

3. Об изменении кодексов по вопросам уголовной ответственности [Электронный ресурс]: Закон Респ. Беларусь от 26 мая 2021 г. № 112-З: принят Палатой представителей 7 мая 2021 г.: одобр. Советом Респ. 7 мая 2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2021.
4. Уголовный кодекс Республики Беларусь [Электронный ресурс]: 09 июля 1999 г., № 275-З: принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г.: в ред. Закона Респ. Беларусь от 26.05.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2021.
5. Следственный комитет Республики Беларусь [Электронный ресурс]. URL: <http://sk.gov.by/ru/news-ru/view/dmitrij-gora-nasha-zadacha-obespechit-spokojnuju-zhizn-nashix-grazhdan-nashego-gosudarstva-10125/> (дата обращения: 30.10.2021).
6. Следственная деятельность: наука, образование, практика: тезисы докладов Международной научно-практической конференции (Минск, 24 июня 2021 г.) / ред. кол. С. Я. Аземша (председатель) и др. Минск: СтройМедиаПроект, 2021.
7. Следственный комитет на заседании коллегии подвел итоги работы в первом полугодии 2021 г. [Электронный ресурс]: постановление коллегии След. ком. Респ. Беларусь, 29 июля 2021 г., № 5кск-дсп // Национальный правовой Интернет-портал Республики Беларусь. URL: <http://pravo.by/novosti/obshchestvtvno-politicheskie-i-v-oblasti-prava/2021/august/65521/> (дата обращения: 30.10.2021).

СОВРЕМЕННАЯ КИБЕРПРЕСТУПНОСТЬ: ВОПРОСЫ ПОНИМАНИЯ И НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ

М. Г. Головенчик

*Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, marina.golovenchik@inbox.ru*

В статье рассматриваются вопросы общественной опасности преступлений, совершаемых в условиях цифрового информационного пространства, указывается на отсутствие единого подхода к пониманию киберпреступлений, предпринята попытка выделения отдельных признаков данных противоправных деяний. Автор уделит внимание вопросам причин и условий, способствующих совершению деяний, являющихся проявлениями киберпреступности, обозначил основные возможные направления противодействия и профилактики совершения киберпреступлений. Обоснована необходимость организации должного сотрудничества правоохранительных органов различных государств в сфере противодействия распространения киберпреступности.

Ключевые слова: киберпреступность; информационная безопасность; цифровое информационное пространство; противодействие киберпреступности; международное сотрудничество.

MODERN CYBERCRIME: ISSUES OF UNDERSTANDING AND DIRECTIONS OF COUNTERACTION

M. G. Goloventchik

*Belarusian State University,
Niezaliežnasci Avenue, 4, 220030, Minsk, the Republic of Belarus, marina.golovenchik@inbox.ru*

The article examines the issues of public safety of crimes committed in the digital information space, indicates the lack of a uniform approach to understanding cybercrimes, an attempt is made to identify individual signs of these illegal acts. The author paid some attention to the causes and conditions that contribute to the commission of acts that are manifestations of cybercrime, outlined the main possible directions for countering and preventing the commission of cybercrime. The

necessity of organizing proper cooperation of law enforcement agencies of various states in the field of countering the spread of cybercrime is substantiated.

Key words: cybercrime; information security; digital information space; countering cybercrime; international cooperation.

На сегодняшний день можно констатировать, что произошедшая в мире научно-техническая революция в значительной степени изменила жизнь абсолютного большинства людей, предоставив им возможность пользоваться достижениями в самых различных отраслях знаний, о которых ранее можно было лишь читать в фантастических романах. Так, еще два-три десятилетия назад многие любители активно следили за новинками в области фотосъемки, приобретая новые аппараты, фото пленку, реактивы для ее проявки и печати фотоснимков. Сегодня же на смену устаревшей технологии пришла цифровая фотография, а от производства фото пленки давно отказались даже ее самые известные производители. Более того, получение высококачественных снимков зачастую рассматривается лишь как опция, которой обладают иные (не специализированные) технические устройства – например, смартфоны, о которых также ничего не было известно всего около двух десятилетий назад. Интересно отметить, что сбываются многие прогнозы, данные футурологами в 80-90-х годах прошлого столетия: появление множества маленьких устройств, подключенных к Интернету (Дж. Безос, 1999), функционирование системы «Умный дом» (Б. Гейтс, 1995), появление умных помощников, способных отследить интересы владельца и подстроиться под них (С. Джобс, 1984), активное и стремительное распространение онлайн-покупок (Дж. Безос, 1999). На сегодняшний день футурологи, давая прогнозы на ближайшие десятилетия, отмечают замену роботами большинства привычных профессий, возникновение конфликтов (в том числе в сфере правового регулирования) между людьми и андроидами, но, кроме того, расширение «темной стороны» Интернета (Darknet), позволяющей обходить установленные государством ограничения, что создает опасность как для граждан, так и для юридических лиц, государства, общества в целом [1].

