Научная статья
УДК.343.985.7:004(470)

Юлия Ивановна Юрина
Барнаульский юридический институт МВД России, Барнаул, Россия, iulia.iurina@mail.ru

НЕКОТОРЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В научной статье автором рассмотрены некоторые направления борьбы правоохранительных органов с преступлениями, совершенными посредством использования информационно-телекоммуникационных технологий. Отмечается, что в настоящее время меры по борьбе с данного рода преступлениями, предпринятые государством, недостаточны и требуют непрерывного совершенствования. Автор обращает внимание на проблему взаимодействия следователя с операторами сотовой связи и кредитно-финансовыми учреждениями при расследовании преступлений данной категории.

Ключевые слова: информационно-телекоммуникационные технологии, сеть Интернет, киберпреступления, запрос, сотовые компании, поручение

Для цитирования: Юрина Ю. И. Некоторые проблемы раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Общество, право, государственность: ретроспектива и перспектива. 2022. № 4 (12). С. 73–77.

Original Article

Julia I. Yurina
Barnaul Law Institute of the Ministry of Internal Affairs of Russia, Barnaul, Russia, iulia.iurina@mail.ru

SOME PROBLEMS OF DETECTION AND INVESTIGATION OF CRIMES COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Abstract. The article considers some areas of law enforcement activities in the fight against crimes committed through the use of information and telecommunication technologies. It is noted that currently the measures taken by the state to combat this kind of crimes are insufficient and require continuous improvement. The author draws attention to the problem of the investigator's interaction with cellular operators and credit and financial institutions in the investigation of crimes of this category.

Keywords: information and telecommunication technologies, Internet, cybercrimes, inquiry, cellular companies, assignment

For citation: Yurina J. I. Some problems of detection and investigation of crimes committed with the use of information and telecommunication technologies // Society, law, statehood: retrospective and perspective. 2022. No. 4 (12). P. 73−77.

В современном мире посредством использования информационно-телекоммуникационных технологий (далее – IT-технологий) в России совершаются хищения денежных средств с банковских счетов граждан, незаконный оборот наркотических, психотропных веществ и их аналогов, оружия и боеприпасов к нему, преступления экстремистской направленности, вербовка новых членов террористических группировок, мошенничества с использованием сотовой связи, а также средств IP-телефонии, кражи персональных данных в больших объемах и их продажа [1].

Согласно характеристике состояния преступности за январь-март 2022 г. в России статистика совершенных киберпреступлений не претерпела изменений по сравнению с данными за прошлый год. Однако по-прежнему каждое четвертое преступление совершается с использованием IT-технологий [2].

Борьба государства с киберпреступлениями ведется повсеместно и разнопланово. В 2021 г. в деятельность органов внутренних дел России внедрены базы данных, предназначенные для дистанционного изобличения кибермошенников, позволяющие устанавливать причастность лиц к серийным преступлениям [3]. В Алтайском крае данный учет функционирует в соответствии с приказом Главного управления Министерства внутренних дел России по Алтайскому краю (далее – ГУ МВД России по АК) от 18 ноября 2021 г. № 499 «Об использовании и пополнении подсистемы ИБД-Ф «Дистанционное мошенничество», на основании которого загружается первичная информация о зарегистрированных сообщениях (заявлениях) о преступлениях, совершенных дистанционным способом с использованием IT-технологий.

На протяжении трех лет в структуре Министерства внутренних дел Российской Федерации (далее – МВД России) создаются новые подразделения, специализирующиеся на противодействии преступлениям, совершаемым с использованием IT-технологий. На начало марта 2021 г. численность сотрудников таких подразделений составила более 5 тыс. человек [4].

Важную роль играют знания и умения сотрудников вышеуказанных подразделений о механизме образования следов преступления в сети Интернет. В. А. Мещерякова считает, что в новых реалиях необходимо включить виртуальные следы, оставленные в ходе совершения компьютерных преступлений, в традиционную классификацию материальных следов преступления [5]. Различаются мнения авторов по поводу соотношения цифровых и виртуальных следов. Вместе с тем ряд специалистов заявляет о наличии информационных следов [6]. По данным Е. С. Переверзевой и А. В. Комова, они находятся исключительно в сетевом пространстве в отличие от цифровых, которые могут быть на материальных носителях (цифровых носителях) [7].

