2022).

гим странам или регионам, или же преступники реально меняют место жительства, переезжая в страны, из которых их депортация маловероятна. Практически всегда используется такое широко распространенное и простое средство, как онлайн-мессенджеры, как правило, мессенджеры, обеспечивающие высокую анонимизацию пользователей (например, *Telegram*) практически не позволяющие правоохранительным органам получать информацию о передаваемых сообщениях [см., например: Смушкин 2022]. За счет использования системы анонимизации, меняющихся прокси-серверов, подменяющих IP-адреса устройств и иных аналогичных технологий в значительной степени нивелируется возможность получения правоохранительными органами криминалистически и оперативно значимой информации [Россинская, Рядовский 2019].

Руководители и организаторы преступных групп стремятся действовать максимально скрытно, используя специальные информационно-телекоммуникационные каналы связи, тщательно скрывая следы своих действий, чтобы затруднить получение доказательств их вины и соучастия в преступлении. Выявление и изобличение низовых звеньев группы не представляет особой угрозы для руководителей, поскольку рядовым соучастниками обычно неизвестны детали преступлений и руководящий состав группы.

Так, остался неустановленным организатор преступной группы, занимавшейся распространением вредоносного программного обеспечения. Он был известен рядовым соучастникам только под сетевым именем и, согласно материалам уголовного дела, использовал «программно-технические средства и прокси-серверы, расположенные на территории иностранных государств, скрывающих реальный IP-адрес его компьютера, по которому можно определить его точное местонахождение»[1].

В транснациональной преступной группе, специализировавшейся на мошенничестве в сфере компьютерной информации (обвинение по ч. 4 ст. 159.6, ч. 3 ст. 272, ч. 2 ст. 273 УК РФ), неустановленный организатор внедрил меры конспирации, в соответствии с которыми взаимодействие между участниками осуществлялось только «с использованием сменяемых под каждое преступление мобильных телефонов с сим-картами, оформленными на посторонних лиц, программных средств обмена сообщениями... обеспечивающих анонимность и затрудняющих идентификацию пользователей»[2].

Во многих случаях остаются неустановленными организаторы преступных групп, занимающихся бесконтактным сбытом наркотических средств с использованием информационных сетей; эти лица поддерживают связь с установщиками «закладок» через аккаунты[3].

Классификация действий при сокрытии высокотехнологичных преступлений

Проведенный анализ показывает, что сокрытие выступает важным элементом способа совершения высокотехнологичных преступлений, имеет сложную многокомпонентную структуру, образуемую совокупностью различных приемов. Для их описания должны привлекаться классификации, проводимые на основе выбора тех или иных признаков.

Классификация по содержанию действий

Наиболее распространенной в криминалистической теории является предложенная Р. С. Белкиным классификация, исходящая из содержания действий по сокрытию преступления и включающая в себя следующие четыре группы таких действий: утаивание, уничтожение, маскировку и фальсификацию криминалистически значимой информации или ее носителей [Белкин 1997: 366]. При сокрытии высокотехнологичных преступлений могут использоваться приемы, относящиеся ко всем указанным группам, из них наиболее часто привлекаются следующие:

маскировка совершения преступления путем шифрования данных, процессов, трафика на компьютерных средствах совершения преступления, предмете посягательства, посреднической компьютерной технике, участвующей в предоставлении дистанционного доступа;

уничтожение (удаление с материального носителя) компьютерной информации, содержащей электронно-цифровые следы преступления.

[1] Приговор Железнодорожного районного суда г. Екатеринбурга от 13 октября 2015 г. по делу № 1-435/2015.

[2] Приговор Якутского городского суда Республики Саха (Якутия) от 26 августа 2019 г. № 1-681/2019 по делу № 1-1462/2018.

[3] См., например: Уголовное дело № 1-454-2017 // Архив Центрального районного суда г. Кемерово.

Менее часто используется такой сложный в доказывании прием маскировки, как инсценировка [Косынкин 2011], в том числе в виде «подброса» невиновным лицам инсценированных следов преступления [Поляков 2019: 120]. В отдельных случаях встречается фальсификация электронных доказательств, которая всегда сопровождается фальсификацией данных в бумажных документах [Сафронов, Поляков 2019]. Полагаем также, что следует учитывать рост числа случаев создания «цифрового алиби» из инсценированных электронно-цифровых следов, когда представляются электронно-цифровые данные, указывающие на непричастность лица к инкриминируемому преступлению в связи с нахождением его в ином месте, выполнением несовместимых с преступлением действий или отсутствием технической или субъективной возможности совершения преступления. Разоблачение такого «цифрового алиби» является сложной и нетипичной задачей. Она может быть решена в рамках тактической операции, которая, на наш взгляд, может именоваться «разоблачением цифрового алиби».

