ТИПОЛОГИЯ КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ ПАНДЕМИИ COVID-19 В РОССИИ И ЗА РУБЕЖОМ

Айнутдинова К.А., *канд. юрид. наук, доцент кафедры уголовного права, Университет управления «ТИСБИ», г. Казань;*

Айнутдинова И.Н., *д-р пед. наук, профессор кафедры иностранных языков, Казанский (Приволжский) федеральный университет, г. Казань*

Аннотация. Цель исследования - проанализировать состояние киберпреступности в условиях пандемии COVID-19 в России и за рубежом. На основе анализа статистики из российских и иностранных источников сделан вывод о схожих детерминантах киберпреступности в различных регионах мира; даются обзор и оценка общим тенденциям роста данного вида преступности; представлена авторская типология киберпреступности в условиях пандемии.

Ключевые слова: киберпреступление, киберпреступность, глобализация, информатизация, цифровизация, типология, пандемия Covid-19.

Abstract. The aim of the study is to analyze the state of cybercrime in the context of the COVID-19 pandemic in Russia and abroad. Based on the analysis of statistics from Russian and foreign sources, it is concluded that there are similar determinants of cybercrime in different regions of the world; an overview and assessment of the general trends in the growth of rates of this type of crime has been provided; the authors' typology of cybercriminality during a pandemic has been presented.

Key words: cybercrime, cybercriminality, globalization, informatization, digitalization, typology, Covid-19 pandemic.

Сегодня мировое сообщество переживает сложный период своего

развития. Набирающие обороты процессы глобализации, информатизации и цифровизации ведут, с одной стороны, к постоянному совершенствованию средств информации и коммуникации, способствуют общению, сближению культур и народов, открывают невиданные ранее перспективы для налаживания демократических торгово-экономических и межгосударственных связей. С другой стороны, те же, казалось бы, позитивные процессы усугубляют неравномерность мирового развития, зачастую провоцируют расширение открытых и тлеющих зон геополитической напряженности [2], создают предпосылки для вмешательства третьих стран в региональные и локальные конфликты, порождают условия для возникновения новых форм деструктивного поведения и роста преступности [3].

В 2019 г. мир впервые за последнее столетие столкнулся с небывалой массовой эпидемией COVID-19. Помимо физических и моральных страданий, вынужденные карантинные меры, связанные с пандемией и введенные для охраны здоровья населения, принесли не только смену привычного жизненного уклада, когда многие сектора социальной, экономической, культурной и политической жизни были переведены в Интернет или онлайн-среду, но и небывалый всплеск киберпреступности или преступности в виртуальном пространстве [10].

Парадоксально, но массовый переход компаний, бизнеса, учебных и торговых учреждений на удаленную работу на пике пандемии имел целый ряд позитивных последствий: он содействовал развитию сферы информационных коммуникаций и технологий, способствовал популяризации инновационных методов и средств передачи и обмена информацией, облегчал налаживание контактов, проведение транзакций и др. [10]. Одновременно вспышка COVID-19 породила у многих чувство неопределенности, уязвимости и непредсказуемости, сместила внимание общества к кризису в области здравоохранения и привела к снижению бдительности к киберзащите. Все это, как следствие, активизировало криминогенный потенциал [2] и повлекло волну преступлений, совершаемых с использованием компьютерных и телекоммуникационных

технологий [1; 7; 9].

Для целей нашего исследования мы обратились к статистическим данным, представленным за период пандемии COVID-19 как международными (Интерпол, Европол и др.), так и российскими правоохранительными органами [1; 7; 9]. Мы также проанализировали материалы, отражающие состояние и динамику роста киперпреступлений того периода в России и за рубежом [1; 7; 9], что позволило сформулировать типологию киперпреступности в условиях пандемии COVID-19. Сравнение законодательной базы по киберпреступности в России и ряде зарубежных стран побудило нас к терминологической конкретизации некоторых преступных деяний, связанных с использованием компьютеров и сети Интернет, и актуализировало рекомендации по пересмотру и расширению российскими законодателями национальных подходов к криминализации киберпреступлений.

В августе 2020 г. Юрген Шток (Jürgen Stock), Генеральный секретарь Интерпола, в своем докладе «Киберпреступность: влияние COVID-19» представил данные о беспрецедентном росте киберугроз и киберпреступности во всем мире в период пандемии COVID-19 с учетом региональных особенностей [9]. Согласно информации французской IT компании «Trend Micro» (https://www.trendmicro.com/), одного из партнеров Интерпола, только за период с января по апрель 2020 г. ею было зарегистрировано 907 тыс. спам-сообщений, 737 инцидентов с вредоносным программным обеспечением (ПО) и более 48 тыс. размещений вредоносных URL-адресов, так или иначе связанных с темой COVID-19. Интерпол в своем докладе дал детальную оценку региональным особенностям киперпреступности на волне COVID-19 и определил тенденции ее развития в различных уголках мира [9].

