КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

DOI: 10.17803/1994-1471.2021.133.12.156-166

М. В. Жижина*,
Д. В. Завьялова**

Возбуждение уголовного дела по факту преступления в сфере компьютерной информации: российский и зарубежный опыт

Аннотация. В статье рассматриваются теоретические и практические основы возбуждения уголовных дел о преступлениях в сфере компьютерной информации. Этап доследственной проверки сообщения о преступлении является достаточно сложным в силу необходимости выявления и закрепления следовой картины, требует привлечения специальных знаний в области информационных технологий, совершения определенных действий, в том числе технического характера, и пр. На основе проведенного авторами анализа отечественных и зарубежных источников, обобщения судебно-следственной практики и процессуальной регламентации разработан алгоритм проведения доследственной проверки сообщений о преступлении данного вида. Особое внимание уделено тактическим рекомендациям по проведению опроса потерпевшего — физического и юридического лица. Представлены иные проверочные и следственные действия в зависимости от типичных версий и ситуаций. Отдельно рассматриваются оперативно-розыскные мероприятия, применяемые для установления факта совершения преступления. Вместе с тем обобщение судебно-следственной практики расследования преступлений в сфере компьютерной информации и анкетирование представителей правоохранительных органов позволили выявить отдельные проблемные моменты, связанные с проведением доследственной проверки сообщений о данных преступлениях, в том числе с порядком обращения потерпевших с сообщениями об инцидентах, с возможностями сбора информации из открытых источников киберпространства в рамках оперативно-розыскных мероприятий и пр. На основе результатов проведенных авторами исследований предлагаются результативные зарубежные

* *Жижина Марина Владимировна*, доктор юридических наук, профессор кафедры криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), главный научный сотрудник ФБУ РФЦСЭ при Минюсте России
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
mzhizhina@yandex.ru

** *Завьялова Дарья Владимировна*, аспирант Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), старший преподаватель Департамента систем судопроизводства и уголовного права, заведующий криминалистической лабораторией Национального исследовательского университета «Высшая школа экономики»
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
dariazav@mail.ru

практики, перенос которых на отечественную почву будет способствовать сокращению латентности данных преступлений, повышению эффективности расследования и раскрытия данной категории уголовных дел.
Ключевые слова: преступления в сфере компьютерной информации; сообщение о преступлении; возбуждение уголовного дела; первоначальный этап; особенности; российская и зарубежная практика; расследование; методика; опрос потерпевшего; следователь; дознаватель.
Для цитирования: *Жижина М. В., Завьялова Д. В.* Возбуждение уголовного дела по факту преступления в сфере компьютерной информации: российский и зарубежный опыт // Актуальные проблемы российского права. — 2021. — Т. 16. — № 12. — С. 156–166. — DOI: 10.17803/1994-1471.2021.133.12.156-166.

Initiation of a Criminal Case for an Offence in the Field of Computer Information: Russian and Foreign Experience

Marina V. Zhizhina, Dr. Sci. (Law), Professor, Department of Criminalistics, Kutafin Moscow State Law University (MSAL); Chief Researcher, Russian Federal Centre of Forensic Science of the Ministry of Justice of the Russian Federation
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
mzhizhina@yandex.ru

Darya V. Zavyalova, Postgraduate student, Kutafin Moscow State Law University (MSAL); Senior Lecturer, Department of Judicial Systems and Criminal Law, Head of the Forensic Laboratory, "Higher School of Economics" National Research University
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
dariazav@mail.ru

Abstract. The paper examines the theoretical and practical foundations of the initiation of criminal cases for crimes in the field of computer information. The stage of pre-investigation verification of a crime report is quite difficult due to the need to identify and consolidate the trace picture, requires the involvement of special knowledge in the field of information technology, the performance of certain actions, including of a technical nature, etc. Based on the analysis of domestic and foreign sources carried out by the authors, generalization of forensic practice and procedural regulation, an algorithm has been developed for conducting a pre-investigation check of reports of a crime of this type. Particular attention is given to tactical recommendations for interviewing a victim, namely an individual and a legal entity. Other verification and investigative actions are presented, depending on typical versions and situations. The operational search measures used to establish the fact of a crime are considered separately. At the same time, the generalization of the forensic practice of investigating crimes in the field of computer information and the questioning of representatives of law enforcement agencies made it possible to identify certain problematic points related to the pre-investigation verification of reports on these crimes, including the procedure for the treatment of victims with reports of incidents, with information from open sources of cyberspace within the framework of operational-search activities, etc. Based on the results of the research conducted by the authors, effective foreign practices are proposed, the transfer of which to domestic soil will help reduce the latency of these crimes, increase the efficiency of investigation and disclosure of this category of criminal cases.
Keywords: crimes in the field of computer information; reporting a crime; criminal proceedings; initial stage; peculiarities; Russian and foreign practice; investigation; technique; questioning the victim; investigator; interrogator.
Cite as: Zhizhina MV, Zavyalova DV. Vozbuzhdenie ugolovnogo dela po faktu prestupleniya v sfere kompyuternoy informatsii: rossiyskiy i zarubezhnyy opyt [Initiation of a Criminal Case for an Offence in the Field of Computer Information: Russian and Foreign Experience]. *Aktual'nye problemy rossijskogo prava*. 2021;16(12):156-166. DOI: 10.17803/1994-1471.2021.133.12.156-166. (In Russ., abstract in Eng.).

