УДК 343.974
DOI: 10.26456/vtpravo/2023.4.178

СОВРЕМЕННОЕ СОСТОЯНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

П.И. Фетисов

ОЧУ ВО «Московский университет имени А.С. Грибоедова», г. Москва

Для построения прогноза развития киберпреступности по отдельным видам посягательств рассматривается группа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Целью исследования является углубление научного знания о видах преступлений, совершаемых посредством сети Интернет, для разработки мер противодействия им. Задача исследования состоит в установлении совокупности преступлений, для совершения которых активно используется интернет-пространство. В работе применялись формально-юридический, системно-структурный, статистический методы научного познания. К результатам относится углубление теории криминологии по рассматриваемым преступлениям для их профилактики. Делается вывод о том, что традиционные способы совершения преступлений совершенствуются посредством кибертехнологий; виды преступлений с их использованием будут качественно обновляться.

Ключевые слова: *Интернет, киберпреступность, цифровые технологии, информационные технологии, социальные сети, криминальные риски.*

Стремительное развитие цифровых технологий обусловило приток миллионов людей на виртуальные площадки не только для общения, поиска информации, но и для реализации своих запросов на получение различных услуг (медицина, целительство, налоги, торговля, обучение и др.). По состоянию на 01.01.2022 г. в России насчитывалось 129,8 млн пользователей Интернета, т. е. 89 % населения от общей его численности (для сравнения, в 2016 г. их было 80 млн) [2]. Представить современное информационное общество без интернет-телевидения, новостных агрегаторов, социальных сетей, сайтов, мобильных мессенджеров и электронной почты невозможно. А потому каждый пользователь Сети может стать потенциальной жертвой киберпреступников [12, с. 25]. Так, по данным Генеральной прокуратуры РФ, за январь-июнь 2023 г. число преступлений, совершенных через мобильную связь и интернет, выросло на 39 % [8].

В Доктрине информационной безопасности Российской Федерации подчеркивается, что методы, способы и средства совершения преступлений с использованием информационных технологий становятся все более изощренными. Значительно возросли и масштабы

такой преступности. Статистический рост количества преступлений отмечается в кредитно-финансовой сфере; в разы увеличилось число посягательств против конституционных прав и свобод человека и гражданина, в том числе нарушающих неприкосновенность частной жизни, личную и семейную тайны, при обработке персональных данных с использованием информационных технологий [3]. В Стратегии национальной безопасности Российской Федерации среди наиболее опасных киберпреступлений названы также легализация преступных доходов, финансирование терроризма, организация незаконного распространения наркотических средств и психотропных веществ и использование в противоправных целях цифровых валют (п. 11 ст. 47) [1]. А потому для обеспечения государственной и общественной безопасности с учетом высокого потенциала информационных угроз для России и ее граждан в качестве приоритетной обозначена цель предупреждения и пресечения правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Структуру киберпреступности образуют две группы преступлений: 1) в сфере компьютерной информации (гл. 28 Уголовного кодекса Российской Федерации (далее – УК РФ)); 2) совершаемые с использованием информационно-телекоммуникационных технологий. Ко второй группе уголовно наказуемых деяний относятся следующие виды посягательств:

1. Преступления против собственности. Согласно отчетам о состоянии преступности, опубликованным Генеральной прокуратурой РФ, основным мотивом совершения преступлений с использованием сети Интернет является корысть. Ведомство отмечает, что в январе-июне 2023 г. зарегистрировано более 166,8 тыс. мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий (или 79,1 % от общего числа мошенничеств). Темп их прироста относительно аналогичного периода 2022 г. увеличился на 40,5 %. Число краж с банковского счета с использованием интернет-технологий составило 56,2 тыс.

Пользователи социальных сетей, сайтов знакомств, будучи потенциальными жертвами, размещают в открытом доступе информацию о себе, включая данные о месте проживания, фотографии из поездок, а также ссылки, репосты, геолокацию, что позволяет злоумышленникам использовать опубликованные сведения для совершения преступлений. Фото или видео интимного характера, которые киберпреступник получает от жертвы в личной переписке, становятся средством вымогательства денежных средств. К примеру, резонансным является дело бывшего оперативника Центра «Э» МВД РФ В., прослужившего в полиции тринадцать лет. Он являлся владельцем паблика «Омбудсмен полиции», а его администратором был Р.К.,

действующий сотрудник УВД на Московском метрополитене. Уволенный из полиции в звании майора В. просил Р.К. оказать ему содействие в трудоустройстве в УВД. После того, как В. отказали в приеме на работу, он решил отомстить приятелю. В. попросил свою знакомую, чтобы она уговорила Р.К. отправить его интимные фото. В. разместил снимки в своем паблике «Омбудсмен полиции», а за их удаление стал требовать у Р.К. 300 тыс. руб. Люблинский районный суд г. Москвы признал В. виновным не только в вымогательстве в отношении Р.К., но и в распространении порнографии. В. разместил два интимных снимка Д. – сотрудницы подразделения по делам несовершеннолетних МВД России [9].