По нашему мнению, представляют определенный теоретический и практический интерес также иные классификации, исходящие из других классифицирующих признаков. Полагаем, что могут быть предложены следующие классификации действий по сокрытию высокотехнологичных преступлений.

Классификация по объекту воздействия

При использовании указанного основания могут быть выделены следующие группы действий:

сокрытие «следов-последствий», указывающих на преступное деяние;

сокрытие следов преступников, которые их персонифицируют и доказывают соучастие в преступлении;

сокрытие самих преступников, прежде всего мест их нахождения.

Классификация по периоду времени

Действия по сокрытию высокотехнологичного преступления могут проводиться в разное время и охватывать следующие периоды:

период подготовки к преступлению;

период непосредственного совершения преступления;

период после совершения преступления.

Эта классификация позволяет выявить такую высокоэффективную форму сокрытия, как ранняя подготовка к нему. При ранней подготовке преступники могут использовать технологии, обеспечивающие возможность сокрытия неправомерного удаленного доступа, осуществляемого на долговременной основе. Для этого создаются, модифицируются или приобретаются специализированные программные средства, позволяющие скрытно управлять автоматизированным рабочим местом объекта посягательства. Примером таких средств являются вредоносные программы, работающие на основе обеспечивающих удаленный доступ к компьютеру сетевых протоколов RDP (*Remote Desktop Protocol*) или VNC (*Virtual Network Computing*) и работающие в скрытом режиме.

Отметим, что в связи с быстрым развитием высокотехнологичной преступности приведенные классификации не являются исчерпывающими, они могут дополняться при расширении судебно-следственной практики.

Заключение

Способ совершения преступления выступает одним из важнейших компонентов криминалистической характеристики преступлений, входящих в определенную криминалистическую группу. В силу этого знание закономерностей, характеризующих способ совершения преступлений, имеет первостепенное значение для криминалистической теории.

Проведенное в настоящей работе исследование показало, что способ совершения высокотехнологичных преступлений всегда является полноструктурным, при этом все элементы его структуры взаимосвязаны вплоть до того, что фактически могут быть неотделимыми друг от друга. Реализация высокотехнологичного способа обычно занимает достаточно продолжительное время, начинаясь с приготовления к преступлению и заканчиваясь сокрытием следов и преступников. В связи с этим элементы способа совершения высокотехнологичных преступлений целесообразно выделять не по периодам их осуществления, а по содержанию решаемых преступниками задач, целям и специфике совершаемых действий, т. е. по содержанию элементов. Подготовка к высокотехнологичному преступлению часто включает в себя такие задачи, решение которых в уголовно-правовом смысле представляет собой совершение отдельного преступления, при этом в криминалистическом понимании эти действия составляют лишь первый элемент

способа совершения всего высокотехнологичного преступления.

Исследование названного способа и его элементов имеет не только теоретическое, но и практическое значение, поскольку индивидуализирует характерные средства и приемы преступной деятельности, позволяет обоснованно выдвигать версии о причинно-следственных и корреляционных связях с другими элементами криминалистической характеристики данных преступлений. Полученные результаты позволяют более эффективно адаптировать к высокотехнологичным преступлениям комплекс узконаправленных криминалистических тактических приемов и рекомендаций, что в итоге способствует формированию методики расследования указанных преступлений.

Список литературы

Jirovský V., Pastorek A., Mühlhäuser M. et al. Cybercrime and Organized Crime // Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). 2018. N. Y.: Association for Computing Machinery Publ., 2020. № 61. P. 1–5.

Milenkoski A., Walter J. Crimeware Trends. Ransomware Developers Turn to Intermittent Encryption to Evade Detection. 2022 // URL: https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection (дата обращения: 11.11.2022).

Белкин Р. С. Курс криминалистики: Криминалистические средства, приемы и рекомендации. М.: Юристъ, 1997. 480 с.