Как справедливо отмечал Р. С. Белкин, эффективность расследования преступлений зависит не только от методически правильного подхода к процессу расследования, но и от оперативности действий, умения организовать силы и средства, которыми располагают органы, ведущие борьбу с преступностью[1]. Особенно значима для всего дальнейшего хода расследования организационная составляющая первоначального этапа, т.к. именно в его рамках происходит собирание и накопление уголовно-релевантной информации. Промедления и ошибки, допущенные у истоков следствия, зачастую предрешают дальнейшие неудачи, препятствуя установлению объективной истины по делу.

Первоначальная стадия уголовного судопроизводства — возбуждение уголовного дела — предопределяется спецификой конкретного вида преступлений. Непосредственно возбуждению уголовных дел о преступлениях в сфере компьютерной информации в Российской Федерации и в зарубежных странах предшествует проверка сообщения о таком преступлении. Необходимость доследственной проверки обусловлена спецификой природы следов, обнаружение которых требует специальных знаний в области информационных технологий, совершения определенных действий, в том числе технического характера, например анализа трафика сети, осмотра лог-файлов системы и пр. Между тем установление достаточности оснований для возбуждения дела становится иногда непростой задачей для правоприменителей. Далеко не всегда очевидны умышленность совершенного деяния и признаки преступления. Так, по результатам проведенного нами анкетирования следователей[2] было установлено, что абсолютное большинство (более 97 % опрошенных) чаще всего испытывают трудности при самостоятельном определении достаточности оснований для возбуждения уголовного дела о преступлениях в сфере компьютерной информации и нуждаются в консультациях специалиста и сборе дополнительной информации об инциденте на основе таких консультаций.

В процессе проверки сообщения о преступлении ее субъекты (дознаватель, орган дознания, следователь, руководитель следственного органа) могут выполнять довольно широкий круг действий — проверочных (результаты которых по общему правилу не являются доказательствами), следственных и иных процессуальных. К ним относятся: получение объяснений, образцов для сравнительного исследования, истребование и изъятие документов и предметов, назначение судебной экспертизы, проведение осмотров (места происшествия, документов, предметов), освидетельствование, требование производства документальных проверок, ревизий, исследований документов, предметов, привлечение к участию в этих действиях специалистов, поручение органу проведения оперативно-розыскных мероприятий (ч. 1 ст. 144 УПК РФ).

Классический алгоритм деятельности сотрудника органа предварительного расследования на стадии возбуждения уголовного дела о совершении любого преступления, в том числе и преступления в сфере компьютерной информации, включает в себя следующие элементы:

1) изучение имеющихся фактических данных (оценка поступившей исходной информации о преступлении);
2) проверка заявления и сообщения, если в исходной информации отсутствуют достаточные данные, указывающие на признаки преступления;
3) выдвижение версий, определение вопросов, подлежащих выяснению;
4) определение круга следственных действий и организационных мероприятий, подлежащих проведению по каждой версии, сроков и последовательности их проведения, а также исполнителей;
5) корректировка плана в соответствии с получаемой информацией;
6) принятие и процессуальное оформление решения о возбуждении уголовного дела[3].

---

[1] *Белкин Р. С.* Курс криминалистики : в 3 т. Т. 1 : Общая теория криминалистики. М., 1997. С. 307.

[2] В анкетировании участвовало 86 респондентов — сотрудников МВД Москвы и Московской области.

[3] См., например: *Филиппов А. Г.* Планирование расследования преступлений // Криминалистика : учеб. для вузов МВД России. Волгоград, 1994. С. 277.

