ПРОБЛЕМЫ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ФИНАНСОВО-ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

PROBLEMS AS TO CRIMINAL MAINTENANCE OF INVESTIGATION OF FINANCIAL AND ECONOMIC CRIMES COMMITTED WITH THE USE OF COMPUTER TECHNOLOGY

УДК 343.985.7

СОТНИКОВА Валерия Владимировна
кандидат юридических наук
БУНИН Кирилл Андреевич

SOTNIKOVA Valeria Vladimirovna
Candidate of Law
BUNIN Kirill Andreevich

Аннотация. *В настоящей статье рассматриваются вопросы, связанные с криминалистической проблематикой расследования финансово-экономических преступлений, совершенных с использованием компьютерных технологий. Рассмотрены недостатки, связанные с порядком назначения судебных экспертиз и порядком собирания отдельных видов доказательств при расследовании рассматриваемой категории уголовных дел. Выявлены некоторые особенности объективной стороны совершения финансово-экономических преступлений с использованием компьютерных технологий.*

Ключевые слова: *расследование преступлений, финансово-экономические преступления, компьютерные технологии, криминалистика.*

Abstract. *This article dwells on issues related to the forensic problems of investigation of financial and economic crimes committed with the use of computer technology. The shortcomings associated with the order of appointment of forensic examinations and the order of collection of certain types of evidence in the investigation of the category of criminal cases are considered. Some features of the objective side of financial and economic crimes with the use of computer technologies are revealed.*

Keywords. *crimes investigation, financial and economic crimes, computer technology, criminology.*

В настоящее время мир переходит в новую фазу своего развития во всех сферах жизнедеятельности человеческого общества, именуемую «информационное общество». По справедливому утверждению Ю.В. Бородакия, «глобальная информатизация в настоящее время активно управляет существованием и жизнедеятельностью государств мирового сообщества, информационные технологии применяются при решении задач обеспечения национальной, военной, экономической безопасности и др.» [1, С. 1]. Процесс цифровизации общества приобретает повсеместный характер (о чем свидетельствует, например, программа «Цифровая экономика Российской

Федерации», согласно которой к 2024 году 97% домохозяйств в России должны иметь широкополосный доступ к интернету (100 Мбит/с), информационные системы и ресурсы органов государственной власти и местного самоуправления должны быть перенесены в государственную единую облачную платформу в полном объеме [4]), что делает вопрос об информационной безопасности общества и государства все более насущным, а борьбу с соответствующими угрозами – все более сложной и актуальной.

Информационная безопасность подразумевает, прежде всего, безопасность, связанную с использованием информационных технологий и различных технических устройств (будь то компьютеры, планшетные компьютеры, смартфоны и иные гаджеты) в повседневной деятельности – иначе говоря, «компьютерную» безопасность. Важно отметить, что одной из главных задач обеспечения такой безопасности является выявление, пресечение, раскрытие и расследование преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий (число которых, если рассматривать статистические данные за январь-ноябрь 2018 года, возросло на 89,6% по сравнению с аналогичным периодом прошлого года [6, С. 7] и составило 156307 преступлений), а равно преступлений в сфере компьютерной информации (отмечен рост на 35,7% в вышеуказанные периоды). Так, Доктрина информационной безопасности Российской Федерации рассматривает данный рост как одну из основных угроз безопасности нашей страны [2].

С учетом изложенного, расследование преступлений, совершенных с использованием компьютерных технологий, приобретает огромную, возрастающую в геометрической прогрессии роль, и априори предполагает проблематику, связанную как с криминалистическим аспектом (проведение отдельных следственных действий), как с уголовно-правовым аспектом (определенные вопросы квалификации действий преступников и отграничения смежных составов), так и с уголовно-процессуальным аспектом (процесс доказывания по уголовному делу). В своей совокупности они

обуславливают несовершенство существующей методики расследования преступлений, которое в перспективе будет шириться и нанесет не только ущерб правам и свободам человека и гражданина в Российской Федерации, но и, прежде всего, национальной безопасности России. Вместе с тем, особый интерес представляет криминалистический аспект, поскольку в практической деятельности он создает наибольшее количество проблем, так как остальные два аспекта связаны с несовершенством законодательства, а криминалистический аспект – с несовершенством технологий и уровня подготовки кадров правоохранительных органов, что, как представляется, гораздо опаснее в свете вышеупомянутого роста преступности в сфере компьютерной информации. Именно поэтому данная статья посвящена криминалистической проблематике расследования преступлений, причем той категории, которая, ввиду развития цифровой экономики (о чем также упоминалось выше), становится все более и более актуализированной.

Криминалистическая характеристика преступлений, так или иначе связанных с использованием компьютерных технологий заключается, прежде всего, в характеристике орудий совершения преступлений – компьютерных программ.