Бертовский Л. В., Сембекова Б. Р. Высокотехнологичные преступления как угроза национальной безопасности // Новеллы материального и процессуального права: материалы Всерос. (нац.) науч.-практ. конф. (май-октябрь 2020 г., г. Красноярск). Красноярск: Краснояр. гос. аграр. ун-т, 2020. С. 127–130.

Борин Б. В. Способ совершения преступлений экономической направленности в теории оперативно-розыскной деятельности // Бизнес в законе. 2014. № 1. С. 162–164.

Быков В. М. Проблемы расследования групповых преступлений: автореф. дис. ... д-ра юрид. наук. М., 1992. 29 с.

Воронин Ю. А., Беляева И. М., Кухтина Т. В. Современные тенденции преступности в цифровой среде // Вестник Южно-Уральского государственного университета. Сер. Право. 2021. Т. 21. № 1. С. 7–12.

Гавло В. К. К вопросу о криминалистической характеристике преступлений // Вопросы повышения эффективности борьбы с преступностью. Томск: Изд-во Томск. ун-та, 1980. С. 118–123.

Гавло В. К., Поляков В. В. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Российский юридический журнал. 2007. № 5. С. 146–152.

Гаврилин Ю. В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: автореф. дис. ... д-ра юрид. наук. М., 2009. 57 с.

Драпкин Л. Я., Уткин М. С. Понятие и структура способа совершения преступления // Проблемы борьбы с преступностью: сб. науч. тр. Омск: Изд-во Омск. ВШМ МВД СССР, 1978. С. 129–134.

Дудников А. Л. Криминалистическое понятие «способ преступления» // Проблемы законности. 2012. № 120. С. 232–242.

Зеленский В. Д. Теоретические вопросы организации расследования преступлений: моногр. Краснодар: КубГАУ, 2011. 156 с.

Зуйков Г. Г. Криминалистическое учение о способе совершения преступления: автореф. дис. ... д-ра юрид. наук. М., 1970. 31 с.

Зуйков Г. Г. Основы криминалистического учения о способе совершения и сокрытия преступления // Криминалистика / под ред. Р. С. Белкина, В. П. Лаврова, И. М. Лузгина. М.: Акад. МВД СССР, 1987. Т. 1. С. 41–57.

Ищенко Е. П. Криминалистические аспекты расследования киберпреступлений // Уголовное производство: процессуальная теория и криминалистическая практика: материалы V Междунар. науч.-практ. конф. 27–29 апреля 2017 г. Симферополь-Алушта: Крымский федеральный университет им. В. И. Вернадского. Симферополь: ИТ «АРИАЛ», 2017. С. 62–64.

Карабанова Е. Н. Социально-правовая природа многообъектных преступлений // Журнал российского права. 2017. № 1. С. 130–138.

Карагодин В. Н. Организованная преступность в банковской деятельности // Организованная преступная деятельность в финансовой, банковской и налоговой сферах экономической деятельности: круглый стол в УрГЮА 23 января 1998 г. Екатеринбург: Изд-во УрГЮА, 1998. С. 43–44.

Колесниченко А. Н. Общие положения методики расследования отдельных видов преступлений: текст лекций. Харьков: Харьков. юрид. ин-т, 1976. 29 с.

Косынкин А. А. Инсценировка как форма противодействия расследованию преступлений в сфере компьютерной информации // Вестник Челябинского государственного университета. «Право». 2011. № 29. С. 78–80.

Левцов В., Демидов Н. Анатомия таргетированной атаки. Часть 1. 2016 // URL: http://sa-mag.ru/archive/article/3170 (дата обращения: 11.11.2022).

Мещеряков В. А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронеж. гос. ун-т, 2001. 176 с.

Образцов В. А. Объекты криминалистической методики расследования преступлений // Алгоритмы и организация решений следственных задач: сб. науч. тр. Иркутск: Изд-во Иркут. ун-та, 1982. С. 9–25.

Осипенко А. Л. Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал. 2010. № 2. С. 121–126.

Поляков В. В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений // Lex Russica. 2022. Т. 75. № 6. С. 85–96.

Поляков В. В. О высокотехнологичных способах совершения преступлений в сфере компьютерной информации // Уголовно-процессуальные и криминалистические чтения на Алтае. Вып. XI–XII: сб. материалов Всерос. науч.-практ. конф. Барнаул: Изд-во Алт. ун-та, 2012. С. 123–126.