Учитывая жестко регламентированные сроки проведения доследственных мероприятий (ч. 1 и 3 ст. 144 УПК РФ), нельзя пренебрегать рекомендацией составления плана предварительной проверки, позволяющей четко и системно предусмотреть все необходимые действия и мероприятия. Субъект доследственной проверки, исходя из личного удобства, выбирает конкретный вид планирования (табличный или свободный формат, схема и пр.).

Нельзя не согласиться с В. В. Коломиновым, что ситуация, складывающаяся на момент получения информации о событии, в значительной степени влияет на весь процесс деятельности следователя[4]. В зависимости от содержания исходной информации происходит выдвижение версий, определение подлежащих выяснению вопросов, а также комплекса подлежащих проведению действий.

Как показал анализ обобщения отечественной судебно-следственной практики[5], основанием возбуждения уголовных дел о преступлениях в сфере компьютерной информации являются, как правило, заявления граждан и организаций — владельцев и законных пользователей компьютерной (цифровой) информации, подвергшейся посягательству (83 % случаев). Значительно реже (примерно в 13 % случаев) соответствующие деяния были обнаружены сотрудниками правоохранительных органов в ходе расследования других преступлений (например, в соответствии с п. 3 ч. 1 ст. 140 УПК РФ по материалам, содержащим результаты оперативно-розыскных мероприятий специализированных подразделений МВД России и ФСБ России[6]). Отметим, что по данной категории дел задержаний с поличным и явок с повинной как оснований возбуждения уголовного дела нами выявлено не было.

Для зарубежных государств приведенная статистика также актуальна. По данным изученных иностранных источников, сообщения потерпевших — наиболее распространенный способ обнаружения преступлений в сфере компьютерной информации в странах СНГ, Европейского Союза, Соединенных Штатах, Австралии, Индии, Канаде[7]. При этом необходимо отметить, что сообщения потерпевших в ряде зарубежных стран носят несколько иной формат.

Во многих странах мира созданы специализированные организации, в которые обращаются жертвы компьютерных преступлений с соответствующими заявлениями. Одна из самых известных организаций такого типа, IC3 (Internet Crime Complaint Center — Центр по рассмотрению заявлений о преступлениях в Интернете), была создана в США в 2000 г. и выполняет координирующую роль для ФБР и правоохранительных органов. Основная ее функция — помочь жертвам компьютерных преступлений подать заявление через онлайн-форму, в которой пострадавший должен ответить на вопросы, касающиеся происшедшего события, правонарушителей (если они известны) и пр. После обработки сотрудниками IC3 заявление при необходимости направляется в соответствующий орган по подведомственности. Существуют подобные службы и в других странах (в Великобритании — Action Fraud[8], в Австралии — Центр кибербезопасности (ACSC[9])) как негосударственные организации и центры реагирования.

---

4 *Коломинов В. В.* Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. … канд. юрид. наук. Иркутск, 2017. С. 90.

5 Изучение и обобщение материалов уголовных дел, приговоров, вынесенных по уголовным делам судами различных инстанций, производилось за период с 2015 по 2020 г. Всего было изучено и использовано 215 материалов дел и судебных актов.

6 Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс».

7 См., например: URL: https://www.ncsc.gov.uk/section/information-for/individuals-families ; https://www.ncsc.gov.uk/information/report-suspicious-emails… (дата обращения: 20.08.2021).

8 URL: https://www.actionfraud.police.uk/what-is-action-fraud (дата обращения: 20.08.2021).

9 URL: https://www.cyber.gov.au/acsc/report (дата обращения: 20.08.2021).

Подобные службы выполняют ряд важных задач, среди которых:

1) упрощение порядка подачи заявлений о произошедшем для пострадавших граждан: службы доступны круглосуточно, дают подробные и понятные инструкции о том, что именно необходимо сообщить, в какой именно орган надлежит обращаться и пр.;
2) снятие потоковой нагрузки с правоохранительных органов, а также принятие информации от тех лиц, которые по каким-либо причинам не хотят обращаться в полицию;
3) сбор большого количества статистической информации, которую обрабатывают с помощью алгоритмов искусственного интеллекта для выявления неочевидных связей между элементами криминалистической характеристики преступлений в сфере компьютерной информации, тенденций их развития.

