

УДК 343

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ УГОЛОВНОГО ПРАВА РОССИИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Семиёхин Владислав Алексеевич

студент группы «ЮМУ-101»

Академии права и национальной безопасности ЧОУ ВО ЮУ (ИУБиП)

Аннотация: Целью данной статьи можно назвать поиск решения проблем использования уголовного права России в условиях развития цифровой экономики. Рассматриваются случаи подобных преступлений и попытка их квалификации. Предполагаются причины возникновения таких проблем. Автор предлагает решение проблем использования уголовного права для цифровой экономики и проблем квалификаций преступлений в данной сфере.

Ключевые слова: уголовное право в экономике, квалификация экономических преступлений, преступления в цифровой экономике.

PROBLEMS OF USING THE CRIMINAL LAW OF RUSSIA IN THE DEVELOPMENT OF THE DIGITAL ECONOMY

Semiyokhin Vladislav Alekseevich

Student group "UMU-101"

Academy of Law and National Security, Southern University (IUBiP)

Abstract: The purpose of this article can be called the search for a solution to the problems of using the criminal law of Russia in the development of the digital economy. Cases of such crimes and an attempt to qualify them are considered. The causes of such problems are suggested. The author offers a solution to the problems of using criminal law for the digital economy and the problems of qualifications of crimes in this area.

Keywords: criminal law in the economy, qualification of economic crimes, crimes in the digital economy.

В последние годы, в России стремительно набирает обороты диджитализация и цифровизация экономики. В пример можно привести много чего, например, как активно начали распространяться электронные деньги, будь то электронные кошельки или банковские карты, будь то дебетовые или кредитные, в больших городах, почти во всех магазинах, в транспорте уже стоят терминалы для оплаты картой, уменьшается

количество наличных денег, всё это является следствием прогресса, внедрения новых технологий в нашу жизнь и глобализации.

Цифровая экономика – это, по своей сути, совокупность отношений между людьми, субъектом в которых выступает данные в цифровой форме. Так же, как и любые отношения, цифровая экономика формирует вокруг себя определённое информационное пространство, при учёте тех потребностей, которые нужны обществу и гражданам, например, потребность в достоверной информации, потребность в использовании информационно – телекоммуникационных технологий, так же потребность в создании новой, цифровой и технологической основы для социальной и экономической сферы.

Диджитализация экономики позволяет хозяйствующим субъектам оптимизировать всё, от производства, до контроля над трудовой дисциплиной.

И всё же, принимая в учёт все плюсы данного явления, нельзя не отметить, что у него так же много минусов в плане безопасности. Поскольку цифровая экономика развивается очень быстро, люди не успевают подумать и о защите данных. В пример можно привести слив данных 60 миллионов банковских карт и их собственников в открытый доступ, в сеть Интернет с серверов Сбербанка. Об утечке 3 ноября 2019 года сообщило издание «Коммерсантъ». По данным издания, они обнаружили на одном из интернет-форумов данные на 60 миллионов банковских карт, из них 18 миллионов до сих пор действующие. [1]

Современные высокие технологии, выступая и объектом, средством преступной деятельности и орудием совершения преступления, порождают и развивают новый вид преступной деятельности – «преступления в сфере высоких технологий».[8]

Так же, компания по кибербезопасности RiskIQ, опубликовало данные своего исследования, в котором говорится, что каждую минуту киберпреступники наносят ущерб в 1 138 888 долларов США по всему миру.

По сравнению с предыдущим годом эта цифра выросла на 280 000 долларов США. По прогнозам этой же компании, ущерб с каждым годом будет увеличиваться, поскольку будет увеличиваться и ландшафт для преступлений, увеличивается аудитория Интернета.

Кроме того, вред от таких преступлений заключается и в наносимом ущербе авторитету органов государственной власти, в компетенцию которых входит регулирование экономической деятельности, в дестабилизации экономики страны и социального положения граждан: увеличение безработицы, развитие теневого бизнеса и оказывает отрицательное влияние на процессы социально-экономического преобразования России в целом.[9]

На Тринадцатом конгрессе ООН по предупреждению преступности и уголовному правосудию, состоявшемуся в 2015 г.1, преимущественно посвящённом противодействию транснациональному криминалитету, в частности была подчеркнута необходимость обеспечения использования экономических, социальных и технологических благ в качестве положительной силы, укрепляющей усилия сотрудничающих стран, направленные на предупреждение новых и возникающих форм преступности и борьбу с ними. Для этого предлагается разрабатывать и осуществлять всеобъемлющие меры реагирования в области предупреждения преступности и уголовного правосудия, в том числе принимать необходимые законодательные и административные меры для эффективного предупреждения новых атак. [6]

Нужны принципиально новые решения, формирование новых принципов и методов права, которое будет эффективно регулировать цифровые процессы и формировать новое законодательство, которое должно быть основой для цифровой экономики, и его можно условно назвать сетевым или цифровым правом. [7]

Оценивая опасности, а также угрозы стремительной цифровизации экономики, наш законодатель предпринимает некоторые решения для противодействия киберпреступности, но, к сожалению, это происходит

точечно и с опозданием, когда уже то или иное преступление было совершено. А поскольку в правительстве большое количество людей попросту стары, средний возраст депутатов в нынешней Государственной Думе составляет практически 50 лет [2], о прогнозировании в направлении киберпреступности не может идти и речи, нельзя предвидеть то, чего не понимаешь.

