Методические рекомендации для частных следователей по идентификации авторов анонимных аккаунтов и электронной переписки

Криони Александр Евгеньевич, *детектив, руководитель Кабинета детектива А.Е. Криони. Москва, ул. Народного Ополчения, д. 34, стр. 1, оф. 138, alex@krioni.com*

Поскольку электронная переписка часто является единственным связующим звеном между потерпевшим и предполагаемым преступником, то идентификация владельца e-mail остается наиболее верным способом для оперативного достижения целей частного расследования. Эта статья является методическим руководством для частных сыщиков, которые регулярно сталкиваются с необходимостью установить личность злоумышленника по его электронному адресу.

Ключевые слова: детектив, аноним, расследование, деятельность частного сыщика.

Recommended practice for private detectives seeking to identify owners of anonymous accounts and email addresses

Krioni Alexander Evgenevich, *private detective A.E. Krioni Detective Bureau. Russia, Moscow, Narodnogo Opolcheniya Street, bld. 34, c. 1, office 138*

Since electronic correspondence is often the only connecting link between a victim and an alleged criminal, identifying the owner of the email address remains the most reliable method for quickly achieving the objective of a private investigation. This article lays out recommended practice for private detectives who are regularly required to determine the identity of a lawbreaker from his email address.

Keywords: detective, private investigator activity, email, anonymous, identify.

Основания. Частное расследование по идентификации владельца e-mail осуществляется в соответствии с Законом РФ «О частной детективной и охранной деятельности в Российской Федерации» [1] .

Данный вид расследования достаточно сложен, так как типовых или рекомендованных форм планирования проведения расследования в этих случаях нет. Каждый детектив должен самостоятельно выделить приоритеты и направления сбора сведений, учитывая требования своего национального законодательства.

На первый взгляд почти открытый характер ведения электронной переписки не представляет трудностей для установлении личности отправителя e-mail. Однако это – заблуждение. К совершению таких посягательств, как интернет-мошенничество, продажа контрафакта, преступники тщательно готовятся: подбирают анонимный почтовый хостинг, ищут публичную точку доступа, используют

специальные аппаратные средства для выхода в сеть Интернет, придумывают замысловатый ник или указывают в подписи сокращенное имя. Участники преступной группы стремятся действовать инкогнито, замаскированно, осторожно и без суеты. С проявлением подозрительности в действиях потерпевшего быстро теряют к нему интерес.

При рекламировании услуг преступники используют вымышленные имена, выдавая себя за добросовестных коммерсантов, менеджеров среднего звена известных коммерческих организаций, государственных корпораций. Переписку ведут грамотно и по существу, со знанием дела.

Мероприятия по планированию идентификации. Обычно расследование начинается с получения e-mail из рук пострадавшего или по инициативе адвоката потерпевшей стороны, что характерно для дел, требующих оперативного, почти без промедлении, вмешательства.

Во всех случаях план расследования должен предусматривать неотложное производство для раскрытия личности преступника по «горячим следам», тесно увязанный и согласованный с планом первоначальных частно-розыскных мероприятий. Планируются опросы потерпевших, обзор и анализ веб-сайтов, на которых опубликованы объявления с изучаемым e-mail.

В оперативном плане предусматриваются мероприятия по обследованию сайтов, интернет-поиску на профильных бизнес-площадках, где преступники могли оставить о себе контактную информацию. В то же время при расследовании следует учитывать и версию о сокрытии заказчиком сведений, связанных с неудачными самостоятельными попытками установить личность злоумышленника.

Первоначальные частно-розыскные действия по делам как о мошенничестве, так и о незаконном использовании товарных знаков направлены на идентификацию владельца e-mail.

При исследовании e-mail выясняются:

- на каком сайте, когда и при каких обстоятельствах потерпевший нашел e-mail злоумышленника;
- сколько человек участвовало в переписке, их имена, как и от какой организации они представлялись;
- оставляли ли преступники другие способы для связи с ними;
- какие способы оплаты предлагали преступники потерпевшему;
- высылали ли преступники какие-либо документы во вложении к письму;
- с какого IP отправлялись письма; страна, город, дата и время отправления;
- вид домена, в котором зарегистрирован e-mail (публичный, частный);
- логин владельца e-mail;
- действующий или недействующий e-mail;
- каковы последствия противоправных действий для потерпевшего.

Располагая исходными данными, детектив производит осмотр сайта с целью обнаружить следы преступления и сопоставить свидетельства потерпевшего с обстановкой события. При расследовании случаев контрафакта или совершения мошенничества к моменту начала расследования, как правило, сайт злоумышленника доступен только через сервис WayBackMachin (waw.archive.org/web), а e-mail его владельцем удален. Исходя из этих особенностей частному детективу следует уметь восстанавливать следы удаленных с сайта преступника публикаций. При осмотре сайта, как и при опросе потерпевшего, проверяется версия о неудачном самостоятельном расследовании стороной потерпевшего.

