УДК 343.54

ОБ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СПОСОБАХ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ И ПОЛОВОЙ СВОБОДЫ

А. Н. Примаков
старший преподаватель кафедры уголовного процесса и криминалистики
Могилевского института МВД (Беларусь)

На основе результатов изучения статистических данных и материалов уголовных дел против половой неприкосновенности и половой свободы в статье с криминалистической точки зрения рассматриваются способы подготовки, совершения и сокрытия данных видов преступлений, связанные с использованием информационно-телекоммуникационных технологий. Определены наиболее вероятные действия преступника для каждого этапа противоправного поведения, а также возможность использования полученных данных в процессе их раскрытия и расследования.

Для успешного расследования указанной категории преступлений предопределена необходимость в изъятии и исследовании компьютерной информации, а также соответствующих следов, оставленных на месте происшествия и иных объектах. Обозначается проблема отсутствия должной уголовно-процессуальной регламентации участия специалиста при получении, фиксации и изъятии таких следов. Предлагаются пути ее решения, в частности через изложение дополнительных положений в уголовно-процессуальном законе.

Ключевые слова: *половая свобода, половая неприкосновенность, способ совершения преступления, информационно-телекоммуникационные технологии, электронные носители информации, цифровые следы.*

Преступления против половой неприкосновенности и половой свободы совершались всегда, во всем мире, на всех социоэкономических уровнях, во всех возрастных группах, начиная с дошкольного и младшего школьного возраста. Однако способы их совершения практически до начала XX в. оставались в основе своей неизменными — требующими обязательного присутствия другого лица (жертвы). В настоящее же время в условиях глобальной цифровизации общественных отношений и их основополагающих социальных институтов, а также активного развития информационно-телекоммуникационных технологий (далее — ИТТ) и их внедрения в повседневную жизнь общества появились новые дистанционные способы совершения данных видов преступлений.

Так, согласно статистическим данным за 2015–2021 гг., предоставленным ИЦ Министерства внутренних дел Республики Беларусь, практически каждое третье преступление, предусмотренное ст. 169 «Развратные действия» и ст. 170 «Понуждение к действиям сексуального характера» Уголовного кодекса Республики Беларусь, совершено дистанционным способом, связанным с использованием ИТТ, как правило, с помощью социальных сетей и мессенджеров [1]. При этом, помимо тенденции роста количества таких противоправных деяний, потерпевшими от их совершения становятся лица не только женского, но и мужского пола, как правило, находящиеся в малолетнем и подростковом возрасте.

Использование в целях совершения половых преступлений ИТТ, коммуникационных сервисов и программ позволяет преступнику избирательно подходить к выбору своих потенциальных жертв, тщательно планировать и реализовывать действия по подготовке и сокрытию преступления, особенно по вуалированию цифровых следов его совершения, что, в свою очередь, существенно затрудняет процесс раскрытия и последующего успешного расследования преступления.

В криминалистической науке имеется множество суждений различных ученых-криминалистов касаемо определения понятия и содержания способа совершения преступления. Так, по мнению Р. С. Белкина, под таковым понимается система

действий по подготовке, совершению и сокрытию общественно опасного деяния, детерминированных условиями внешней среды и психофизиологическими свойствами личности [2, с. 217]. Практически аналогичное, чуть более конкретизированное, определение способа преступления высказывает Г. Г. Зуйков [3, с. 10]. В свою очередь, И. Ш. Жордания определяет его как систему взаимосвязанных, целенаправленных актов поведения, операций, приемов, движений, применяемых преступником при совершении противоправного деяния [4, с. 12]. По мнению В. Н. Кудрявцева, способ преступления — это заранее подготовленный алгоритм действий и приемов, используемых лицом для совершения преступления [5, с. 71].