Поляков В. В. Основы формирования криминалистической методики расследования высокотехнологичных преступлений // Уголовное судопроизводство: правовое, криминалистическое и оперативно-розыскное обеспечение / под ред. С. И. Давыдова. Барнаул: Изд-во Алт. ун-та, 2019. С. 114–126.

Поляков В. В. Понятие средств совершения высокотехнологичных преступлений // Уголовно-процессуальные и криминалистические чтения на Алтае. Вып. XVII: сб. науч. ст. XIX Междунар. науч.-практ. конф. / отв. ред. С. И. Давыдов, В. В. Поляков. Барнаул: Изд-во Алт. ун-та, 2021. С. 76–86.

Поляков В. В., Лапин С. А. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2. С. 162–166.

Поляков В. В., Слободян С. М. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. 2007. Т. 310. № 1. С. 212–216.

Россинская Е. Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия ТулГУ. Экономические и юридические науки. 2016. № 3–2. С. 109–117.

Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3. С. 87–99.

Сафронов А. Ю., Поляков В. В. Проблемы юридического и лингвистического определения фальсификации доказательств в уголовном судопроизводстве // Юрислингвистика. 2019. № 12. С. 13–17.

Сергеев С. М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник Санкт-Петербургского университета МВД России. 2017. № 1. С. 137–140.

Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. Т. 17. № 3. С. 102–111.

Сомик К. В., Хабибулин А. Г. Обнаружение и документирование цифровых следов высокотехнологичных финансовых преступлений: вопросы теории и практики // Теория государства и права. 2020. № 2. С. 212–218.

Трунцевский Ю. В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения // Российский следователь. 2014. № 21. С. 19–21.

Уткин М. С. Особенности расследования и предупреждения хищений в потребительской кооперации: автореф. дис. ... канд. юрид. наук. Свердловск, 1975. 22 с.

Шурухнов Н. Г. Современная преступность (истоки, направленность, техническая оснащенность, способы совершения, сокрытия): содержание рекомендаций по раскрытию и расследованию // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4–2. С. 123–136.

Виталий Викторович Поляков – кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета. 656049, Российская Федерация, Барнаул, пр. Ленина, д. 61. E-mail: agupolyakov@gmail.com.

ORCID: 0000-0002-6774-8414

Structure and Content of the High-Tech Crime Method

The article considers the criminalistic group of high-tech crimes, which is distinguished on the basis of criminalistic criteria. It is proved that the most important identifying feature of these criminal acts is the method of crime. It is always fully structured, while its elements (preparation for a crime, its commission and concealment of traces) are mutually dependent and cannot always be separated chronologically. The analysis of the main features characterizing the content of individual elements of the method of crime is carried out. The main tasks solved in preparation for high-tech crimes are identified.

The most important features of the element of committing a crime are described. The classification of the concealment of the crimes under consideration was carried out on the basis of criteria that included the content of the concealment actions, the period of their implementation, and the object of influence. The techniques and means used by criminals to obstruct the investigation, including when staging a crime, are considered. The high dynamics of improving the techniques included in the method of high-tech crimes is noted.

Keywords: *method of crimes, means of crimes, preparation of crimes, concealment of crimes, computer crimes, high-tech crimes*

Recommended citation

Polyakov V. V. Struktura i soderzhanie sposoba sovershenia vysokotekhnologichnykh prestuplenii [Structure and Content of the High-Tech Crime Method], *Rossiiskoe pravo: obrazovanie, praktika, nauka*, 2023, no. 1, pp. 27–39, DOI: 10.34076/2410_2709_2023_1_27.

References

Belkin R. S. *Kurs kriminalistiki: Kriminalisticheskie sredstva, priemy i rekomendatsii* [Forensic Course: Forensic Tools, Techniques and Recommendations], Moscow, Yurist, 1997, vol. 3, 480 p.

Bertovskii L. V., Sembekova B. R. *Vysokotekhnologichnye prestupleniya kak ugroza natsional'noi bezopasnosti* [High-Tech Crimes as a Threat to National Security], *Novelly material'nogo i protsessual'nogo prava* [Novels of Substantive and Procedural Law]: conference papers, Krasnoyarsk, Krasnoyar. gos. agrar. un-t, 2020, pp. 127–130.

