УДК 343

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ КВАЛИФИКАЦИИ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Кибальник А.Г.
д.ю.н., профессор кафедры «Уголовно-правовое дисциплины»
ЧОУ ВО ЮУ (ИУБиП)
Коханова В.С.
к.э.н., доцент, Руководитель Академии экономики и управления
ЧОУ ВО ЮУ (ИУБиП)

Аннотация: Набирающая обороты цифровая экономика несет в себе не только положительные факторы для развития страны, но также и негативные стороны. В основном, негативные стороны раскрываются в различных правонарушениях, что вызвано, в том числе, отсутствием правовой базы, четко обозначающей ключевые понятия цифровой экономики, права и обязанности сторон.
Ключевые слова: цифровая экономика, экономические преступления, ИКТ, киберугрозы, уклонение от уплаты налогов, финансовые институты.

CRIMINAL LAW ASPECTS OF THE QUALIFICATION OF ECONOMIC CRIMES IN THE DIGITAL ECONOMY

Kibalnik A.G.
Doctor of Law, Professor of Department of Criminal Law Disciplines
PEI HE SU (IMBL)
Kokhanova V.S.
Cand. of econ.sc., Associate Professor
Head of the Academy of Economics and Management
PEI HE SU (IMBL)

Abstract: The growing digital economy carries not only positive factors for the development of the country, but also negative aspects. Basically, the negative sides are revealed in various offenses, which is caused, inter alia, by the lack of a legal framework that clearly indicates the key concepts of the digital economy, the rights and obligations of the parties.
Keywords: digital economy, economic crime, ICT, cyberthreats, tax evasion, financial institutions.

Традиционно финансовый сектор воспринимается как некий зарегулированный и весьма консервативный элемент экономики, а модель доходности этого элемента неизменна долгое время.

Тем не менее, новые и передовые технологии в течение следующих десяти лет окажут сильное влияние на финансовый сектор. В последние годы резко выросла популярность использования передовых информационных технологий. По индексу развития информационно-коммуникационных технологий Россия в 2017 г. занимает 45 место в мире, в то время как лидирующие места занимают Исландия, Южная Корея, Швейцария, а последнее республика Эритрея [1].

В то же время, Россия по состоянию 2017 года занимает 7 место в мире по количеству пользователей сети интернет, насчитывается более 109,5 миллионов пользователей, что соответствует 71,7% населения страны. Развивающиеся технологии вынуждают финансовый сектор следовать за трендом и задумываться о внедрении инноваций.

Более 40% финансовых органов и посредников, включая поставщиков услуг по переводу денег, а также фондовых бирж, ежегодно подвергаются большим потерям, связанным с экономическими преступлениями. Причиной является использование централизованных систем баз данных для операций и управления капиталом. Централизованная система баз данных уязвима и очень подвержена кибератакам. Как только хакер получает доступ к такой системе, забрать деньги для него не составит труда. Это приводит к необходимости разработки более безопасных систем, способных справиться с подобными атаками.

По информации Банка России, только в 2015 году в общей сложности были совершены покушения на хищение 4 млрд рублей в электронном виде, и 61% попыток увенчался успехом. По данным Генпрокуратуры РФ, в период с января по август 2018 года правоохранительными органами РФ было зарегистрировано 107 980 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в

сфере компьютерной информации с ущербом в размере почти 400 млрд рублей, что на 43,6% больше аналогичного показателя годом ранее, а расследовано около 30 тыс. преступлений.

По предварительной оценке специалистов Сбербанка, ущерб российской экономике от киберугроз за 2018 год составил 1 трлн рублей, и сумма эта – неокончательная, так как не все финансовые организации готовы признать факт кибератаки и раскрыть реальную сумму ущерба [3].

Само понятие «преступление в сфере экономики» включает в себя преступления против собственности, преступления в сфере экономической деятельности и преступления против интересов службы в коммерческих и иных организациях. Все это подробно трактуется и разъясняется УК РФ в главах 21-23.

Рассмотрим подробнее динамику числа осужденных за преступления в сфере экономики (таблица 1).

