Научная статья
https://doi.org/ 10.24412/2220-2404-2024-11-15
УДК 343.2/.7

ЦИФРОВОЕ УГОЛОВНОЕ ПРАВО: ПЕРСПЕКТИВЫ ФОРМИРОВАНИЯ И РАЗВИТИЯ (ЧАСТЬ 1)

Лебедев С.Я., Джафарли В.Ф.
Российский государственный университет имени А.Н. Косыгина

Аннотация. *Цель. В статье обосновывается актуальность и целесообразность формирования и дальнейшего развития научно-исследовательского проекта «Цифровое уголовное право». Авторы убеждены в необходимости широкого использования инновационного инструментария эпохи 6-го технологического уклада в предупреждении как традиционной, так и киберпреступности. В процессе изучения проблем были использованы общенаучные (анализ, синтез, индукция и дедукция) и частно-научные (уголовно-правовой и криминологический) методы исследования. В результате проведенного анализа сделаны выводы о том, что имеющиеся ресурсы обеспечения безопасности от нарастающего вала цифровых преступлений находятся далеко за пределами адекватного их общественно опасному потенциалу уголовно-правового и призванного реализовывать его правоохранительного контроля. Выводы и заключения: материалы публикации могут быть использованы в целях цифровой модернизации уголовного законодательства и правоохранительной практики, формирования и развития системы криминологической кибербезопасности значимых объектов от всей совокупности преступных посягательств.*

Ключевые слова: *цифровое уголовное право, цифровые преступления, цифровые наказания, криминологическая кибербезопасность, цифровая модернизация законодательства и правоохранительной практики.*

DIGITAL CRIMINAL LAW: PROSPECTS OF FORMATION AND DEVELOPMENT (PART 1)

Semyon Ya. Lebedev, Vugar F. Dzhafarli
Kosygin Russian State University

Abstract. *Goal. The article substantiates the relevance and expediency of the formation and further development of the research project "Digital Criminal Law". The authors are convinced of the need for widespread use of innovative tools of the era of the 6th technological order in the prevention of both traditional and cybercrime. In the process of studying the problems, general scientific (analysis, synthesis, induction and deduction) and private scientific (criminal law and criminological) methods of cognition were used. As a result of the analysis, it was concluded that the available resources to ensure security from the growing wave of digital crimes are far beyond the limits of their adequate socially dangerous potential of criminal law and law enforcement control designed to implement it. Conclusions and conclusions. The materials of the publication can be used for the purpose of digital modernization of criminal legislation and law enforcement practice, the formation and development of a system of criminological cybersecurity of significant objects from the totality of criminal encroachments.*

Keywords: *digital criminal law, digital crimes, digital punishments, criminological cybersecurity, digital modernization of legislation and law enforcement practice.*

Введение.

Жизнь в эпоху глобальных социальных трансформаций, вызванных активным развитием характерных для 6-го технологического уклада цивилизационных отношений, так называемых НБИКС- (нано-, био-, инфо-, когни-, социо-) технологий, сопровождаемых, ставшими уже обычными для всех без исключения сфер человеческой деятельности, цифровыми стандартами, неизбежно сопряжена далеко не только с положительными, но и серьезными отрицательными последствиями для многих социальных практик. При этом, погружаясь в пучину цифровых соблазнов, человечество запаздывает с осознанием их стремительно нарастающего угрожающего, порой разрушительного для традиционных ком-

муникативных связей цифрового потенциала, а поэтому пока крайне мало делает для надежного обеспечения от него своей безопасности. К сожалению, все, что касается, прежде всего, правовых ресурсов обеспечения таковой от нарастающего вала цифровых преступлений сегодня, попрежнему, находится далеко за пределами адекватного их общественно опасному потенциалу уголовно-правового и призванного реализовывать его правоохранительного контроля.

Обсуждение.

Обеспокоенные отмеченными обстоятельствами, авторы настоящей публикации, вначале каждый персонально [1; 2; 3; 4; 5], а в последние несколько лет сообща [6; 7; 8; 9; 10], продолжая уже вместе ранее заявленную и аргументированную в профессиональном пространстве тему правового обеспечения безопасности от цифровой преступности, смеют предложить профессиональному юридическому сообществу инновационную идею разработки самостоятельного *цифрового уголовно-правового сегмента социально-правового контроля над преступностью в киберпространстве.*

Авторская убежденность в необходимости и целесообразности такового сформировалась под влиянием не только личных многолетних наблюдений за развивающимися цифровыми технологиями, криминологического анализа исходящих от них криминогенных и собственно преступных киберугроз, но и периодического общения с представителями IT-сообщества, изучения существующих правовых документов, научных разработок и практик кибербезопасности, личного (своего, своих близких, знакомых, сослуживцев), в том числе, зачастую, печального виктимологического опыта, связанного с ущербом от киберпреступных посягательств и др. Всё это рождает твердую уверенность в том, что *адекватным противопоставлением цифровой преступности может быть только система цифровой безопасности, основанная, опять-таки, на адекватном цифровом уголовно-правовом ресурсе*.

