УДК 343.644.4
ББК Х408.113
DOI: 10.14529/law200202

СТРАТЕГИЧЕСКИЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В ЦИФРОВОЙ СФЕРЕ: СТРАНОВЕДЧЕСКИЙ АНАЛИЗ

Ю. А. Воронин, И. М. Беляева, Т. В. Кухтина
Южно-Уральский государственный университет, г. Челябинск

Статья посвящена анализу стратегии и практики противодействия современных государств (главным образом России и США) доминирующим видам цифровой преступности. Речь идет о реализации комплекса мер в отношении наиболее опасных и распространенных террористических и корыстно-мошеннических преступлений, совершаемых в цифровой среде или путем использования цифровых технологий. В статье дается также оценка степени эффективности предпринимаемых в России и США усилий по стабилизации сложившейся ситуации. По мнению авторов статьи, создание и совершенствование систем противодействия цифровой преступности именно в упомянутых государствах отличаются наибольшим динамизмом и сравнительно высоким уровнем результативности. Но очевидно и то, что стратегически взвешенный подход к реализации мер противодействия цифровой преступности требует согласованных усилий не только Российской Федерации и Соединенных Штатов Америки, но и всего мирового сообщества. Сделан вывод о том, что существующий концептуальный подход к профилактическому элементу этой стратегии нуждается в дальнейшей модернизации.

Ключевые слова: цифровая преступность, преступления в сфере цифровой информации, кибербезопасность, стратегия противодействия, международное сотрудничество.

1. Мировое развитие информационно-цифровой среды (сферы), являясь объективно неизбежным процессом, приносит не только позитивные результаты, но одновременно порождает сложные, в том числе негативные, социальные и правовые последствия. Это в свою очередь требует опережающего принятия мер безопасности, нейтрализующих или предотвращающих криминальные проявления в данной сфере, и в этой связи усиления государственного контроля над состоянием информационно-цифрового пространства [1, с. 14]. Все более очевидной становится также необходимость максимального использования странами мирового сообщества не только их национального, но и международного опыта в ходе разработки и реализации антикриминогенных мер в информационно-цифровой среде, а также их межгосударственной координации. Есть основания констатировать, что усилия большинства государств в этом плане сконцентрированы главным образом на двух основных направлениях противодействия угрозам информационно-цифровой безопасности. Речь идет, во-первых, об упреждающем противодействии кибертеррористическим атакам и, во-вторых, о предупреждении и нейтрализации так называемых цифровых преступлений «общеуголовного характера».

2. В рамках первого упомянутого направления важнейшей задачей реализации информационно-цифровой стратегии стран мирового сообщества в отношении кибертеррористических атак является их блокирование путем использования организационных, правовых средств и электронных технологий

защиты государствами своей безопасности. Особенно отчетливо в минувшие два десятилетия это прослеживается в Российской Федерации и Соединенных Штатах Америки в ходе реализации ими мер противодействия террористическим структурам.

Так, на территории Российской Федерации угрозы использования террористами информационно-цифровых систем для осуществления террористических операций в виде посягательств на безопасность критически важных инфраструктур – оборонных, промышленных, банковских и т.д. – стали очевидной реальностью. В этой связи обеспечение национальной безопасности России было бы просто невозможным без постоянного совершенствования и активизации данного сегмента противодействия цифровой преступно-

сти. Это касается как национального антитеррористического законодательства, так и деятельности спецслужб, диктуя одновременно необходимость укрепления сотрудничества с другими государствами в соответствующей сфере.

В частности, правовую основу, обеспечивающую стратегические направления в противодействии кибертерроризму в Российской Федерации, образует целый ряд основополагающих документов. Среди них – Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»; Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Указ Президента РФ от 31 декабря 2015 г. № 683 «О стратегии национальной безопасности Российской Федерации».

Основными же субъектами системы координации мер противодействия данному виду терроризма являются Президент Российской Федерации, Совет безопасности РФ, Национальный антитеррористический комитет с его оперативным штабом, Антитеррористические комиссии в субъектах Российской Федерации вместе с их оперативными штабами. Важнейшая роль отведена также деятельности соответствующих силовых структур – ФСБ и МВД РФ. При этом именно на ФСБ в первую очередь Указом Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» возложены полномочия по решению упомянутых задач, связанных с противодействием кибератакам на информационные системы и информационно-телекоммуникационные сети России, в том числе находящиеся в ее дипломатических представительствах за рубежом.

