ТАКТИКА ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ, НАПРАВЛЕННЫХ НА ПОЛУЧЕНИЕ ЦИФРОВОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Атакулов Бекзод Абдухалил угли
независимый соискатель кафедры Уголовного процессуального права Ташкентского государственного юридического университета
bekatakuloff@gmail.com
ORCID: 0009-0005-3621-4208

Аннотация: *В настоящей научной статье автор раскрыл особенности реализации тактики проведения следственных действий, направленных на получение цифровой информации в ходе расследования киберпреступлений. Учитывая практическую сложность расследования данной группы преступлений, именно данные следственные действия, на взгляд автора, являются актуальными и ориентирующими на производство других следственных действий по уголовному делу. Благодаря проведенному исследованию автор последовательно приходит к выводу, что механизм и тактику проведения данных первоначальных следственных действий необходимо систематизировать, а также обеспечивать подготовку начинающего персонала следователей и специалистов органов внутренних дел на основе научно построенных гипотез-материалов данной тактики.*

Ключевые слова: *Киберпреступления, цифровая информация, оперативная информация, расследование, обыск, осмотр, место происшествия, компьютерные сети, протокол.*

KIBERJINOYATLARNI TERGOV QILISHDA RAQAMLI MA’LUMOTLARNI OLISHGA QARATILGAN TERGOV XARAKATLARINI O‘TKAZISH TAKTIKASI

Atakulov Bekzod Abduhalil o‘g‘li
Toshkent davlat yuridik universiteti
Jinoyat protsessual huquqi kafedrasi
mustaqil izlanuvchisi
bekatakuloff@gmail.com
ORCID: 0009-0005-3621-4208

Annotatsiya: *Ushbu ilmiy maqolada muallif kiber jinoyatlarni tergov qilish jarayonida raqamli ma'lumot olishga qaratilgan tergov harakatlarining taktikasini amalga oshirish xususiyatlarini ochib berdi. Ushbu jinoyatlar guruhini tergov qilishning amaliy*

murakkabligini hisobga olgan holda, bu tergov harakatlari, muallifning fikriga ko'ra, tegishli va jinoyat ishida boshqa tergov harakatlarini ishlab chiqarishga qaratilgan. Tadqiqot tufayli muallif ketma-ket ushbu dastlabki tergov harakatlarining mexanizmi va taktikasini tizimlashtirish, shuningdek, tergovchilar va ichki ishlar organlari mutaxassislarining boshlang'ich xodimlarini ilmiy asoslangan gipotezalar-ushbu taktika materiallari asosida tayyorlashni ta'minlash kerak degan xulosaga keladi.

Kalit so'zlar: *Kiber jinoyatlar, raqamli ma'lumotlar, operatsion ma'lumotlar, tergov, qidiruv, tekshirish, voqea joylari, kompyuter tarmoqlari, protokol.*

TACTICS FOR CONDUCTING INVESTIGATIVE ACTIONS AIMED AT OBTAINING DIGITAL INFORMATION DURING THE INVESTIGATION OF CYBERCRIMES

Atakulov Bekzod Abduhalil o‘g‘li
independent researcher of the Department
of Criminal Procedure Law
Tashkent State University of Law
bekatakuloff@gmail.com
ORCID: 0009-0005-3621-4208

Abstract: *In this scientific article, the author has revealed the specifics of the implementation of the tactics of investigative actions aimed at obtaining digital information during the investigation of cybercrimes. Given the practical complexity of the investigation of this group of crimes, it is these investigative actions, in the author's opinion, that are relevant and oriented to the production of other investigative actions in a criminal case. Thanks to the conducted research, the author consistently comes to the conclusion that the mechanism and tactics of conducting these initial investigative actions need to be systematized, as well as to provide training for novice staff of investigators and specialists of internal affairs bodies on the basis of scientifically constructed hypotheses-materials of this tactic.*

Keywords: *Cybercrimes, digital information, operational information, investigation, search, inspection, accident sites, computer networks, protocol.*

Введение.

Актуальность исследования в научной статье обусловливается теми факторами, которые существуют в практике расследования киберпреступлений: дезорганизованность, фрагментированный характер проведения следственных действий, отсутствие четких инструкций и тактики в части проведения следственных действий, направленных на получение цифровой информации при расследовании

киберпреступлений, что повышает научный интерес к изучению соответствующей тематики исследования.

Цель настоящей научной статьи состоит в том, чтобы наглядно показать, с какими особенностями связаны следственные действия, направленные на получение цифровой информации при расследовании киберпреступлений, особенно на начальных этапах действий по возбужденному уголовному делу.

Научная разработанность данной темы выражена в наличии комплексных прикладных исследований правового характера таких авторов, как Д.М.Берова, Е.С.Шевченко, Н.Р.Шевко, И.О.Казакова, З.О.Трофимов, A. Ashworth, S.Bronitt, B.McSherry, G.Janke, R.Odenthal и многих других исследователей.

