УДК 343.98:002.5 DOI: 10.24412/2411-2275-2021-1-92-95

КОЛИЕВ В.В., ШАХКЕЛДОВ Ф.Г.

МЕТОДИКА РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Ключевые слова: информационно-коммуникационные технологии, киберпреступность, компьютерное моделирование, электронное устройство, интернет-провайдер, веб-сайт.

В статье анализируется статистика преступлений в сфере информационно-коммуникационных технологий; предложен обобщенный механизм проведения следственных действий, направленных на поиск преступных элементов; рассмотрены общие методы, используемые в процессе расследования большинства цифровых преступлений, а также инструменты для каждого типа киберпреступности, доступные для выполнения криминалистической деятельности. На примере типичной следственной ситуации (незаконное списание денежных средств с банковского счета) определена методика расследования указанного преступного деяния. Отмечается, что проведение дальнейших следственных мероприятий возможно как без использования специальных знаний и оборудования, так и с его применением. Проведение следственных мероприятий зависит также от места совершения преступлений. Так, если хищение совершено через банкомат, то при проведении осмотра места совершения преступления не следует ограничиваться осмотром непосредственно места совершения преступления, необходимо обеспечить расширение границ территории осмотра и/или определить новые места осмотра исходя из потенциально-возможных вариантов ухода преступника с места преступления.

KOLIEV, V.V., SHAKHKELDOV, F.G.

METHODOLOGY FOR SOLVING CRIMES COMMITTED USING INFORMATION-COMMUNICATIONS TECHNOLOGIES

Key words: information-communication technologies, cybercrime, computer modeling, electronic device, Internet provider, website.

In the article analyzed the statistics of crimes in the field of information-communications technologies; proposed a generalized mechanism for conducting investigative actions aimed at finding criminal elements; considered the general methods used in the process of investigating most digital crimes, as well as tools for each type of cybercrime available for performing forensic activities. On the example of a typical investigative situation (illegal debit of funds from a bank account), it is determined the methodology for investigating the indicated criminal act. It is noted that further investigative measures are possible both without the use of special knowledge and equipment, and with its use. The conduct of investigative measures also depends on the place where the crimes were committed. So, if the theft is committed through an ATM, then during the inspection of the crime scene, one should not be limited to the inspection of the crime scene itself, it is necessary to expand the boundaries of the inspection territory and / or determine new inspection sites based on the potential options for the criminal's departure from the crime scene.

Одним из видов преступлений, количество которых растет в последнее десятилетие с огромной скоростью, являются преступные деяния, совершаемые с использованием информационно-коммуникационных технологий. Так, согласно официальным данным правоохранительных органов, в 2016 году было зарегистрировано 65 949 указанных преступлений, а в 2017 году рост зарегистрированных аналогичных деяний составил 24638 деяния, что составляет более 37% [3]. В 2020 году рост по сравнению с предыдущим периодом составил 73, % [4].

Рост преступлений сопровождается изменением способов их совершения и сокрытия ввиду постоянных изменений в области телекоммуникаций и информационных технологий. Расследование таких деяний должно осуществляться лицами, имеющими определенный набор знаний и компетенций в сфере IT-технологий, с помощью инструментов и средств, разработанных и применяемых в информационной среде. В этом заключается специфика расследования исследуемых преступлений. Поэтому, в целях изменения общих показателей статистики исследуемых преступных посягательств важно обеспечить качественное, грамотное и профессиональное их расследование.

Учитывая специфику расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, отметим, что существует необходимость в подготовке для практических сотрудников органов предварительного следствия рекомендаций и приемов, направленных на повышение эффективности их действий при раскрытии и расследовании данных деяний.

Хотя методы розыска преступников могут варьироваться в зависимости от типа расследуемой киберпреступности, а также от того, кто ведет расследование, большинство цифровых преступлений подчиняются некоторым общим методам, используемым в процессе расследования.

Во-первых, важно обеспечить проверку предыстории совершения преступления. Так, ее создание и определение с известными фактами поможет следователям установить отправную

точку для установления того, с чем они сталкиваются и каким объемом информации они располагают при обработке первоначального отчета о киберпреступности.

