УГОЛОВНО-ПРАВОВОЙ БЛОК

Научная статья
УДК 343.71:[004.77:316.472.4](470)

Ильфат Давлетнурович Бадамшин
Уфимский юридический институт МВД России, Уфа, Россия, Badam02@mail.ru

СОЦИАЛЬНЫЕ СЕТИ КАК СРЕДСТВО И СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ

Аннотация. Социальные сети играют важную роль в жизни современного общества, что позволяет злоумышленникам использовать их для совершения преступлений. Большинство пользователей социальных сетей, вступающих в контакт с другими участниками данного сегмента, строят общение на взаимном доверии, создавая благоприятные условия для реализации преступных замыслов. В данной статье рассмотрены наиболее часто встречающиеся схемы, в которых социальные сети выступают средством и способом совершения преступлений против собственности. В ходе исследования проведен анализ преступности в социальных сетях на примерах судебной практики, где отражены характеристики данного вида преступлений, такие как общественная опасность, анонимность, трансграничность.

Ключевые слова: социальные сети, Интернет, информационные технологии, информационная безопасность, преступление, собственность, криптовалюта, судебная практика.

Для цитирования: Бадамшин И. Д. Социальные сети как средство и способ совершения преступлений против собственности // Право: ретроспектива и перспектива. 2022. № 2 (10). С. 42–47.

Original Article

Ilfat D. Badamshin
Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia, Badam02@mail.ru

SOCIAL NETWORKS AS A MEANS AND A WAY TO COMMIT CRIMES AGAINST PROPERTY

Abstract. Social networks play an important role in the lives of modern society, which allows the attackers to use them for committing crimes. Most users of social networks, who come into contact with other participants in this segment, build communication on mutual trust, creating favorable conditions for the implementation of criminal designs. This article discusses the most common schemes in which social networks act as a means and a way of committing crimes against property. In the course of the study, crime analysis was carried out in social networks in examples of judicial practice, where the characteristics of this type of crime are reflected, such as public danger, anonymity, cross-border.

Keywords: social networks, Internet, information technology, information security, crime, property, cryptocurrency, judicial practice.

For citation: Badamshin I. D. Social networks as a means and a way to commit crimes against property // Law: retrospective and perspective. 2022. No. 2 (10). P. 42–47.

Социальные сети на сегодняшний день – это важный элемент жизни каждого человека. При этом социальные сети давно перестали быть исключительно средством общения, сейчас в данном информационном пространстве лица осуществляют профессиональную деятельность, становятся лидерами мнений, формируя экономическую и политическую повестку дня. По этой причине злоумышленники все чаще рассматрива-

ют социальные сети как средство и способ совершения преступлений против собственности.

Основной характеристикой социальный сетей является то, что они позволяют в максимально короткое время распространить различного рода информацию, в том числе, не соответствующую действительности и даже формирующую состав преступления, что не всегда подконтрольно сотрудникам правоохранительных органов [1, с. 265].

Наиболее распространенной схемой, направленной на хищение денежных средств, является обращение в социальных сетях к конкретному лицу или к группе лиц с просьбой о материальной помощи. При этом умысел может быть направлен как на знакомое лицо, так и на группу незнакомых лиц (чаще всего реализуется второй вариант путем взлома страницы в социальной сети незнакомого человека и написание просьб о денежной помощи по всему списку подписанных на него «друзей», «фолловеров» и т. д.). Социальная сеть в этом случае дает неоспоримое преимущество – личный профиль человека с определенной репутацией многих лиц может ввести в заблуждение, поэтому они дополнительно не уточняют детали запрашиваемой денежной помощи. Исходя из анализа судебной практики такие деяния наиболее часто квалифицируются по ст.ст. 158, 159, 163 Уголовного кодекса Российской Федерации (далее – УК РФ) с учетом размера причиненного ущерба и в соответствии с обстоятельствами совершенного деяния.

В отдельных случаях социальная сеть также используется как средство быстрого знакомства, а впоследствии и получения «быстрых денег» от конкретного лица. Так, согласно материалам уголовного дела № 1-74/2018, рассмотренного 28 июня 2018 года Калининским районным судом Краснодарского края [2], социальная сеть использовалась подсудимыми Г. и Л. с целью получения денежных средств от потерпевшего якобы необходимых для покрытия затрат на бензин. Социальная сеть «Друг Вокруг» в данном случае помогла реализовать преступный умысел, сделав хищение чужого имущества быстрым и удобным с точки зрения реализации. Действия подсудимых были квалифицированы по ч. 2 ст. 159 УК РФ.