Методология исследования в настоящей научной статье предполагает применение системного метода, а также методов анализа, синтеза, индукции, дедукции и моделирования в части обобщения полученных выводов.

Основная часть.

Информатизация общества превратилась в новую эпоху жизни человечества, так как связана с расширением сфер деятельности в сети Интернет, очень тяжело уследить за всем многообразием проявления этой стороны общественной жизни. Наряду со стремительным развитием технологий быстро развивается и соответствующая киберпреступность [1, с.173]. С сожалением приходится констатировать такой факт, что на данный момент сотрудники правоохранительных органов отстают от киберпреступников, нарушающих законодательство в ИКТ-сфере. Территориальные органы не могут должным образом обеспечить специалистов, что происходит из-за слабого материально-технического обеспечения первых специалистами.

Количество пользователей компьютерных сетей достигло глобального количества. А также к этому всему прибавляется набирающая популярность «криптовалютная лихорадка». Все это только способствует развитию преступности в сфере компьютерных технологий.

Специфика киберпреступлений создает сложнейшие задачи для сотрудников правоохранительных органов при их раскрытии. По мнению Э. Дж. Эшворта, «структура преступлений обманного характера необычна тем, что позволяет считать деяние оконченным независимо от того, получена ли в результате деяния реальная выгода и причинены ли реальные убытки» [2, p.552], в связи с этим на практике могут возникать проблемы не только с квалификацией киберпреступлений, но и со следственными действиями, связанными с их расследованием (в особенности, со стадией проведения следственных действий, направленных на получение цифровой информации).

Следует отметить, что на практике к новой электронной технологии относится применение электронных ключей. Электронный ключ – это устройство с памятью,

которое было выполнено благодаря специальной микросхеме. Сам ключ вводится в порт компьютера, предназначенного для подключения принтера, и легко выводится.

Таким образом, очевидно, что наличие и использование оперативной информации зачастую может сыграть решающую роль при поиске в ЭВМ. Однако успешное преодоление защиты еще не решает все проблемы собирания цифровых доказательств в компьютере.

Следует отметить, что тактические особенности поиска компьютерной информации зависят также от функционального состояния ЭВМ и ее периферийных устройств на момент осмотра или обыска. Первоначальная цифровая информация может быть либо зафиксирована на постоянном носителе, либо храниться в ЭВМ.

Трудность с обобщением материалов следственной и судебной практики по каждому преступлению, специфичность информации, получаемой в процессе предварительного расследования, но ключевым фактором, затрудняющим предварительное расследование, выступает недостаточная компетентность лиц, занимающихся выявлением и раскрытием киберпреступлений.

Первоначальный этап расследования киберпреступлений зачастую характеризуется возникновением сложных следственных ситуаций, например, имеется факт совершенного киберпреступления, но сведения о лице, его совершившим либо отсутствуют, либо местонахождение преступника неизвестно. На практике возникают случаи, когда местонахождение злоумышленника установлено, но задержание подозреваемого вызывает ряд сложностей, так как преступление совершалось лицом, находящимся за территорией Республики Узбекистан. Исходя из этого, можно сделать вывод, что международное сотрудничество в борьбе с киберпреступностью является залогом качественного расследования преступлений подобной направленности.

Далее, следует отметить, что первоочередным и неотложным следственным действием является осмотр места происшествия. В ходе данного следственного действия выявляются цифровые следы, оставленные преступником [3, с.128].

Прибыв на место происшествия следователь должен выполнить конкретные действия, направленные на получение цифровой информации, сохранение следов и обстановки преступного события:

- организовать охрану территории и удалить посторонних лиц;
- сохранить все объекты места совершения преступления в том состоянии в котором они находятся на момент начала следственного действия (включенные ПК должны остаться включенными и наоборот;
- произвести опрос потерпевшего о произошедшем;
- составить подробный протокол о случившемся [4, с.15].

При осмотре в целях поиска цифровой информации наиболее правильным будет использовать тактический прием «от центра к периферии». При этом отправной

точкой начала следственного действия может являться персональный компьютер, электронный терминал и т.д. [5, с.98].

Ученые подразделяют осмотр места происшествия на детальный и обзорный при действиях, связанных с получением цифровой информации.

Первый вид осмотра, направленного на получение цифровой информации, связан с тем, что следователь определяет определенные границы места осмотра в техническом устройстве, через которое, предполагается совершение преступления, или в котором могут быть отражены следы последствий этого преступления. И все эти признаки также входят в круг цифровой информации. Также следует добавить, при осмотре места происшествия технического устройство, где совершено киберпреступление, следователь осматривает:

– место хранения и обработки цифровой информации;
– место, где находился преступник во время совершения киберпреступления;
– место хранения информации в компьютере; место наступления вредных последствий.

