DOI: 10.18287/2542-047X-2019-5-3-141-146
УДК 343.7

Дата поступления статьи: 2/IX/2019
Дата принятия статьи: 21/IX/2019

Г. Р. Григорян

СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ И ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ ОСНОВАНИЯ КРИМИНАЛИЗАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

© Григорян Гарик Рафикович (garik00063@yandex.ru), аспирант, кафедра уголовного права и криминологии юридического факультета, **Самарский национальный исследовательский университет имени академика С. П. Королева**, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.
Автор 4 научных публикаций, в том числе научных статей: «Особенности способов совершения преступлений, предусмотренных статьей 159.6 УК РФ», «Мошенничество в сфере компьютерной информации в системе преступлений в сфере собственности».
Область научных интересов: мошенничество в сфере компьютерной информации

АННОТАЦИЯ

В статье проводится анализ социально-экономических и информационно-технологических оснований криминализации мошенничества в сфере компьютерной информации. Показано, что фактор социально-экономический обусловленности и уголовно-правовой охраны информационной и экономической безопасности предопределен становлением и развитием в современном мире цифровой экономики. Что касается информационно-технологических факторов обусловленности уголовно-правовой охраны экономических отношений, они связаны с процессами формирования информационного общества. Как утверждается, в условиях действия новых объективных закономерностей следует смена парадигм уголовно-правовой охраны отношений собственности, и акцент смещается в сторону защиты имущественных и иных экономических отношений в сфере использования информационных и коммуникационных технологий от различного рода неправомерных вмешательств и нарушений. Делается вывод, что механизм уголовно-правового регулирования информационных имущественных отношений нуждается в конструировании новых составов преступлений, смежных с нормами о традиционном мошенничестве, совершаемом с использованием обмана или злоупотребления доверием в отношении исключительно чужих вещей как объектов физического мира или права на имущество.

Ключевые слова: уголовно-правовая охрана информационного общества и цифровой экономики, преступления в сфере экономики, преступления против собственности, мошенничество, мошенничество в сфере компьютерной информации, преступления в сфере компьютерной информации.

Цитирование. Григорян Г. Р. Социально-экономические и информационно-технологические основания криминализации мошенничества в сфере компьютерной информации // Юридический вестник Самарского университета. 2019. Т. 5. № 3. С. 141–146. DOI: https://doi.org/10.18287/2542-047X-2019-5-3-141-146.

DOI: 10.18287/2542-047X-2019-5-3-141-146
UDC 343.7
Submitted: 2/IX/2019
Accepted: 21/IX/2019

G. R. Grigoryan

SOCIO-ECONOMIC AND INFORMATION TECHNOLOGY BASES OF CRIMINALIZATION OF FRAUD IN COMPUTER INFORMATION

© Grigoryan Garik Rafikovich (grigoryangarik@yandex.ru), postgraduate student, Department of Criminal Law and Criminology, Faculty of Law, **Samara National Research University**, 34, Moskovskoye shosse, Samara, 443086, Russian Federation.
Author of 4 scientific works, including scientific articles: «Features of methods of committing crimes under Article 159.6 of the Criminal Code», «Fraud in the field of computer information in the system of crimes in the field of property».
Research interests: computer information fraud.

ABSTRACT

The article analyzes socio-economic and information technology bases of criminalization of fraud in the field of computer information. It is shown that the socio-economic factor of conditionality of the criminal law protection of information and economic security is predetermined by the emergence and development in the modern world of the digital economy. As for information technology factors of conditionality of criminal law protection of economic relations, they are associated with the processes of formation of the information society. According to the author, under the conditions of action of new objective laws, paradigms of criminal law protection of property relations change, and the focus shifts towards protecting property and other economic relations in the use of information and communication technologies from various unlawful interventions and violations. It is concluded that the mechanism of criminal law regulation of information property relations requires the construction of new offenses related to the rules on traditional fraud committed using deception or abuse of trust in relation to exclusively alien things as objects of the physical world or right to property.