Среди ученых дискуссионным также является определение понятия «информационно-коммуникационные технологии». Однако, проанализировав позиции различных авторов [6; 7, с. 295], наиболее точным, на наш взгляд, представляется определение, данное в модельном законе «Об электронных государственных услугах», принятом постановлением Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств от 7 апреля 2010 г. № 34-7. Так, в ст. 2 данного Закона указано, что ИТТ — это совокупность методов и способов поиска, сбора, хранения, обработки и передачи (распространения) информации, доступ к которой и передача которой осуществляется с помощью информационно-телекоммуникационной сети [8]. При этом, как справедливо отмечает Е. И. Боброва, функционирование этих информационных процессов осуществляется с помощью различных технических устройств, телекоммуникационных средств, электронных носителей информации, коммуникационных сервисов и программ [9, с. 55].

Таким образом, под способом совершения преступлений применительно к данному виду преступлений следует понимать систему действий по подготовке, совершению и сокрытию сексуального посягательства, осуществляемого с помощью информационно-телекоммуникационных средств, электронных носителей информации, коммуникационных сервисов и программ, детерминированного условиями внешней среды и психофизическими свойствами личности.

Способ преступных действий выступает как своеобразный фактор, обуславливающий закономерности возникновения доказательств и источник информации, необходимый для разработки всех составных частей криминалистики (техники, тактики и методики расследования), в целях раскрытия и расследования полового преступления, установления лица, его совершившего [10, с. 53]. В. Н. Чулахов отмечает, что, проанализировав эти действия, можно установить фактическое и правовое содержание расследуемого события, мотивы действий его участников, а также выделить навыки личности преступника, возникшие вне связи с совершением преступления, и преступные, сформированные в процессе противоправной деятельности, которые, как правило, формируются в ходе подготовки к преступлению и совершенствуются при повторных аналогичных преступлениях [11, с. 206–207]. В нашем случае это прежде всего индивидуально-психологические признаки личности, характеризующие: уровень интеллекта преступника, его способность логично и рационально мыслить; его сексуальные наклонности (гомосексуальные, педофильные и т. д.), наличие психических отклонений (расстройств), тип преступника и т. п.

Представляется, что одним из основных направлений криминалистического познания преступного события является поэтапное исследование личности преступника и способа совершения преступления, особенностей его действий в конкретных ситуациях, их содержания и взаимосвязей между собой [12, с. 56].

Результаты изучения материалов уголовных дел позволили установить, что перед совершением развратных действий и понуждений к действиям сексуального характера путем шантажа в социальных сетях и мессенджерах преступники, как правило, осуществляют следующие подготовительные действия:

– регистрируют учетную запись на чужие или вымышленные идентификационные данные;

– верифицируют учетную запись через «фейковый» абонентский номер и (или) электронную почту;

– проводят мониторинг аккаунтов потенциальных жертв с открытым доступом;

– отправляют сообщения потерпевшим (начинают переписку) с предложением о дружбе, с просьбой об оказании помощи и т. д.;

– осуществляют несанкционированный доступ к аккаунту потерпевшего лица с целью получения конфиденциальных сведений о его личности.

Половые преступления, связанные с использованием ИТТ, совершаются тремя основными способами:

1) посредством осуществляемого в социальных сетях или мессенджерах шантажа — выдвижения требования совершить действия сексуального характера, сопровождающегося угрозой в случае отказа распространить сведения, которые потерпевшее лицо желало бы сохранить в тайне;

2) путем передачи в социальных сетях или мессенджерах лицу, заведомо не достигшему шестнадцатилетнего возраста, порнографических фотоизображений и (или) видеозаписей (онлайн-груминг);

3) путем проведения с помощью информационно-коммуникационных сетей и мессенджеров либо мобильной связи бесед сексуального содержания с лицами, не достигшими шестнадцатилетнего возраста.

После совершения противоправных действий преступники наиболее часто с целью их сокрытия:

– удаляют детализации телефонных соединений или сообщений (переписок) с потерпевшими;

– удаляют используемые для совершения преступления учетные записи в социальной сети или мессенджере;

– удаляют аккаунты электронной почты, посредством которых осуществлялась верификация учетной записи;

– придумывают ложные алиби и дают ложные показания;

– угрожают потерпевшим разгласить сведения, которые последние желали бы сохранить в тайне;

– меняют места жительства или места наиболее частого пребывания.