При обзорном осмотре следователю следует выяснить: имеется ли у компьютера подключение к локальной сети (какой вид у данной сети: проводная или беспроводная); имел ли место удаленный доступ при совершении преступления. По окончанию осмотра следователь должен нарисовать схему осматриваемого помещения с точным расположением оборудования относящегося к киберперступлению. [6]

Детальный осмотр с целью поиска цифровой информации позволяет совершать поочерёдный осмотр всех элементов оборудования, которое каким-либо образом относится к киберпреступлению: компьютер и все его составляющие, части киберпространства, устройств связи, модемов, материальных носителей информации, а также документов, относящихся к совершенному киберпреступлению.

Сложность при производстве данного следственного действия состоит в том, что большинство следов преступления имеют цифровую форму. Подобные следы представляют собой компьютерную информацию, которая имеет высокую скорость трансформации, что создает основания говорить о том, что уже сегодня существует необходимость разработки новых методов и процедур обнаружения, фиксации и обеспечения сохранности цифровых следов.

На практике следами цифровой информации являются:

– вирусы;
– совокупность вредоносных программ и следов их деятельности;
– следы несанкционированного доступа к системе;
– программы для удаленного администрирования;
– журнальные файлы событий АРМ;
– журнальные файлы антивирусных продуктов и систем защиты от вторжений;

– следы установки специфического программного обеспечения -сканеры портов, программы для шифрования дисков.

В настоящее время как на практике, так и в юридической литературе существует дискуссия по поводу привлечения к производству осмотра места происшествия при расследовании киберпреступлений следственно-оперативной группы. Д.А. Илюшин отмечает, что «осмотр места происшествия необходимо проводить следственной-оперативной группой, укомплектованной следующим составом: следователь, оперуполномоченные, специалист-криминалист» [7, с.118].

Противоположная точка зрения у А.Н. Яковлева и Н.В. Олиндер, которые считают, что «основные функции потенциальных участников такой группы успешно выполняет следователь и привлеченный к производству следственного действия специалист, оказывающий как консультационное, так и доказательственное содействие следователю. Если специалист отсутствует, то появляется необходимость привлекать разных лиц, в совокупности обладающих необходимым опытом и базой знаний» [8, с.100].

В разных странах, при расследованиях киберпреступлений осмотр места происшествия в целях поиска цифровой информации имеет свои особенности.

Следует отметить, что федеральное уголовное законодательство Австралии отличает бесчестную кражу, совершенную посредством ИКТ, от обманных преступлений, нацеленных на получение собственности или услуги (любых прав, льгот, привилегий) путем обмана [9]. При этом на практике работы правоохранительных органов Австралии обманы с кредитными картами, и кражи от мошенничества отличить друг от друга сложно [10, с.747].

Также в правоприменительной практике как компьютерные обманы квалифицируются следующие деяния: кража информации с компьютеров, принадлежащих финансовым учреждениям, а также используемых в государственной торговой деятельности; кража средств электронного кошелька путем изменения учетных данных [11, p. 23, 205], распространение вирусов [12], предложения фиктивных вакансий, направленные по электронной почте; сбор конфиденциальной информации и ее последующее использование для получения выгоды [13], мошенничество с кредитными картами [14, p. 231—232], и многие другие. При чем получение информации о совершении данных правонарушений зачастую затрудняется временными ограничениями и относительно слабой технической оснащенностью государственных органов.

Так в США процедура производства такого следственного действий как осмотр места происшествия не так детально регламентирована. На практике полицейские в Америке лишь проверяют признаки преступления в зарегистрированном сообщении о преступлении. По факту полицейские лишь проводят оперативно-розыскные действия, направленные на поиск следов, оставленных преступником при совершении

преступления. Стоит заметить, что полученные на данном этапе сведения о совершенном преступлении не являются судебными доказательствами, они имеют место лишь при применении мер процессуального принуждения. Однако независимо от того, была достигнута эта цель или нет, полицейскому следует осмотреть это место, чтобы обнаружить следы и иные вещественные доказательства [15, с.35-42]. Таким образом, в законодательстве США отсутствуют жесткие требования к процессуальной форме сбора доказательств в отличии от законодательства.

Уголовно-процессуальный кодекс Франции вообще не содержит такого следственного действия как осмотр места происшествия, в процессе которого возможны изъятие и фиксация орудий, предметов, следов и др. Таким образом, данное следственное действие, в сравнении с аналогом стран СНГ, выглядит как комплексное действие, с особой направленностью на выявление, сохранение и изъятие следов преступления, установление виновных лиц.