Следует подчеркнуть, что Российское государство параллельно прилагает настойчивые усилия по активизации и укреплению международного сотрудничества в этой области. Так, 18 ноября 2019 года Российской Федерацией были внесены на рассмотрение Третьего комитета сессии Генеральной ассамблеи ООН и одобрены большинством голосов (вопреки позиции США) пакет предложений и резолюция «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Эти документы включают формулировки соответствующих международных принципов взаимодействия государств в связи с назревшей необходимостью укрепления безопасности глобальных телекоммуникационных и информационно-цифровых систем в борьбе как с кибертерроризмом, так и с общеуголовной цифровой преступностью. Кроме того, Российской Федерацией предложено создать систему международного слежения за добросовестностью выполнения государствами взятых на себя обязательств в этой сфере. Дальнейшее согласование спецкомитетом ООН плана и порядка реализации указанных инициатив намечено на август 2020 года.

Свидетельством стремления к укреплению такого сотрудничества являются также усилия российской стороны в этом направлении на региональном уровне. В частности, ярким примером тому служит инициированное Российской Федерацией и ратифицированное затем государствами – членами ШОС (в данном случае – Россией, Казахстаном, Таджикистаном) межправительственное соглашение о сотрудничестве в сфере обеспечения международной информационной безопасности от актов кибертерроризма и общеуголовной компьютерной преступности. Правда, от ратификации упомянутого соглашения воздержалась Китайская Народная Республика.

Что же касается Соединенных Штатов Америки, то реализация их стратегии противодействия кибертерроризму является одной из важнейших задач и соответствующим направлением деятельности Национального контртеррористического центра, Национального Агентства Безопасности (АНБ), Центра защиты национальной инфраструктуры (в составе ФБР), Государственного департамента и Государственного казначейства США, а также целого ряда других государственных учреждений, сотрудничающих в рамках так называемых «Совместных антитеррористических сил» (Joint Terrorism Forces) на всей территории страны. И это вполне объяснимо. Как справедливо отмечают многие специалисты, поскольку атаки на компьютерные сети, включая распространение компьютерных вирусов, играют все более важную роль не только в политических, но в особенности в военных операциях XXI века, то в силу этого война с применением информационных технологий стала новой концепцией цифрового про-

тивостояния с кибертерроризмом. Власти США хорошо понимают высокую вероятность угрозы террористических акций в сфере электронных технологий и принимают соответствующие контрмеры. Среди них – интенсивное развитие национальной сети рабочих групп упомянутых секретных служб по предотвращению, обнаружению и расследованию различных электронных террористических атак на жизненно важные инфраструктуры и финансово-платежные системы США. Сюда же, по мнению российских экспертов, следует отнести и развитие специальной электронной базы ФБР об организациях и лицах, причастных или потенциально причастных к внутреннему и международному терроризму [3, с. 88, 94; 5, с. 9].

Правда, следует, к сожалению, отметить, что при очевидном понимании важности разработки и реализации мер информационно-цифровой безопасности по противодействию угрозам террористического (как впрочем и общекриминального) характера, Соединенные Штаты пока не очень стремятся к практическому осуществлению международных договоренностей о сотрудничестве в этой области [7, с. 7]. Так, еще в 2006 году США ратифицировали Конвенцию Совета Европы по борьбе с киберпреступностью (так называемую Будапештскую конвенцию), вступившую в силу в 2007 году. Но конкретных шагов по реальному сотрудничеству в этой области они демонстрируют пока сравнительно мало. Между тем более принципиальную позицию в этом плане декларируют многие европейские государства, предпринимая при этом вполне конкретные меры. Так, решением Совета ЕС создан постоянно действующий юридический механизм введения санкций за кибератаки, осуществляемые физическими и юридическими лицами. В частности, Евросоюз намерен вводить запретительные меры, направленные на противодействие кибератакам, которые представляют внешнюю угрозу не только для стран ЕС, но и для государств, не входящих в Евросоюз, а также за атаки на международные организации. В новый черный список также будут вноситься «лица и организации, которые предоставляли организаторам кибернетических атак техническую, финансовую или интеллектуальную поддержку».