Суть проблемы заключается в том, что в существующем гибридном мире, как пространстве слияния реального и виртуального миров, отличающимся возможностью совершения любых потребных для человека действий, включая противоправные, преступные, происходит трансформация их привычных форм из реальных в виртуальные. В этом случае, последние объективно выходят из-под реального контроля, а виртуального, как известно, для них пока не существует. Исключением является лишь техническая нейтрализация существующими структурами кибербезопасности (например, Лаборатория Касперского, Group-IB, Инфосекьюрити и др.), так называемых DDos-атак, связанных с хакерским проникновением в интерактивные информационные ресурсы пользователей с целью блокирования их действий в интернет-сети.

При этом и сами IT-специалисты, и юридически оценивающие их кибербезопасную деятельность правоведы, безусловно, убеждены в явной противоправности какой-либо нейтрализующей акции в отношении тех или иных кибератак. Последние – суть преступление. Пресечение же преступлений и, более того, их расследование (кстати, именно такую свою деятельность до недавнего времени открыто рекламировала компания Group-IB) – прерогатива правоохранительных органов. И какой бы социально полезной по своему позиционируемому эффекту ни была деятельность негосударственных служб безопасности по пресечению и расследованию киберпреступлений, от этого она менее противоправной не становится. Вспоминаются, в этом случае, аналогии с «правоохранительной» деятельностью так называемых «санитаров общества», устраняющих из социальной жизни педофилов, незаконных мигрантов, коррупционеров и т.п.

Таким образом, инновационная преступность, проявляющая себя в киберпространстве, большей своей частью, не попадает в зону влияния правоохранительной практики как раз из-за отсутствия таковой в этом виртуальном пространстве. Грешный же человек, сосредоточенный на совершении преступлений, находит для себя в современном гибридном мире гораздо больше возможностей для криминальной самореализации, нежели в реальном, пока ещё традиционно подконтрольном существующему уголовному закону и практике его применения.

IT-специалисту, да, видимо, и любому более-менее продвинутому пользователю, хорошо известно, что вполне удобное и относительно безопасное существование человека в рассматриваемом гибридном мире обеспечивается:

- более высокой, по сравнению с реальными возможностями, результативностью (эффективностью) достижения цели какой-либо деятельности;

- низкой (часто, бесплатной) стоимостью привлекаемых для этого информационно-телекоммуникационных технологий (ИКТ);

- доступностью цифровой инфраструктуры и, главное, – анонимностью источника (субъекта) инициации действия (деяния), а следовательно, – относительной защищённостью от любого внешнего воздействия, исходящего от реального источника правоохранения.

По-человечески понимая преимущества гибридного мира для любого индивида, стремящегося к безграничной свободе, всё же не стоит забывать о том, что, исходящий от такового и от его поведения в гибридном пространстве вред (общественная опасность), безусловно, должен быть предотвращён. Во всяком случае, ориентация общества и государства на предупреждение, нейтрализацию такой общественной опасности преступлений, совершаемых в киберпространстве, либо на ликвидацию (компенсацию) их общественно опасных последствий, в том числе обеспечиваемой уголовной ответственностью и связанным с ней уголовным наказанием, должна целиком и полностью соответствовать нарастающим криминальным киберугрозам. Поэтому специалисты, некоторые из научных трудов которых в области уголовного права и криминологии уже упоминались выше, обоснованно рассматривают обеспечение кибербезопасности от преступлений, совершаемых, опять-таки, в виртуальном пространстве, в качестве перспективного уголовно-политического приоритета. Важно отметить, что при этом, в основном, доминируют размышления по поводу необходимости трансформации уголовно-правовых признаков преступлений, приобретающих в киберпространстве соответствующие инновационно-технологические формы, не изменяющие в целом традиционной содержательной стороны таких уголовно наказуемых деяний. То есть, цифровое преступление, большей частью, сохраняет привычные для человека стандарты его традиционных пороков, облачённых в мотивационные стимулы удовлетворения своих паразитических потребностей (алчность – воровство, жестокость – насилие, хитроумность – обман, извращённость – сексуальная распущенность, гедонизм – алкоголизация, наркомания и др.) Цифровой ресурс здесь выступает для «злодея» исключительно более приемлемым, зачастую, более надежным и, что важно, безопасным средством достижения криминального успеха. Уголовный же закон, нацеленный на традиционные формы общественно опасного деяния, просто не «дотягивается» своим «ручным» ресурсом до цифрового преступления и, тем более, цифрового преступника. И думается, что сколь бы активнее он (закон) не стремился с помощью специалистов в области уголовного права отформатировать в этом своем доселе обычном качестве новые цифровые образы уголовно наказуемых деяний, всё равно реально настигнуть их таковой будет не в состоянии. Поэтому, как нам представляется, единственно приемлемым способом достижения целей уголовного права в условиях цифровизации преступности должна стать *цифровизация уголовного закона; то есть, включение его самого в информационно-технологические механизмы пространства виртуального мира*.