Дистанционно может совершаться и мошенничество. Виновный размещает объявление о продаже товаров или оказании услуг, требуя перевода полной оплаты или ее части, а затем либо отправляет по почте вещь, не соответствующую по качеству стоимости, либо блокирует покупателя и исчезает (в науке эта схема получила название виртуального товарообмена). Имеют место случаи, когда мошенник, напротив, использует объявления потерпевшего и для «перевода» денег на карту получает секретную информацию жертвы (пин-код от карты, CVV-код, личные данные) [15, с. 137].

Объектом внимания мошенников становятся и одинокие женщины, ушедшие в сетевое пространство для поиска спутника жизни. Схема романтического аферист в социальных сетях и на сайте знакомств одна – втереться в доверие к жертве и поиграть на ее чувствах. После непродолжительной переписки мошенник признается в чувствах и, используя разные предлоги, просит помочь в трудной ситуации с деньгами. Причем такие манипуляции могут совершаться и в отношении мужчин, когда по ту сторону экрана находится якобы красотка, желающая выйти замуж. К примеру, Новочебоксарский городской суд Чувашской Республики признал виновным С., который вступил в сговор с неустановленным лицом, владеющим иностранными языками. Он зарегистрировался на зарубежном сайте знакомств, осуществив рассылку писем на электронный ящик мужчинам, желающим познакомиться с женщиной из России для создания семьи. Один из них, гражданин Польши, ответил на письмо, после чего С. совместно с другим соучастником направлял потерпевшему письма «от девушки». В ходе переписки на любовные темы С. обратился к потерпевшему с просьбой прислать деньги для оформления визы и заграничного паспорта для поездки «девушки» в Польшу. Затем С. требовал перевода денег на авиабилет, оплату штрафа по кредитному договору, проведение срочной операции. Всего потерпевшими по делу были признаны четыре иностранных гражданина из Австрии, Польши и Чехии, а общий ущерб составил более 500 тыс. руб. [19].

2. Преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ. Правоприменительная практика и специалисты отмечают рост фактов купли-продажи наркотиков через Интернет. Число таких преступлений увеличилось на 21 % в сравнении с предыдущим годом [10, с. 63]. Исследователи, изучившие структуру преступности в социальных сетях и на других интернет-площадках, указывают на большую долю в них деяний, связанных с незаконным оборотом наркотических средств и психотропных веществ. По данным В.С. Соловьева, в выборке приговоров по делам, где использовались информационно-коммуникационные технологии, их оказалось 24,5 % (незаконные приобретение и сбыт наркотиков) [14, с. 61]. Масштабы наркопреступности в сети Интернет сложно оценить в цифрах, поскольку на показатели ее выявления и раскрытия влияют следующие меры конспирации: использование крупными наркодилерами криптовалюты в качестве платы, а также теневого сегмента сети Интернет (Hydra, Даркнет, TOR), мессенджеров (в большинстве приговоров – Telegram) и закрытых групп в социальных сетях для переписки с покупателями; распределение ролей (закладчики, кураторы интернет-магазинов, администраторы, курьеры), при котором организаторы сети избегают уголовной ответственности. Колоссальный криминальный доход от продажи запрещенных препаратов легализуется при помощи уже отработанных преступных схем обналичивания прибыли. Так, Советский районный суд г. Орла признал виновными в сбыте наркотических средств Ф-ву, Ш. и В. Для конспирации преступной деятельности группа использовала приложение Telegram (чат-бот), работающее с помощью Интернета, в которой оператор онлайн-магазина принимал «заказ». Соучастники общались с покупателями под вымышленными именами. Сбыт наркотиков осуществлялся через закладки, приспособленные или приисканные укромные места, незаметные для неосведомленных лиц. Ш. и Ф-ва являлись «фасовщиками-закладчиками» наркотических средств. Они расфасовывали, хранили и доставляли их к тайнику для сбыта; В. разрабатывал планы и способы совершаемых преступлений, приискивал наркотики, покупателей, распределял денежные средства [17].

