УДК 343.982:004.056.53 https://doi.org/10.24158/pep.2018.6.15

Швец Сергей Владимирович

**доктор юридических наук, доцент,
профессор кафедры криминалистики
Кубанского государственного аграрного
университета имени И.Т. Трубилина**

Павлюков Виталий Владимирович

**соискатель кафедры криминалистики
Кубанского государственного аграрного
университета имени И.Т. Трубилина**

ПРЕОДОЛЕНИЕ СРЕДСТВ КОМПЬЮТЕРНОЙ ЗАЩИТЫ КАК НЕОБХОДИМЫЙ СПОСОБ РЕАЛИЗАЦИИ ОПЕРАТИВНО-РАЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Аннотация:
В статье исследуются вопросы организационно-технического обеспечения получения оперативно значимой компьютерной информации путем преодоления средств ее защиты. Особое внимание уделяется характеристике получения компьютерной информации в качестве самостоятельного оперативно-разыскного мероприятия. Авторами рассматриваются примеры и способы получения компьютерной информации о противоправной деятельности как на компьютерных устройствах при наличии физического доступа, так и удаленно при помощи компьютерной сети. Интерес представляют примеры открытой судебной практики Российской Федерации, связанной с получением компьютерной информации. Показаны как практические, так и законодательные пути получения компьютерной информации в зарубежных странах. Ученые приходят к выводу, что на современном этапе развития информационных технологий не остается шансов оперативно получить компьютерную информацию без преодоления компьютерной защиты, поэтому закономерно и обоснованно предлагается законодательное закрепление подобных действий.

Ключевые слова:
компьютерная защита, оперативно-разыскное мероприятие, получение компьютерной информации, взлом, хакер, киберпреступность.

Shvets Sergey Vladimirovich

**LL.D, Professor,
Criminalistics Department,
Kuban State Agrarian University**

Pavlyukov Vitaly Vladimirovich

**External PhD student,
Criminalistics Department,
Kuban State Agrarian University**

BYPASSING COMPUTER SECURITY AS A NECESSARY WAY TO ACQUIRE COMPUTER INFORMATION WITHIN SEARCH ACTIVITIES

Summary:
The research considers the logistical issues of acquiring promptly relevant computer information bypassing the security system. The emphasis is placed on the aspects of getting computer information as an individual search activity. The authors present the case studies and ways of receiving computer information on illegal activity both from computer devices when one has a direct access and remotely through a network. Russian open court practice in this regard is of particular interest. Both practical and legal ways of acquiring computer information in foreign countries are considered. The researchers conclude that, at the present stage of the IT development, there is no chance to get computer information in a proper time without bypassing the computer security, so it is natural and reasonable to legislate such actions.

Keywords:
computer security, search activity, acquiring computer information, hacking, hacker, cybercrime.

Достижения в области информационных технологий существенно расширили и облегчили доступ человечества к различным информационным ресурсам, предоставив в распоряжение пользователей надежно защищенные способы обработки, хранения, систематизации и передачи компьютерной информации, позволив использовать последнюю в различных целях, в том числе и преступных.

Решение задач, связанных с получением зашифрованных массивов данных подразделениями органов внутренних дел, имеющих значение в процессе расследования, становится одним из важнейших ответов современной преступности. Это также обусловлено тем, что совершаемые преступления все чаще реализуются при помощи компьютерных технологий, где ухищрения, к которым прибегают злоумышленники в процессе использования компьютерной информации, постоянно видоизменяются и совершенствуются.

С целью получения сведений о противоправной деятельности, реализуемой при помощи компьютерной информации, были введены некоторые дополнения в законодательные акты, например Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». В частности, статья 6 федерального закона «Об оперативно-разыскной деятельности» была дополнена оперативно-разыскным мероприятием «получение компьютерной информации» [1].

По этому поводу С.В. Баженов, ссылаясь на руководство ФСБ России, в ведомственных разъяснениях к вышеуказанному закону полагает, что мероприятие «получение компьютерной информации» будет проводиться по решению суда соответствующими оперативно-техническими подразделениями и позволит осуществлять копирование компьютерной информации, ее изъятие с жестких дисков сетевых компьютеров или серверов в информационно-телекоммуникационной сети Интернет, в том числе из облачных хранилищ, т. е. сводит его к получению информации путем удаленного доступа к компьютеру или серверу в сети Интернет [2, с. 31].