3. Вторым наиболее важным направлениием анализируемой стратегии противодействия криминальным угрозам в России и Соединенных Штатах являются правоохранительные и финансово-технологические меры названных государств в отношении общеуголовной, главным образом корыстно-мошеннической, цифровой преступности.

Особенно это актуально для Российской Федерации. Так, по данным МВД РФ, в общем числе зарегистрированных в 2019 году преступлений удельный вес так называемых киберпреступлений (совершенных через интернет или с помощью мобильной связи) вырос по сравнению с предыдущим годом, с девяти процентов до 14,5 %, то есть почти на 70 %. При этом около половины таких преступлений относятся к категориям тяжких и особо тяжких. Совершенно очевидно, что зашкаливающий уровень похищения клиентской базы персональных данных, кибермошенничества и компьютерного шантажа диктуют жесткую необходимость дальнейшего развития комплекса финансово-технологических мер по защите от утечек цифровой информации, в том числе от широкой практики ее «сливов» со стороны сотрудников банковских структур. Ведь, несмотря на то, что Россия входит в число стран-лидеров по уровню развития «финтеха», по-прежнему остается уязвимой сервисная система ее банков, неуклонно растет число похищений денежных средств с клиентских счетов. В стране каждый месяц происходит около трех тысяч попыток похищения денежных средств с помощью цифровых программ, позволяющих получить удаленный доступ к персональным данным клиентов. Крупные банки теряют на этом до 10 млн рублей ежемесячно [4].

В этой связи именно на правоохранительные органы, прежде всего на МВД РФ, возложена реализация задачи противодействия общеуголовной цифровой преступности. В частности, в компетенцию соответствующей структуры МВД России (Управления «К») входят:

– противодействие корыстно-мошенническим деяниям с использованием возможностей электронных платежных систем, вредоносных программ для ЭВМ;

– выявление и пресечение корыстных преступлений, связанных с незаконным использованием ресурсов сетей сотовой, телекоммуникационной связи, в том числе сети Интернет;

– пресечение неправомерного доступа в этих целях к коммерческим каналам спутникового и кабельного телевидения;

– пресечение иных преступлений в сфере информационно-цифровых технологий.

Помимо осуществления оперативно-розыскных задач, полиции все чаще приходится заниматься следственной деятельностью в отношении преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Только в 2019 году число таких расследований сотрудниками МВД – дознавателями и следователями – возросло на 62 %. В связи с этим МВД России создало в структуре следственного департамента и территориальных органов предварительного следствия отдельные подразделения для борьбы с IT-преступлениями [4].

Наряду с мерами противодействия высокотехнологичной цифровой преступности средствами правоохранительных органов и спецслужб, следует упомянуть о существенном вкладе Банка России в предупреждение несанкционированных проникновений и компьютерных взломов в кредитно-финансовой сфере. Речь идет о деятельности входящего в его структуру Центра мониторинга и профилактики кибератак со стороны криминальных элементов с целью личного обогащения посредством взлома компьютерной сети кредитно-финансовых организаций. Причем указанные функции данное подразделение Банка России осуществляет в тесном взаимодействии с ФСБ и МВД РФ. Кроме того, активно пропагандируемое Центробанком в последнее время внедрение биометрических технологий, электронных средств распознавания голоса своих клиентов и ряда других современных методов цифровой защиты также является существенным вкладом в повышение уровня безопасности функционирования банковских структур.

При этом параллельно с очевидной необходимостью активизации финансово-технологических мер стратегическая концепция противодействия общеуголовной цифровой преступности в России включает в себя решение задачи повышения «цифровой» грамотности пользователей сервисов путем широкого развития сети специальных семинаров и тренингов по основам кибербезопасности, по культивированию навыков «кибергигиены».

Что же касается Соединенных Штатов Америки, то этот (так называемый общеуголовный) сегмент противодействия цифровой преступности также приобретает все большую значимость. Увеличение объемов электронно-цифровой информации, совершенствование технологий, облегчающих доступ к этим ресурсам, существенно повышают эффективность коммерческого шпионажа, корыстно-мошеннических преступлений, электронного пиратства, особенно в финансово-банковской сфере. В результате причиняется огромный материальный ущерб экономике Соединенных Штатов, достигающий в годовом исчислении примерно 300 и более миллиардов долларов [6, с. 107]. Вполне естественно, что задача противодействия высокотехнологичной цифровой преступности в США в значительной степени ложится на специализированные подразделения ФБР, оснащенные самыми передовыми программными инструментами. Но успех в осуществлении этого направления работы не может быть обеспечен лишь силами специализированных структур данного ведомства. С учетом проникновения цифровых технологий в каждую «клеточку» экономического организма американского социума и государства принципиально важным является использование самих финансовых институтов в противостоянии с киберпреступлениями.