Так, в Африке широкое распространение получили: тематический COVID-19 фишинг (рассылка мошеннических сообщений, источник которых маскируется под надежный, не являясь таковым, для получения доступа к конфиденциальным данным пользователей – их логинам и паролям); сексторсия (нефизические формы принуждения для вымогательства у жертвы сексуальных

услуг); мошеннические схемы (мимикрирование под несуществующие благотворительные организации с целью принуждения сделать пожертвование); распространение дезинформации в социальных сетях об услугах и препаратах, связанных с лечением COVID-19, и др.

На Американском континенте в период карантина также был отмечен резкий всплеск фишинговых и мошеннических атак, при этом преступники с целью завладения конфиденциальной или секретной информацией стремились получить доступ к базам данных компаний малого и среднего бизнеса в условиях, когда сотрудники этих организаций находились на удаленном режиме работы. Характерными для этого региона стали повсеместные атаки вымогателей, проводимые, в основном, путем внедрения вредоносного ПО, известного как шифровальщик LockBit. По определению АО «Лаборатория Касперского» [4], это самоуправляемое вредоносное ПО, именуемое также «криптовирусом», блокирует доступ к компьютерным системам и требует от пользователя выкуп за восстановление данных, при этом LockBit автоматически отыскивает подходящую «платежеспособную» жертву, самостоятельно распространяется по сети компании и зашифровывает все данные на зараженных устройствах. В период пандемии многие крупные американские предприятия, включая медицинские компании, финансовые учреждения и даже правительственные организации, стали жертвами злоумышленников, практикующих вымогательство при помощи ПО LockBit. Для Американского региона также оказались характерными использование социальных сетей для сексуальной эксплуатации детей в сети Интернет и распространение видео и фотопродукции со сценами насилия и сексуальной эксплуатации детей.

Основные тенденции в Азиатско-Тихоокеанском регионе (ASP) включают мошенничество и фишинг, связанные с COVID-19, а также незаконную онлайн-продажу поддельных медицинских принадлежностей, инструментов, лекарств и средств индивидуальной защиты [9; 10]. Киберпреступники часто использовали уязвимости оборудования для видео и телеконференций, нарушали нормальную работу образовательных учреждений, зачастую вторгаясь в учебный процесс из

хулиганских побуждений. Также к региональным особенностям АТР можно отнести множество фейковых новостей и вал дезинформации в социальных сетях.

Страны Ближнего Востока и Северной Африки (MENA) отличились ростом использования социальных сетей для распространения фейков, связанных с COVID-19, и незаконной продажи фармацевтической и парафармацевтической продукции, якобы имеющей отношение к коронавирусу. Было также отмечено увеличение числа регистраций вредоносных доменов, заявляющих в анонсах о предоставлении якобы достоверной статистики по распространению COVID-19. При этом фиксировалось много случаев фишинга и онлайн-мошенничества [9].

Фишинг и мошенничество в сети Интернет не обошли и Европейский Союз. Еще в начале коронакризиса в Европе расширилась онлайн продажа поддельных средств защиты и медикаментов, при этом фальсификаторы ловко использовали в своих целях временную нехватку медицинских масок и средств дезинфекции [10]. Другие злоумышленники, пользуясь снижением мобильности граждан, пребыванием большой части населения на удаленной работе и ограничением общественной жизни, а также растущим числом людей, испытывающих на фоне пандемии тревогу и страхи и ищущих любую информацию о COVID-19 онлайн, не преминули массированно регистрировать вредоносные домены с ключевыми словами «COVID» и «Corona». Эти зарегистрированные доменные имена составляли основу для многих преступных деяний, однако на сегодняшний день ситуация, по данным Европола, взята под контроль и стабилизировалась [1; 10].