Key words: criminal law protection of information society and digital economy, economic crimes, crimes against property, fraud, fraud in the field of computer information, crimes in the field of computer information.

Citation. Grigoryan G. R. *Sotsial'no-ekonomicheskie i informatsionno-tekhnologicheskie osnovaniya kriminalizatsii moshennichestva v sfere komp'yuternoi informatsii* [Socio-economic and information technology bases of criminalization of fraud in computer information]. *Iuridicheskii vestnik Samarskogo universiteta* [Juridical Journal of Samara University], 2019, Vol. 5, no. 3, pp. 141–146. DOI: https://doi.org/10.18287/2542-047X-2019-5-3-141-146 [in Russian].

Законодатель при выборе объекта уголовно-правовой охраны и установления уголовно-правового запрета должен учитывать прежде всего социальную обусловленность определенных общественных отношений, их значение и роль для всей системы общественных отношений [1, с. 171]. Норма уголовного права является эффективной, если она социально обусловлена. Детерминированность новых уголовно-правовых предписаний о мошенничестве в сфере компьютерной информации также следует считать основой их эффективного действия.

Облечение в новые реалии, информационно-технологические формы на основе социально-экономических предпосылок и уголовно-правовой охраны имущественных отношений вызвано прежде всего тем, что в России протекает процесс перехода на постиндустриальную стадию развития – информационное общество и цифровую экономику. Заметим, что «мошенничества в сфере компьютерной информации» характерны для информационного общества и будут расти количественно и изменяться качественно, модифицируясь и усложняясь в такого рода социуме. Отсюда как в России, так в мире с приоритетным направлением развития экономики в цифровом формате усиливается и ответственность государств за безопасность данных социально-экономических и информационно-технологических процессов.

В 2017 году количество преступлений, которые совершены в форме мошенничества (ст. 159–159^6 УК РФ), по сравнению с аналогичным периодом 2016 года, увеличилось на 6,6 % и составило 222 772. Количество преступлений в форме мошенничества, предварительно расследованных преступлений увеличилось на 2,6 % и составило 56 178, из них по 45 078 преступлениям уголовные дела направлены в суд. В 2018 году количество преступлений, совершенных в форме мошенничества (ст. 159–159^6), по сравнению с аналогичным периодом 2017 года, снизилось на 3,5 % и составило 215 036. С января по март 2019 года количество

преступлений, совершенных в форме мошенничества (ст. 159–159[6]), по сравнению с аналогичным периодом 2018 года, увеличилось на 10,9 % и составило 62 257. На 10 % увеличилось число предварительно расследованных преступлений в форме мошенничества, составив 16 926 деяний, из которых по 14 378 (+4,8 %) уголовные дела направлены в суд [2]. При этом следует принимать во внимание гиперлатентность мошенничества и его специальных видов, а также смежных с ним преступлений в сфере экономики.

Обратимся к анализу социально-экономических и информационно-технологических оснований криминализации мошенничества в сфере компьютерной информации.

Американский экономист Ф. Машлуп, который исследовал информационный сектор экономики на примере США, практически одновременно с профессором Токийского технологического института Ю. Хаяши ввели термин «информационное общество». Исследователи в своих трудах информационное общество определяли как социум, в котором компьютерные технологии смогут обеспечить людям доступ к надежным источникам информации и высокий уровень автоматизации производственных процессов. В информационном социуме растет число людей, которые заняты в сфере компьютерных технологий, коммуникациями и производством информационных услуг и высокотехнологических продуктов. В таком социуме углубляются процессы информатизации, связанные с использованием телефонии, радио, телевидения, сети Интернет, традиционных и электронных СМИ, электронной демократии, электронного государства, единой инфраструктуры электронного правительства, цифровых рынков, электронных социальных и хозяйствующих сетей, национальных технологических платформ онлайн-образования, онлайн-медицины, Национальной электронной библиотеки, получением финансовых, государственных, муниципальных и иных услуг в электронной форме.