Примечательно, что совершение преступлений осуществляется не только с использованием вредоносных программ, которые были специально для этого созданы. Преступления совершаются также и с использованием абсолютно легальных программ.

Рассмотрим следующий случай. К компьютеру определенного пользователя был получен неправомерный доступ с использованием программ для удаленного управления, контроля и администрирования, которыми пользуется огромное количество пользователей в повседневной деятельности, например, с помощью таких программ, как RMS, Ammyy Admin, TeamViewer, LiteManager и других. Данные программы абсолютно легальны, что дает преступнику определенные преимущества. После модификации одной из вышеупомянутых программ (причем проведенная модификация, как правило,

переносит данную программу в класс RiskWare – условно-опасные программы, которые в лучшем случае антивирусами лишь детектируются, но не блокируются) преступник может получить несанкционированный доступ к компьютеру другого пользователя и, заблокировав информацию, находящуюся на компьютере, либо каким-либо иным способом сделав ее не пригодной к использованию, потребовать передачи с пользователя денежных средств за разблокировку информации. Такие противоправные действия квалифицируются по статье 159.6 УК РФ «Мошенничество в сфере компьютерной информации» [8]. Однако именно легальность используемой программы создает определенные проблемы доказывания – прежде всего это касается назначения и проведения компьютерных экспертиз в рамках проводимого расследования.

Вместе с тем, допускаются ошибки и при назначении компьютерных экспертиз для исследования вредоносных программ. Отметим, что компьютерная экспертиза имеет важное значение при определении признаков, по которым та или иная программа признается вредоносной. Основной ошибкой при назначении данной экспертизы является постановка следующего вопроса: «Является ли представленная на исследование компьютерная программа вредоносной?». Данный вопрос в компетенцию эксперта не входит, поскольку исходя из анализа диспозиции статьи 273 УК РФ, определяющей такие технические признаки вредоносной программы, как наличие определенного функционала, предполагающего возможность блокирования, модифицирования, удаления компьютерной информации, а также ее установку и деятельность без ведома пользователя, для признания программы вредоносной необходимо также установить наличие правовых признаков вредоносной программы: создание разработчиком программы с умыслом совершения посредством нее преступления и субъективное восприятие потерпевшим опасности той или иной компьютерной программы, о деятельности которой он осведомлен [7]. Наличие таких признаков устанавливается исключительно следователем и судом.

Следует охарактеризовать способы, используемые преступниками для получения несанкционированного доступа к содержимому компьютера пользователя. На самом деле, выбор способов и средств на сегодняшний день весьма разнообразен, однако наиболее распространенными являются следующие:

1. Использование вредоносной компьютерной программой уязвимостей операционной системы – один из самых часто встречающихся способов получения неправомерного доступа к компьютеру пользователя. Так, в качестве наиболее яркого примера следует привести масштабную кибератаку с использованием программы-шифровальщика WannaCry, имевшей место в мае 2017 года. В результате атаки пострадали компьютеры в 74 странах мира, наибольший ущерб был причинен России, Индии, Украине, Тайваню. Указанная программа, используя уязвимости операционной системы Windows, проникала на компьютер, после чего, получив доступ к локальной сети (если компьютер был подключен к такой сети), заражала все остальные компьютеры той же сети, действуя по принципу программы-червя. Именно поэтому наибольший ущерб был причинен корпоративным организациям.

2. Проникновение вредоносной программы в компьютер при скачивании содержимого электронного письма, в котором такая программа заложена. Довольно часто пользователям приходит письма, в которых вложен или документ, содержащий вредоносную программу, или ссылка, переход по которой приведет к заражению компьютера. Важно отметить, что зачастую такие письма очень похожи на официальные (например, рассылка от государственных органов власти).

Так, Эксперты центра безопасности компании Positive Technologies зафиксировали группировку, организовавшую кибератаку на оборонно-промышленный комплекс России. Злоумышленники заражали компьютерные сети оборонных и промышленных предприятий, рассылая письма с вредоносным программным обеспечением: зараженные письма были отправлены с такими темами, как «компенсация военнослужащим за аренду

жилья» и «повышение зарплаты военнослужащим», а для рассылки использовались электронные адреса mo_mil@mail.ru и mo.belo@bk.ru.

«Главной задачей кампании SongXY, рассылавшей данные письма, был шпионаж, и используемое вредоносное программное обеспечение после попадания в корпоративную систему жертвы позволяло злоумышленникам не только скрытно следить за пользователями, но и удаленно контролировать зараженную систему», – говорится в исследовании Positive Technologies [10].

3. Осуществление физического доступа к компьютеру пользователя и загрузка в него вредоносного программного обеспечения.