Положительные результаты работы таких служб можно подтвердить следующими данными. В ходе исследования нами было установлено, что зарегистрированных заявлений о совершении компьютерных преступлениях относительно общего количества населения в странах с таким информированием и организациями-посредниками больше, чем в тех, где их нет. Так, например, в Австралии и Канаде приблизительно 0,2 % от общего количества населения уведомило какую-либо организацию о компьютерном преступлении за 2020 г. В США и Великобритании — около 0,3 %. Для России же этот показатель составил только 0,09 %, что лишний раз подтверждает высочайшую латентность данной категории преступлений, т.к. в этот омраченный пандемией год редкий пользователь компьютера не столкнулся хотя бы с попыткой взлома системы.

Кроме того, на примере Великобритании можно отметить колоссальную разницу, которая существует между уведомлением непосредственно правоохранительных органов и других организаций о подобных инцидентах. По данным IC3, за 2020 г. в Великобритании было зафиксировано 216 633 сообщений о компьютерных преступлениях, в то время как непосредственно в полицию поступило только 27 187 заявлений[10].

На наш взгляд, заимствование подобной практики — создание специализированной службы для жертв компьютерных преступлений, в которую можно было бы обратиться в онлайн-формате, аккумулирующей высокие технологии и квалифицированных сотрудников, — позволило бы оказывать реальную помощь и поддержку потерпевшим, минимизировать временны́е издержки и ошибки, допускаемые на этапе доследственной проверки, значительно повысить результативность расследования преступлений в сфере компьютерной информации в России.

Приступая к проведению проверки, ее субъект должен объективно установить наличие фактов, изложенных в заявлении о нарушении целостности (конфиденциальности) информации в компьютерной системе, сети; о наличии причинной связи между неправомерными действиями и наступившими последствиями, предусмотренными диспозицией ст. 272 и 274 УК РФ, в виде копирования, уничтожения, модификации, блокирования информации (для возбуждения уголовного дела по ст. 273 УК РФ наступление таких последствий не обязательно); о предварительном размере ущерба, причиненного в результате преступных действий.

На начальном этапе проверки выдвигается несколько рабочих версий о происшедшем, каждая из которых подлежит тщательной проверке:

— соответствующее преступление, предусмотренное ст. 272–274, 274.1 УК РФ имело место;
— контрверсия — преступления не было, заявившее лицо добросовестно заблуждается;
— инцидент имел место, однако он произошел не в результате преднамеренных неправомерных действий, а был вызван, например, ошибками, неумышленным неправильным поведением персонала потерпевшей организации при техническом обслуживании или

[10] URL: https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Cyber-crime-trends.pdf (дата обращения: 20.08.2021).

ремонте компьютера, компьютерной системы или сети; случайными неумышленными повреждениями аппаратуры; ошибочными действиями оператора в процессе работы, приведшими к разрушению информационных данных или неправильным обращением с машинными носителями информации в ходе их использования и хранения и т.д.[11]

По получении заявления о преступлении следует проведение опроса заявившего лица — потенциального потерпевшего. При этом необходимо выяснить:

— при каких обстоятельствах было обнаружено преступление, продолжается ли оно, как долго продолжалось или сколько произошло эпизодов, случалось ли подобное раньше;
— подробные характеристики предмета преступного посягательства: тип и назначение компьютерной (цифровой) информации, ее реквизиты, носитель, на котором она находится, также с его реквизитами, наличие доступа к ней, кодов и паролей;
— неблагоприятные последствия, которые заявитель связывает с преступным посягательством, характер и размер ущерба;
— навыки в сфере информационных технологий пострадавшего, были ли им предприняты самостоятельные шаги по пресечению преступной деятельности, попытки ликвидировать последствия или выяснить источник атаки; в чем они заключались;
— основания, на которых заявитель владеет компьютерной (цифровой) информацией с документальным подтверждением (например, договоры с провайдером, аренды или купли-продажи определенного оборудования и др.);
— коммуникативные и иные технические характеристики используемой компьютерной техники;
— мнение о механизме совершенного преступления, а также причинах и условиях наступления преступного результата.

Если заявителем является юридическое лицо, то дополнительно следует выяснить: вид деятельности и местонахождение юридического лица, режим его работы (требования внутреннего распорядка, штатного кадрового расписания, должностных инструкций и т. д.); кто является пользователем атакованного компьютера, существует ли на предприятии система информационной безопасности, как она построена, кто является ответственным лицом и пр[12].