Предлагаемый новый информационно-технологический концепт модернизации уголовно-правового ресурса, превентивно нацеленного на инновационную преступность, должен, на наш взгляд, включать в себя *модернизацию (реконструкцию, переформатирование)* под цифровые стандарты с у щ е с т в у ю щ и х уголовно-правовых форм воздействия на преступления (преступность), оставляя в них, большей частью, классическое уголовно-правовое и криминологическое содержание, адаптированное к цифровой реальности. Предполагается, что концентрация осуществляемого в мониторинговом режиме цифрового уголовно-правового контроля над преступностью, включённого в общую систему обеспечения кибербезопасности, способна не только максимально фиксировать преступления, совершаемые в киберпространстве, но одновременно создавать информационную базу для формирования инновационно-технологической системы криминологической кибербезопасности, а вместе с ней – инновационно-технологической системы цифрового правосудия; то есть - киберправосудия.

Между тем, до сих пор наше традиционное материальное право, обозначающее, что есть правонарушение и преступление, и вместе с ним -процессуальное право, регламентирующее правовые механизмы воздействия на правонарушителей (преступников), демонстрируют себя в «аналоговом» режиме, тогда как система правоохранительного контроля всё более демонстрирует стремление к «цифровому» формату[1].

[1] Приведенное определение скорее тянет на аллегорию, так как не вполне адекватно, опять-таки, с точки зрения технической и технологической материи, отражает истинную суть означенного физического феномена, однако, позволим себе предположить, что большинству специалистов суть подобного сравнения, обозначаемого авторами в контексте обсуждаемой проблемы, будет понятна.

Результаты.

Произведенный уголовно-правовой, криминологический и технологический анализ состояния преступности в современном мире и, соответственно, существующей правоохранительной практики, демонстрирует криминальные потенциалы как цифровых средств, так и цифровых преступников, противодействие которым путем использования имеющихся государственных правовых, кадровых и информационно-технологических ресурсов представляется невозможным. Исходя из того, что организованной цифровой преступности, по сути, противостоит немногочисленный штат Управления МВД РФ по организации борьбы с противоправным использованием информационно-коммуникационных технологий, необходимо в корне изменить всю систему реагирования на цифровые угрозы.

Заключение.

Необходима цифровая модернизация под цифровые стандарты существующих уголовно-правовых форм воздействия на преступления (преступность), с условием неизменности классического уголовно-правового и криминологического содержания, адаптированного к цифровой реальности. В результате этого, цифровой уголовно-правовой контроль способен не только к фиксации киберпреступлений, но одновременно - и к формированию, и развитию систем криминологической кибербезопасности и цифрового правосудия.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Лебедев С.Я. Киберкриминология: к систематизации научного знания о технологических инновациях преступности и её предупреждения. Выступление на заседании Санкт-Петербургского международного криминологического клуба, Санкт-Петербург, 28 февраля 2014 г. / Шестаков Д.А., Дикаев С.У., Данилов А.П. Летопись Санкт-Петербургского международного криминологического клуба. Год 2014 // Криминология: вчера, сегодня, завтра. 2015. № 1.

2. Лебедев С.Я. Право и безопасность в цифровом мире / Сборник статей по материалам IV Всероссийской научно-практической конференции «Уголовно-правовое воздействие и его роль в предупреждении преступности». Саратов: Саратовская государственная юридическая академия, 2019.

3. Лебедев С.Я. Цифровой безопасности – цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. 2019, № 4. С. 17-25.

