Научная статья
https://doi.org/10.24412/2658-7335-2024-4-15
**УДК 343.1**

Attribution
cc by

# «ЭЛЕКТРОННЫЕ СЛЕДЫ», ИССЛЕДУЕМЫЕ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ

***Ханинёва О.В.***
*Краснодарский университет МВД России*

***Аннотация****. В статье автором рассматриваются понятия «интернет-сайт», «хостинг», «провайдер», «cookie-файлы», особенности содержащейся в них информации, необходимой для выявления, раскрытия и расследования преступлений, связанных с использованием информационно-телекоммуникационных технологий. Целью исследования является изучение информации, размещенной на данных ресурсах, а также - особенности анализа полученных сведений и использования их в процессе доказывания по уголовным делам, возбужденным по фактам мошенничеств, совершенных с использованием сети Интернет. Проведен анализ работы следственных и оперативных подразделений ряда субъектов Российской Федерации, задействованных в предупреждении, раскрытии и расследований вышеуказанной категории преступлений, в результате которого, автором предлагается метод изучения и анализа ряда факторов, влияющих на своевременное и качественное раскрытие преступлений и установления лиц, их совершивших.*

***Ключевые слова:*** *мошенничество, взаимодействие, расследование, правоохранительные органы, интернет-сайт, информация, анализ.*

# "ELECTRONIC TRACES" INVESTIGATED IN THE INVESTIGATION OF FRAUD COMMITTED USING IT TECHNOLOGIES

***Olga V. Khanineva***
*Krasnodar University of the Ministry of Internal Affairs of Russia*

***Abstract.*** *In the article, the author examines the concepts of an Internet site, the features of the information contained therein necessary for the identification, disclosure and investigation of crimes related to the use of information and telecommunications technologies. The purpose of the study is to study the information posted on these resources, as well as the specifics of analyzing the information received and using it in the process of proving criminal cases initiated on the facts of fraud committed using the Internet. The analysis of the work of investigative and operational units of a number of subjects of the Russian Federation involved in the prevention, disclosure and investigation of the above-mentioned category of crimes is carried out. As a result, the author proposes a method for studying and analyzing a number of factors affecting the timely and high-quality disclosure of crimes and the identification of their perpetrators.*

***Keywords****: fraud, interaction, investigation, law enforcement agencies, website, information, analysis.*

**Введение.**

Видите ли, Вы свое будущее без информационно-телекоммуникационной сети Интернет? Думаю, ответ очевиден… Предполагаю, что в мыслях даже промелькнуло желание воспользоваться в будущем даже чем-то большим, чем предлагает в настоящее время Интернет, чем-то сверхскоростным, позволяющим совершать нереальные в настоящее время действия и получать новые возможности и продукты.

В этой связи, мы можем наблюдать увеличение количества пользователей сети с каждым днем. Лиц - из разных возрастных и социальных групп населения планеты.

Всемирная паутина используется не только для поиска информации и коммуникации, но и для ведения электронной коммерческой деятельности, здравоохранения, обучения и т.п. Поэтому этот информационный ресурс остается подходящей средой для развития кибер-преступности, и, с появлением новых научно-технических достижений, возникают все

© Ханинёва О.В., 2024

новые и новые способы совершения преступлений. Данная проблема носит глобальный характер.

Однако не стоит забывать о том, что в системе правоохранительных органов Российской Федерации (далее - РФ), в частности, в Министерстве внутренних дел РФ, в 2022 году, по указанию Президента В.В. Путина, созданы специализированные подразделения и отделы по борьбе с мошенничествами, совершенными с использованием информационно-телекоммуникационных технологий, входящих в составы следственных и оперативных подразделений управления уголовного розыска субъектов РФ. А для борьбы с иными, так называемыми кибер-преступлениями, - управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК)[1].

**Обсуждение.**

Говоря о профессионализме должностных лиц, призванных противодействовать рассматриваемому виду преступлений, необходимо отметить важность понимания той специфической информации, с которой приходится сталкиваться.