Приведенный перечень не является исчерпывающим и должен уточняться в зависимости от конкретной исходной ситуации и способа совершения преступления (удаленное или непосредственное воздействие). Кроме того, сто́ит поддержать рекомендацию американских криминалистов в том, что необходимо выяснить политику организации относительно возможности использования ее сотрудниками личных персональных цифровых устройств и носителей информации на рабочем месте[13]. Свободное использование последних зачастую создает ситуацию, благоприятствующую совершению преступлений, что необходимо учитывать при построении частных версий о произошедшем.

Несмотря на различный процессуальный порядок проведения и статус, тактические особенности получения объяснений от потерпевшего во многом сходны с тактикой его допроса, которые обстоятельно изложены в криминалистической литературе[14]. Для субъекта доследственной

[11] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.

[12] *Вехов Б. В.* Особенности расследования преступлений, совершаемых с использованием электронно-вычислительной техники : учеб.-метод. пособие. М., 2000. С. 18–19.

[13] *Edwards G.* Cybercrime Investigator's Handbook. Wiley, 2019. P. 67.

[14] См., например: *Кузьмин М. Н., Солонникова Н. В.* Особенности тактики производства допроса потерпевшего в ходе расследования мошенничества в сфере компьютерной информации // Гуманитарные, социально-экономические и общественные науки. 2018. № 12. С. 111–113 ; *Аксенова Л. Ю.* Тактические и психологические аспекты допроса // Психопедагогика в правоохранительных органах. 2019. № 1 (76). С. 111–117.

проверки действенны рекомендации установления психологического контакта[15]. Представляется интересной точка зрения В. М. Быкова, предлагающего учитывать при этом криминалистический тип потерпевших исходя из особенностей занятой позиции и поведения, выделяя четыре варианта: активных и неактивных добросовестных потерпевших, неустойчивых, а также недобросовестных потерпевших[16].

Проведенный анализ зарубежных источников позволил выявить актуальные варианты, используемые нашими коллегами. Так, например, в Скандинавии (Швеция и Финляндия) практикуется получение объяснений от заявителя по телефону, во Франции опрос может проводиться в неформальной обстановке на нейтральной территории, что, несомненно, более комфортно для потерпевшего. Такие подходы обоснованы необходимостью как можно более оперативного получения уголовно-релевантной информации на этом этапе расследования, а также снижения влияния стрессогенных факторов на потерпевшего, налаживанием необходимого контакта. В то же время мы отмечаем определенную несвоевременность заимствования подобного опыта, который сложно реализуем в условиях кадрового дефицита в правоохранительных органах Российской Федерации.

Вместе с тем лицу, осуществляющему проверочные действия, следует ориентироваться на типичные ситуации возбуждения уголовного дела данной категории. К ним относятся:

1) заявители (администрация организации, владелец компьютерной информации) сами выявили факт преступления или признаки совершенного преступления, но не смогли установить конкретных лиц, в связи с чем обратились в правоохранительные органы;
2) заявители (администрация организации, потерпевший) не только обнаружили преступление, его признаки, но и выявили установочные данные подозреваемого лица (чаще всего это номер телефона, сообщенный провайдером услуг сети Интернет, или IP-адрес, если подсоединение к компьютерной сети произведено с использованием Интернета)[17].

Соответственно, планировать дальнейшую деятельность необходимо с их учетом. Она, как правило, включает[18]:

— осмотр места происшествия — места обнаружения следов преступления с обязательным осмотром компьютерного устройства, электронных носителей и содержащейся на них компьютерной информации;
— получение письменных объяснений у лиц, имеющих доступ к ЭВМ, на которых ссылается заявитель или имеются данные о них как о возможных свидетелях происшедшего события. При этом особую важность представляют объяснения компетентных сотрудников потерпевшей организации — администраторов сети, инженеров-программистов, разработавших программное обеспечение и осуществляющих его сопровождение (т.е. отладку и обслуживание), операторов, специалистов, занимающихся эксплуатацией и ремонтом компьютерной техники; системных программистов, инженеров по средствам связи и телекоммуникационному оборудованию, специалистов, обеспечивающих информационную безопасность, работников службы безопасности и др. Из данных объяснений следует уяснить обстоятельства обнаружения факта преступления (признаки его совершения, способы и средства, наступившие негативные последствия), наличие

[15] *Таркинский А. И.* Психологический контакт в структуре допроса потерпевшего и свидетеля // Вестник Дагестанского государственного университета. 2011. № 2. С. 248–252.

[16] *Быков В. М.* Допрос потерпевшего // Законность. 2014. № 6. С. 27–32.

[17] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.