Особое доказательственное значение для раскрытия и расследования преступлений рассматриваемой категории, совершенных способами, связанными с использованием ИТТ, приобретает компьютерная информация, а соответственно, цифровые следы — сведения (данные, сообщения), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов [13, с. 10].

Местом обнаружения таких следов выступают как материальные, так и информационные объекты: сайты глобальной сети Интернет, учетные записи (аккаунты) и профили пользователей в различных социальных сетях и мессенджерах («ВКонтакте», WhatsApp, Viber, Telegram и др.), базы данных операторов сотовой связи, жесткие диски персональных компьютеров и ноутбуков (макбуков), средства мобильной связи, планшеты, их карты памяти и т. д. [14]. При этом наиболее часто, по нашим данным, компьютерная информация (цифровые следы преступлений) изымается в электронном виде при осмотре места происшествия либо иных предметов в виде:

– копий совместных сообщений (переписки) преступника и потерпевшего, если таковые имеются, с прикрепленными фотоизображениями и видеозаписями порнографического содержания;

– детализаций телефонных соединений;

– копий сообщений (уведомлений) электронной почты;

– копий голосовых сообщений в виде аудио-, видеофайлов;

– компьютерных (цифровых) данных, содержащих информацию об истории браузера, кэше (местах хранения копий файлов используемых программ), IP-адресе устройства, с помощью которого осуществлялось подключение к сети Интернет, сведения об учетной записи пользователя, ее идентификационном номере (ID), о наличии либо отсутствии доступа к аккаунту, его логине и пароле, о хеш-файлах.

Для использования ИТТ в процессе раскрытия и расследования преступлений, в том числе по рассматриваемой категории, следователь (лицо, производящее дознание) обязан: проверить методику применения используемых технических средств, поскольку она должна быть научно обоснованной и рекомендованной к практическому использованию; соблюдать установленный процессуальный порядок, законные права и интересы лица, в отношении которого проводятся следственные действия; принимать меры к недопущению искажения полученной (изъятой) информации. Несоблюдение либо нарушение указанных общих требований может привести к тому, что изъятые источники доказательств в последующем в суде могут быть признаны недопустимыми.

При проверке сообщений о преступлениях, в том числе по рассматриваемой категории, отмечается ряд проблем, связанных с копированием (изъятием) компьютерной информации с ее электронных носителей. Специалист для проведения таких следственных действий привлекается на общих основаниях по усмотрению следователя. Вместе с тем, по нашему мнению, участие специалиста, как правило из IT-сферы, для оказания помощи по фиксации и изъятию электронных носителей информации не требуется. Однако использовать его специальные знания необходимо при осуществлении фиксации и изъятия компьютерной (цифровой) информации.

Иными словами, изъять электронные носители информации (например, системный блок компьютера или его жесткий диск, ноутбук, мобильный телефон и др.), если для этого не требуется использование специальных знаний, следователь может самостоятельно, без привлечения специалиста. А вот для фиксации и изъятия компьютерных следов с указанных электронных носителей либо с сайтов в сети Интернет и их удаленных (накопительных) серверов, обеспечения их сохранности и возможности использования в качестве доказательства по уголовному делу участие специалиста представляется обязательным.

Соответственно, для более качественного и эффективного осуществления следственных действий в уголовно-процессуальном законе необходимо дополнительно регламентировать положения, предусматривающие порядок привлечения специалиста при проведении следственных действий, в ходе которых осуществляется фиксация и изъятие компьютерной информации с электронных носителей, а именно, обозначить его участие обязательным.

Таким образом, в заключение отметим, что в настоящее время значительное количество преступлений против половой неприкосновенности и половой свободы подготавливается и совершается способами, связанными с ИТТ. Использование вышеуказанных сведений об особенностях их криминалистической характеристики в процессе раскрытия и расследования данных видов преступлений представляется особенно важным, поскольку с их помощью можно выдвинуть наиболее вероятные версии о личности и подготовительных действиях преступника, об оставленных цифровых следах, о жертве и предшествующем попаданию в криминогенную ситуацию ее поведении, о характере и конкретном способе совершения сексуального посягательства.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ИЦ МВД Республики Беларусь // Отчет о регистрации и предварительном расследовании преступлений против половой свободы и половой неприкосновенности в Республике Беларусь и лицах, их совершивших, 2015–2021 гг.