Так, 23 апреля 2018 года в ч. 3 ст. 158 УК РФ был дополнен новый способ квалификации преступления «совершение кражи», а именно «совершение кражи с банковского счёта, а равно в отношении электронных денежных средств» [3].

По мнению отдельных специалистов, данное решение учитывает необходимость дополнительной защиты финансовых интересов граждан, кредитных организаций и государства в целом, а также предоставляет правоприменителям возможность задействовать весь спектр оперативно-розыскных мероприятий [4, с. 49].

По-моему же мнению, проблема тут состоит в том, что правотворец механически приравнивает кражу в особо крупном размере и кражу денег с банковского счёта. Это априори неверно, поскольку преступник может украсть небольшую сумму денег с банковской карты или же электронного счёта, а судить его будут, будто он украл значительную сумму денежных средств и считаю, что данная поправка в закон была неверной и её нужно отменить.

К сожалению, правотворец никак не затронул статью 163 УК РФ о вымогательстве. Данная статья не позволяет должным образом оценить требование передачи денежных средств или иного цифрового имущества, будь то аккаунты в социальных сетях, аккаунты в онлайн играх и интернет магазинах, связанных с блокировкой или дальнейшим распространением информации, или же просто повреждением этой информации.

А такие преступления всё больше распространяются. Так, в пример можно привести кибератаки на информационные ресурсы некоторых стран, в

этом списке также находится и Российская Федерация, компьютерного вируса «WannaCry». По подсчётам от этого вируса пострадало более 500 000 компьютеров, которые принадлежали частным лицам, различным организациям, а также правительственным учреждениям. [5]

В правоприменительной практике такие преступления чаще всего квалифицируют по статьям 272 и 273 УК РФ, что, на мой взгляд, не полностью раскрывает такие преступления, поскольку они затрагивают только часть деяния, а именно неправомерное владение чужим компьютером, а та часть с вымогательством остаётся в неведении.

Я думаю, нужно, чтобы правотворец внёс определённые законопроекты, которые бы могли изменить ситуацию, поскольку цифровая экономика всё сильнее развивается, и остановить это развитие невозможно. Следует переработать больше количество законов под современные нужды, а не просто «затыкать дырку в бочке только тогда, когда она будет пробита», это нужно делать комплексно. Задача правотворца предвидеть то место, где может появиться «дыра» и своевременно её закрыть.

В заключение хочется сказать, что цифровизация экономики и интернет- имущества будет и дальше развиваться с огромной скоростью, и проблема отчуждения законотворческого органа нашей страны будет только обостряться. Если так и продолжится, то под угрозой может оказаться вся система уголовного права, поскольку в интернете уже большое скопление капитала и он будет только увеличиваться, а мошенников всё больше будет привлекать этот «лакомый кусочек».

СПИСОК ЛИТЕРАТУРЫ

1. Фонтанка ру. «В Сеть попали данные 60 миллионов кредитных карт Сбербанка. В «сливе» подозревают сотрудников» [Электронный ресурс]. – URL: <https://m.fontanka.ru/2019/10/03/009/>.
2. Коммерсантъ «Возраст депутатов» [Электронный ресурс]. – URL: <https://www.kommersant.ru/doc/441448>.
3. Уголовный кодекс Российской Федерации [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/57b5c7b83fcd2cf40cabe2042f2d8f04ed6875ad/.

4. Иванов И.С., Рязанцева С.В. Современный подход к определению мер уголовной ответственности за хищение денежных средств, находящихся на банковском счете, и электронных денежных средств // Российский следователь. – 2018. – № 8.
5. Коммерсантъ «Владимир Путин назвал спецслужбы США источником WannaCry» [Электронный ресурс]. – URL: <http://www.kommersant.ru/doc/3297338>.
6. Иванцов С.В., Спасенников Б.А., Борисов С.В. Проблемы предупреждения преступлений в сфере цифровой экономики [Электронный ресурс] // Актуальные вопросы образования и науки. – 2017. – №2 (60). – С. 20-24. – URL: https://elibrary.ru/download/elibrary_30146334_61775491.pdf.
7. Голоскоков Л.В. Предпосылки построения цифровой экономики и минимизация экономических преступлений [Электронный ресурс] // Синергия. – 2018. – №2. – С. 67-73. – URL: https://elibrary.ru/download/elibrary_35629122_94409005.pdf.
8. Фоменко А. И. О некоторых мерах предупреждения преступлений в сфере компьютерной информации [Электронный ресурс] // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2018. – №5 (96). – 95-97. – URL: https://elibrary.ru/download/elibrary_32856597_63178994.pdf.
9. Фоменко А. И. К вопросу об уголовно правовой охране сферы высоких технологий как необходимого условия стабильного регионального развития [Электронный ресурс] // Интеллектуальные ресурсы – региональному развитию. – 2015. – №5. – С. 217-222. – URL: https://elibrary.ru/download/elibrary_25516464_39043404.pdf.