Полагаем, что виртуальные, информационные и цифровые следы следует рассматривать как тождественные понятия. Примерами таких следов являются: MAC-адреса сетевого оборудования (компьютера, роутера, сетевой карты и т. п.); IP-адреса компьютера в сети и других устройств; адрес электронной почты; ID в социальных сетях (идентификатор пользователя); идентификационный номер банковской карты и транзакции, произведенные с ней; номер телефона; информация о соединениях абонента; данные геолокации (базовой станции, мобильного телефона или любого девайса, подключенного к Интернету) и т. п.

Верно отмечает И. Б. Воробьева, что для обнаружения, фиксации и изъятия данных следов требуются принципиально новые методы, средства и технологии [8, с. 195]. Эксперты экспертно-криминалистических центров МВД России используют различные инновационные программные комплексы в ходе проведения экспертиз, направленных в первую очередь на поиск явных, скрытых, ранее удаленных данных на электронных носителях. Как известно, к цифровым следам преступления относятся не только мобильные телефоны, компьютеры, планшеты, но и явная или неявная информация в виде платежных операций, передача запрещенной информации (экстремизм, терроризм и т. д.) посредством мессенджеров, социальных сетей и др.

В целях обнаружения, фиксации и изъятия вышеуказанных следов появляется необходимость взаимодействия на стадии предварительного расследования с сотрудниками территориальных органов внутренних дел Алтайского края (далее – ТОВД АК), что подтверждается распоряжением начальника ГУ МВД России по АК от 1 февраля 2022 г. № 12 «О мерах по повышению эффективности раскрытия и расследования

преступлений, совершенных с использованием IT-технологий».

Взаимодействие следователя с ТОВД АК при раскрытии и расследовании уголовных дел, совершенных с использованием IT-технологий, осуществляется при производстве следственных действий и оперативно-розыскных мероприятий, направленных на получение информационных следов преступления. В целях получения таковых направляются запросы в кредитно-финансовые учреждения и сотовые компании, к Интернет-провайдерам и администраторам различных социальных сетей. Процедура отправки запросов обязательна и урегулирована нормативно. Так, согласно распоряжению начальника ГУ МВД России по АК от 1 февраля 2022 г. № 12 «О мерах по повышению эффективности раскрытия и расследования преступлений, совершенных с использованием IT-технологий» в срок не позднее 3 суток с момента возбуждения уголовного дела следователю либо дознавателю необходимо направить запрос в кредитно-финансовое учреждение с целью получения информации о вкладах и счетах граждан.

В соответствии со ст. 21 Уголовно-процессуального кодекса Российской Федерации запросы руководителя следственного органа, следователя, органа дознания и дознавателя, предъявленные в пределах их полномочий, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами. Однако срок исполнения данным нормативно-правовым актом не определен.

При принятии решения о направлении запроса для следователя (дознавателя) помимо правильной постановки вопросов важной задачей является определение точного адреса учреждения, куда направляется запрос, и срока его исполнения. Поскольку направление осуществляется путем отправки письма почтовым переводом, то срок получения информации, представляющей интерес следствию, занимает длительный период времени и негативным образом влияет на эффективность раскрытия преступления.

Существуют примеры создания аппаратно-программных комплексов, предназначенных для замены существующего между уполномоченными государственными органами и различными организациями бумажного документооборота по предоставлению информации (по мотивированному запросу уполномоченных органов) на электронный документооборот. Данная система сокращает время предоставления требуемой информации, минимизирует бумажный документооборот и сокращает издержки. Однако на сегодняшний день учреждений и организаций, с которыми территориальные органы министерства внутренних дел заключили соглашение об электронном обмене информации, незначительное количество.

В настоящее время нет единого перечня адресов и исходных данных различных организаций, учреждений, операторов сотовой связи. Поиск информации для следователя является затратным по времени, а использование устаревших данных может привести к направлению повторных запросов и пустой трате ресурсов.

Анализируя вышесказанное, можно выдвинуть следующие предложения по совершенствованию взаимодействия следователя с кредитно-финансовыми учреждениями, сотовыми компаниями, Интернет-провайдерами, администраторами социальных сетей при раскрытии и расследовании уголовных дел, совершенных с использованием IT-технологий:

– разработка единого аппаратно-программного комплекса, предназначенного для пользования следователей (дознавателей), замена существующего между уполномоченными государственными органами и различными организациями бумажного документооборота по предоставлению информации (по мотивированному запросу уполномоченных органов) на электронный документооборот;

– создание ведомственного сайта, подлежащего постоянному обновлению, с перечнем контактных номеров и адресов различных организаций, с указанием возможностей ускоренного направления запроса и соответствующего подразделения, отвечающего за

взаимодействие с кредитно-финансовыми учреждения и операторами сотовой связи;

– установление аппаратного и программного обеспечения в территориальные органы МВД России с доступом в сеть Интернет.