Очень часто преступления, направленные против собственности, именно в социальных сетях коррелируют с честью и репутацией потерпевших. Материальные ресурсы вымогаются по причине уведомления потерпевших о том, что могут быть массово распространены сведения, порочащие личность конкретного человека. В этом случае социальная сеть играет роль инструмента незаконного получения материальных ресурсов, подавления воли и запугивания, в некоторых случаях – распространения порочащих, часто неправдоподобных, сведений.

Так, согласно материалам уголовного дела № 1-99/2020, рассмотренного 2 июля 2020 года Свердловским районным судом г. Белгорода, подсудимый М. посредством социальной сети «ВКонтакте» вымогал денежные средства у потерпевшего, высказывая угрозу о том, что если денежные средства не будут переведены на его счет, он распространит сведения, позорящие потерпевшего, а именно сведения о нетрадиционной сексуальной ориентации и склонности к педофилии последнего, путем их опубликования в социальной сети «ВКонтакте» [3].

Новейшие эквиваленты валюты – цифровая валюта или криптовалюта – также часто становятся инструментом преступлений против собственности, совершаемых в социальных сетях или с помощью их применения [4, с. 364].

Понятие «цифровая валюта» раскрывается в п. 1 ст. 3 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» как совокупность электронных данных, которые содержатся в информационной системе [5].

Зачастую преступники пользуются незнанием и неосведомленностью граждан о криптовалютах, что позволяет субъектам

преступления заявлять о себе как об эксперте в сфере криптовалютных операций. Социальные сети «пестрят» заявлениями о крупных заработках, о желании обучить всех особенностям торговли криптовалютой, что на самом деле почти всегда является разновидностью финансовой пирамиды и ведет к потере денежных вложений потерпевших лиц. Социальная сеть при этом выступает инструментом пиара и массового привлечения лиц, желающих обогатиться быстро на одном из новых финансовых инструментов. Именно по такой схеме действовал подсудимый З., чьи действия впоследствии были квалифицированы судом по ч. 4 ст. 159 УК РФ [6].

Очень серьезные последствия для физических лиц в экономическом плане также формируют так называемые «профессиональные» аккаунты в социальных сетях с предлагаемыми инфопродуктами в виде астрологических предсказаний, составления натальных карт, гаданий на таро или с помощью иного инструментария, «чистки» ауры, различных эзотерических курсов. Так же как и в случае с криптовалютой основной упор делается на бренде лица или группы лиц, а также на обещании предоставить определенные преимущества от пользования услугой. Иногда эти обещания граничат с явно противозаконными действиями – нанесением психологического и физического вреда третьим лицам, а в худшем случае доведением до самоубийства. Социальная сеть в таких случаях также выступает как источник массового распространения сведений о данном аккаунте, именно поэтому подобные курсы и услуги стали так распространены на сегодняшний день.

Стоит отметить, что на федеральном уровне предпринимались попытки по ограничению подобной активности – в 2014 году был предложен соответствующий законопроект [7]. Однако при рассмотрении законопроекта в первом чтении он не был принят. Это формирует, по нашему мнению, острую необходимость в урегулировании подобных отношений на уровне федерального закона.

Одной из противозаконных тенденций, которая в обязательном порядке должна быть больше исследована и в отношении которой должны быть предприняты комплексные меры по пресечению, является распространение социальных сетей изначально преступного направления [8, с. 296]. Прежде всего, это целый сегмент Интернета – Даркнет, который часто выступает в качестве инструмента незаконного получения персональных данных, данных банковских карт и расчетных счетов, иной личной информации, с помощью которой можно совершить преступление против собственности.

Так, согласно материалам уголовного дела № 1-33/2019, рассмотренного 27 ноября 2019 года Автозаводским районным судом г. Тольятти, группа лиц по предварительному сговору осуществляла действия, охватываемые составом ст. 158 УК РФ, с использованием интернет-площадки Даркнет, а именно получали из данной сети:

– сведения личного характера, в том числе: паспортные данные, сведения об открытых счетах в банках, иные персональные данные, позволяющие в дальнейшем совершить кражу дистанционным способом;

– контактные данные для непосредственной реализации преступного умысла;

– реквизиты расчетных счетов, на которые переводились украденные денежные средства в качестве промежуточного этапа, в результате чего обналичивались и распределялись между участвующими в преступном сговоре лицами [9].