Borin B. V. Sposob soversheniya prestuplenii ekonomicheskoi napravlennosti v teorii operativno-rozysknoi deyatel'nosti [The Method of Committing Economic Crimes in the Theory of Operational-Search Activity], *Biznes v zakone*, 2014, no. 1, pp. 162–164.

Bykov V. M. *Problemy rassledovaniya gruppovykh prestuplenii* [Problems of Investigation of Group Crimes]: autoabstr. of cand. jur. sc. thesis, Moscow, 1992, 29 p.

Drapkin L. Ya., Utkin M. S. *Ponyatie i struktura sposoba sovershеniya prestupleniya* [The Concept and Structure of the Method of Committing Crime], *Problemy bor'by s prestupnost'yu* [Problems in the Fight Against Crime], Omsk, Izd-vo Omsk. VShM MVD SSSR, 1978, pp. 129–134.

Dudnikov A. L. Kriminalisticheskoe ponyatie «sposob prestupleniya» [Forensic Concept «Method of Crime»], *Problemy zakonnosti*, 2012, no. 120, pp. 232–242.

Gavlo V. K. K voprosu o kriminalisticheskoi kharakteristike prestuplenii [To the Question of the Forensic Characterization of Crimes], *Voprosy povysheniya effektivnosti bor'by s prestupnost'yu* [Issues of Increasing the Effectiveness of the Fight Against Crime], Tomsk, Izd-vo Tomsk. un-ta, 1980, pp. 118–123.

Gavlo V. K., Polyakov V. V. Sledovaya kartina i ee znachenie dlya rassledovaniya prestuplenii, svyazannykh s nepravomernym udalennym dostupom k komp'yuternoi informatsii [The Trace Picture and Its Significance for the Investigation of Crimes Related to Illegal Remote Access to Computer Information], *Rossiiskii yuridicheskii zhurnal*, 2007, no. 57, pp. 146–152.

Gavrilin Yu. V. *Rassledovanie prestuplenii, posyagayushchikh na informatsionnuyu bezopasnost' v ekonomicheskoi sfere: teoreticheskie, organizatsionno-takticheskie i metodicheskie osnovy* [Investigation of Crimes Encroaching on Information Security in the Economic Sphere: Theoretical, Organizational, Tactical and Methodological Foundations]: autoabstr. of doct. jur. sc. thesis, Moscow, 2009, 57 p.

Ishchenko E. P. *Kriminalisticheskie aspekty rassledovaniya kiberprestuplenii* [Forensic Aspects of Cybercrime Investigation], *Ugolovnoe proizvodstvo: protsessual'naya teoriya i kriminalisticheskaya praktika* [Criminal Proceedings: Procedural Theory and Forensic Practice]: conference papers, Simferopol', IT ARIAL, 2017, pp. 62–64.

Jirovský V., Pastorek A., Mühlhäuser M. et al. *Cybercrime and Organized Crime, Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018):* conference papers, New York, Association for Computing Machinery Publ., 2018, no. 61, pp. 1–5.

Karabanova E. N. Sotsial'no-pravovaya priroda mnogoob"ektnykh prestuplenii [Socio-Legal Nature of Multi-Objective Crimes], *Zhurnal rossiiskogo prava*, 2017, no. 1, pp. 130–138.

Karagodin V. N. *Organizovannaya prestupnost' v bankovskoi deyatel'nosti* [Organized Crime in Banking], *Organizovannaya prestupnaya deyatel'nost' v finansovoi, bankovskoi i nalogovoi sferakh ekonomicheskoi deyatel'nosti* [Organized Crime in Financial, Banking and Tax Significant Economic Activities], Ekaterinburg, Izd-vo UrGYuA, 1998, pp. 43–44.

Kolesnichenko A. N. *Obshchie polozheniya metodiki rassledovaniya otdel'nykh vidov prestuplenii* [General Provisions of the Methodology for Investigating Certain Types of Crimes], Khar'kov, Khar'kov. yurid. in-t, 1976, 29 p.

Kosynkin A. A. Instsenirovka kak forma protivodeistviya rassledovaniyu prestuplenii v sfere komp'yuternoi informatsii [Dramatization as a Form of Counteraction to the Investigation of Crimes in the Field of Computer Information], *Vestnik Chelyabinskogo gosudarstvennogo universiteta. Pravo*, 2011, no. 29, pp. 78–80.