К сожалению, нельзя не признать, что научно-технический прогресс, предоставляя блага цивилизации, одновременно создает значительные предпосылки к развитию нового вида преступности – киберпреступности, значимой характеристикой которой является использование современных технических средств, информационных и коммуникационных технологий для совершения противоправных деяний. Количество подобных преступлений с каждым годом растет. При этом специалисты отмечают, что «глобальные убытки от киберпреступности ... в 2021 году, как ожидается, вырастут до более чем 6 триллионов долларов» [2], а «затраты, связанные с киберпреступностью, будут расти ежегодно на 15% в течение следующих пяти лет» [3]. О росте рассматриваемых преступлений говорят и представители правоохранительных органов Беларуси. Так, по словам заместителя начальника управления по противодействию киберпреступности криминальной милиции УВД Миноблисполкома Н.Н. Ковалева, «по итогам августа текущего (2021) года на территории Минской области совершено свыше 1400 киберпреступлений. За аналогичный период прошлого года – 1100. Наблюдается постоянный рост» [4].

Несмотря на то, что к данной проблеме обращались многие исследователи в области права, социологии, политологии, международных отношений и проч., вплоть до сегодняшнего дня не удалось выработать единого унифицированного подхода к пониманию самой сути этого асоциального явления, которое уже можно рассматривать в качестве одной из глобальных проблем современности. В качестве возможных предпосылок такой неопределенности может послужить тот факт, что нередко ученые пытаются определить понятие «киберпреступность» через иные, столь же неоднозначные трактовки. Например, в специальной литературе обнаруживается высказывание С.В. Воронцовой о том, что «термин киберпреступность используется для определения преступности в виртуальном пространстве, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в локальных и глобальных сетях» [5, с. 14]. Иными словами, исследователь связывает термин киберпреступность с категорией «виртуальное пространство». Однако и эта категория все еще не имеет своего однозначного толкования, а указывающие на этот в целом верный признак ученые нередко синонимизируют его, выделяя цифровое пространство (Л.В. Иванова, Г.В. Перегожина [6]), киберпространство (И.Г. Чекунов [7, с. 43–44]), информационное пространство (Е.С. Смольянинов [8, с. 126]) и проч.

Более верным с точки зрения методологии определения и понимания видится позиция В.А. Номоконова, предложившего более 15 лет назад широкий подход к пониманию категории «киберпреступность». Суть такого подхода состоит в том, что киберпреступность, выступая в качестве родового понятия, включает в себя не только посягательства на информационную безопасность (компьютерные преступления в узком смысле этого слова), но также и иные преступные деяния, для которых воздействие на цифровую информацию, хранящуюся на машинных носителях или в сети, является способом совершения преступления [9, с. 75].

На справедливость подобного широкого подхода указывают и практические работники Управления Организации Объединенных Наций по наркотикам и преступности. В разработанном ими специальном образовательном модуле «Введение в киберпреступность» отмечается, что киберпреступность, являясь родовой категорией, включает в себя два самостоятельных вида: киберзависимые преступления и преступления, совершаемые посредством кибертехнологий [10]. К числу киберзависимых преступлений сотрудники названного управления относят такие деяния, в которых модификация компьютерной информации выступает самоцелью (компьютерные преступления в узком смысле слова в трактовке В.А. Номоконова). Преступлениями же, совершаемыми посредством кибертехнологий, в пособии признаются все прочие преступные деяния, для которых использование информационных или коммуникационных технологий, модификация информации, хранящейся на машинных носителях или в сетях, передаваемой по линиям передачи данных, выступает средством или орудием совершения преступления, что практически воспроизводит позицию В.А. Номоконова.

Таким образом, в качестве основных характерных признаков, свойственных проявлениям киберпреступности, следует назвать особый способ совершения преступления (уничтожение или модификация цифровой информации), а также особый признак среды совершения преступления – цифрового информационного пространства. Последний из названных признаков (среда совершения преступления) в настоящее время не находит своего отражения в рамках классического понимания структуры объективной стороны состава преступления, однако вопрос о необходимости включения подобного признака в объективную сторону диктует сама практика реализации уголовного законодательства и квалификации совершаемых деяний, поскольку ни к одному из устоявшихся в науке признаков, характеризующих объективную сторону преступления (место, время, способ, обстановка совершения преступления) цифровое информационное пространство в полной мере отнести нельзя.