[18] *Вехов В. Б.* Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // Эксперт-криминалист. 2013. № 4. С. 2–4.

и функционирование информационной защиты, ее недостатки, иные причины и условия, которые могли быть использованы для совершения противоправных действий[19];
- ознакомление с технологией использования документированной компьютерной информации в конкретном технологическом процессе или операции;
- изучение правовой основы операции, итогом которой явилось событие, изложенное в сообщении о преступлении;
- консультации со специалистами;
- истребование необходимых материалов (документов), свидетельствующих о противоправности события либо отражающих незаконность проведения операции в сфере обработки компьютерной информации (например, журналы регистрации событий (NetFlow), предоставляемые поставщиком интернет-услуг);
- осмотр и исследование предметов и документов, которые проводятся с участием специалиста, как правило, в рамках осмотра места происшествия. Заключение по результатам исследования излагается в протоколе следственного действия или приобщается к нему в письменном виде в качестве приложения (ст. 58, 80 УПК РФ). Исследование может быть проведено и специализированным органом дознания в виде оперативно-розыскного мероприятия — исследования предметов и документов (ст. 6 Федерального закона «Об оперативно-розыскной деятельности»[20]);
- назначение экспертиз, проведение ревизий, документальных или иных проверок. При этом сто́ит отметить обязательность проведения судебной компьютерно-технической экспертизы, предметом которой являются изъятые по делу электронные носители информации и т.д., с целью обнаружения вредоносного программного обеспечения, иных сведений, имеющих значение для выявления признаков преступления, что обусловлено спецификой процесса доказывания;
- проведение иных следственных действий, направленных на закрепление следов и выявление лиц, совершивших преступление (например, осмотр ЭВМ, с которых предположительно осуществлена DoS/DDoS-атака и др.).

Приведенный перечень не является исчерпывающим и может быть дополнен иными необходимыми действиями и оперативно-розыскными мероприятиями (ОРМ), зависящими от конкретной ситуации.

В частности, в качестве ОРМ на этапе доследственной проверки по данной категории дел могут быть проведены:

а) наблюдение и контрольная закупка (например, при продаже, распространении носителей с вредоносными компьютерными программами);
б) перехват и регистрация информации электронной почты лиц, причастных к преступлению;
в) оперативное наблюдение с ведением фото- и видеосъемки;
г) оперативный эксперимент;
д) изъятие компьютерной техники (машинных носителей);
е) использование специальных химических средств (химловушек) при фиксации использования компьютерного оборудования в целях неправомерного доступа;
ж) снятие информации с технических каналов связи;
з) получение компьютерной информации и др. (ст. 6 Федерального закона «Об оперативно-розыскной деятельности»).

Проведение ОРМ, направленных на получение уголовно-релевантной информации на этапе проверки сообщения о преступлении в сфере компьютерной информации, должно создавать,

[19] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.

[20] URL: http://www.consultant.ru/document/cons_doc_LAW_7519/7367463b83418fbb4a8e0a259864c246fb9b365a/.

по справедливому замечанию Р. Г. Драпезо, эффект эмерджентности[21]. Только комплексный подход обеспечит необходимую результативность, что демонстрирует судебно-следственная практика. Так, при проверке сообщения о преступлениях, предусмотренных ч. 2 ст. 272 и ч. 2 ст. 273, в отношении гр-на Д., были проведены следующие ОРМ: «наведение справок» (в том числе с использованием сети Интернет) и «проверочная закупка», в ходе которого сотрудник правоохранительных органов приобрел у злоумышленника модифицированный устройство с пультом дистанционного управления и смарт-картой НАО «Национальная спутниковая компания» («Триколор ТВ»). Запоминающее устройство в составе ресивера предназначалось для декодирования защищенных спутниковых телеканалов ограниченного доступа и, таким образом, обеспечивало несанкционированный доступ к просмотру кодированных спутниковых телеканалов. В результате проведенного комплекса оперативно-розыскных мероприятий была установлена достаточность информации о неправомерных действиях[22].

Вместе с тем проведенные нами анализ судебно-следственной практики, обобщение литературных источников позволили выявить, с одной стороны, ряд проблемных моментов при проведении ОРМ в Интернете при доследственной проверке сообщений о преступлении данного вида, с другой — ряд мировых практик, заимствование которых, позволило бы их разрешить, минимизировать временны́е затраты и исключить ошибки в деятельности правоохранительных органов.