Для работы по выявлению, раскрытию и расследованию вышеуказанных преступлений, совершенных с использованием IT-технологий, сотрудники заинтересованных подразделений, особенно вновь прибывшие на данную «линию», должны постоянно самообразовываться, изучать и анализировать особенности используемого преступниками информационного поля, средств и способов совершения мошенничеств, сокрытия следов их совершения, реализации похищенного имущества, порядка обнаружения и сбора доказательной базы для привлечения мошенников к уголовной ответственности, и возмещению причиненного ущерба потерпевшим.

Тем не менее, существует мнение о том, что нет нераскрываемых преступлений, и это, как в большинстве своем показывает практика, - правда. Дело в том, что интернет-пространство, также, как и соединения по мобильной связи, или движение денежных средств по счетам, будь они виртуальные или «привычные», оставляют в некоем специфическом данным областям поле, следы.

В работе по выявлению, раскрытию, расследованию и предупреждению таких мошенничеств, главное понимать - как остаются такие следы, уметь их обнаруживать и анализировать.

Автором данной статьи будут перечислены некоторые из основных средств и «полей» в которых преступники могут оставлять, так называемые «информационные» следы, включая данные:

- о своей личности (анкетные данные, серии и номера документов, удостоверяющих личность, в том числе содержащих фото, адреса регистрации, дату рождения и т.п.);
- об используемых средствах связи (марка, модель, IMEI мобильных устройств),
- о банковских счетах, картах, номерах телефонов, ip-адресах и иной информации, получив которую возможно установление лиц, их совершивших, их задержание, установление места нахождения похищенного имущества и принятие мер к его изъятию.

Итак, интернет-сайт - это совокупность страниц, объединенных одной тематикой, дизайном, а также взаимосвязанной системой ссылок. Каждая страница может содержать в себе видео- и фотоизображения, аудиофайлы, рекламные блоки и много другое, аналогичную информацию таким образом может в себе содержать и интернет-сайт [2, с. *267-268*].

Часто встречается такая схема мошеннических действий, при которой злоумышленник создает сайты в виде интернет-магазинов, и похищает денежные средства под видом продажи отдельных товаров.

Реализуя свой преступный умысел, направленный на хищение чужого имущества, путем обмана и злоупотребления доверием, он указывает заведомо ложную, не соответствующую действительности информацию. Товары выставляются в объявлениях по цене, как правило значительно дешевле рыночной стоимости. Для подтверждения добросовестности продавца, мошенником размещаются ложные положительные отзывы «предыдущих покупателей».

Для обмана, в части малого остатка товара и быстрой его раскупаемости, а значит - «нужности» клиентам и хорошего качества – преступниками делаются пометки «срочная продажа», «распродажа», «ликвидация товара» и т.п., которые привлекают людей скидками в объявлениях. Все это «заманивает» людей, провоцирует психику человека обратить свое внимание на данного продавца и товар, и побуждает вступить с ним в диалог для приобретения товара или услуги.

© Ханинёва О.В., 2024

Сотрудникам следственных и оперативных подразделений, чтобы получить информацию в отношении лица, создавшего мошеннический интернет-сайт следует знать, что для работоспособности сайта необходимо выполнить два условия: во-первых - зарегистрировать доменное имя и, во-вторых - арендовать хостинг.

Домен — это название сайта, его адрес в сети интернет. Домен в интернете — это то, что мы вводим в адресную строку браузера, например, avito.ru или mail.ru. [3]

Само доменное имя, также, как и хостинг, регистрируется у специальных организаций, и требует внесения пользователем регулярной абонентской платы. Для регистрации лицу необходимо передать в распоряжение организации личные документы, а для последнего - естественно будут использоваться дистанционные способы оплаты, то есть некие финансовые транзакции, оставляющие все те же искомые нами следы.

Таким образом, учитывая то, что при таком взаимодействии предполагается контакт, оставляющий те или иные следы, следователи и оперативники могут установить этого пользователя.

При раскрытии и расследовании мошенничеств необходимо в обязательном порядке направить соответствующий запрос в организацию – регистратор, по итогам исполнения, которого возможно получить информацию, аналогичную информации, предоставляемой хостинг-провайдером.

