2. *Винокуров, А. Ю.* О некоторых вопросах прокурорского надзора в связи с принятием Федерального закона «О порядке отбывания административного ареста» / А. Ю. Винокуров // Право и политика. – 2014. – № 10. – С. 1561–1566.

3. *Винокуров, А. Ю.* Административное преследование как функция прокуратуры Российской Федерации: теоретические, правовые и организационные аспекты: моногр. / А. Ю. Винокуров; ун-т прокуратуры Рос. Федерации. – М.: Проспект, 2019. – 552 с.

4. *Винокуров, А. Ю.* Участие прокурора в рассмотрении судами дел об административных правонарушениях: проблемы межфункционального разграничения / А. Ю. Винокуров // Проблемы реализации полномочий прокурора в гражданском, административном и арбитражном процессе: сб. материалов круглого стола (Москва, 26 октября 2018 г.) / под общ. ред. Н. В. Субановой; сост. и науч. ред. М. В. Маматов, О. В. Боброва; ун-т прокуратуры Рос. Федерации. – М., 2019. – С. 19–26.

5. *Винокуров, А. Ю.* О некоторых вопросах правового регулирования деятельности органов прокуратуры государств – участников СНГ по осуществлению административного преследования / А. Ю. Винокуров // Административное и муниципальное право. – 2015. – № 6. – С. 609–616.

6. *Винокуров, А. Ю.* Предмет и пределы осуществляемого прокурорами административного преследования / А. Ю. Винокуров // Актуальные вопросы права и законности в Российской Федерации: сб. материалов науч.-практич. конф. (Москва, 8 октября 2018 г.). – М.: Московск. гос. ун-т, 2018. – С. 3–6.

7. *Винокуров, А. Ю.* О некоторых вопросах закрепления в кодифицированных актах государств – участников СНГ полномочий прокуроров по осуществлению административного преследования / А. Ю. Винокуров // Административное и муниципальное право. – 2015. – № 7. – С. 719–725.

УДК 343.1:343.5 (476)

ПРОБЛЕМЫ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ, В ХОДЕ КОТОРЫХ ИСПОЛЬЗУЕТСЯ КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ

Гринько Валерий Павлович

старший прокурор управления Генеральной прокуратуры Республики Беларусь, ул. Интернациональная, 22, 220030 Минск, Республика Беларусь, valerijgrinko@gmail.com

Аннотация. В статье отмечается, что интеграция современных информационных технологий во все сферы человеческой деятельности привела к информатизации и компьютеризации преступности; с использованием компьютерных средств и систем возможно совершение практически любых преступлений. Рассматриваются вопросы проведения следственных действий, в ходе которых следователем используется компьютерная информация. Автором затрагиваются отдельные проблемы проведения осмотра компьютерных устройств, необходимость получения санкции прокурора.

Ключевые слова: выемка, компьютерная информация, осмотр электронных устройств, тайна переписки, осмотр и выемка почтово-телеграфных отправлений.

ISSUES OF CONDUCTING INVESTIGATIVE ACTIVITIES IN WHICH COMPUTER INFORMATION IS USED

Valery Grinko

Senior Prosecutor of the Department of the Prosecutor General's Office of the Republic Belarus, 22 Internatsionalnaya Str., 220030 Minsk, Republic of Belarus, valerijgrinko@gmail.com

Abstract. The paper notes that the integration of modern information technologies in all spheres of human activity has led to the informatization and computerization of crime, when it is possible to commit almost any crime by means of computer tools and systems. Deals with the issues of individual investigative activities, during which the investigator uses computer information. The author touches upon some problems of inspection of computer devices, the need to obtain the approval of the prosecutor.

Keywords: seizure, computer information, inspection of electronic devices, secrecy of correspondence, inspection and seizure of postal and Telegraph items.

Введение. Технологии, построенные на использовании микроэлектроники, являющиеся технологиями пятого технологического уклада в экономике, нашли свое воплощение в миллиардах мобильных электронных устройств по всему миру. Сейчас трудно представить нашу жизнь без ежедневного их использования. Однако любая из технологий, улучшающих качество жизни человека, в список которых можно с полной уверенностью включить Интернет и другие телекоммуникационные сети, имеет оборотную сторону. В случае с веб-технологиями это проявляется в использовании информации в целях подготовки, совершения и сокрытия преступной деятельности.