В современном мире экономическое развитие государства все больше попадает в зависимость от информационных технологий. «Высокие» технологии влияют и на развитие рыночной экономики. Сырьевая экономика преобразовывается в экономику цифровую. Потребности населения постепенно переориентируются на быстрый поиск и получение достоверной информации и возможность оперативного обмена ею [3, с. 103]. Тому свидетельство – использование сети Интернет для приобретения или продажи товаров и услуг, денежные переводы, различного рода оплаты, получение государственных и муниципальных услуг.

Цифровая экономика представляет собой такой тип хозяйственной деятельности, который, оказывая существенное влияние на темпы роста ВВП Российской Федерации, прямо связан с активным развитием цифровых информационно-коммуникационных технологий, сервисов по предоставлению различных онлайн-услуг, электронных платежей, интернет площадки для торговли, краудфандинга. Этот тип экономики предполагает использование данных в цифровой форме, которые являются ключевым фактором производства во всех социально-экономических сферах, а также наукоемких технологий (нейротехнологии и искусственный интеллект; квантовые технологии; системы распределенного реестра; новые производственные технологии; компоненты робототехники и сенсорика; промышленный Интернет; технологии беспроводной связи; технологии виртуальной и дополненной реальностей), которые позволяют ускорять процесс производства, обрабатывать большой объем информации за короткий промежуток времени.

Проводя заседание Совета по стратегическому развитию, В. В. Путин, отметил, что цифровая экономика – это не отдельная отрасль, по сути это уклад жизни, новая основа для развития системы государственного управления, экономики, национальной безопасности и т. д. [4].

Международные принципы по информатизации общества и подходы к его созданию определены Окинавской хартией глобального информационного общества 2000 г., Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии» 2003 г., Планом действий Тунисского обязательства 2005 г. В целях получения максимума выгоды экономической и социальной для информационного общества рекомендуют следующие принципы и подходы. Во-первых, это поддержка в развитии конкуренции и открытия рынков для информационной технологии и телекоммуникационной продукции и услуг, включая недопущение ущемления и основанного на затратах подключения к основным телекоммуникациям. Во-вторых, это защита прав интеллектуальной собственности на информационные технологии, развитие конкуренции на рынке «высоких» технологий и широкое внедрение новых технологий. В-третьих, обязательное использование лицензионной продукции государственными органами. В-четвертых, это освобождение электронных переводов от таможенных пошлин. В-пятых, упорядоченные подходы к налогообложению электронной торговли, основанные на обычных принципах, включая недискриминацию, равноправие, упрощенность и прочие ключевые элементы, согласованные в контексте работы Организации экономического сотрудничества и развития (ОЭСР). В-шестых, рост доверия потребителя к электронным рынкам в соответствии с руководящими принципами ОЭСР, в том числе с помощью действенных саморегулирующих инициатив, таких как кодексы поведения, маркировка, иные программы подтверждения надежности, и исследование вариантов исключения сложностей, которые испытывают потребители в ходе трансграничных споров, включая применение альтернативных механизмов разрешения споров. В-седьмых, развитие и высокоэффективное применение электронной идентификации, электрон-

ной подписи, криптографии и других средств обеспечения надежности и достоверности операций. Наконец, работа по созданию надежного и свободного от преступности интернет-пространства, как указано в Руководящих принципах по безопасности информационных систем ОЭСР в борьбе с преступностью в компьютерной сфере [5].

Начиная с 2009 г. Международным союзом электросвязи ежегодно публикуется отчет The Measuring the Information Society Report [6] (англ. – Отчет об измерении информационного общества). В отчете представлен рейтинг стран, который основывается на индексе развития информационных технологий.

Россия в этом рейтинге стран по индексу развития информационно-коммуникационных технологий (ИКТ) в 2012 г. заняла 41-е место, 2016 г. – 43-е, 2017 г. – 45-е [7]. Указом Президента Российской Федерации от 9 мая 2017 г. № 203 место в рейтинге стран по индексу развития информационно-коммуникационных технологий входит в Стратегию развития информационного общества в Российской Федерации на 2017–2030 годы и Государственную программу Российской Федерации «Информационное общество», утвержденную постановлением Правительства РФ от от 15 апреля 2014 г. № 313 [8].