Помимо использования различных компьютерных программ, для совершения преступлений в сфере компьютерной информации или с использованием компьютерных технологий применяются различные аппаратно-программные устройства [9, С. 44-47], которые во многом уникальны, поскольку создаются для решения конкретных задач. Среди них выделяются такие устройства, как:

1. Устройства для записи тех или иных действий пользователя на компьютере, которые могут включаться как внутрь корпуса, так и в разрыв кабеля клавиатуры, подключаемой к компьютеру. Иногда такие устройства маскируют под USB-Flash-накопитель.

2. Аппаратно-программные комплексы – сложные устройства, выполняющие работу сразу нескольких устройств. Например, в аспекте рассмотрения хищений денежных средств из банкоматов интерес представляют такие аппаратно-программные комплексы, как Black Box, которые подключают к механизму выдачи денег в банкомате посредством его установки в корпус банкомата. После установки управление банкоматом может осуществляться даже со смартфона.

Очевидно, что криминалистическая характеристика преступлений, связанных с применением компьютерных технологий, была бы неполной без рассмотрения тех особенностей проведения некоторых следственных

действий, которые присущи тактике и методике компьютерной криминалистики.

Первая и самая главная особенность проведения следственных действий при расследовании указанной категории преступлений заключается в том, что в них обязательно участие специалиста в соответствующей области знаний. При этом действия специалиста по получению доступа к компьютерной информации, ее извлечению надлежит протоколировать, поскольку в ходе дальнейшего расследования может появиться необходимость повторного получения доступа к той компьютерной системе, из которой была извлечена интересующая следствие информация.

Большое значение имеют вопросы фиксации изымаемой компьютерной информации в протоколе. Не представляет особой сложности отразить в протоколе следственного действия индивидуальные признаки flash-накопителя или иного устройства, содержащего необходимую следствию информацию, и изымаемого вместе с ней (например, такие признаки, как внешний вид носителя и его какие-либо характерные черты (надписи, наклейки), серийный номер устройства). Вместе с тем, нередки случаи, когда информация изымается непосредственно с работающего компьютера или с удаленного ресурса, поэтому определить, соответствует ли исследуемая компьютерная информация изъятой, очень трудно. В таких случаях проверка информации на идентичность возможна с помощью хэш-суммы (контрольной суммы) – запись о том или ином результате обработки информации, которая вычисляется по определенному алгоритму (например, алгоритм MD5, который записывает такой результат в виде 32-значной последовательности шестнадцатеричного кода). Такая последовательность может быть занесена в протокол следственного действия [3].

Важно рассмотреть некоторые особенности производства такого следственного действия, как осмотр места происшествия. Сложности связаны с осмотром содержимого компьютера – следует обратить внимание на наличие в нем специфического программного обеспечения (например, программ для

шифрования информации), криптоконтейнеров (зашифрованных данных, которые защищены от взлома и перехвата), а также следует снять копии содержимого жесткого диска. При этом жесткий диск компьютера изымается (при необходимости создается его физическая или логическая копия, если физическая копия не может быть создана). Также необходимо проверить осматриваемый компьютер на наличие активных сетевых подключений, при их наличии следует их отключить.

Такое следственное действие, как обыск, имея своей целью выявление следов совершенного преступления на компьютере подозреваемого, предполагает внезапность и оперативность проводимого мероприятия. Именно поэтому целесообразно пресечь попытки подозреваемых заблокировать или уничтожить информацию, хранящуюся на компьютерах, в том числе с использованием различных компьютерных устройств и программ. Также стоит проводить фотографирование экранов компьютеров с целью отслеживания отображаемого на экране.

Важно отметить, что при расследовании преступлений, связанных с применением компьютерных технологий, допускается большое количество ошибок, истинной природой который является не только формальная подготовка к проведению следственных действий (либо полное отсутствие такой подготовки), но и низкий уровень квалификации сотрудников правоохранительных органов (поскольку многие следователи и оперативные сотрудники банально не знают, что информация может быть уничтожена и простым выдергиванием силового кабеля из компьютера). На наш взгляд, неподготовленность сотрудников к расследованию подобных преступлений уже наносит серьезный ущерб в аспекте защиты прав и свобод человека и гражданина Российской Федерации, а также национальной и информационной безопасности в целом. Повышение квалификации работников правоохранительных органов (в том числе прокурорских работников и судей), формирование у них определенного уровня знаний и навыков должно иметь место и быть организовано в кратчайшие сроки. Соответственно, это

предполагает внесение изменений и в стандарты образования, по которым обучаются будущие кадры правоохранительных органов, и в программы, по которым идет переподготовка кадрового состава правоохранительных органов Российской Федерации. Организацию и проведение переподготовки следует возложить на организации, обладающие достаточной квалификацией в сфере обеспечения компьютерной безопасности. Например, на АО «Лаборатория Касперского» (которая уже проводит специализированные курсы по расследованию кибермошенничества и преступлений в сфере информационной безопасности, сотрудничая в этом с МВД России).