3. Преступления против половой свободы и половой неприкосновенности. Цифровые и информационно-телекоммуникационные технологии трансформировали отношения между людьми в сфере сексуальных отношений. Проявлением цифросексуализма является секстинг, т. е. пересылка сообщений эротического содержания, интимных фотографий и видеозаписей [13, с. 50]. При оценке криминологических рисков специалисты прогнозируют значительное увеличение показателей «сексуализированных» преступлений. На просторах Глобальной сети процветает торговля девственностью, фиксируются многочисленные факты сексуального

развращения несовершеннолетних и др. [4, с. 162]. Цифросексуализм, как пишет В.С. Соловьев, повышает риск совершения посягательств на половую неприкосновенность несовершеннолетних. «Виртуальные педофилы» подыскивают жертву в социальных сетях и закрытых группах, а затем отправляют ей видеоматериалы эротического или порнографического характера [11, с. 65]. Так, Курганинским районным судом Краснодарского края постановлен обвинительный приговор по уголовному делу в отношении местного жителя, осуществлявшего рассылку детям сообщений и фотографий сексуального характера [18]. В других случаях преступники вступают в переписку с детьми, склоняют их к отправке своих интимных фото. Председатель Следственного комитета РФ А.И. Бастрыкин видит проблему в том, что «в большинстве случаев дети, совершившие первый неверный шаг, отправив фото или видео, продолжают находиться во власти педофила, выполняя все более изощренные требования. Педофилы умело манипулируют детьми, играя на чувстве страха, вины, стыда, боязни быть разоблаченными перед одноклассниками или друзьями, а самые близкие люди не объясняют им, что поддаваться на интернет-шантаж ни в коем случае не следует» [6, с. 7].

4. Преступления против общественной нравственности. Трансформация интернет-пространства в платформу для криминальной деятельности способствовала виртуальному рекрутингу взрослых и несовершеннолетних в занятие проституцией и порнографией. В теневой части Глобальной сети размещается детское порно. Особую категорию жриц любви составляют «элитные» проститутки, наем которых для богатых и известных осуществляется при помощи онлайн-ресурсов. Как отмечает И.С. Алихаджиева, «продажа элитных сексуальных услуг ушла в закрытые сегменты сети Интернета – Dark Web и бесплатные приложения и мессенджеры (например, WhatsApp, Telegram). Рабочей площадкой эскортной проституции выступает, к примеру, запрещенная в России сеть, где по профилю и качественным фотосъемкам гламурной жизни определяется ценник работницы этой сферы» [5, с. 182].

Рынок коммерческих сексуальных услуг посредством Интернета стал более закрытым, а значит и виктимным для его участников. Поиск клиентов секс-работницы осуществляют в социальных сетях, мессенджерах и на сайтах знакомств. Подобный подход к организации своей работы позволяет им не платить сутенерам, преступным сообществам и правоохранителям, однако во много раз увеличивает риск стать жертвой вора, насильника или убийцы. Например, Санкт-Петербургский городской суд вынес приговор мужчине, убившему проститутку с особой жестокостью. На сайте объявлений индивидуалок, работающих без сутенеров, преступник выбрал жертву по высокой стоимости услуги и возможности связаться с ней по мессенджеру. Купив заранее нож и телефон, он пришел к ней домой, где избил и нанес не

менее сорока ударов ножом. Пресс-служба ГСУ СК РФ по Санкт-Петербургу сообщила, что мотивом убийства явился кредит в банке, долг по которому составил 270 тыс. руб. [7].

5. Преступления против неприкосновенности частной жизни, чести и достоинства личности. Исследователи отмечают высокие риски использования персональных данных, размещенных их владельцами в киберпространстве [16, с. 142]. Конфиденциальная информация продается в теневой части Интернета в виде систематизированных личных данных сотен тысяч людей, похищенных посредством взлома компьютерных систем крупнейших банков, перевозчиков, сервисов услуг, магазинов и др. Известны случаи, когда злоумышленники использовали «слитые» базы персональных данных для мошенничества или вымогательства, а при отказе потерпевшего платить, в Сеть размещалась информация, способная навредить репутации жертвы, распространялись порочащие сведения (диссинг). Другой формой онлайн-травли является аутинг, когда публикуется личная информация, к примеру адрес или телефон идентифицированной жертвы, на который приходят сообщения с оскорблением и угрозами насилием. Травля в цифровом пространстве может выражаться в унижении достоинства человека, злых шутках в комментариях, постах и др. По данным опроса социальной сети «ВКонтакте», 60 % пользователей сталкивались с агрессией на площадке.

Подводя итоги исследования, следует отметить, что структуру преступности, связанной с использованием информационных технологий, образуют не только рассмотренные посягательства. Ввиду множества видов преступлений, совершаемых виртуально, не представляется возможным в одной статье дать обстоятельную характеристику каждому. Дальнейшее расширение сферы применения высоких технологий и их модернизация позволяют прогнозировать появление новых способов использования сети Интернет в криминальных целях, а значит и качественно негативных изменений преступности в целом. Отсюда задачей криминологической науки является разработка мер по минимизации рисков, связанных с перемещением значительной части злоумышленников во Всемирную сеть для преступных целей.