В этой связи следует согласиться с М. А. Ефремовой, по мнению которой социально-экономический фактор обусловленности уголовно-правовой охраны информационной безопасности, куда входят уголовно-правовые нормы об ответственности за мошенничество в сфере компьютерной информации, связан с развитием в нашей стране нового типа общества, в котором во главе угла стоят информация и информационные технологии [9, с. 103]. При этом государство, следуя приоритетному сценарию развития информационного общества в России, должно обеспечивать благоприятные условия для применения, поддержки и развития информационных и коммуникационных технологий. Одна из немаловажных задач в этой связи заключается в совершенствовании законодательства Российской Федерации и приведении его в соответствие с новыми экономическими и информационно-технологическими условиями. В пункте 31 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, особо подчеркивается необходимость совершенствования нормативно-правового регулирования в сфере обеспечения безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий.

Данное обстоятельство в полной мере относится и к уголовному законодательству в сфере экономики. Очевидно, что становление информационного общества и цифровой экономики требует переосмысления парадигмы уголовно-правовой охраны традиционных отношений собственности [2, с. 52]. Как известно, мошенничество в сфере компьютерной информации – новый вид имущественного преступления в сфере компьютерной информации, который имеет ряд особенностей, отличающих его от традиционного мошенничества.

Во-первых, это многообъектный характер мошенничества в сфере компьютерной информации, где непосредственным объектом являются конкретные имущественные отношения, а в роли дополнительного обязательного объекта выступает общественная безопасность.

Во-вторых, касаясь способов традиционного мошенничества и иных имущественных преступлений («обман», «злоупотребление доверием», «тайность», «открытость»), подчеркнем, что при совершении мошенничества в сфере компьютерной информации данные методы «оттесняются» способами, основанными на современных информационных технологиях передачи, получения, обработки электронных данных, сообщений с помощью ЭВМ, системы ЭВМ или их сети. Эти криминальные приемы могут быть, с одной стороны, специальными разновидностями обмана и злоупотребления доверием, с другой – смежными с обманом и злоупотреблением доверием способами преступного посягательства либо даже не имеющими ничего общего с ними. В самом деле, неправомерные уловки корыстного характера с использованием ЭВМ, системы ЭВМ или их сети можно признать как преступное деяние даже при отсутствии их обязательных признаков обмана или злоупотребления доверием. Например, это вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей путем целенаправленного воздействия программных средств на серверы, средства вычислительной техники (компьютеры, смартфоны и пр.) или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу неправомерно завладеть чужим имуществом или приобрести право на него.

В статье 159^6 УК РФ, предусматривающей ответственность за мошенничество в сфере компьютерной информации, способами совершения преступления являются: ввод, удаление, блокирование, модификация компьютерной информации, иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Как представляется, по мере развития информационного общества и цифровых технологий состав преступления, предусмотренный в ст. 159^6 УК РФ и относящийся к числу специальных видов мошенничества, будет трансформироваться в самостоятельный вид имущественного преступления или отдельной группы преступлений, совершаемых во взаимосвязанных сферах имущественных и информационно-технологических отношений.

В этой связи одной из задач законодателя является уточнение социально-правовой природы рассматриваемого деликта и определение месторасположения нормативных положений об уголовной ответственности за компьютерное мошенничество с учетом его многообъектного характера.