Levtsov V., Demidov N. *Anatomiya targetirovannoi ataki. Chast' 1* [Anatomy of a Targeted Attack. Part 1], 2016, available at: http://samag.ru/archive/article/3170 (accessed: 11.11.2022).

Meshcheryakov V. A. *Prestupleniya v sfere komp'yuternoi informatsii: pravovoi i kriminalisticheskii analiz* [Crimes in the Field of Computer Information: Legal and Forensic Analysis], Voronezh, Voronezh. gos. un-t, 2001, 176 p.

Milenkoski A., Walter J. *Crimeware Trends. Ransomware Developers Turn to Intermittent Encryption to Evade Detection*, 2022, available at: https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection (accessed: 11.11.2022).

Obraztsov V. A. *Ob"ekty kriminalisticheskoi metodiki rassledovaniya prestuplenii* [Objects of Forensic Methodology for Investigating Crimes], *Algoritmy i organizatsiya reshenii sledstvennykh zadach* [Algorithms and Organization of Solutions to Investigative Tasks]: conference papers, Irkutsk, Izd-vo Irkut. un-ta, 1982, pp. 9–25.

Osipenko A. L. Osobennosti rassledovaniya setevykh komp'yuternykh prestuplenii [Features of the Investigation of Network Computer Crimes], *Rossiiskii yuridicheskii zhurnal*, 2010, no. 2, pp. 121–126.

Polyakov V. V. Istochniki i printsipy formirovaniya chastnoi metodiki rassledovaniya vysokotekhnologichnykh prestuplenii [Sources and Principles of Formation of a Private Methodology for Investigating High-Tech Crimes], *Lex Russica*, 2022, vol. 75, no. 6, pp. 85–96.

Polyakov V. V. O *vysokotekhnologichnykh sposobakh sovershenia prestuplenii v sfere komp'yuternoi informatsii* [On High-Tech Methods of Committing Crimes in the Field of Computer Information], *Ugolovno-protsessual'nye i kriminalisticheskie chteniya na Altae. Vyp. XI–XII* [Criminal Procedure and Forensic Readings in Altai. Issue XI–XII]: conference papers, Barnaul, Izd-vo Alt. un-ta, 2012, pp. 123–126.

Polyakov V. V. *Osnovy formirovaniya kriminalisticheskoi metodiki rassledovaniya vysokotekhnologichnykh prestuplenii* [Fundamentals of the Formation of a Forensic Methodology for Investigating the Most Serious Crimes], Davydov S. I. (ed.) *Ugolovnoe sudoproizvodstvo: pravovoe, kriminalisticheskoe i operativno-rozysknoe obespechenie* [Criminal Proceedings: Legal, Forensic and Operational-Search Support], Barnaul, Izd-vo Alt. un-ta, 2019, pp. 114–126.

Polyakov V. V. Ponyatie sredstv sovershenia vysokotekhnologichnykh prestuplenii [The Concept of Means of Committing High-Tech Crimes], Davydov S. I., Polyakov V. V. (eds.) *Problemy bor'by s prestupnost'yu v usloviyakh tsifrovizatsii* [Problems of Combating Crime in the Context of Digitalization]: conference papers, Barnaul, Izd-vo Alt. un-ta, 2021, pp. 76–86.

Polyakov V. V., Lapin S. A. Sredstva sovershenia komp'yuternykh prestuplenii [Means of Committing Computer Crimes], *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2014, vol. 32, no. 2, pp. 162–166.

Polyakov V. V., Slobodyan S. M. Analiz vysokotekhnologichnykh sposobov nepravomernogo udalennogo dostupa k komp'yuternoi informatsii [Analysis of High-Tech Methods of Illegal Remote Access to Computer Information], *Izvestiya Tomskogo politekhnicheskogo universiteta*, 2007, vol. 310, no. 1, pp. 212–216.

Rossinskaya E. R. K voprosu o chastnoi teorii informatsionno-komp'yuternogo obespecheniya kriminalisticheskoi deyatel'nosti [To the Question of a Private Theory of Information and Computer Support for Criminalistic Activity], *Izvestiya TulGU. Ekonomicheskie i yuridicheskie nauki*, 2016, no. 3–2, pp. 109–117.