Данное предложение касается раскрытия потенциала и возможностей использования так называемых открытых источников информации, которыми активно используются в рамках ОРМ как в России, так и за рубежом. К таковым относятся: социальные сети, блоги, «открытый» Интернет, содержащий сайты, индексируемые поисковиками, и связанные с ними материалы (например, копии, которые можно воспроизвести для конкретного периода, момента времени), «темный» Интернет (dark web), почтовые сервисы, архивы, карты, официальные данные учреждений, реестры, игровые площадки и др. В нашей стране в методическом плане разработок по оптимальному их использованию нами не было выявлено, в связи с чем мы обратились зарубежному опыту.

Иностранные методики включают в себя два класса рекомендаций:

1) правила работы с отдельными источниками информации (сайтами, социальными сетями, картами, поисковиками и пр.);
2) применение специализированного программного обеспечения (ПО).

К общим правилам-рекомендациям можно отнести, например, следующие: при работе с социальными сетями необходимо учитывать уровень навыков подозреваемого — если есть основания предполагать, что лицо квалифицировано в сфере информационных технологий, то при изучении его социальных сетей необходимо предпринимать дополнительные меры предосторожности (например, использовать VPN, чтобы наблюдаемому лицу было невозможно проследить обратную связь с правоохранительными органами). В связи с этим любые манипуляции с открытыми источниками следует проводить с участием специалиста, обладающего соответствующими навыками, либо предварительно проконсультировавшись с ним. Необходимо чрезвычайно внимательно относиться к логинам, ник-неймам пользователей, именам почтовых ящиков, т.к. они могут быть полезны при

[21] *Драпезо Р. Г.* Исходные ситуации по преступлениям, совершаемым с использованием сети Интернет, и способы легализации оперативно-розыскной информации // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий. Барнаул : Изд-во Алт. ун-та, 2018. С. 94–95.

[22] Петушинский районный суд (Владимирская область). Приговор № 1-85/2020 от 02.07.2020 по делу № 1-85/2020.

[23] См. подробнее: *Bilton N*. American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road. 2017.

установлении личности и связей между людьми в сети. Так, например, именно благодаря никнейму на форуме и имени почтового ящика удалось установить реальную личность Росса Ульбрихта — создателя первого крупного черного рынка в даркнете — «Шелкового пути»[23].

Сбор информации из открытых источников рекомендуется осуществлять с помощью специализированного ПО, например: Maltego[24] позволяет выявлять связи между людьми, компаниями, доменами и пр., исследуя различные открытые источники информации; Intelligence X[25] позволяет просматривать «исторические версии» сайтов, все изменения, которые на них происходили; Recon-ng[26] позволяет полностью автоматизировать поиск информации по открытым источникам, значительно экономя время и др.

Учитывая широкую распространенность открытых источников информации в России и их незаменимость в криминалистическом плане, а также технические возможности специализированного ПО, облегчающего поиск необходимой информации, на наш взгляд, целесообразна разработка соответствующего комплексного методического обеспечения по их корректному использованию для отечественных правоохранителей.

Оперативная информация, полученная на этапе рассмотрения сообщения о преступлении, может послужить основанием для возбуждения уголовного дела, быть впоследствии использована как ориентирующая при планировании проведения различных следственных действий либо приобщена к материалам дела в качестве доказательства. Легализация данных, полученных оперативных путем, происходит в результате:

1) привлечения для проведения предварительного исследования специалиста, составляющего соответствующую справку;
2) ее нормативно предусмотренного оформления[27].

По результатам проведения доследственной проверки принимается решение о возбуждении уголовного дела, об отказе в его возбуждении или передачи сообщения о преступлении по подследственности в порядке ст. 151 УПК РФ.

БИБЛИОГРАФИЯ

1. *Аксенова Л. Ю.* Тактические и психологические аспекты допроса // Психопедагогика в правоохранительных органах. — 2019. — № 1 (76). — С. 111–117.
2. *Белкин Р. С.* Курс криминалистики : в 3 т. Т. 1 : Общая теория криминалистики. — М., 1997. — 408 с.
3. *Быков В. М.* Допрос потерпевшего // Законность. — 2014. — № 6. — С. 27–32.
4. *Вехов Б. В.* Особенности расследования преступлений, совершаемых с использованием электронно-вычислительной техники : учеб.-метод. пособие. — М., 2000. — 70 с
5. *Вехов В. Б.* Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // Эксперт-криминалист. — 2013. — № 4. — С. 2–4.
6. *Драпезо Р. Г.* Исходные ситуации по преступлениям, совершаемым с использованием сети Интернет, и способы легализации оперативно-розыскной информации // Уголовно-процессуальные и кримина-

[24] URL: https://www.maltego.com (дата обращения: 20.08.2021).