Другая проблема – нормативное описание «компьютерного мошенничества» в уголовном законе. Полагаю, что это преступное посягательство нельзя сводить исключительно к хищению чужого имущества и даже к неправомерному приобретению права на чужое имущество. В научных работах начала XXI века такого рода деликты предлагалось определять как «получение выгоды путем использования ЭВМ». Так, по мнению А. Г. Безверхова, «получение выгоды путем использования ЭВМ» представляет собой незаконное безвозмездное получение имущественной выгоды в значительном размере путем использования ЭВМ, системы ЭВМ или их сети, основной состав которого следует отнести к преступлению небольшой тяжести. То же деяние, совершенное группой лиц по предварительному сговору или лицом с использованием своего служебного положения, является преступлением средней тяжести. То же деяние, совершенное организованной группой либо в крупном размере следует признавать тяжким преступлением. Наконец, то же деяние, совершенное в особо крупном размере, – особо тяжкое преступление [10, с. 357]

В. В. Хилюта считает, что к компьютерным преступлениям должны относиться только противозаконные действия в сфере автоматизированной обработки информации. В этой связи этот ученый-юрист полагает, что УК должен содержать норму, которая бы предусматривала ответственность за «хищение имущества путем модификации результатов автоматизированной обработки данных компьютерной системы». По мнению В. В. Хилюты, предлагаемой нормой охватывались бы противоправные деяния, совершаемые с использованием средств компьютерной техники, сотовой связи, сети Интернет и т. п. [11, с. 65–66]

В § 263а УК Федеративной Республики Германии компьютерное мошенничество определяется как противоправное получение имущественной выгоды и нанесение вреда имуществу другого лица воздействием на результат обработки данных ЭВМ, составлением неправильных программ, использованием неправильных или неполных данных, неправомочным применением данных или влиянием на такой процесс каким-либо иным неправомочном воздействием [12]. При этом под имуществом в германской уголовно-правовой доктрине понимается вся совокупность экономических благ потерпевшего, включая вещи, права требования и иные объекты гражданских прав.

В заключение еще раз подчеркнем, что механизм уголовно-правового регулирования информационных имущественных отношений нуждается в конструировании новых составов преступлений, смежных с нормами о традиционном мошенничестве, совершаемом с использованием обмана или злоупотребления доверием в отношении исключительно чужих вещей как объектов физического мира или права на имущество. На это же обстоятельство указывают социально-экономические и информационно-технологические основания криминализации общественно опасного имущественного поведения в сфере компьютерной информации. При этом, как представляется, речь должна идти не о специальных составах мошенничества («компьютерном», «с использованием электронных средств платежа» или иных аналогичных традиционному мошенничеству конструкциях), а о самостоятельном виде двухобъектного имущественного преступления с вышеописанными особенностями объективной стороны.

Библиографический список

1. Коржанский Н. И. Объект и предмет уголовно-правовой охраны. М.: Изд-во Акад. МВД СССР, 1980. 248 с. URL: https://ru.b-ok.cc/book/3040689/9731db.

2. URL: http://crimestat.ru/51 (дата обращения: 04.09.2019).

3. Ефремова М. А. Уголовно-правовая охрана информационной безопасности: дис. ... канд. юрид. наук. М., 2017. 426 с. URL: http://www.agprf.org/userfiles/ufiles/dis_sovet/diss/2018/Efremova/%D0%94%D0%B8%D1%81%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D0%B8%D1%8F%20%D0%95%D1%84%D1%80%D0%B5%D0%BC%D0%BE%D0%B2%D0%BE%D0%B9%20%D0%9C.%D0%90.pdf.

4. URL: http://www.kremlin.ru/events/president/news/54983 (дата обращения: 05.09.2019).

5. URL: http://www.kremlin.ru/supplement/3170 (дата обращения: 05.09.2019).

6. URL: http://www.itu.int/en/publications/ITU-D/Pages/default.aspx (дата обращения: 05.09.2019).

7. URL: http://www.cnews.ru/news/top/2018-04 (дата обращения: 05.09.2019).

8. Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)» // Собрание законодательства Российской Федерации. 2014. № 18 (ч. II). Ст. 2159. URL: http://www.consultant.ru/document/cons_doc_LAW_162184.

9. Ефремова М. А. Уголовно-правовая охрана информационной безопасности. М.: Изд-во «Юрлитинформ», 2018. 312 с. URL: https://elibrary.ru/item.asp?id=30081476.