Еще одной особенностью киберпреступности в Европе стало активное внедрение вредоносного ПО, известного как Ransomware, или трояны-вымогатели, с атакой на сайты критической инфраструктуры или медицинских учреждений. Киберпреступники обычно используют это ПО в качестве шифровальщиков (когда шифруются ценные файлы и базы данных) или блокировщиков (когда просто полностью блокируется доступ к устройству) [1;

6]. В любом случае для восстановления работы с пользователя всегда требуется выкуп – в среднем, это около $300. Еще один тренд киберпреступности на пике вспышки пандемии COVID-19 в Европе наблюдался в сегменте увеличения числа распределенных атак типа «отказа в обслуживании» (DDoS attacks) [5]. DDoS-атака отправляет на атакуемый веб-ресурс большое количество запросов с целью превысить способность сайта обрабатывать их, что, в итоге, вызывает отказ в обслуживании, и сайт «обваливается». Стандартные цели DDoS-атак – это препятствие работе компаний и организаций, связанных с предоставлением онлайн-услуг, крупных поисковых систем и СМИ-порталов. Все чаще фиксируются случаи клонирования официальных правительственных сайтов с целью кражи конфиденциальных данных пользователей или воздействия на информационное пространство, что впоследствии может быть использовано для распространения ложной и недостоверной информации о COVID-19 и в дальнейших кибератаках [1; 6; 10].

Пандемия COVID-19 и связанные с ней ограничения в России несколько изменили криминогенную ситуацию в стране, а, следовательно, и привычную структуру, и динамику преступлений. Изучив статистику о киберпреступности, отчет Генпрокуратуры РФ «Состояние преступности в России» за январь-декабрь 2020 г. и данные МВД РФ за тот же период, авторы пришли к выводу, что на фоне общего снижения традиционной преступности резко выделяется рост числа киберпреступлений. В частности, как следует из статистики, опубликованной на сайте МВД РФ, «рост IT-преступности только за январь-июнь 2020 г. составил 91,7%, по сравнению с аналогичным периодом 2019 г., а удельный вес данных противоправных деяний в общей структуре преступности достиг 22,3%». По данным Прокуратуры РФ [7], за последние 5 лет число преступлений, совершенных с использованием информационно-телекоммуникационных технологий (ИКТ) или в сфере компьютерной информации, увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8% до 25%. При этом большинство киберпреступлений совершалось с использованием сети Интернет или при помощи средств

мобильной связи. По данным на декабрь 2020 г., это 300,3 тыс. и 218,7 тыс. совершенных преступлений соответственно [7]. Наиболее распространены также мошенничества в сфере ИКТ или компьютерной информации; на них приходится около 70% всех хищений, совершенных путем обмана или злоупотребления доверием (237,1 тыс.), при этом при совершении 25,8 тыс. мошенничеств использовались электронные средства платежа [7].

Рост активности киберпреступников отмечают и эксперты российских компаний в сфере кибербезопасности. По их мнению, в период пандемии COVID-19 люди стали больше пользоваться сетевыми ресурсами и онлайн-сервисами, что породило волну мошенничества, связанного с оказанием услуг в сети Интернет, навязыванием фейковых лотерей и розыгрышей, а доля фишинга с принуждением перехода пользователей на поддельные сайты и страницы выросла в период карантина, как минимум, вдвое (с 9% до 18%). Также перевод многих операций и расчетов в онлайн привел к скачку количества попыток прямого взлома веб-ресурсов, а обострение конкуренции и борьба за клиентов в онлайн-среде вызвали всплеск DDoS-атак. Эксперты «Лаборатории Касперского» фиксируют рост на 40% общего объема киберпреступлений в отношении бизнес-компаний, при этом финансовые организации и их клиенты сталкиваются с новыми угрозами, нацеленными на похищение банковских и персональных данных [6]. Среди преступных трендов в России отмечается рост банковских троянов, пришедших на смену вредоносным шифровальщикам-вымогателям, а также атаки на мобильные приложения, сайты ритейла, финансовые сервисы и корпоративный сектор [5; 6].

Анализ криминогенной обстановки в России и за рубежом в условиях пандемии доказал, что внезапные, но необходимые на тот момент карантинные меры и фактический перевод всех сфер жизнедеятельности правительств, организаций и граждан в онлайн-формат породили лавину киберпреступности. На смену традиционным вызовам (экологическая деградация, техногенные катастрофы, международный терроризм, нелегальный оборот оружия, организованная преступность, наркотрафик и многое другое), а порой и вдобавок

к ним, пришли угрозы нового поколения [2], которые в контексте глобализации, цифровизации и пандемии COVID приобрели действительно планетарный размах. Несмотря на некоторые региональные особенности, киберпреступность в различных точках мира в период пандемии COVID-19 была обусловлена схожей системой детерминант и, фактически, развивалась по единому сценарию. Не случайно, что для всех стран стали общими негативные тенденции ее роста и распространения. Выводы Интерпола позволили нам сформулировать типологию киберпреступности в России и за рубежом в условиях пандемии COVID-19 [9].