Несмотря на указанное разъяснение, «получение компьютерной информации» стало и дальше отождествляться с такими оперативно-разыскными мероприятиями (далее – ОРМ), как снятие информации с технических каналов связи, прослушивание телефонных переговоров и т. д. [3, с. 179]. На наш взгляд, это недостаточно корректно, что вызывает необходимость определения места и роли получения компьютерной информации среди остальных ОРМ.

Прежде всего стоит отметить, что получение компьютерной информации не следует путать с таким оперативно-разыскным мероприятием, как снятие информации с каналов связи. Согласно ст. 8 федерального закона «Об оперативно-разыскной деятельности», снятие информации с технических каналов связи допускается на основании судебного решения и при наличии ограниченного перечня оснований, указанных в этой статье [4]. Комментарий к закону «Об оперативно-разыскной деятельности» разъясняет, что «снятие информации с технических каналов связи» определяется как негласный контроль, заключающийся в совокупности действий по получению оперативно значимых сведений, их фиксации путем съема специальными техническими средствами электромагнитных и других физических полей, возникающих при передаче информации по сетям электронной связи, в работе компьютерной сети, баз данных, телекоммуникационных систем [5]. Необходимо заметить, что такое мероприятие, как снятие информации с технических каналов связи, является длительным по времени и не всегда дает положительный результат.

По этому поводу Д.В. Кузченко и Е.В. Кушпель указывают, что обмен письмами как информационными сообщениями подразумевает разрыв во времени между передачей сообщения и получением его лицом, которому такое сообщение предназначено, и воспринимается через орган зрения. Именно разрыв во времени позволяет наложить арест на носитель информации, произвести его осмотр и выемку, что невозможно при непосредственном обмене речевыми сообщениями. Компьютерные технологии информационного обмена совмещают в себе особенности «привычных» видов коммуникации. Сообщения электронной почты, как правило, находятся на сервере до того момента, пока пользователь не получит их. После этого такие сообщения удаляются [6, с. 40].

Исходя из сказанного, стоит также обозначить, что снятие информации с технических каналов связи подразумевает перехват данных, которые передаются по компьютерным сетям, где, в отличие от привычной передачи бумажного письма, цифровое сообщение передается за доли секунд и зачастую является зашифрованным, ведь сейчас практически каждый современный протокол передачи данных обладает криптографической защитой. Также нужно знать место, откуда будет происходить отправка данных, а это может быть как домашний провайдер, так и мобильный телефон, что делает практически невозможным осуществление такого ОРМ, как «снятие информации с технических каналов связи».

До настоящего времени остается нерешенным вопрос получения компьютерной информации, передаваемой, например, посредством получившей широкую популярность системы IP-телефонии Skype. Это обусловлено как техническими трудностями классификации и фильтрации трафика Skype, так и сложностями дешифрации информации, передаваемой пользователями. Другим примером проприетарного программного продукта является еще одно известное программное обеспечение TeamViewer, предназначенное для удаленного управления компьютером [7, с. 29]. Обоснованно возникает необходимость оперативно получать компьютерную информацию путем преодоления компьютерной защиты. Однако вышеобозначенное указывает, что новое ОРМ «получение компьютерной информации», равно как и другие ОРМ, связанные с использованием компьютерной информации, не предоставляет такую возможность.

Зарубежный исследователь Г. Браун, рассматривая проблему получения компьютерной информации, утверждает, что Россия применяет стратегию использования хакеров и их навыков.

Однако такие суждения основываются лишь на том, что Правительство Российской Федерации позволяет гражданам своей страны практиковать в своей повседневной деятельности такие киберинструменты, посредством которых можно получать несанкционированный доступ к компьютерной информации.

Автор акцентирует внимание на том, что киберпреступникам разрешено оттачивать свои хакерские навыки и свои хакерские инструменты, которые в дальнейшем государство будет использовать в своих интересах. По мнению Г. Брауна, реализуя такую деятельность, хакеры могут заходить очень далеко, используя, например, свои навыки против целого государства – США.

Осуждая необоснованные хакерские действия со стороны Российской Федерации, Г. Браун в своей статье приводит пример, когда Правительства США позволяет своим гражданам с «кибервозможностями» использовать последние в определенных обстоятельствах. Одним из таких фактов является случай, когда Федеральное бюро расследований США не смогло получить доступ к iPhone террористов, которые убили 14 человек в Сан-Бернардино, Калифорния, где Apple отказалась помочь, тогда Бюро заплатило хакерам за выполнение этой задачи.