Компьютеры, мобильные телефоны, навигаторы, телевизоры с возможностью выхода в Интернет и Skype становятся носителями огромного количества цифровой информации, и, следовательно, преступления, совершаемые с использованием этих устройств, оставляют в них электронные криминалистически значимые следы.

Способ передачи сообщений посредством электронной почты набирает все большую популярность. В настоящее время преимущественная часть деловой переписки ведется в форме обмена электронными письмами. Не меньшее распространение получили и системы мгновенного обмена сообщениями (так называемые «мессенджеры» – WhatsApp, Viber, Telegram и прочие). Посредством электронной почты

и мессенджеров передаются не только текстовые сообщения, но и фотографии, видео, документы.

Эти распространенные средства связи широко используются не только в законных целях, но и для подготовки и организации всевозможных преступлений. Мобильные телефоны и иные устройства используются при совершении преступлений экстремистской и террористической направленности, в сфере экономики, компьютерной информации, телефонного мошенничества, торговли наркотиками и оружием, распространения детской порнографии.

Глубокое понимание технических возможностей средств мобильной связи по хранению в них текстовой и звуковой информации, фото- и видеозаписей, содержания SMS- и MMS-сообщений, по анализу входящих и исходящих звонков и сообщений как источника сведений о социальных связях субъекта и т. д. существенно расширяет доказательственную базу уголовного дела.

Использование электронных устройств (сотовых телефонов, смартфонов, планшетных компьютеров, портативных устройств GPS и др.) в приготовлении, совершении преступлений, сокрытии его следов требует совершенствования действующего законодательства в целях использования содержащейся в них информации в качестве доказательств.

Основная часть. Хранимая в электронных устройствах информация разнообразна и может иметь важное оперативное и доказательственное значение.

Актуальным стал вопрос, связанный с изъятием, фиксацией и исследованием информации, содержащейся в таких средствах. Ценность такой информации очевидна для выявления, раскрытия и расследования преступлений, идентификации неопознанных трупов и др. Ведь с помощью данной информации следователь может определить местонахождение субъекта преступления, его соучастников, свидетелей, потерпевших в определенное время, ознакомиться с журналом звонков, содержанием СМС-переписок, чатов и т. д.

К такой информации можно, помимо сведений об исходящих и входящих звонках, продолжительности вызовов, в частности отнести:

- сведения о финансовых операциях в мобильных приложениях, связанных с банковскими (Мобильный банкинг и т. п.) и подобными услугами (ПэйПал, Киви-кошелек и др.);
- сведения из социальных сетей (Фейсбук, ВКонтакте, Одноклассники, Инстаграм), которые включают в себя перечень контактов, переписку, лайки, репосты, загруженные и выгруженные видео, аудио, фото и др.;

• сведения о посещении сайтов, загрузке документов. Например, покупки в интернет-магазинах и др.;

• сведения из мессенджеров;

• сведения из других многообразных приложений (например, Google Карты сохраняет информацию о перемещениях);

• фото, аудио и видео, которые снимал владелец мобильного устройства.

Первым шагом на пути унификации действующего процессуального законодательства Республики Беларусь и его адаптации к современным возможностям совершению преступлений с использованием компьютерной техники стало включение в УПК Республики Беларусь (далее – УПК) термина «компьютерная информация» [1].

Так, в ч. 2 ст. 173 и ст. 203 УПК внесены дополнения, дающие возможность следователю производить осмотр компьютерной информации, в том числе до возбуждения уголовного дела. Статью 204 УПК дополнила часть 3–1, в соответствии с которой при невозможности (нецелесообразности) изъятия объекта, содержащего компьютерную информацию, имеющую значение для уголовного дела или материалов проверки, при осмотре допускается ее копирование (фиксация), о чем в протоколе делается запись.

Вступившие в силу с 15 апреля 2021 г. изменения в Закон «Об оперативно-розыскной деятельности» также были рассчитаны для работы с компьютерной информацией; в ст. 2 данного закона впервые дано определение понятию «компьютерная информация», под которой понимаются сведения, воспринимаемые (воспринятые) комплексом программно-технических средств [2].

До внесения указанных дополнений следственная практика при получении такой важной информации, содержащейся в компьютерной технике, складывалась весьма разрозненно.

По своей природе и назначению осмотр компьютерной информации и ее извлечение не подпадало ни под одно следственное действие, предусмотренное УПК, при этом имелась острая потребность и техническая возможность его производства.