Список литературы

1. Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

2. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 год // СЗ РФ. 2017. № 20. Ст. 2901.

3. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

4. Алихаджиева И.С. О новых тенденциях современной секс-индустрии и ее криминологических рисках // Актуальные проблемы российского права. 2021. Т. 16. № 4. С. 160–173.

5. Алихаджиева И.С. Организация занятия элитной проституцией в сети Интернет // Известия Юго-Западного государственного университета. Серия: История и право. 2018. Т. 8. № 4 (29). С. 179–185.

6. Бастрыкин А.И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 5–12.

7. В Петербурге мужчина убил проститутку, чтобы погасить кредит [Электронный ресурс]. URL: https://rg.ru/2023/07/20/lollm9u562680499082 (дата обращения: 22.10.2023).

8. В России число совершенных через мобильную связь и интернет преступлений выросло на 39% [Электронный ресурс]. URL: https://tass.ru/obschestvo/18417795?ysclid=loler8qxv312372608 (дата обращения: 22.10.2023).

9. «Омбудсмен полиции» получил пять лет колонии за вымогательство и распространение порнографии [Электронный ресурс]. URL: https://www.bfm.ru/news/505798?ysclid=lofsveub69888099163 (дата обращения: 22.10.2023).

10. Пинкевич Т.В. Обеспечение криминологической безопасности в условиях в условиях цифровой трансформации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 2 (48). С. 63–68.

11. Родивилин И.П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. 2017. № 4 (67). С. 25–29.

12. Родивилин И.П., Коломинов В.В., Брыжак Д.Э. Интеллектуальный разврат несовершеннолетних в сети Интернет // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1 (27). С. 64–76.

13. Соловьев В.С. Криминологические риски цифросексуализма // Вестник Российской правовой академии. 2020. № 3. С. 47–56.

14. Соловьев В.С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. 2016. № 1. С. 60–72.

15. Сынгаевский Д.В. Мошенничество в глобальной сети Интернет как объект виктимологического исследования // Современный юрист. 2013. № 4. С. 136–144.

16. Хохлова Е.В. Социальная обусловленность уголовной ответственности за преступления, связанные с персональными данными // Вестник Тверского государственного университета. Серия Право. 2022. № 3 (71). С. 141–148.

17. Приговор Советского районного суда г. Орла от 21.05.2020 г. по делу № 1-115/2019 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/c4dPrSYf9Eg1 (дата обращения: 25.10.2023).

18. Приговор Курганинского районного суда Краснодарского края от 12.05.2022 по делу № 1-223/2017 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/XvHrPQUlnDWQ/ (дата обращения: 22.10.2023).

19. Приговор Новочебоксарского городского суд Чувашской Республики от 27.09.2017 по делу № 1-223/2017 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/OHcRkrvsjZNj/ (дата обращения 29.10.2023).

Об авторе:

ФЕТИСОВ Павел Ильич – аспирант кафедры уголовно-правовых дисциплин, криминологии и уголовно-исполнительного права ОЧУ ВО «Московский университет имени А.С. Грибоедова (ИМПЭ им. А.С. Грибоедова)» (105066, г. Москва, ул. Новая Басманная, 35, стр. 1); e-mail: kamenskiy.maxim@mail.ru

CURRENT STATE OF CRIMES COMMITTED USING INFORMATION TECHNOLOGIES

P.I. Fetisov

Moscow University named after A.S. Griboedov, Moscow

To build a forecast of the development of cybercrime for certain types of encroachments, a group of crimes committed using information and telecommunication technologies is considered. The purpose of the study is to deepen scientific knowledge about the types of crimes committed through the Internet to develop countermeasures against them. The task of the study is to establish the totality of crimes for which the Internet space is actively used. The work used formal-legal, system-structural, statistical methods of scientific knowledge. The results include deepening the theory of criminology on the crimes in question for their prevention. It is concluded that traditional methods of committing crimes are being improved through cyber technologies; types of crimes with their use will be qualitatively updated.

Keywords: *Internet, cybercrime, digital technologies, information technologies, social networks, criminal risks.*

About author:

FETISOV Pavel – graduate student in the Department of Criminal Law, Criminology and Penal Law of the Moscow University named after A.S. Griboedov (IMPE named after A.S. Griboedov), 105066, Moscow, Novaya Basmannaya St., 35, p. 1, e-mail: kamenskiy.maxim@mail.ru

Фетисов П.И. Современное состояние преступлений, совершаемых с использованием информационных технологий // Вестник ТвГУ. Серия: Право. 2023. № 4 (76). С. 178–185.

Статья поступила в редакцию 10.11.2023 г.

Подписана в печать 27.11.2023 г.