4. Джафарли В.Ф. Уголовная ответственность за совершение хищений в банковской сфере, связанных с использованием электронных платежных средств: дис. … канд. юрид. наук. М., 2003. 168 с.

5. Джафарли В.Ф. О созвучности тезиса «Цифровой безопасности – цифровой уголовно-правовой ресурс» теории криминологической безопасности в сфере информационных технологий // Криминология: вчера, сегодня, завтра. 2019. № 4. С. 47-54.

6. Лебедев С.Я., Джафарли В.Ф. Механизм цифровизации уголовного закона и перспективы его применения в киберпространстве // Наука и жизнь Казахстана. Международный научный журнал. 2020. № 10. С. 185-194.

7. Лебедев С.Я., Джафарли В.Ф. Перспективы развития уголовно-правовых инноваций в системе обеспечения криминологической кибербезопасности // Гуманитарные, социально-экономические и общественные науки. 2021. № 5. С. 125-130.

8. Джафарли В.Ф. Криминология кибербезопасности: в 5 т. / под ред. С.Я. Лебедева. М.: Проспект, 2022. 1392 с.

9. Джафарли В.Ф. Криминологическая кибербезопасность: теоретические, правовые и технологические основы / под ред. С.Я. Лебедева. 2-е изд., перераб. и доп. М.: Проспект, 2024. 480 с.

10. Лебедев С.Я., Джафарли В.Ф. Цифровое уголовное право. М.: Издательство Проспект, 2024. 392 с.

References:

1. Lebedev S.Y. Cybercriminology: towards the systematization of scientific knowledge about technological innovations of crime and its prevention. Speech at the meeting of the St. Petersburg International Criminological Club, St. Petersburg, February 28, 2014 / Shestakov D.A., Dikaev S.U., Danilov A.P. Chronicle of the St. Petersburg International Criminological Club. The year 2014 // Criminology: yesterday, today, tomorrow. 2015. № 1.

2. Lebedev S.Y. Law and security in the digital world / Collection of articles based on the materials of the IV All-Russian scientific and practical conference "Criminal law impact and its role in crime prevention". Saratov: Saratov State Law Academy, 2019.

3. Lebedev S.Y. Digital security – digital criminal law resource // Criminology: yesterday, today, tomorrow. 2019, No. 4. pp. 17-25.

4. Dzhafarli V.F. Criminal liability for embezzlement in the banking sector related to the use of electronic means of payment: dis. ... cand. Jurid. M., 2003. 168 p.

5. Dzhafarli V.F. On the consonance of the thesis "Digital security – digital criminal law resource" of the theory of criminological security in the field of information technology // Criminology: yesterday, today, tomorrow. 2019. No. 4. pp. 47-54.

6. Lebedev S.Y., Dzhafarli V.F. The mechanism of digitalization of the criminal law and prospects for its application in cyberspace // Science and Life of Kazakhstan. International Scientific Journal. 2020. No. 10. pp. 185-194.

7. Lebedev S.Y., Dzhafarli V.F. Prospects for the development of criminal law innovations in the system of ensuring criminological cybersecurity // Humanities, socio-economic and social sciences. 2021. No. 5. pp. 125-130.

8. Dzhafarli V.F. Criminology of cybersecurity: in 5 volumes / edited by S.Y. Lebedev. M.: Prospekt, 2022. 1392 p.

9. Dzhafarli V.F. Criminological cybersecurity: theoretical, legal and technological foundations / ed. by S.Y. Lebedev. 2nd ed., reprint. and additional m.: Prospect, 2024. 480 p.

10. Lebedev S.Y., Jafarli V.F. Digital criminal law. Moscow: Prospekt Publishing House, 2024. 392 p.

Информация об авторах:

Лебедев Семен Яковлевич, доктор юридических наук, профессор, Заслуженный юрист РФ, заведующий кафедрой уголовного права и адвокатуры, Российский государственный университет имени А.Н. Косыгина, e-mail: lebesem@yandex.ru.

Джафарли Вугар Фуад оглы, доктор юридических наук, доцент, профессор кафедры уголовного права и адвокатуры, Российский государственный университет имени А.Н. Косыгина, e-mail: nizami.66@mail.ru.

Semyon Ya. Lebedev, Doctor of Law, Professor, Honored Lawyer of the Russian Federation, Head of the Department of Criminal Law and Advocacy, Kosygin Russian State University.

Vugar F. Dzhafarli, Doctor of Law, Associate Professor, Professor of the Department of Criminal Law and Advocacy, Kosygin Russian State University.