Во-вторых, одна из самых важных вещей, которую должен сделать любой работник правоохранительных органов, уполномоченный на расследование таких преступлений, это собрать как можно больше информации об инциденте. К такой информации можно отнести следующие сведения: Была ли это автоматическая атака или целенаправленное преступление? Была ли какая-то открытая возможность для этого нападения? Каковы масштабы преступного события и его влияние? Может ли эта атака быть выполнена кем-либо или определенными людьми с определенными навыками? Кто потенциальные подозреваемые? Какие цифровые преступления были совершены? Где можно найти доказательства? Есть ли у нас доступ к таким источникам доказательств? Эти и другие вопросы являются ценными соображениями в процессе сбора информации.

Как указывает Д.М. Берова, для расследования таких преступлений важно использовать различные криминалистические средства и методы (например, методы моделирования, компьютерного моделирования, анализ материалов уголовных дел предшествующих лет и т. п.), при помощи которых проводится реконструкция преступного механизма [1]. Кроме того, помимо специалистов в области компьютерной техники, технологий и информации при расследовании уголовных дел рассматриваемой категории наиболее востребованы специалисты в сфере финансов, кредита и аудита, экономической безопасности, банковского дела, медицины и охраны труда и др.

Следует отметить, что многие национальные и федеральные агентства используют интервью и отчеты о слежке, чтобы получить доказательства киберпреступности. Наблюдение включает в себя не только камеры видеонаблюдения, видео и фотографии, но и наблюдение за электронными устройствами, которые подробно описывают, что и когда используется, как оно используется, а также все цифровое поведение субъекта, связанное с преступным деянием.

Отслеживание и идентификация преступников - этот следующий шаг, который выполняется в процессе сбора информации, в зависимости от того, сколько информации уже имеется в наличии. Чтобы идентифицировать преступников, стоящих за кибератакой, как частные, так и государственные службы безопасности часто работают с интернет-провайдерами и сетевыми компаниями, чтобы получить ценную информацию о своих подключениях, а также исторические данные, веб-сайты и протоколы, используемые в течение времени их подключения. Это самый медленный этап, поскольку для получения доступа к необходимым данным требуется юридическое разрешение на доступ к персональным данным.

Как только следственные органы и оперативные работники собрали достаточно данных о совершенном преступлении с использованием информационно-коммуникационных технологий, требуется изучить цифровые системы, которые были задействованы, или те, которые предположительно были вовлечены в осуществление атаки или иного преступного деяния. Этот процесс включает в себя анализ необработанных данных сетевого подключения, жестких дисков, файловых систем, кэширующих устройств, оперативной памяти и многого другого. Как только начнется судебно-медицинская экспертиза, сотрудникам правоохранительных органов важно обеспечить исследование всех имеющихся следов, найти отпечатки пальцев в системных файлах, сетевых и сервисных журналах, электронной почте, истории просмотра веб-страниц и т. д.

Как указывает А.А. Ваценко, существуют тысячи инструментов для каждого типа киберпреступности, доступных для выполнения криминалистической деятельности. К их числу можно отнести следующие [2]:

- Live Response. Используется при обнаружении, контроле и устранении угрозы в работающей системной среде;

- SIFT-это коллекция криминалистических инструментов, созданная для того, чтобы помочь группам реагирования на инциденты и правоохранительным органам исследовать цифровые криминалистические данные в нескольких системах. Так, когда расследование требует поддержки изображений, как вида доказательства преступного деяния, то эта система отлично работает с отдельными файлами raw-изображений, AFF (Advanced Forensic Format), EWF (Expert Witness Format, EnCase), AFM (AFF с внешними метаданными) и многими другими.

- TSK, The Sleuth Kit - набор криминалистических инструментов с открытым исходным кодом для Unix и Windows, который помогает исследователям анализировать образы дисков и восстанавливать файлы с этих устройств. Его функции включают полную поддержку синтаксического анализа различных файловых систем, таких как FAT/exFAT, NTFS, Ext2/3/4, UFS 1/2, HFS, ISO 9660 и YAFFS2, что приводит к анализу практически любого образа или диска для операционных систем Windows, Linux и Unix.