Хостинг — это услуга по хранению сайта. Она нужна, чтобы пользователи интернета могли посещать его круглосуточно. Компания, которая предоставляет эту услугу, называется хостером, или хостинг-провайдером. Понятие происходит от английского слова host, что значит «хозяин, принимающий гостей» [4].

Чтобы арендовать хостинг, необходимо составить соответствующий договор и оплатить предоставляемые услуги, что также оставит те самые, «нужные» следы преступной деятельности, для последующего изучения и раскрытия преступления.

Помимо этого, к ранее обозначенным документам (личным и денежным) прибавится образец электронной или скан подписи преступника, так как для аренды хостинга предполагаются только договорные официальные правоотношения.

Расследуя уголовные дела о мошенничествах, совершенных в сети Интернет и направив запрос хостинг-провайдеру, возможно получить информацию:

- о лице, осуществившем аренду;

- используемые им банковские карты и счета для оплаты аренды;

- IP-адреса, электронные почтовые ящики, абонентские номера и другую информацию, имеющую значение для дела.

Хостинг-провайдеров и регистраторов доменных имен огромное множество, поэтому для верного направления запроса необходимо правильно получать первоначальные сведения по сайту, или WHOIS-сведения.

Итак, установить регистратора доменного имени и хостинг провайдера мошеннического сайта можно самостоятельно следователю/оперуполномоченному, с использованием открытых источников в сети Интернет, например, такого как www.reg.ru.

Теперь рассмотрим алгоритм действий: при посещении страницы вышеуказанного сайта мы увидим поисковую строку, в которую необходимо ввести доменное имя сайта мошенника, и, путем нажатия кнопки «Whois» - получить необходимую информацию. В результате, мы получим ответ в виде текста, в содержании которого интерес представляют следующие две графы:

Первая строка - «Registrar» (или «регистратор»), которая обозначает данные организации, у которой было зарегистрировано доменное имя. В случае с рассмотренным в примером, с сайтом www.psou.site - это ООО «Регистратор доменных имен Рег.Ру». Указанному юридическому лицу и следует направлять соответствующий запрос. Юридический адрес, адрес электронной почты или для направлений запросов, возможно установить самостоятельно, также в сети Интернет, связавшись с контактным лицом.

И вторая строка - «Name Server» (или «DNS сервер»), которая содержит название сайта организации, предоставляющей хостинг для сайта. Для рассматриваемого нами сайта это все тот же ООО «Регистратор доменных имен Рег.Ру (REG.RU)».

Таким образом, мы установили, что доменное имя сайта www.psou.site было зарегистрировано у организации ООО «Рег.Ру», а также, что у данной организации был арендован хостинг для размещения сайта.

Кроме этого, следователям и оперуполномоченным, противодействующим «электронным» или «дистанционным» мошенничествам, необхо-

© Ханинёва О.В., 2024

димо понимать и то, что множество интернет-сайтов хранят информацию о своих пользователях, то есть «остаются следы».

Причем, они могут носить и бытовой характер (например, обучение на какой-то платформе с целью получения дополнительного образования; приобретение подарка для семьи; сдача анализов в клинике и т.п.), которые позволят идентифицировать преступника при каких-то сомнениях или показаниях, о том, что не он, а кто-то от его имени совершил преступления.

А также, эти следы могут свидетельствовать о преступной деятельности, с которыми необходимо работать для полноты и объективности расследования. Сбор и анализ такой информации происходит посредством Cookie-файлов.

Cookie-файл - это фрагмент данных, который интернет-сайт передает в интернет-браузер (Google, Chrome, Mozilla, и т.п.) своего нового пользователя, чтобы идентифицировать его.