Итак, первая категория киберпреступлений, по нашему мнению, основана на определенных схемах для получения выгоды за счет жертвы; кибератаки обычно нацелены на широкую аудиторию частных лиц и включают различные виды Интернет-мошенничества, вредоносные домены и фишинг [3]. Следующая категория нацелена на компании и организации, работа которых связана с предоставлением онлайн-услуг и сетевой торговлей; сюда можно отнести вредоносные программы-вымогатели, трояны и DDoS-атаки. Третья категория киберпреступлений несет, на наш взгляд, наиболее опасные угрозы безопасности и устойчивому развитию стран, так как киберпреступники избирают своей целью правительственные сайты и домены, объекты критической инфраструктуры и информационное пространство; сюда можно отнести вредоносное ПО для сбора персональных и конфиденциальных данных [5], клонирование сайтов и страниц государственных органов и злонамеренное массовое распространение фейков и дезинформации. Следует также отметить, что для максимизации ущерба и финансовой выгоды киберпреступники в условиях пандемии COVID-19 избрали тактику смещения своих целей с единичных атак на частных лиц и малый бизнес и перешли на массовые атаки крупных корпораций и даже правительств, дабы нарушить функционирование критически важных объектов жизнеобеспечения, посеять смуту и хаос, чтобы дестабилизировать деятельность государства [10].

Представленная типология, безусловно, не является исчерпывающей.

Более того, некоторые термины, которые мы использовали для описания киберпреступлений (например, «фишинг», «DDoS-атаки» и пр.), охватывают действия, которые могут быть отнесены к более, чем одной категории. Тем не менее, мы полагаем, что представленная типология может служить отправной точкой для обсуждения явления киберпреступности в период пандемии COVID.

В заключение хотелось бы обратить внимание на то, что широко используемая юристами и IT-специалистами терминология при описании тех или иных преступлений в киберпространстве не находит пока своего отражения в уголовном законе России. Глава 28 УК РФ в статьях 272–274 [8], посвященных уголовной ответственности за совершение киберпреступлений (преступлений в сфере компьютерной информации), дает лишь ориентиры для определения роли и места того или иного вновь возникающего или уже длительное время совершаемого в киберпространстве специфического преступного деяния и порождает практику казуального (индивидуального) толкования норм права. Вероятно, настало время для российских законодателей признать масштаб проблемы киберпреступности и вне условий пандемии, пересмотреть и расширить национальные подходы к криминализации целого ряда киберпреступлений [3].

Список источников:

1. Боль К. Поймать вирус киберпреступности, дезинформации и пандемии COVID-19: отчет (на рус. яз.) / Кэтрин де Боль / Исполнительный директор, Европол, 3 апреля 2020. - 12 с.

2. Голина В.В. Криминогенный потенциал общества: понятие, содержание, формы реализации // Проблемы законности. - 2012. - № 119. - С. 186-197.

3. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. - 2019. - № 1. - С. 25-33.

4. Касперский Е.В. Шифровальщик LockBit – что нужно знать. [Электронный ресурс]. - URL: https://www.kaspersky.ru/resource-

center/threats/lockbit-ransomware (15.02.2021).

5. Касперский Е.В. Распределенные сетевые атаки / DDoS. [Электронный ресурс]. - URL: https://www.kaspersky.ru/resource-center/threats/ddos-attacks (19.02.2021).

6. Касперский Е.В. Что такое Ransomware / Kaspersky Daily. [Электронный ресурс]. - URL: https://www.kaspersky.ru/blog/ransomware-for-dummies/13579/ (20.02.2021).

7. Состояние преступности в России за янв.-дек. 2020 г. / Отчет Генпрокуратуры РФ / Портал правовой статистики. [Электронный ресурс]. - URL: http://crimestat.ru/analytics (12.02.2021).

8. Уголовный кодекс РФ от 13.06.1996 г. № 63-ФЗ (ред. от 30.12.2020). [Электронный ресурс]. - URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (17.02.2021).

9. Stock J. Cybercrime: COVID-19 Impact. INTERPOL Cybercrime Analysis Report / Jürgen Stock / INTERPOL General Secretariat, Lyon, France (August 2020). - P. 20.

10. Tett G. Why Covid-19 is a gift for cyber criminals / FT Magazine. [Electronic resource]. - URL: https://www.ft.com/content/935a9004-0aa5-47a2-897a-2fe173116cc9 (14.02.2021).