Правовой базой организационных шагов в этом направлении послужил принятый Конгрессом США в 2015 году «Акт о кибербезопасности» (CSA). В свою очередь его финансовую основу обеспечило включение этого законодательного акта в «Акт о консолидированных ассигнованиях» 2016 года (Consolidated Appropriations Act). Оба они легитимизируют процесс обмена информацией о кибератаках между, с одной стороны, бизнес-организациями (главным образом, кредитно-финансовыми структурами), а с другой – правительственными подразделениями, согласившимися принять участие в этой совместной работе.

В частности, в США в рамках самого мощного национального Центра по обмену и анализу информации о финансовых услугах функционирует специальное подразделение по борьбе с киберпреступлениями, посягающими на финансовые институты, – Центр по финансовому системному анализу и устойчивости. Одной из важнейших его функций является координация антихакерской деятельности американских банков в тесном

взаимодействии с правительственными организациями, прежде всего с мощным потенциалом ФБР. При этом упомянутый Центр демонстрирует чрезвычайную результативность благодаря финансовой и кадровой поддержке со стороны восьми крупнейших банковских структур страны. Среди них – «Бэнк оф Америка», «ГолднеэнЗакс», «Морган Стэнли» и ряд других мощных финансово-кредитных организаций. Правда, оценивая сложившуюся ситуацию в целом, приходится констатировать следующее. Борьба с киберпреступниками в Соединенных Штатах идет давно и с переменным успехом. На каждый новый изощренный метод защиты финансово-кредитных структур хакеры отвечают созданием новых вирусных программ, новых технологий взлома. И это противостояние, похоже, продолжится в обозримом будущем.

4. В заключение следует отметить, что о какой бы стране ни шла речь, успешность проанализированных и ряда других направлений стабилизации криминогенной ситуации предполагает, с одной стороны, обязательное соблюдение определенного баланса между свободой граждан на получение и распространение идей и информации, и с другой – необходимость эффективной борьбы против существующего воздействия криминогенных факторов информационно-цифровой сферы на национальную безопасность, территориальную целостность и общественный порядок в стране (см.: Распоряжение Правительства Российской Федерации от 26 июля 2006 г. № 1060-р «О подписании «Европейской конвенции о трансграничном телевидении»).

Следует также отдавать себе отчет в том, что реализация рассмотренных элементов тратегии противодействия цифровой преступности может принести положительные результаты лишь при реальном налаживании международного сотрудничества в деле разработки и принятия глобальных цифровых стандартов, при отказе всех государств от дестабилизации киберпространства и от использования интернета в качестве инструмента цифровой агрессии друг против друга. Лишь согласованные усилия членов мирового сообщества в области использования информационно-цифровых технологий способны предотвратить нарастающее обострение «цифровой войны» [2, с. 39].

Литература

1. Воронин, Ю. А. Преступления в сфере обращения цифровой информации и их детерминанты / Ю. А. Воронин // Виктимология. – 2020. – № 1 (23). – С. 74–80.

2. Воронин, Ю. А. Криминогенные факторы в информационно-цифровой среде / Ю. А. Воронин // Smart Law for Smart Industry: сб. научных статей. – М., 2020. – С. 35–41.

3. Ефремов, А. Е. Этапы развития законодательства США по борьбе с терроризмом после 11 сентября 2001 года / А. Е. Ефремов // Журнал зарубежного законодательства и сравнительного правоведения. – 2017. – № 3. – С. 88–94.

4. Жаткин, Р. «Темная сторона финтеха» / Р. Жаткин. URL: https://novayagazeta.ru/ articles/2019/11/02/82607.

5. Канафина, Г. Е. К вопросу о политике США в области борьбы с международным терроризмом / Г. Е. Канафина. URL: http://www.Albest.ru.

6. Лапшин, С. И. Преступность в области информационных технологий / С. И. Лапшин // Технологии и средства связи. – 1997. – № 1. – С. 107–110.