Таким образом, рассмотренные выше вопросы криминалистической характеристики преступлений, связанных с применением компьютерных технологий, представляют собой необходимую для осуществления расследования указанной категории преступлений совокупность знаний и навыков, которой современные сотрудники правоохранительных органов, к сожалению, не обладают. Вместе с тем, процесс цифровизации и информатизации человеческого общества ставит перед нами вопрос о необходимости формирования у сотрудников данной базы. Организация деятельности по соответствующей подготовке должна стать делом уже сегодняшнего дня, и усилия в этом должны прилагать все мы, как образовательные, так и правоохранительные организации (например, как это делает Московский городской суд [5]).

ЛИТЕРАТУРА:

1. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть I) // Вопросы кибербезопасности. 2013. № 1.
2. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

3. Минин А.Я. О специфике противодействия киберпреступности // Российский следователь. 2013. № 8.
4. Программа «Цифровая экономика Российской Федерации»: утв. распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р // Собрание законодательства РФ. 2017. № 32. Ст. 5138.
5. Сайт Московского городского суда. [Электронный ресурс]. URL: https://mos-gorsud.ru (дата обращения: 26.01.2019).
6. Состояние преступности в России: январь-ноябрь 2018 года // ФКУ «Главный информационно-аналитический центр» МВД России. М., 2018.
7. Тарасов А.М. Киберугрозы, прогнозы, предложения // Информационное право. 2014. № 3.
8. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.
9. Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации // Российский следователь. 2016. № 10.
10. Эксперты обнаружили атаку хакеров на военно-промышленный комплекс России // РБК – новости, акции, курсы валют. [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/08/02/2018/5a7c3ee29a79471c93ab30b3 (дата обращения: 26.01.2019).

REFERENCES:

1. Borodakiy Yu.V., Dobrodeev A.Yu., Butusov I.V. Cybersecurity as a major factor in national and international security of the XXI century (part I) // Cybersecurity questions. 2013. № 1.
2. The Doctrine of Information Security of the Russian Federation: app. by the Decree of the President of the Russian Federation. December 5, 2016, № 646 // The collection of the legislation of the Russian Federation. 2016. № 50. A. 7074.
3. Minin A.Ya. About the specifics of the cybercrime prevention // Russian investigator. 2013. № 8.

4. Program «Digital Economy of the Russian Federation»: app. by the Order of the Government of the Russian Federation. July 28, 2017, № 1632-p // The collection of the legislation of the Russian Federation. 2017. № 32. A. 5138.
5. The website of the Moscow City Court. [Electronic resource]. URL: https://mos-gorsud.ru (Access date: 26/01/2019).
6. State of crime in Russia: January-November 2018 // FCO «Main information and analytical center» of the Ministry of Internal Affairs of Russia. M., 2018.
7. Tarasov A.M. Cyberthreats, forecasts, proposals // Information law. 2014. № 3.
8. Criminal Code of the Russian Federation. June 13, 1996, № 63 // The collection of the legislation of the Russian Federation. 1996. № 25. A. 2954.
9. Chekunov I.G., Shumov R.N. The current state of cybercrime in the Russian Federation // Russian investigator. 2016. № 10.
10. Experts have discovered the attack of hackers on the military-industrial complex of Russia // RBC-news, stocks, exchange rates. [Electronic resource]. URL: https://www.rbc.ru/technology_and_media/08/02/2018/5a7c3ee29a79471c93ab30b3 (Access date: 26/01/2019).

Сотникова Валерия Владимировна
кандидат юридических наук
старший преподаватель кафедры уголовного права
Военный университет Министерства обороны Российской Федерации
111033, г. Москва, Волочаевская ул., д. ¾.
iris1806@yandex.ru

Бунин Кирилл Андреевич
курсант прокурорско-следственного факультета
Военный университет Министерства обороны Российской Федерации
111033, г. Москва, Волочаевская ул., д. ¾.
prokvp@mail.ru

Sotnikova Valeria Vladimirovna
Candidate of Law
Senior Lecturer at the Department of Criminal Law
Military University of the Defence Ministry of the Russian Federation
Volochaevskaya ul., d.¾, Moscow, Russia, 111033

Bunin Kirill Andreevich
Cadet of the Prosecution and Investigation Faculty
Military University of the Ministry of Defence of the Russian Federation
Volochaevskaya ul., d.¾, Moscow, Russia, 111033

12.00.12 – Криминалистика, судебно-экспертная деятельность, оперативно-розыскная деятельность