По сути, осмотр компьютерной информации и извлечение данных из электронных устройств завуалировался под способ производства другого следственного действия – осмотра предмета. Закон Республики Беларусь от 6 января 2021 г. № 85-З «Об изменении кодексов по вопросам уголовной ответственности» устранил указанный пробел в законодательстве.

Вместе с тем, открытым остается вопрос о необходимости получения санкции прокурора на осмотр компьютерной информации.

На современном этапе развития информационных технологий в следственной и судебной практике компьютерная информация стала повсеместно использоваться в целях расследования преступлений и доказывания обстоятельств их совершения. В свою очередь, процедуры ограничения права на тайну переписки, почтовых, телефонных переговоров, телеграфных и иных сообщений в ходе проведения следственных действий правоприменителями стали рассматриваться в разной правовой плоскости.

Ключевое значение в данном случае имеет гарантия допустимости полученных доказательств, т. е. соблюдения требований Конституции Республики Беларусь и УПК, касающихся законности их сбора и фиксации в процессуальных документах.

В связи с этим в статье речь пойдет о конституционности изъятия (выемки) и осмотра электронных устройств, законности использования содержащейся в электронном устройстве информации без санкции прокурора.

Изъять электронное устройство следователь может при производстве:

- осмотра места происшествия (ст. 203 УПК);
- осмотра трупа (ст. 205 УПК);
- обыска (ст. 208 УПК);
- выемки (ст. 209 УПК);
- личного обыска подозреваемого, обвиняемого (ст. 211 УПК).

Кроме того, выемку электронного устройства могут осуществить сотрудники органа дознания по письменному поручению следователя, в производстве которого находится уголовное дело.

Данные об изъятии должны включаться в протокол соответствующего следственного действия. Нередки ситуации, при которых телефон изымается, и сотрудники правоохранительных органов получают доступ к охраняемым законом сведениям, содержащим персональные данные, без санкции прокурора, которая в этом случае необходима. Такие данные могут быть использованы против лица, у которого изъято электронное устройство.

В законодательстве Республики Беларусь предусмотрено несколько видов тайн, которые подлежат охране (государственная тайна [3], банковская тайна [4], налоговая тайна [5] и др.).

В статье 13 УПК закреплен принцип охраны личной жизни, основу которого составляют положения ст. 28 Конституции Республики Беларусь о праве гражданина на защиту от незаконного вмешательства в личную жизнь (в том числе от посягательства на тайну корреспонденции, телефонных и иных сообщений, на честь и достоинство). Данный

принцип также воспроизводит норму ст. 17 Международного пакта о недопустимости произвольного вмешательства в личную или семейную жизнь человека.

Ограничение права на охрану личной жизни допускается только в случаях и в порядке, предусмотренных УПК. При этом вторжение в сферу личной жизни должно быть обоснованным, осуществляться согласно мотивированному постановлению соответствующего должностного лица органа уголовного преследования, быть санкционировано прокурором, его заместителем либо осуществлено по постановлению Председателя Следственного комитета Республики Беларусь, Председателя Комитета государственной безопасности Республики Беларусь или лиц, исполняющих их обязанности.

Основания и алгоритм проведения обыска, выемки, наложения ареста на почтово-телеграфные и иные отправления, прослушивания и записи переговоров, ведущихся по техническим каналам связи, иных переговоров установлены в гл. 24 УПК.

В практике имеют место случаи, при которых мобильный телефон или иное электронное устройство изымается, и сотрудники правоохранительных органов получают доступ к охраняемым законом сведениям, содержащим персональные данные, без санкции прокурора, которое в этом случае необходимо. Такие данные могут быть использованы против лица, у которого изъято электронное устройство.

Причем, как представляется, в случае извлечения из телефона данных записной книжки, заметок в календаре (информации, лишенной содержательного наполнения) санкцию прокурора получать не нужно. Если же извлекаются данные СМС, переписка в социальных сетях, Skype, по электронной почте, чатах и т. п., т. е. те сведения, которые наполнены содержанием, необходимо обращаться с ходатайством к прокурору о получении санкции.

С учетом природы и степени вмешательства в личную жизнь осмотр личной переписки, содержащейся в мобильном телефоне, фактически идентичен осмотру почтово-телеграфным и иным отправлениям, который в соответствии с ч. 1 ст. 213 УПК производится с санкции прокурора.