Стоит отметить, что незаконные денежные операции активно набирают оборот в Даркнете. По этой причине видится необходимым принятие комплексных мер по борьбе с даркнет-преступностью, направленной, в том числе, на собственность и имущество других лиц. Некоторые авторы предлагают обширные технические и организационные меры, включающие в том числе блокировки VPN-сервисов и любых анонимайзеров, получение данных с открытых веб-сайтов, отслеживание денежных потоков, взлом и работу под прикрытием [10, с. 128].

Такие меры кажутся очень действенными и при условии централизованного урегулирования данного вопроса, а также при наличии актуальных разработок в сфере обнаружения в сети подозрительной активности могут оказать существенное влияние на минимизацию негативных последствий от использования Даркнет.

В этой же сфере отметим очень удачное законодательное новшество 2017 года в рамках Федерального закона от 29 июля 2017 г. № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», согласно которому владельцам анонимайзеров и VPN-сервисов запрещено предоставлять возможность их использования в Российской Федерации для получения доступа к заблокированным информационным ресурсам [11]. На данный момент необходима организация массового отслеживания подобных сервисов и их немедленная блокировка, что требует принципиально новых навыков со стороны правоохранительных органов и органов власти в сфере информационных технологий и массовых коммуникаций.

Исходя из анализа судебной практики и актуального законодательства, можно отметить явные пробелы в системе нормативных актов, которые позволяют на данный момент осуществлять виновным лицам преступный умысел против собственности с помощью такого инструментария, как социальные сети. В этой связи представляется целесообразным дополнить вышеуказанный Федеральный закон «Об информации, информационных технологиях и о защите информации» статьями, регламентирующими ответственность владельцев аккаунтов с изначально противоправной тематикой (колдовство, гадания, привороты, финансовые пирамиды и прочее). Кроме этого, в главе 21 УК РФ в ряде статей (158, 159 и 163 УК РФ) необходимо предусмотреть квалифицирующий признак – осуществление преступных действий через социальные сети (что подразумевает массовое распространение информации, воздействие сразу на нескольких потерпевших).

СПИСОК ИСТОЧНИКОВ

1. Бадамшин И. Д., Литвина А. В., Кулиев И. Б. Преступления в сфере информационно-телекоммуникационных технологий: тенденции и противодействие // Евразийский юридический журнал. 2022. № 2 (165). С. 265–266.

2. Приговор Калининского районного суда Краснодарского края № 1-74/2018 от 28 июня 2018 г. по делу № 1-74/2018 // СудАкт. URL: https://sudact.ru/regular/doc/DfXhCYeEvQlw/?regular (дата обращения: 30.03.2022).

3. Приговор Свердловского районного суда г. Белгорода № 1-99/2020 от 2 июля 2020 г. по делу № 1-99/2020 // СудАкт. URL: https:// https://sudact.ru/regular/doc/YIaqac9YHKgB/ (дата обращения: 30.03.2022).

4. Литвина А. В. Уголовно-правовая оценка использования криптовалют и других виртуальных активов в противоправных целях // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. 2021. № 1. С. 364–368.

5. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 г. № 259-ФЗ // Собрание законодательства Российской Федерации. 3 августа 2020 г. № 31 (часть I). Ст. 5018.

6. Приговор Кировского районного суда г. Омска (Омская область) № 1-482/2020 от 16 июля 2020 г. по делу № 1-482/2020 // СудАкт. URL: https://sudact.ru/regular/doc/dnN3OerlvDlT/?regular-txt (дата обращения: 30.03.2022).

7. О внесении изменений в отдельные законодательные акты Российской Федерации в части ограничений распространения информации и защиты населения и информационного пространства от негативного влияния деятельности астрологов, гадалок, магов, спиритов, экстрасенсов, в том числе в целях диагностики и воздействия на человека, его здоровье, духовный мир, имущество, а также иных лиц,

осуществляющих указанные воздействия под различными производными (знахарь, колдун, ясновидец, провидец и другие) либо скрытыми (эксперт, специалист, консультант) наименованиями: Законопроект от 21 января 2014 г. № 432935-6 // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество». URL: https://sozd.duma.gov.ru/bill/432935-6 (дата обращения: 30.03.2022).