Исследование e-mail следует начинать с обстоятельного обзора поисковых машин: Яндекс, Google, Hotmail, Yahoo. Преступник может указать свой e-mail

как контактный при регистрации доменного имени, в подписи к сообщениям на форумах, на досках объявлении или в личных комментариях.

При исследовании форумов необходимо обратить внимание на информацию, которую в открытом доступе оставил владелец e-mail. Публичность предполагает публикацию персональных данных владельца аккаунта в форумах, блогах, других средствах массовой информации, доступных как зарегистрированным, так и незарегистрированным пользователям. Данные пользователей форумов являются открытыми к публикации заинтересованных лиц, которые могут знакомиться с персональными данными пользователя и статистикой его сообщений например, пройдя обычную процедуру регистрации. Особое внимание следует уделить сведениям, доступным через личный кабинет пользователя e-mail (ник, имя, возраст, пол, город, интересы, количество оставленных сообщений, дополнительный e-mail, номер телефона, Skype, Icq, дата регистрации и дата последнего оставленного сообщения, а также графическое представление пользователя – аватар).

Если есть основания, что преступник нигде более не использовал e-mail, то последующие мероприятия направлены на детальное изучение логина (все, что до знака «@»). Злоумышленник, придумывая логин, может использовать элементы своего имени, фамилии или отчества, год рождения (чаще всего это две последние цифры).

Путем пробной регистрации проводится поиск в других наиболее популярных почтовых сервисах (mail.ru, yandex.ru, gmail.com, yahoo.com, hotmail.com), а также в социальных сетях и интернет-мессенджерах (Facebook, Twitter, Skype, Мой Мир@Mail.ru, Vk, Ok). Данные логина во вновь обнаруженном e-mail или аккаунте должны соответствовать логину исходного почтового ящика. В случае обнаружения аккаунта или e-mail с видоизмененным логином, например добавлены тире, цифра или точка, следует отказаться от его дальнейшего исследования и вернуться к изначальному варианту написания.

Если есть основания полагать, что обнаруженный e-mail имеет точно такой же логин, частный сыщик может воспользоваться сервисом восстановления пароля к новому аккаунту. Дело в том, что при попытке восстановить пароль доступа к личному кабинету почтовый сервис предлагает ответить на вопрос, который дополнительно характеризует пользователя. Иногда злоумышленник для восстановления пароля выбирает вариант отправки сообщения на дополнительный e-mail или мобильный телефон.

Несмотря на то что информация о номере телефона или e-mail отражена неполностью, в ряде случаев данное обстоятельство дает положительный эффект. Например, если для восстановления пароля почтовый сервис (обычно gmail.com) предлагает отправить письмо на другой почтовый ящик пользователя, то при внимательном сопоставлении можно обнаружить сходство с искомым электронным ящиком и, таким образом, удостовериться в том, что злоумышленник пользуется как минимум двумя почтовыми ящиками.

Не менее важным вопросом идентификации является соблюдение конфиденциальности и требований нормативных актов к процедурам частного расследования. Так, во избежание уведомления владельца e-mail о подозрении на попытку несанкционированного доступа к его аккаунту не следует пытаться использовать службу восстановления пароля более одного-двух раз. Вот почему при осуществлении частно-розыскных действий в сети Интернет детективу необходимо взять в привычку сопровождать каждое свое действие сохранением снимка экрана.

При этом следует учитывать, что логин может быть абсолютно вымышленным и не иметь отношения к действительному имени владельца e-mail. Поэтому на заключительном этапе расследования детектив должен попробовать установить контакт с предполагаемым владельцем электронного ящика для получения достаточной уверенности в том, что собранные им сведения не содержат существенных ошибок.

Обнаруженные частным сыщиком сведения о владельце e-mail подразделяются на те, которые, скорее всего, имеют отношение к делу (прямые), и те, которые к делу имеют отношение меньше всего (косвенные). При написании отчета детективом сведения о прямых фактах должны быть учтены следующим образом:

– если детектив пришел к выводу, что обнаруженные сведения имеют прямое отношение к автору e-mail, то детектив должен подготовить отчет с обоснованием достоверности вывода;
– если из-за недостатка информации или недостаточной собственной квалификации детектив не смог установить личность владельца e-mail, то он должен подготовить отчет, но может отказаться делать выводы по расследованию.

Типичными нарушениями, выявляемыми в ходе расследования по идентификации владельца e-mail являются:

– несоответствие отдельных мероприятий детектива требованиям действующих нормативных актов;
– использование форм и методов сбора информации в ущерб конфиденциальности;
– отсутствие в отчете причинно-следственной связи свидетельств идентификации.

Литература

1. Закон РФ от 11.01.1992 № 2487-1 «О частной охранной и детективной деятельности в Российской Федерации» // Российская газета. – 1992. – Апр.