[25] URL: https://intelx.io (дата обращения: 20.08.2021).

[26] URL: https://tools.kali.org/information-gathering/recon-ng (дата обращения: 20.08.2021).

[27] Приказ МВД России № 776, Минобороны России № 703, ФСБ России 3 509, ФСО России № 507, ФТС России № 1820, СВР России 3 42, ФСИН России 3 535, ФСКН России № 398, СК России 3 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // URL: http://www.consultant.ru/document/cons_doc_LAW_155629/.

листические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий. — Барнаул : Изд-во Алт. ун-та, 2018. — С. 94–95.
7. *Коломинов В. В.* Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. … канд. юрид. наук. — Иркутск, 2017. — 211 с.
8. *Кузьмин М. Н., Солонникова Н. В.* Особенности тактики производства допроса потерпевшего в ходе расследования мошенничества в сфере компьютерной информации // Гуманитарные, социально-экономические и общественные науки. — 2018. — № 12. — С. 111–113.
9. Криминалистика / отв. ред. Б. П. Смагоринский ; М-во внутр. дел Рос. Федерации, Высш. следств. шк. — Волгоград : ВСШ, 1994. — 559 с.
10. *Таркинский А. И.* Психологический контакт в структуре допроса потерпевшего и свидетеля // Вестник Дагестанского государственного университета. — 2011. — № 2. — С. 248–252.
11. *Edwards G.* Cybercrime Investigator's Handbook. — Wiley, 2019.
12. *Bilton N.* American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road. — 2017.

Материал поступил в редакцию 23 августа 2021 г.

REFERENCES (TRANSLITERATION)

1. Aksenova L. Yu. Takticheskie i psihologicheskie aspekty doprosa // Psihopedagogika v pravoohranitel'nyh organah. — 2019. — № 1 (76). — S. 111–117.
2. Belkin R. S. Kurs kriminalistiki : v 3 t. T. 1 : Obshchaya teoriya kriminalistiki. — M., 1997. — 408 s.
3. Bykov V. M. Dopros poterpevshego // Zakonnost'. — 2014. — № 6. — S. 27–32.
4. Vekhov B. V. Osobennosti rassledovaniya prestuplenij, sovershaemyh s ispol'zovaniem elektronno-vychislitel'noj tekhniki : ucheb.-metod. posobie. — M., 2000. — 70 s
5. Vekhov V. B. Osobennosti provedeniya dosledstvennoj proverki po delam o prestupleniyah v sfere komp'yuternoj informacii // Ekspert-kriminalist. — 2013. — № 4. — S. 2–4.
6. Drapezo R. G. Iskhodnye situacii po prestupleniyam, sovershaemym s ispol'zovaniem seti Internet, i sposoby legalizacii operativno-rozysknoj informacii // Ugolovno-processual'nye i kriminalisticheskie chteniya na Altae: problemy i perspektivy protivodejstviya prestupleniyam, sovershaemym s primeneniem informacionnyh tekhnologij. — Barnaul : Izd-vo Alt. un-ta, 2018. — S. 94–95.
7. Kolominov V. V. Rassledovanie moshennichestva v sfere komp'yuternoj informacii: nauchno-teoreticheskaya osnova i prikladnye aspekty pervonachal'nogo etapa : dis. … kand. yurid. nauk. — Irkutsk, 2017. — 211 s.
8. Kuz'min M. N., Solonnikova N. V. Osobennosti taktiki proizvodstva doprosa poterpevshego v hode rassledovaniya moshennichestva v sfere komp'yuternoj informacii // Gumanitarnye, social'no-ekonomicheskie i obshchestvennye nauki. — 2018. — № 12. — S. 111–113.
9. Kriminalistika / otv. red. B. P. Smagorinskij ; M-vo vnutr. del Ros. Federacii, Vyssh. sledstv. shk. — Volgograd : VSSh, 1994. — 559 s.
10. Tarkinskij A. I. Psihologicheskij kontakt v strukture doprosa poterpevshego i svidetelya // Vestnik Dagestanskogo gosudarstvennogo universiteta. — 2011. — № 2. — S. 248–252.
11. Edwards G. Cybercrime Investigator's Handbook. — Wiley, 2019.
12. Bilton N. American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road. — 2017.