X-Ways Криминалистика - программное обеспечение является одним из наиболее полных криминалистических наборов для операционных систем на базе Windows. Он широко поддерживается практически для любой версии Windows, что делает его одним из лучших на этом конкретном рынке и позволяет легко работать с такими версиями, как Windows XP/2003/Vista/2008/7/8/8.1/2012/10*, поддержка как 32-Битных, так и 64-битных версий. Одна из его особенностей - это его портативность, что позволяет запускать его с карты памяти и легко переносить с одного компьютера на другой. Его основные функции включают в себя: возможность выполнять клонирование дисков и создание образов, чтение разделов из файлов raw - изображений, жестких дисков, RAID-массивов, LVM2 и многое другое. Он также предлагает расширенное обнаружение удаленных разделов на FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4 и т.д., а также расширенное вырезание файлов и создание каталогов файлов и каталогов. CAINE-это не простое приложение для расследования киберпреступлений или набор программ, это полный дистрибутив Linux, используемый для цифрового криминалистического анализа.

Например, может сложиться такая следственная ситуация, что ни следователь, ни потерпевший, не обладают сведениями относительно личности преступников, совершивших преступление. Одним из самых распространенных преступлений такого типа является незаконное списание денежных средств с банковского счета.

В такой ситуации характеристика типичной следственной ситуации будет следующая:

Это будет общая следственная ситуация в рамках установления преступников, которая требует проведения безотлагательных следственных мероприятий, сложившаяся относительно динамичных объектов, при которой проведение дальнейших следственных мероприятий возможно как без использования специальных знаний и оборудования, так и с его применением. При этом количество и вариативность таковых мероприятий ограничены. Для расследования такого деяния правоохранительные органы должны обеспечить направление запроса в кредитную организацию о предоставлении сведений и информации о субъекте, совершившем незаконное списание. Если списание средств произошло с применением электронных пластиковых карт и мобильного банка, то важно обеспечить запрос оператору связи, предоставляющему услуги провайдера связи. Незаконное списание через банкомат является преступлением, расследование которого важно обеспечить с привлечением собственника здания (помещения), в котором располагается банковский терминал в целях получения видео с камер фиксации и кредитной организации (собственника терминала), который может предоставить видео с камер, встроенных в банкомат.

Проведение следственных мероприятий зависит от места совершения преступлений. Так, если хищение совершено через банкомат, то при проведении осмотра места совершения преступления не следует ограничиваться осмотром непосредственно места совершения преступления, необходимо обеспечить расширение границ территории осмотра и/или определить новые места осмотра исходя из потенциально-возможных вариантов ухода преступника с места преступления. Это необходимо в целях выявления всех имеющихся следов преступления, а также формирования иной доказательственной базы и определение вариантов поиска преступников исходя из направления его движения.

Литература и источники

1. Берова Д.М. Расследование киберпреступлений // Пробелы в российском законодательстве. 2018. №1. С. 173-175.
2. Ваценко А.А. Обзор техник компьютерной криминалистики / Бюллетень науки и практики. 2020. С. 167-174.
3. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // [Электронный ресурс] Режим доступа: https://genproc.gov.ru/smi/news/genproc/news-1431104.
4. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года // [Электронный ресурс] Режим доступа: https://мвд.рф/reports/item/22678184/.

References and Sources

1. Berova D.M. Rassledovanie kiberprestuplenij // Probely v rossijskom zakonodatel'stve. 2018. №1. S. 173-175.
2. Vacenko A.A. Obzor tekhnik komp'yuternoj kriminalistiki / Byulleten' nauki i praktiki. 2020. S. 167-174.

3. O prestupleniyah, sovershaemyh s ispol'zovaniem sovremennyh informacionno-kommunikacionnyh tekhnologij // [Elektronnyj resurs] Rezhim dostupa: https://genproc.gov.ru/smi/news/genproc/news-1431104.
4. Kratkaya harakteristika sostoyaniya prestupnosti v Rossijskoj Federacii za yanvar' - dekabr' 2020 goda // [Elektronnyj resurs] Rezhim dostupa: https://mvd.rf/reports/item/22678184/.

КОЛИЕВ ВАДИМ ВИТАЛЬЕВИЧ - кандидат юридических наук, доцент, начальник кафедры криминалистики Ставропольского филиала Краснодарского университета МВД России, полковник полиции (vadim.koliev@yandex.ru).
ШАХКЕЛДОВ ФРИДРИХ ГРИГОРЬЕВИЧ - доктор юридических наук, доцент, профессор кафедры криминалистики и оперативно-розыскной деятельности Ростовского юридического института МВД России (armani@mail.ru)..
KOLIEV, VADIM V. – Ph.D. in Law, Associate Professor, Head of the Department of Criminology, Stavropol Branch of the Krasnodar University of the Ministry of Internal Affairs of Russia, Police Colonel.
SHAKHKELDOV, FRIDRIKH G. - Doctor of Law, Associate Professor, Honorary Lawyer of Russia, Honored Lawyer of Kuban, Chairman of the Kuban Collegium of Advocates, Professor of the Department of Criminalistics and Operational - Investigative Activities of the Rostov Law Institute of the Ministry of Internal Affairs of the Russian Federation

УДК 347.1 DOI: 10.24412/2411-2275-2021-1-95-101

ВИЛЬДАНОВА М.М.