Можно предположить, что ученый поддерживает такую инициативу и подчеркивает тот факт, что правительство будет работать с хакерами для укрепления национальной обороны. Примером здесь является программа «Взломай Пентагон», в которой предлагается вознаграждение хакерам, если последние найдут и сообщат об уязвимостях в компьютерных сетях [8].

Вышеописанный факт не единственный. Стоит также привести пример, когда были рассекречены случаи несанкционированного получения компьютерной информации Центральным разведывательным управлением (ЦРУ) США. Так, 7 марта 2017 г. произошло недооцененное экспертами событие: Wikileaks начал публикацию информации под кодовым названием Vault 7, содержащей подробности работы ЦРУ. В документах раскрываются сведения о наличии у спецслужб готовых эксплойтов для множества 0day-уязвимостей в различном программном обеспечении. К примеру, именно через такие 0day-уязвимости ЦРУ компрометирует мобильные устройства и перехватывает сообщения популярных мессенджеров (WhatsApp, Signal, Telegram, Weibo, Confide и Clockman): спецслужбы не взламывают шифрование, а компрометируют само устройство, на котором установлено приложение. Только в операционной системе Apple – iOS ЦРУ сумело найти семь различных уязвимостей и создало для них как минимум четырнадцать эксплойтов. 23 марта на Wikileaks был также опубликован ряд проектов ЦРУ, при помощи которых спецслужбы заражают технику Apple (Mac, iPhone) вирусом, который продолжает «жить» даже после переустановки операционной системы. Например, одним из таких вирусов является Night-Skies, который предназначен для заражения iPhone и устанавливается на чистые устройства, только что вышедшие с конвейеров фабрик. Становится очевидным, что ЦРУ давно имеет физическую возможность внедряться в логистическую цепочку Apple, заражая устройства прямо «из коробки» [9].

Россия идет по несколько иному пути. В.Ф. Васюков, рассматривая российский опыт получения судебного решения на проведение ОРМ, связанных с получением компьютерной информации, указывает, что, если информация выбыла из сферы ответственности организации (должностного лица) путем фиксации ее, например, в памяти мобильного компьютерного устройства, она как таковая уже не подлежит защите с помощью судебного контроля [10, с. 67].

По этому поводу В.Ф. Васюков приводит в пример позицию Конституционного суда РФ, выраженную в его Определении от 8 апреля 2010 г. № 433-О-О. В последнем указано: при рассмотрении жалобы гражданина на нарушение его конституционных прав, а именно, вопреки правовой позиции Конституционного суда Российской Федерации, выраженной в Определении от 2 октября 2003 г. № 345-О, органам предварительного следствия без вынесения соответствующего судебного решения позволено производить осмотр мобильных телефонов, изъятых у подозреваемых в совершении преступлений при заключении их под стражу, а при исследовании в судебном заседании протоколов следственных действий – оглашать сведения, содержащиеся в электронной памяти этих мобильных телефонов. Однако, как отмечал заявитель, применение в его деле оспариваемых норм уголовно-процессуального закона привело к ограничению его прав на тайну телефонных переговоров, на неприкосновенность частной жизни и на судебную защиту, гарантированных ст. 23 (ч. 2), 24 (ч. 1) и 46 (ч. 1) Конституции Российской Федерации. Но все же впоследствии Конституционный суд РФ постановил, что не может считаться ограничением прав на тайну телефонных переговоров, на неприкосновенность частной жизни и на судебную защиту осмотр мобильных телефонов, изъятых у подозреваемых в совершении преступлений при заключении их под стражу, а при исследовании в суде протоколов следственных действий – оглашение сведений, содержащихся в электронной памяти этих мобильных телефонов [11].

Однако существуют и такие обстоятельства, при которых не представляется возможным получить физический доступ к устройству, на котором может быть зафиксирована компьютерная информация оперативного значения. К примеру, когда компьютерная информация хранится и

передается при помощи программного обеспечения, установленного на удаленном сервере, физически расположенном в другом государстве. В свою очередь, не лишним будет отметить, что осуществление противоправных действий в сети происходит еще и при помощи вымышленных или неполных анкетных данных, где закономерно возникает вопрос, например, о принадлежности почтового ящика конкретному человеку.