При следующих посещениях данного сайта, информация о подключившемся пользователе будет увеличиваться, при этом сайт самостоятельно запомнит:

- предпочитаемый вами язык;
- последние просматриваемые вами страницы;
- ваши логины и пароли - именно благодаря Cookie - файлам вам не нужно каждый раз заново вводить пароли в социальных сетях и других сайтах;
- историю ваших посещений (данная функция Cookie как раз и имеет для следователя или оперуполномоченного ключевое значение). [5. *С. 135-139*]

Ведь логины и пароли - это идентификаторы, которые знает только пользователь, а это лишнее косвенное доказательство по дела. История последних посещений анализируется относительно даты и времени совершения преступления, подготовки к его совершению, либо распоряжению похищенным или сокрытие следов преступной деятельности, что также имеет доказательственное значение в целом, и создает ту самую объективность расследования преступлений.

Важной особенностью Cookie-файлов является их неизменность - мошенник сколько угодно раз может менять свой IP-адрес через VPN, проходить регистрацию с разных абонентских номеров, но сайт все равно поймет, что все это время к нему подключается один и тот же пользователь - то есть, используется браузер одного и того же персонального компьютера [6].

**Результаты.**

Каким же образом полученная информация может помочь при расследовании уголовного дела?

Предлагаем ответ на данный вопрос на примере мошеннической схемы через сайт «Авито»: Фигурант «А» размещает на сайте «Авито» объявления о продаже лодочных моторов «Yamaha», при этом, перед входом на сайт подключается к VPN (сегодня есть много доступных бесплатных приложений, которые можно самостоятельно установить на мобильный телефон с помощью «Google Play» и иных подобных источников), чтобы его реальный IP-адрес оставался неизвестным.

По одному из таких объявлений ему звонит потенциальный потерпевший, и после переговоров, с целью реализации своего желания совершить покупку лодочного мотора, вносит предоплату на счет указанной «продавцом» банковской карты или абонентского номера, тем самым став жертвой мошеннических действий.

Начиная работу по установлению преступника, исходя из показаний заявителя о сайте, на котором состоялась «купля-продажа», зная ник нейм «продавца», следователю или оперуполномоченному следует направить запрос администрации сайта «Авито» в (ООО «КЕХеКоммерц») адрес: 125047, г. Москва, ул. Лесная, д.7, e-mail: compliance@avito.ru, о предоставлении информации о лице, разместившем данное объявление.

Помимо этого, необходимо провести анализ Cookie - файлов мошенника, с целью установления всех объявлений, которые размещались с браузера данного персонального компьютера, а также информации обо всех IP-адресах, использованных для посещения сайта. При этом особое внимание необходимо обращать в том числе на запросы пользователя о картинках на которых изображаются те самые лодочные моторы «Yamaha» различных модификаций, цветов корпуса, года изготовления и т.п. отличительных черт, которые преступник возможно выкладывал в своих объявлениях.

Это и будет значимая информация для расследуемого уголовного дела, так как по обнаруженным сведениям оперуполномоченный может проанализировать мошенничества, ранее совершенные и зарегистрированные в оперативной сводке по субъекту в целом.

Далее, направить необходимые запросы по иным субъектам РФ, с целью проведения ана-

© Ханинёва О.В., 2024

лиза преступлений по схожим данным «проданного объекта». Это делается для обмена информацией, сбора уже установленных ранее данных о лице, что способствует организации взаимодействия подразделений правоохранительных органов других субъектов РФ для глобальной работы по задержанию преступника, возбуждению уголовных дел и их соединению, при наличии оснований, предусмотренных УПК РФ.

**Заключение.**

Подводя итоги вопросов, рассмотренных в статье, и в результате проведенного анализа информации, автор приходит к выводу о том, что имея изначальную информацию лишь по одному объявлению, размещенному в сети Интернет на каком-либо сайте, возможно получить сведения по всем объявлениям, размещенным указанным лицом, принять меры к его розыску и задержанию, а также максимально возможному возмещению причиненного потерпевшим ущерба.

В любом случае, при работе по выявлению, раскрытию и расследованию мошенничеств, совершенных с использованием средств связи и сети Интернет, сотрудникам правоохранительных органов необходимо обращать внимание на все получаемые данные из различных источников. Своевременно уметь их анализировать и продолжать направлять запросы для получения новой информации, имеющей значение для дела, так как в виртуальной сети преступники оставляют также много следов своей преступной деятельности, как и в реальности. Однако современным сотрудникам полиции необходимо иметь навыки для ее обнаружения и использования, а также постоянно их совершенствовать.