Rossinskaya E. R., Ryadovskii I. A. Sovremennye sposoby komp'yuternykh prestuplenii i zakonomernosti ikh realizatsii [Modern Methods of Computer Crimes and Patterns of Their Implementation], *Lex Russica*, 2019, no. 3, pp. 87–99.

Safronov A. Yu., Polyakov V. V. Problemy yuridicheskogo i lingvisticheskogo opredeleniya fal'sifikatsii dokazatel'stv v ugolovnom sudoproizvodstve [Problems of Legal and Linguistic Definition of Falsification of Evidence in Criminal Proceedings], *Yurislingvistika*, 2019, no. 12, pp. 13–17.

Sergeev S. M. Nekotorye problemy protivodeistviya ispol'zovaniyu v prestupnoi deyatel'nosti sredstv obespecheniya anonimizatsii pol'zovatelya v seti Internet [Some Problems of Countering the Use in Criminal Activities of Means to Ensure the Anonymization of the User on the Internet], *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii*, 2017, vol. 73, no. 1, pp. 137–140.

Shurukhnov N. G. Sovremennaya prestupnost' (istoki, napravlennost', tekhnicheskaya osnashchennost', sposoby sovershenia, sokrytiya): soderzhanie rekomendatsii po raskrytiyu i rassledovaniyu [Modern Crime (Origins, Orientation, Technical Equipment, Methods of Commission, Concealment): Content of Recommendations for Disclosure and Investigation], *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki*, 2013, no. 4–2, pp. 123–136.

Smushkin A. B. Kriminalisticheskie aspekty issledovaniya darkneta v tselyakh rassledovaniya prestuplenii [Forensic Aspects of the Study of the Darknet in Order to Investigate Crimes], *Aktual'nye problemy rossiiskogo prava*, 2022, vol. 17, no. 3, pp. 102–111.

Somik K. V., Khabibulin A. G. Obnaruzhenie i dokumentirovanie tsifrovykh sledov vysokotekhnologichnykh finansovykh prestuplenii: voprosy teorii i praktiki [Detection and Documentation of Digital Traces of High-Tech Financial Crimes: Issues of Theory and Practice], *Teoriya gosudarstva i prava,* 2020, no. 2, pp. 212–218.

Truntsevskii Yu. V. Kiberprestupleniya v korporativnoi srede: riski, otsenka i mery preduprezhdeniya [Cybercrime in the Corporate Environment: Risks, Assessment and Prevention Measures], *Rossiiskii sledovatel'*, 2014, no. 21, pp. 19–21.

Utkin M. S. *Osobennosti rassledovaniya i preduprezhdeniya khishchenii v potrebitel'skoi kooperatsii* [Features of the Investigation and Prevention of Theft in Consumer Cooperation]: autoabstr. of cand. jur. sc. thesis, Sverdlovsk, 1975, 22 p.

Voronin Yu. A., Belyaeva I. M., Kukhtina T. V. Sovremennye tendentsii prestupnosti v tsifrovoi srede [Modern Crime Trends in the Digital Environment], *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Ser. Pravo,* 2021, vol. 21, no. 1, pp. 7–12.

Zelenskii V. D. *Teoreticheskie voprosy organizatsii rassledovaniya prestuplenii* [Theoretical Issues of Organizing the Investigation of Crimes], Krasnodar, KubGAU, 2011, 156 p.

Zuikov G. G. *Kriminalisticheskoe uchenie o sposobe sovershenia prestupleniya* [Forensic Doctrine About the Method of Committing Crime]: autoabstr. of doct. jur. sc. thesis, Moscow, 1970, 31 p.

Zuikov G. G. *Osnovy kriminalisticheskogo ucheniya o sposobe sovershenia i sokrytiya prestupleniya* [Fundamentals of Forensic Doctrine on the Method of Committing and Concealing a Crime], Belkin R. S., Lavrov V. P., Luzgin I. M. (eds.) *Kriminalistika* [Criminalistics], Moscow, Akad. MVD SSSR, 1987, vol. 1, pp. 41–57.

Vitaly Polyakov – candidate of juridical sciences, associate professor of the Department of criminal procedure and criminalistics, Altai State University. 656049, Russian Federation, Barnaul, Lenina ave., 61. E-mail: agupolyakov@gmail.com.

ORCID: 0000-0002-6774-8414

Дата поступления в редакцию / Received: 03.12.2022

Дата принятия решения об опубликовании / Accepted: 23.01.2023