Интересный вывод по этому поводу делает Е.В. Митин, который под отсутствием правового регулирования электронных сообщений обозначил, что электронный почтовый ящик, созданный пользователем на почтовом сервере, считается принадлежащим гражданину, если в регистрационных формах указаны реальные данные этого гражданина, в противном случае электронный почтовый ящик считается не принадлежащим гражданину. В случае нарушения тайны переписки по данному электронному почтовому ящику состав преступления, предусмотренного ст. 138 УК РФ (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) отсутствует, так как отсутствует объект преступления.

Так, в случае указания вымышленных данных при создании электронного почтового ящика отсутствует возможность установления принадлежности электронного почтового ящика конкретному гражданину, а следовательно, нет возможности установить факт нарушения конституционного права данного гражданина [12, с. 272]. Поэтому стоит предположить, что, получив доступ к такому почтовому ящику, оперативный сотрудник не нарушит конституционные права граждан и для реализации таких действий не требуется судебного решения.

На данный момент после нахождения в открытых источниках компьютерной информации, которая может представлять оперативный интерес или которая явно указывает на факт готовящегося или совершаемого преступления, необходимо перепроверить данную информацию и впоследствии отследить источник ее опубликования. Проверяя правдивость данной информации, все чаще прибегают к методу социальной инженерии, где на сайте, на котором была получена данная информация, задают уточняющие вопросы по теме, тем самым пытаясь удостовериться в ее актуальности. Далее необходимо перейти к стадии установления личности, т. е. установить, кто опубликовал данную информацию.

Так, например, реализуя ОРМ «получение компьютерной информации», в социальной сети «ВКонтакте» был установлен гр. «Д», который совершил массовое распространение экстремистских материалов, а именно: 1 февраля 2017 г. в прокуратуру города Новороссийска из отдела полиции (Восточного района) Управления МВД России по городу Новороссийску поступил материал проверки по факту распространения гр. «Д» экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов, в сети Интернет.

Из представленных материалов проверки следует, что 11 января 2017 г. в результате проведения оперативно-разыскных мероприятий «получение компьютерной информации» установлено, что по адресу в сети Интернет https://vk.com/... расположена страница пользователя под псевдонимом (именем) «Д», город Новороссийск, который на своей странице в неустановленное время, но не ранее января 2015 г. и не позднее октября 2015 г., в разделе аудиозаписи добавил аудиоматериал: «П». Указанный текст песни идентичен с содержанием песни «П», которое решением Волгоградского городского суда от 7 ноября 2012 г. признано экстремистским и внесено в федеральный список экстремистских материалов [13].

Как можно заметить, оперативно-разыскное мероприятие «получение компьютерной информации» осуществлялось при помощи браузера, когда после регистрации на сайте «ВКонтакте» стали известны и доступны, а именно отражены в открытом доступе на сайте https://vk.com/..., анкетные данные правонарушителя.

В процессе выявления оперативно значимой информации по преступлению экстремистской направленности проведение ОРМ «получение компьютерной информации» предоставило возможность осуществить сбор и фиксацию оперативными сотрудниками необходимой информации. Несмотря на такие действия, при помощи рассматриваемого ОРМ было бы не лишним установить и зафиксировать и то, на какие интернет-сайты заходил пользователь, с какими лицами вел интернет-переписку, какими интернет-источниками пользовался. Но такие действия возможно реализовать при том условии, если информация находится в открытом доступе и доступна для общего просмотра. Поэтому для того, чтобы исследовать полную картину и выявить, где пользователь мог взять запрещенный контент, необходимо получить полный доступ к используемой им компьютерной информации. Здесь стоит учитывать, что могут возникнуть такие ситуации, когда, например, получение и передача компьютерной информации осуществляются не только с помощью браузера, но и посредством различных проприетарных программных продуктов, в том числе использующих надежные средства шифрования.

С целью решения данной проблемы мы провели анализ практики зарубежных стран, где особый интерес представляет, в частности, законодательство Австралии. Так, с целью обеспечения расследования незаконной деятельности в интернете в Австралии принят Закон о надзоре за устройствами (Surveillance Devices Act) 2007 г. В соответствии с ним полиция Австралии получает официальное разрешение устанавливать на компьютеры подозреваемых преступников вирусы («троянских коней») или шпионы (spyware) при помощи упомянутого в законе «устройства наблюдения за данными». Под последним понимается любое устройство или программа, способные использоваться для записи или мониторинга ввода и вывода информации с компьютера. В секции 17 закона сказано, что сотрудник правоохранительных органов может подать заявку на выдачу ордера на устройство наблюдения. Интерес здесь представляет и секция 18, где отмечено, что заявление сотрудником правоохранительных органов может быть сделано по телефону, факсу, электронной почте или любым другим средством связи [14], что, на наш взгляд, позволяет действовать оперативно.