8. Литвина А. В. Особенности правового регулирования уголовной ответственности за преступления, связанные с незаконным изготовлением и оборотом порнографических материалов или предметов // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. 2019. № 1. С. 294–297.

9. Приговор Автозаводского районного суда г. Тольятти № 1-24/2017 от 27 ноября 2019 г. по делу № 1-33/2019 // СудАкт. URL: https://sudact.ru/regular/doc/HnKXurlsuPQ4/?regular (дата обращения: 30.03.2022).

10. Мазур А. А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет // Вестник Российского университета кооперации. 2018. № 3(33). С. 126–129.

11. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 29 июля 2017 г. № 276-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_221230/ (дата обращения: 30.03.2022).

REFERENCES

1. Badamshin I. D., Litvina A. V., Kuliev I. B. Crimes in the field of information and telecommunication technologies: trends and counteraction // Eurasian legal journal. 2022. No. 2 (165). P. 265–266. (In Russ.)

2. Judgment of the Kalininsky District Court of the Krasnodar Territory No. 1-74/2018 dated June 28, 2018 in case No. 1-74/2018 // Sudakt. URL: https://sudact.ru/regular/doc/DfXhCYeEvQlw/?regular (date of access: 30.03.2022). (In Russ.)

3. Judgment of the Sverdlovsk District Court of Belgorod No. 1-99/2020 dated July 2, 2020 in case No. 1-99/2020 // SudAkt. URL: https:// https://sudact.ru/regular/doc/YIaqac9YHKgB/ (date of access: 30.03.2022). (In Russ.)

4. Litvina A. V. Criminal-legal assessment of the use of cryptocurrencies and other virtual assets for illegal purposes // Actual problems of the state and society in the field of ensuring the rights and freedoms of man and citizen. 2021. No. 1. P. 364–368. (In Russ.)

5. On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation: federal law of July 31, 2020 No. 259-FZ // Collected Legislation of the Russian Federation. August 3, 2020 No. 31 (Part I). Art. 5018. (In Russ.)

6. Sentence of the Kirovsky District Court of Omsk (Omsk Region) No. 1-482/2020 dated July 16, 2020 in case. No. 1-482/2020 // SudAkt. URL: https://sudact.ru/regular/doc/dnN3OerlvDlT/?regular-txt (date of access: 30.03.2022). (In Russ.)

7. On amendments to certain legislative acts of the Russian Federation regarding restrictions on the dissemination of information and protection of the population and the information space from the negative impact of the activities of astrologers, fortune-tellers, magicians, spiritualists, psychics, including for the purpose of diagnosing and influencing a person, his health, the spiritual world, property, as well as other persons carrying out these influences under various derivatives (healer, sorcerer, clairvoyant, seer and others) or hidden (expert, specialist, consultant) names: Draft Law of January 21, 2014 No. 432935-6 // System for ensuring the legislative activity of the State automated system «Lawmaking». URL: https://sozd.duma.gov.ru/bill/432935-6 (date of access: 30.03.2022). (In Russ.)

8. Litvina A. V. Peculiarities of legal regulation of criminal liability for crimes related to illegal production and circulation of pornographic materials or objects // Actual problems of the state and society in the field of ensuring the rights and freedoms of man and citizen. 2019. No. 1. P. 294–297. (In Russ.)

9. Sentence of the Avtozavodsky District Court of Togliatti No. 1-24/2017 dated November 27, 2019 in case. No. 1-33/2019 // SudAkt. URL: https://sudact.ru/regular/doc/HnKXurlsuPQ4/?regular (accessed 30.03.2022). (In Russ.)

10. Mazur A. A. Actual problems of crime prevention in the Darknet social network // Bulletin of the Russian University of Cooperation. 2018. No. 3(33). P. 126–129. (In Russ.)

11. On Amendments to the Federal Law «On Information, Information Technologies and Information Protection»: Federal Law of July 29, 2017 No. 276-FZ // RLC «ConsultantPlus». URL: http://www.consultant.ru/document/cons_doc_LAW_221230/ (date of access: 30.03.2022). (In Russ.)

Информация об авторе:
Бадамшин И. Д. – кандидат юридических наук, доцент.

Information about author:
Badamshin I. D. – Candidate of Law, Associate Professor.

Статья поступила в редакцию: 19.04.2022; одобрена после рецензирования: 05.05.2022; принята к публикации: 24.06.2022.
The article was submitted: 19.04.2022; approved after reviewing: 05.05.2022; accepted for publication: 24.06.2022.