Несмотря на то, что УПК прямо не закрепляет обязанность следователя получать санкцию прокурора на осмотр СМС-переписки, эта обязанность вытекает из других норм как уголовно-процессуального закона и положений Конституции Республики Беларусь, так и из международных норм, закрепленных в Конвенции о защите прав человека и основных свобод.

Очевидно, что приведенные выше положения предполагают защиту тайны личной жизни, требуя санкции прокурора на любые оперативно-розыскные мероприятия и следственные действия, которые могут ее нарушить.

Зачастую в ходе осмотра сотового телефона его владелец сообщает следователю установленный в нем пароль, выражает готовность представить распечатку телефонных соединений с используемого им номера, не возражает против исследования имеющихся в телефоне сообщений и сведений о телефонных соединениях. В связи с этим существует мнение, что нет оснований полагать, что были нарушены конституционные права этого лица.

Вместе с тем, обоснование выводов о законности проведенного следственного действия тем, что со стороны участников уголовного процесса не поступило возражений на осмотр СМС-переписки, а телефон был выдан добровольно, представляется малоубедительным. Ведь не учтено, что СМС-переписка имеет двусторонний характер и содержит мысли не только потерпевшего, но и других лиц, пусть и имеющих отношение к делу, но вообще никак не уведомленных о том, что их личная переписка будет достоянием органов предварительного следствия.

Кроме того, представляется, что не исключена возможность оказания психологического давления со стороны сотрудников правоохранительных органов, под действием которого лицо сообщает пароль, не возражает против осмотра, предоставляет распечатку и т. п.

Заключение. Таким образом, на основе анализа законодательства, зарубежного опыта считаем необходимым внести изменения в нормы уголовно-процессуального законодательства, выражающиеся в том, что изъятие электронного устройства допустимо и без санкции прокурора, однако осмотр любой хранящейся в нем информации возможен только после получения санкции прокурора на это. Получение такой санкции не должно ставиться в зависимость от того, согласен ли владелец электронного устройства на его осмотр. Кроме того, следует понимать, что закон должен справедливо предусматривать форс-мажорные ситуации, когда времени на получение санкции прокурора может не быть.

В связи с этим в УПК необходимо предусмотреть норму, предусматривающую, что в исключительных случаях, когда осмотр компьютерной информации не терпит отлагательства, он может быть проведен по постановлению следователя, органа дознания без санкции прокурора с последующим направлением ему в течение 24 часов сообщения о проведенном осмотре.

Резюмируя вышесказанное, следует упомянуть о том, что законодателем был определен необходимый фарватер дальнейшего развития уголовно-процессуального законодательства, который позволяет следователю получать компьютерную информацию, имеющую доказательственное значение. В свою очередь в настоящее время необходимо на основе всестороннего юридического и логического анализа внедрять новые механизмы, позволяющие использовать информационные технологии для противодействия преступности.

Эффективность получения доказательственной информации, размещенной в сети Интернет, также напрямую зависит от тактической и технической компетенции следователя. Грамотная организация взаимодействия со специалистами, оперативными работниками, учет технических особенностей различных носителей цифровой информации при их обнаружении, фиксации и изъятии обеспечат высокое качество раскрытия и расследования преступлений.

Список цитированных источников

1. Об изменении кодексов по вопросам уголовной ответственности [Электронный ресурс]: Закон Респ. Беларусь, 6 янв. 2021 г., № 85-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

2. *Ерошенко, Н. А.* О новациях Закона об оперативно-розыскной деятельности / Н. А. Ерошенко // Законность и правопорядок. – 2021. – № 1. – С. 10–11.

3. О государственных секретах [Электронный ресурс]: Закон Респ. Беларусь, 19 июля 2010 г., № 170-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

4. Банковский кодекс Республики Беларусь [Электронный ресурс]: 25 окт. 2000 г., № 443-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

5. Налоговый кодекс Республики Беларусь [Электронный ресурс]: 19 дек. 2002 г., № 166-З: в ред. Закона Респ. Беларусь от 30 дек. 2018 г., № 159-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

УДК 343.133.2

ПРИМИРЕНИЕ С УЧАСТИЕМ МЕДИАТОРА: ИСТОРИЯ И ОСОБЕННОСТИ БЕЛОРУССКОЙ МОДЕЛИ

Зайцева Людмила Львовна

кандидат юридических наук, доцент, заведующий кафедрой прокурорской деятельности, учреждение образования «Институт переподготовки и повышения квалификации судей, работников прокуратуры, судов