В Германии наряду с основным составом мошенничества (§ 263 УК) в преступлениях против имущества как целого сформулирован специальный состав — компьютерное мошенничество (§ 263а УК), введенное в уголовное законодательство в целях необходимости уголовного преследования за использование в мошеннических схемах компьютерных технологий и различных программных манипуляций [16, p. 83, 275].

Соответственно, в ФРГ осмотр проводится на стадии предварительного расследования сотрудниками полиции и прокуратуры, по итогам которого составляется протокол. При осмотре работает и эксперт, приглашенный обвиняемым, или иными сторонами уголовного дела [17, с.169].

Заключение.

На основании всего изложенного, можно сделать вывод, что производство следственных действий на первоначальном этапе расследования при расследовании преступлений в сфере компьютерной информации имеет определенные особенности, которые вызывают определенные трудности у следователей, особенно на первоначальном этапе расследования в целях получения цифровой информации о совершенном киберпреступлении. Каждое завершенное уголовное дело для следователя означает наличие определенного опыта, и наличие такого положительного опыта по киберпреступлениям приветствуется, особенно если у следователя к моменту расследования таких преступлений уже были специальные познания и ориентиры.

В целом, на наш взгляд, представляется необходимым создать общие для правоохранительных органов механизм и тактику проведения данных первоначальных следственных действий необходимо систематизировать, а также обеспечивать подготовку начинающего персонала следователей и специалистов органов внутренних дел на основе научно построенных гипотез-материалов данной тактики.

СНОСКИ/IQTIBOSLAR/REFERENCES

1. Берова Д.М. Расследование киберпреступлений // Пробелы в российском законодательстве. - 2018. - № 2. - С. 173-175.

2. Ashworth A. J. United Kingdom // The Handbook of Comparative Criminal Law / eds. by K. J. Heller, M. D. Dubber. Stanford; California, 2011. P. 552.

3. Шевченко Е.С. Тактика отдельных следственных действий при расследовании киберпреступлений // Закон и право. - 2015. - № 8. - С. 128-138.

4. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения // Ученые записки Казанского юридического института МВД России. - 2016. - № 1. - С. 13-16.

5. Казакова И.О., Костенко Т.А. К вопросу о расследовании киберпреступлений в РФ // Студенческий вестник. - 2019. - № 22-2 (72). - С. 98-99.

6. Трофимов З.О. Особенности производства следственных действий на первоначальном этапе расследования киберпреступлений: отечественный и зарубежный опыт. Журнал «Юридическая наука». 2019 г. ВАК // Источник: https://cyberleninka.ru/article/n/osobennosti-proizvodstva-sledstvennyh-deystviy-na-pervonachalnom-etape-rassledovaniya-kiberprestupleniy-otechestvennyy-i

7. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет: дисс. канд. юрид. наук: 12.00.09. - Волгоград, 2008. - 233 с.

8. Яковлев А.Н. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методическое пособие. - М., 2012. -182 с.

9. Mazzone A. Identity Fraud — Government Legislative Responses // Victorian Government Solicitor's Office. URL: http://vgso.vic.gov.au/sites/default/files/publications/Identity%20 Fraud%20-%20Government%20Legislative%20Responses.pdf.

10. Bronitt S., McSherry B. Principles of Criminal Law. 3rd ed. Sydney, 2006. P. 746—748.

11. Federal Criminal Law and its Enforcement / N. Abrams, S. S. Beale, S. R. Klein. 5th ed. West, 2010. P. 23, 205.

12. Computer and Internet Fraud // Cornell University Law School. Legal Information Institute. URL: http://www.law.cornell. edu/wex/computer_and_internet_fraud.

13. Identity Theft (FAQ) // Nolo. Law for All. URL: http:// www.nolo.com/legal-encyclopedia/identity-theft-faq-29074.html; What is Illegal under Local, State and Federal Laws? Federal Computer Security Violations // Cornell University. IT Cornell. URL: http://www.it.cornell.edu/policies/university/privacy/ responsible/illegal.cfm.

14. Janke G. Kompendium Wirtschaftskriminalitat. Peter Lang GmbH International Verlag der Wissenschaften. Frankfurt am Main, 2008.

15. Хамидуллин Р.С., Малых А.А. Опыт использования специальных знаний при осмотрах мест происшествий в России и США // Полицейская и следственная деятельность. - 2016. - № 2. - С. 35-42.

16. Odenthal R. Korruption und Mitarbeiterkriminalitat: Wirtschaftskriminalitat vorbeugen, erkennen und aufdecken. 2., vollstandig Qberarbeitete und erweiterte Auflage. Gabler I GWV Fachverlage GmbH, Wiesbaden, 2009.

17. Гаврилин Ю В Расследование неправомерного доступа к компьютерной информации: дисс. канд. юрид. наук: 12.00.09. - М., 2009. - 210 с.