Полагаем, что указанный опыт требует более детального изучения и внедрения его положительных примеров в практику противодействия киберпреступности в РФ. Убеждены, что при оперативной работе по получению компьютерной информации, которая зашифрована или хранится за пределами государства, неизбежной становится потребность применения таких оперативно-разыскных мероприятий, которые: во-первых, не будут требовать прохождения длительной процедуры санкционирования последних вышестоящим руководством ОВД или судом, и, во-вторых, будут позволять использовать оперативные методы, связанные с преодолением компьютерной защиты. Нормативная реализация указанных инициатив повысит эффективность практики противодействия киберпреступности, позволит экономить время и средства проведения ОРМ. С учетом сказанного целесообразно в ст. 6 федерального закона «Об оперативно-разыскной деятельности» указать, что сотрудникам полиции в ходе проведения оперативно-разыскных мероприятий разрешено использовать информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические и иные средства, позволяющие, в частности, преодолевать средства компьютерной защиты и не причиняющие ущерба жизни и здоровью людей, а также не наносящие вреда окружающей среде.

Ссылки:

1. Об оперативно-разыскной деятельности [Электронный ресурс] : федер. закон РФ от 12 авг. 1995 г. № 144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Баженов С.В. Оперативно-разыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. 2017. № 2 (65). С. 31–33.
3. Павлюков В.В. Правовые аспекты получения и защиты компьютерной информации в сети Интернет // Вестник Дальневосточного юридического института МВД России. 2017. № 3 (40). С. 178–182.
4. Об оперативно-разыскной деятельности.
5. Дубягин Ю.П., Дубягина О.П., Михайлычев Е.А. Комментарий к Федеральному закону «Об оперативно-разыскной деятельности» (постатейный). М., 2005. 144 с.
6. Кузченко Д.В., Кушпель Е.В. О некоторых тактических особенностях поиска, фиксации и изъятия компьютерной информации в ходе наложения ареста на почтово-телеграфные отправления и при контроле и записи переговоров // Вестник Барнаульского юридического института МВД России. 2011. № 1 (20). С. 39–41.
7. Шогенов Т.К. Вопросы технического обеспечения проведения оперативно-разыскного мероприятия «Снятие информации с технических каналов связи» // Спецтехника и связь. 2013. № 6. С. 28–31.
8. Brown G.D. The Cyber Longbow & Other Information Strategies: U.S. National Security and Cyberspace [Электронный ресурс] // Penn State Journal of Law & International Affairs. 2017. Vol. 5, iss. 1. URL: https://elibrary.law.psu.edu/cgi/viewcontent.cgi?referer=https://www.google.ru/&httpsredir=1&article=1155&context=jlia (дата обращения: 27.06.2018).
9. Нефёдова М. Wikileaks опубликовала файлы ЦРУ, рассказав, как спецслужбы ломают смартфоны и телевизоры [Электронный ресурс] // Хакер. 2017. № 218. 7 марта. URL: https://xakep.ru/2017/03/07/vault-7/ (дата обращения: 27.06.2018).
10. Васюков В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. 2016. № 10 (142). С. 64–67.
11. Об отказе в принятии к рассмотрению жалобы гражданина Тарасова Николая Алексеевича на нарушение его конституционных прав частью первой статьи 176 и частью первой статьи 285 Уголовно-процессуального кодекса Российской Федерации [Электронный ресурс] : определение Конституционного суда Российской Федерации от 8 апр. 2010 г. № 433-О-О. Доступ из справ.-правовой системы «КонсультантПлюс».
12. Митин Е.В. Право на тайну сообщений, передаваемых по электронным почтовым ящикам: проблемы реализации // Теория и практика общественного развития. 2012. № 9. С. 271–273.
13. Постановление Ленинского районного суда (г. Новороссийск) № 5-140/2017 от 6 марта 2017 г. по делу № 5-140/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc/V44WiYrQDdLt/ (дата обращения: 18.12.2017).
14. Surveillance Devices Act No. 64 of 2007 [Электронный ресурс] // New South Wales Consolidated Acts. URL: http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol_act/sda2007210/ (дата обращения: 22.12.2017).