Для определения направлений противодействия киберпреступности необходимо, в первую очередь, обратить внимание на ее детерминанты. В частности, следует отметить такие факторы, обуславливающие возможность совершения киберпреступлений, как возможность обеспечения анонимности лица, действующего противоправно в условиях цифровой информационной среды (что, кроме прочего, имеет существенное значение для высокого уровня латентности рассматриваемой группы преступлений); существование значительного количества программных компонентов, способных к автоматическому функционированию без участия пользователя; существенное отставание правового регулирования от стремительно развивающихся технологий; недостаточная проработанность вопросов уголовно-процессуального доказывания с учетом специфики совершения киберпреступлений (собираения и фиксации электронных доказательств в совокупности с возможностью их быстрого изменения или уничтожения, особенностей приобщения их к материалам уголовного дела и проч.); отсутствие значительных материальных затрат, необходимых для подготовки и совершения киберпреступления и т.д.

Приведенная совокупность причин и условий, способствующих совершению преступлений рассматриваемой категории, не может претендовать на роль исчерпывающего перечня. Зачастую на совершение подобных противоправных деяний оказывают существенное влияние субъективные факторы, такие как уровень технической подготовленности субъекта, его мотивация, достигаемые цели и т.д. Вместе с тем, даже приведенных детерминант достаточно для того, чтобы сделать вывод о необходимости уделения более пристального внимания вопросам противодействия проявлениям киберпреступности. В частности, уже сегодня наблюдается острая потребность подготовке соответствующих специалистов, способных не только дать юридическую оценку содеянному, но и разобратся в самом механизме совершения противоправного деяния (подчас достаточно сложном, предполагающем многократную передачу информации от одного адресата другому).

Также актуальной является задача повышения квалификации сотрудников служб безопасности предприятий, учреждений, организаций с тем, чтобы они могли на собственном уровне обеспечить должную информационную без-

опасность от возможных внешних воздействий. Дальнейшего развития требует пропаганда личной информационной безопасности граждан.

Наконец, законодательным органам и дипломатическим службам всех без исключения государств следует активизировать работу по совершенствованию действующего законодательства, направленного на внедрение действенных правовых механизмов противодействия киберпреступности, обеспечение необходимого и оперативного взаимодействия правоохранительных органов различных стран, поскольку киберпреступность на сегодняшний день обладает значимым фактором транснациональности, не признающей ни государственных границ, ни особенностей функционирования внутреннего уголовного, уголовно-процессуального и иного законодательства.

Указанные меры противодействия и профилактики киберпреступлений должны предприниматься постоянно, обладать системностью и продолжать свое развитие по мере появления новых угроз в условиях цифровой информационной среды. Только в этом случае можно будет говорить о возможности полноценной защиты информационной безопасности граждан, субъектов хозяйствования, общества и государства.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Прогнозы 2030. Заглянем в будущее // Территория будущего 2030 [Электронный ресурс]. – URL: http://future2030.space/ru_2030. Дата доступа: 03.11.2021.
2. По данным Cybersecurity Ventures, киберпреступность превысит 6 триллионов долларов в 2021 году // NBC 5 [Электронный ресурс]. URL: <https://www.nbcdfw.com/news/tech/cybercrime-to-top-6-trillion-in-2021-north-texas-security-firm-says/2636083/>. Дата доступа: 03.11.2021.
3. 40+ статистических данных и фактов о кибербезопасности на 2021 год // Website Rating [Электронный ресурс]. URL: <https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/>. Дата доступа: 03.11.2021.
4. В Беларуси растет число киберпреступлений // Sputnik Беларусь [Электронный ресурс]. – URL: <https://sputnik.by/20210907/v-belarusi-rastet-chislo-kiberprestupleniy--1056275651.html>. – Дата доступа: 04.11.2021.
5. Воронцова, С.В. Киберпреступность: проблемы квалификации преступных деяний / С.В. Воронцова // Российская юстиция. 2011. № 2. С. 14–15.
6. Иванова, Л.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений / Л.В. Иванова, Г.В. Перегожина // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. – 2020. – Том 6. – № 4 (24). – С. 155–171.
7. Чекунов, И.Г. Киберпреступность: понятие и классификация / И.Г. Чекунов // Российский следователь. 2012. № 2. С. 37–44.
8. Ищук, Я.Г. Цифровая криминология: учебное пособие / Я.Г. Ищук, Т.В. Пинкевич, Е.С. Смольянинов. М.: Академия управления МВД России, 2021. 244 с.
9. Номоконов, В.А. Актуальные проблемы борьбы с киберпреступностью / В.А. Номоконов // Компьютерная преступность и кибертерроризм: сборник научных работ. Запорожье: Центр исследования компьютерной преступности, 2004. Вып. 1. С. 72–76.
10. Введение в киберпреступность // Организация Объединенных Наций [Электронный ресурс]. URL: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_1_Introduction_to_Cybercrime_RU.pdf. Дата доступа: 04.11.2021.