Подводя итог, можно выделить положительные моменты борьбы государства с киберпреступностью, однако ее рост не останавливается. Это означает, что необходимо принять дополнительные меры, а именно провести работу по совершенствованию внешнего взаимодействия следователя с кредитно-финансовыми учреждениями, сотовыми компаниями, Интернет-провайдерами, администраторами различных социальных сетей, в том числе международных, при раскрытии и расследовании уголовных дел, совершенных с использованием IT-технологий.

СПИСОК ИСТОЧНИКОВ

1. Нугаева Э. Д. К вопросу о способе совершения мошенничества под предлогом оказания квалифицированной платной парапсихологической помощи на расстоянии по телефону // Евразийский юридический журнал. 2016. № 3 (94). С. 205−208.

2. В МВД России будут созданы новые подразделения по борьбе с преступностью в сфере высоких технологий. URL: https://мвд.рф/news/ item/18809813/ (дата обращения: 12.09.2022).

3. В МВД сообщили о внедрении программы для изобличения серийных кибермошенников. URL: https://tass.ru/obschestvo/10825525?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 12.09.2022).

4. Краткая характеристика состояния преступности в Российской Федерации за январь-март 2022 года. URL: https://мвд.рф/reports/item/ 29705686/ (дата обращения: 12.09.2022).

5. Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5. С. 265−270.

6. Сафаргалиева О. Н. О понятии и содержании следов в криминалистике // Вестник ОмГУ. Серия. Право. 2010. № 2. URL: https://cyberleninka.ru/article/n/o-ponyatii-i-soderzhanii-sledov-v-kriminalistike (дата обращения: 12.09.2022).

7. Переверзева Е. С., Комов А. В. Виртуальные и цифровые следы: новый подход в понимании // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). URL: https://cyberleninka.ru/article/n/virtualnye-i-tsifrovye-sledy-novyy-podhod-v-ponimanii (дата обращения: 12.09.2022).

8. Воробьева И. Б. Применение больших данных (Big data) при прогнозировании и расследовании преступлений // Вестник Саратовской государственной юридической академии. 2021. № 3 (140). С. 195–202.

REFERENCES

1. Nugaeva E. D. To the question of the method of committing fraud under the pretext of providing qualified paid parapsychological assistance at a distance by telephone // Eurasian Law Journal. 2016. No. 3 (94). P. 205–208. (In Russ.)

2. The Russian Ministry of Internal Affairs will create new units to combat high-tech crime. URL: https://mvd.rf/news/item/18809813/ (date of access: 12.09.2022). (In Russ.)

3. The Ministry of Internal Affairs announced the introduction of a program to expose serial cyber fraudsters. URL: https://tass.ru/obschestvo/10825525?utm_source=yandex. ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (date of access: 12.09.2022). (In Russ.)

4. Brief description of the state of crime in the Russian Federation for January-March 2022. URL: https://mvd.rf/reports/item/29705686/ (date of access: 12.09.2022). (In Russ.)

5. Meshcheryakov V. A. Traces of crimes in the sphere of high technologies // Forensic Library. 2013. No. 5. P. 265–270. (In Russ.)

6. Safargalieva O. N. On the concept and content of traces in criminalistics // Bulletin Omsk State University. Series. Law. 2010. № 2. URL: https://cyberleninka.ru/article/n/o-ponyatii-i-soderzhanii-sledov-v-kriminalistike (date of access: 12.09.2022). (In Russ.)

7. Pereverzeva E. S., Komov A. V. Virtual and digital traces: a new approach in understanding // Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2021. No. 1 (89). URL: https://cyberleninka.ru/article/n/virtualnye-i-tsifrovye-sledy-novyy-podhod-v-ponimanii (date of access: 12.09.2022). (In Russ.)

8. Vorobyeva I. B. The use of big data (Big data) in predicting and investigating crimes // Bulletin of the Saratov State Law Academy. 2021. No. 3 (140). P. 195–202. (In Russ.)

Статья поступила в редакцию 12.09.202; одобрена после рецензирования 20.09.2022; принята к публикации 15.12.2022.

The article was submitted 12.09.2022; approved after reviewing 20.09.2022; accepted for publication 15.12.2022.

.