**Конфликт интересов**

Не указан.

**Рецензия**

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

**Conflict of Interest**

None declared.

**Review**

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

***Литература:***

1. *https://www.kommersant.ru/doc/5592758. Дата обращения 14.03.2024*

2. *Бондарь А.Г., Теунаев А.С.У. Криминальный аспект использования отдельных видов инфокоммуникационных инструментов. Евразийский юридический журнал. 2022. № 2 (165). С. 267-268 http://elibrary.ru/item.asp?id=48277649 (дата обращения 16.03.2024)*

3. *https://www.nic.ru/help/chto-takoe-domennoe-imya-domen_10984.html (дата обращения 19.03.2024)*

4. *https://skillbox.ru/media/marketing/chto-takoe-khosting-dlya-sayta-i-kak-ego-vybrat/ (дата обращения 19.03.2024)*

5. *Гришин А.В., Ломовская А.В. Роль оперативно-розыскной деятельности при выявлении и раскрытии преступлений в сфере компьютерной информации. Сборник статей XIX Международной научно-практической конференции, посвященной памяти советского и российского ученого-криминалиста Вениамина Константиновича Гавло, доктора юридических наук, профессора, заслуженного деятеля науки РФ, заслуженного юриста РФ. Барнаул, 2021. С. 135-139. http://elibrary.ru/item.asp?id=47304569 (дата обращения 19.03.2024)*

6. *Проваторов И.О. СООКІЕ-ФАЙЛЫ КАК СРЕДСТВО ДЕАНОНИМИЗАЦИИ МОШЕННИКА В СЕТИ ИНТЕРНЕТ. В сборнике: АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ. Сборник научных статей международных научно-практических конференций. Санкт-Петербург, 2022. С. 158-161. http://elibrary.ru/item.asp?id=49495284 (дата обращения 01.10.2024)*

***References:***

*1. https://www.kommersant.ru/doc/5592758. Access date 03/14/2024*

*2. Bondar A.G., Teunaev A.S.U. The criminal aspect of the use of certain types of infocommunication tools. Eurasian legal journal. 2022. No. 2 (165). P. 267-268 http://elibrary.ru/item.asp?id=48277649 (access date 03/16/2024)*

*3.https://www.nic.ru/help/chto-takoe-domennoe-imya-domen_10984.html (accessed March 19, 2024)*

© Ханинёва О.В., 2024

*4. https://skillbox.ru/media/marketing/chto-takoe-khosting-dlya-sayta-i-kak-ego-vybrat/ (date accessed 03/19/2024)*

*5. Grishin A.V., Lomovskaya A.V. The role of operational-search activities in identifying and solving crimes in the field of computer information. Collection of articles of the 19th International Scientific and Practical Conference dedicated to the memory of the Soviet and Russian forensic scientist Veniamin Konstantinovich Gavlo, Doctor of Law, Professor, Honored Scientist of the Russian Federation, Honored Lawyer of the Russian Federation. Barnaul, 2021. pp. 135-139. http://elibrary.ru/item.asp?id=47304569 (date accessed 03/19/2024)*

*6. Provatorov I.O. COOKIES AS A MEANS OF DEANONYMIZING A FRAUDSTER ON THE INTERNET. In the collection: CURRENT PROBLEMS OF PRELIMINARY INVESTIGATION. Collection of scientific articles of international scientific and practical conferences. St. Petersburg, 2022. pp. 158-161. http://elibrary.ru/item.asp?id=49495284 (accessed 01.10.2024)*

**Информация об авторе:**
**Ханинева Ольга Владимировна**, старший преподаватель кафедры уголовного процесса, Краснодарский университет МВД России, hanineva83@mail.ru
**Olga V. Khanineva**, Senior Lecturer at the Department of Criminal Procedur, Krasnodar University of the Ministry of Internal Affairs of Russia.

© Ханинёва О.В., 2024