О РЕГУЛИРОВАНИИ ПРАВООТНОШЕНИЙ АКЦИОНЕРНЫХ ОБЩЕСТВ С АКЦИОНЕРАМИ, СВЕДЕНИЯ О КОТОРЫХ ОТСУТСТВУЮТ И КОТОРЫЕ НЕ ОСУЩЕСТВЛЯЮТ ПРАВА АКЦИОНЕРОВ НА ПРОТЯЖЕНИИ ДЛИТЕЛЬНОГО ВРЕМЕНИ

Ключевые слова: публичные акционерные общества, непубличные акционерные общества, реорганизация, голосование на собрание, получение дивидендов, кворум, выкуп акций.

Предметом рассмотрения в статье является анализ проблемы взаимоотношений общества с акционерами, сведения о которых отсутствуют и которые не осуществляют свои права на протяжении длительного периода времени («потерянные» акционеры). В работе исследуется регулирование данного вопроса в зарубежных странах, таких как Франция, Великобритания, США и Япония. Автором даны конкретные предложения относительно мер по поиску «потерянных» акционеров и урегулированию их правоотношений с обществом. В частности, рассматриваются возможности перехода акций «потерянных» акционеров к государству, принудительной продажи акций самому обществу. Создаваемое правовое регулирование вопросов «потерянных» акционеров должно гарантировать соблюдение баланса интересов акционерного общества и акционера, исключив возможность злоупотреблений, в частности, манипулирования с целью устранения от голосования неугодных акционеров и размывания корпоративного контроля.

VILDANOVA, M.M.

ON THE REGULATION OF LEGAL RELATIONS OF JOINT-STOCK COMPANIES WITH SHAREHOLDERS INFORMATION ABOUT WHICH IS NOT AVAILABLE AND WHICH DO NOT EXERCISE THE RIGHTS OF SHAREHOLDERS FOR A LONG TIME

Key words: public joint-stock companies, non-public joint-stock companies, reorganization, voting at the meeting, receipt of dividends, quorum, share repurchase.

This article provides the analysis of the problem of the company's relations with shareholders, information about which is not available and who do not exercise the rights for a long period of time ("missing" shareholders). In the article examines the regulation of this issue in foreign countries, such as France, the United Kingdom, the United States and Japan. The author gives specific proposals on measures to find the "missing" shareholders and to settle their legal relations with the company. In particular, the possibility of transferring the shares of "missing" shareholders to the state or the forced sale of shares to the company itself is being considered. The created legal regulation of the issues of "missing" shareholders should ensure that the balance of interests of the joint-stock company and the shareholder is maintained, excluding the possibility of abuse, in particular, manipulation in order to eliminate unwanted shareholders from voting and dilute corporate control.

Проблема правового режима «потерянных» акционеров актуальна для акционерных обществ в юрисдикциях различных государств, развивающихся в условиях рыночной экономики, но не имеет единообразного решения в национальных законодательствах. Наличие таких акционеров создает дополнительные и вряд ли оправданные издержки акционерному обществу, в частности, отражение невыплаченных дивидендов в отчетности, направление заведомо возвратных уведомлений о проведении общего собрания. Порой оно является существенным барьером для осуществления различных корпоративных мероприятий в связи с отсутствием кворума (к примеру, в связи с преобразованием непубличных акционерных обществ в публичные и т.д.). Проблема «потерянных» акционеров была предметом анализа в юридической литературе [1-3], однако конкретного ее решения пока не найдено.

Для учета распределения пакетов акций и оценки объема прав необходимо, чтобы в Едином государственном реестре юридических лиц (ЕГРЮЛ) было четко зафиксировано количество ценных бумаг. Вместе с тем, по сей день встречаются ситуации, когда в ЕГРЮЛ числится исключенное из него общество, которое не может распорядиться принадлежащими ему акциями,