7. Усилинский, Ф. А. Кибертерроризм в России: его свойства и особенности / Ф. А. Усилинский // Право и кибербезопасность. – 2014. – № 1. – С. 6–11.

Воронин Юрий Александрович – доктор юридических наук, профессор кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: voroninya@yandex.ru.

Беляева Ирина Михайловна – кандидат юридических наук, доцент, заведующая кафедрой уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: irina69@bk.ru.

Кухтина Татьяна Владимировна – старший преподаватель кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: upiuip@mail.ru.

Статья поступила в редакцию 4 марта 2020 г.

DOI: 10.14529/law200202

STRATEGIC DIRECTIONS OF COUNTERING CRIME IN THE DIGITAL SPHERE: CROSS-CULTURAL ANALYSIS

Yu. A. Voronin, I. M. Belyeva, T. V. Kukhtina
South Urals State University, Chelyabinsk, Russian Federation

The article is devoted to the analysis of the strategy and practice of counteracting modern states (mainly Russia and the USA) to the dominant types of digital crime. We are talking about implementing a set of measures in relation to the most dangerous and widespread terrorist and mercenary-fraudulent crimes committed in the digital environment or through the use of digital technologies. The article also assesses the degree of effectiveness of efforts being made in Russia and the United States to stabilize the current situation. According to the authors of the article, the creation and improvement of digital crime counteraction systems in these countries is characterized by the greatest dynamism and a relatively high level of effectiveness. But it is also obvious that a strategically balanced approach to the implementation of measures to combat digital crime requires the concerted efforts of not only the Russian Federation and the United States of America, but also the entire world community. It is concluded that the existing conceptual approach to the preventive element of this strategy needs further modernization.

Keywords: digital criminality, crimes in the sphere of digital information, cybersecurity, strategy of combating, international collaboration.

References

1. Voronin YU. A. [Crimes in the sphere of digital information and their determinants]. *Viktimologiya [Victimology]*, 2020, no. 1, pp. 74–80. (in Russ.)

2. Voronin YU. A [Criminogenic factors in the information and digital environment] V kn.: Smart Law for Smart Industry: sb. nauchnykh statey [In the book.: Smart Lab for Smart Industry: collection of scientific articles]. Moscow, 2020, pp. 35–41. (in Russ.)

3. Efremov A. E. [Stages of development of US legislation to combat terrorism after September 11, 2001]. *ZHurnal zaru-bezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya [Journal of foreign legislation and comparative law]*, 2017, no. 3, pp. 88–94. (in Russ.)

4. ZHatkin R. «Temnaya storona fintekha» ["The dark side of FINTECH"]. Available at: https://novayagazeta.ru/articles/2019/11/02/82607.

5. Kanafina G. E. *K voprosu o politike SSHA v oblasti bor'by s mezhdunarodnym terrorizmom* [On the issue of US policy in the field of combating international terrorism]. Available at: http://www.Albest.ru.

6. Lapshin S. I. [Crime in the field of information technologies]. *Tekhnologii i sredstva svyazi [Technologies and means of communication]*, 1997, no. 1, pp. 107–110. (in Russ.)

7. Usilinskiy F. A. [Cyberterrorism in Russia: its properties and features]. *Pravo i kiberbezopasnost' [Law and cybersecurity],* 2014, no. 1, pp. 6–11. (in Russ.)

Yuri Alexandrovich Voronin – Doctor of Sciences (Law), Professor of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: voroninya@yandex.ru.

Irina Mikhailovna Belyaeva – Candidate of Sciences (Law), Chair of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: irina69@bk.ru.

Tatyana Vladimirovna Kukhtina – Research assistant of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: upiuip@mail.ru.

Received 4 March 2020.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Воронин, Ю. А. Стратегические направления противодействия преступности в цифровой сфере: страноведческий анализ / Ю. А. Воронин, И. М. Беляева, Т. В. Кухтина // Вестник ЮУрГУ. Серия «Право». – 2020. – Т. 20, № 2. – С. 12–18. DOI: 10.14529/law200202.

FOR CITATION

Voronin YU. A., Belyeva I. M., Kukhtina T. V. Strategic directions of countering crime in the digital sphere: cross-cultural analysis. *Bulletin of the South Ural State University. Ser. Law*, 2020, vol. 20, no. 1, pp. 12–18. (in Russ.) DOI: 10.14529/law200202.