2. Белкин, Р. С. Криминалистическая энциклопедия / Р. С. Белкин. — М., 1997. — 339 с.

3. Зуйков, Г. Г. Криминалистическое понятие и значение способа совершения преступления / Г. Г. Зуйков // Труды Высшей школы Министерства охраны общественного порядка СССР. — М., 1967. — Вып. 15. — С. 51–57.

4. Жордания, И. Ш. Структура и правовое значение способа совершения преступления / И. Ш. Жордания. — Тбилиси. — 1977. — 302 с.

5. Кудрявцев, В. Н. Объективная сторона преступления / В. Н. Кудрявцев. — М., 1960. — 245 с.

6. Роберт, И. В. Толковый словарь терминов понятийного аппарата информатизации образования / И. В. Роберт, Т. А. Лавина. — М. : Лаборатория знаний, 2014. — 69 с.

7. Мухина, Ю. Р. Соотношение понятий «информационные технологии» и современные информационные технологии» в обучении / Ю. Р. Мухина // Молодой ученый. — 2009. — № 11. — С. 295–298.

8. О модельном законе «Об электронных государственных услугах» [Электронный ресурс] : постановление Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств, 7 апр. 2010 г., № 34-7. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2022.

9. Боброва, Е. И. Информационно-коммуникационные технологии / Е. И. Боброва. — Кемерово : КемГУКИ, 2010. — 156 с.

10. Зуйков, Г. Г. Криминалистическое учение о способе совершения преступления : автореф. дис. … д-ра юрид. наук / Г. Г. Зуйков. — М., 1970. — С. 10.

11. Чулахов, В. Н. Криминалистическое учение о навыках и привычках человека : монография / В. Н. Чулахов ; под ред. Е. Р. Россинской. — М. : Юрлитинформ, 2007. — С. 206–207.

12. Багмет, А. М. Расследование изнасилования и иных насильственных действий сексуального характера, совершенных в отношении несовершеннолетних и/или несовершеннолетними в составе группы : учеб. пособие для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / А. М. Багмет, В. В. Бычков, А. М. Сажаев. — М. : ЮНИТИ-ДАНА, 2017. — С. 63.

13. Милашев, В. А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. … канд. юрид. наук / В. А. Милашев. — М., 2007. — С. 10.

14. Кирсанова, С. О, Виртуальные следы: понятие, сущность, проблемы [Электронный ресурс] / С. О. Кирсанова, А. А. Калинина // Скиф. — 2018. — № 3 (19). — Режим доступа: https://cyberleninka.ru/article/n/virtualnye-sledy-ponyatie-suschnost-problemy. — Дата доступа: 12.10.2022.

Поступила в редакцию: 19.10.2022 г.

Primakov A. N.

ON INFORMATION AND TELECOMMUNICATION WAYS OF COMMITTING CRIMES AGAINST SEXUAL INTEGRITY AND SEXUAL FREEDOM

Based on the results of the study of statistical data and materials of criminal cases against sexual integrity and sexual freedom, the article examines from a forensic point of view the methods of preparation, commission and concealment of these types of crimes related to the use of information and telecommunication technologies. The most probable actions of the criminal for each stage of illegal behavior are determined, as well as the possibility of using the data obtained in the process of their disclosure and investigation.

For the successful investigation of this category of crimes, the need for the seizure and investigation of computer information, as well as the corresponding traces left at the scene and other objects, is predetermined. The problem of the lack of proper criminal procedural regulation of the participation of a specialist in obtaining, fixing and removing such traces is indicated. The ways of its solution are proposed, in particular, by setting out additional provisions in the Criminal Procedure Law.

Keywords: *sexual freedom, sexual inviolability, method of committing a crime, information technology, electronic media, digital traces.*