10. Безверхов А. Г. Имущественные преступления. Самара: Изд-во «Самарский университет», 2002. 429 с. URL: https://ru.b-ok.cc/book/3077228/6220f2.

11. Хилюта В. В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. 2013. № 5 (10). С. 55–65. URL: https://elibrary.ru/item.asp?id=20345709.

12. Уголовный кодекс Федеративной Республики Германии. СПб.: Изд-во «Юридический центр Пресс», 2003. 524 с. URL: https://constitutions.ru/?p=5854.

References

1. Korzhansky N. I. *Ob"ekt i predmet ugolovno-pravovoi okhrany* [Object and subject of criminal law protection]. M.: Izd-vo Akad. MVD SSSR, 1980, 248 p. Available at: https://ru.b-ok.cc/book/3040689/9731db [in Russian].

2. Available at: http://crimestat.ru/51 (accessed 04.09.2019) [in Russian].

3. Efremova M. A. *Ugolovno-pravovaya okhrana informatsionnoi bezopasnosti: dis. ... kand. yurid. nauk* [Criminal-legal protection of information security: Candidate's of Legal Sciences thesis]. M., 2017, 426 p. Available at: http://www.agprf.org/userfiles/ufiles/dis_sovet/diss/2018/Efremova/%D0%94%D0%B8%D1%81%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D0%B8%D1%8F%20%D0%95%D1%84%D1%80%D0%B5%D0%BC%D0%BE%D0%B2%D0%BE%D0%B9%20%D0%9C.%D0%90..pdf [in Russian].

4. Available at: http://www.kremlin.ru/events/president/news/54983 (accessed 05.09.2019) [in Russian].

5. Available at: http://www.kremlin.ru/supplement/3170 (accessed 05.09.2019) [in Russian].

6. Available at: http://www.itu.int/en/publications/ITU-D/Pages/default.aspx (accessed 05.09.2019) [in Russian].

7. Available at: http://www.cnews.ru/news/top/2018-04 (accessed 05.09.2019) [in Russian].

8. *Postanovlenie Pravitel'stva RF ot 15.04.2014 № 313 «Ob utverzhdenii gosudarstvennoi programmy Rossiiskoi Federatsii «Informatsionnoe obshchestvo (2011–2020 gody)»* [Decree of the Government of the Russian Federation as of 15.04.2014 № 313 «On approval of the state program of the Russian Federation «Information Society (2011–2020)»]. *Sobranie zakonodatel'stva Rossiiskoi Federatsii* [Collected legislation of the Russian Federation], 2014, no. 18 (part II), Article 2159. Available at: http://www.consultant.ru/document/cons_doc_LAW_162184 [in Russian].

9. Efremova M. A. *Ugolovno–pravovaya okhrana informatsionnoi bezopasnosti* [Criminal–legal protection of information security]. M.: Izd-vo «Yurlitinform», 2018, 312 p. Available at: https://elibrary.ru/item.asp?id=30081476 [in Russian].

10. Bezverkhov A. G. *Imushchestvennye prestupleniya* [Property crimes]. Samara: Izd-vo «Samarskii universitet», 2002, 429 p. Available at: https://ru.b-ok.cc/book/3077228/6220f2 [in Russian].

11. Khiluta V. V. *Khishchenie s ispol'zovaniem komp'yuternoi tekhniki ili komp'yuternoe moshennichestvo?* [A Theft Using Computer Equipment or Computer Fraud?] *Biblioteka kriminalista* [Forensic Library], 2013, no. 5 (10), pp. 55–65. Available at: https://elibrary.ru/item.asp?id=20345709 [in Russian].

12. *Ugolovnyi kodeks Federativnoi Respubliki Germanii* [Criminal Code of the Federal Republic of Germany]. SPb.: Izd-vo «Yuridicheskii tsentr Press», 2003, 524 p. Available at: https://constitutions.ru/?p=5854 [in Russian].