Таблица 1 – Данные о числе осужденных за преступления в сфере экономики

Виды преступлений	Статьи УК РФ	Всего осуждено, человек		
		2017 год	2018 год	1 полугодие 2019 года
Всего по гл. 21 УК РФ	158-168	263 774	249 231	111 274
Всего по гл. 22 УК РФ	169- 200.5	6 375	7 717	3 831
Всего по гл. 23 УК РФ	201- 204.2	498	368	175
Итого		270 647	257 316	115 280

Динамика, приведенная в таблице 1 свидетельствует о том, что наблюдается рост числа осужденных за преступления в сфере экономической деятельности.

Рассмотрим динамику именно экономических преступлений, сущность которых раскрывается УК РФ в главе 22.

Таблица 2 – Динамика состава преступлений в сфере экономической деятельности, 2018-2019 годы

Виды преступлений	Статьи УК РФ	2017 год	2018 год	Динамика	2019 год

Всего по гл. 22 УК РФ	169- 200.3	6 375	7 717	1 342	3 831
Незаконные предпринимательство и банковская деятельность, лжепредпринимательство	171-173.2	3 096	4 570	1 474	2 490
Легализация денежных средств или иного имущества, приобретенных другими лицами	174	5	15	10	2
Легализация денежных средств или иного имущества, приобретенных лицом	174.1	28	18	-10	10
Приобретение или сбыт имущества, заведомо добытого преступным путем	175 ч. 1	1 245	1 153	-92	414
Приобретение или сбыт имущества, заведомо добытого преступным путем при отягчающих обстоятельствах	175 ч. ч. 2-3	76	82	6	23
Изготовление или сбыт поддельных денег, ценных бумаг, иных платежных документов	186-187	576	537	-39	265
Иные незаконные действия с валютными ценностями	191-193.1	95	0	-95	0
Контрабанда	188 ч. 1	0	1	1	1
Контрабанда при отягчающих обстоятельствах	188 ч. ч. 2-4	2	54	52	17
Иные нарушения таможенного законодательства	189, 190, 194	48	90	42	52
Уклонение от уплаты налогов	198-199.2	547	566	19	278
Контрабанда наличных денежных средств и (или) денежных инструментов	200.1	32	39	7	20

На рисунке 1 приведем динамику структуры преступлений в сфере экономической деятельности, 2018-2019 годы. Как видно, наибольшую долю занимают преступления, определяемые как «незаконные предпринимательство и банковская деятельность, лжепредпринимательство» в соответствии со статьями 171-173.2 УК РФ.


2017 год
Незаконные предпринимательство и банковская деятельность, лжепредпринимательство; 3 096
Уклонение от уплаты налогов; 547
Изготовление или сбыт поддельных денег, ценных бумаг, иных платежных документов; 576
Приобретение или сбыт имущества, заведомо добытого преступным путем; 1 245

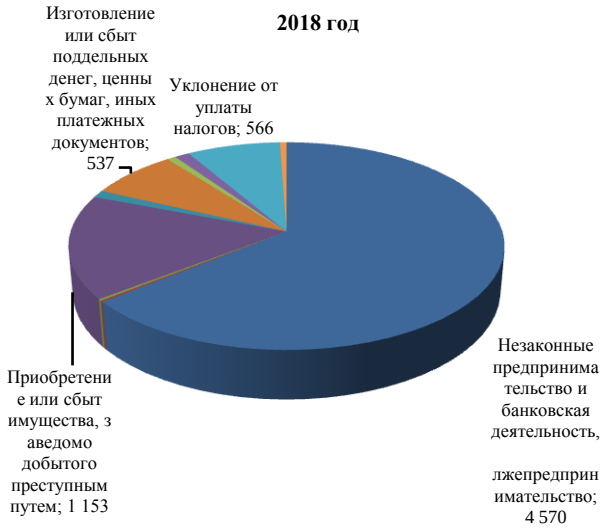
2018 год
Изготовление или сбыт поддельных денег, ценных бумаг, иных платежных документов; 537
Уклонение от уплаты налогов; 566
Приобретение или сбыт имущества, заведомо добытого преступным путем; 1 153
Незаконные предпринимательство и банковская деятельность, лжепредпринимательство; 4 570

Рисунок 1 – Динамика структуры преступлений в сфере экономической деятельности, 2018-2019 годы

Как мы видим, уголовный кодекс не вводит особых категорий для определения новых видов преступлений, появившихся в связи с развитием цифровых технологий. Категория «киберпреступник» так же не имеет нормативно-правовой основы. Однако существовать эти понятия не перестают. Более того, отсутствие законодательно закрепленной дефиниции не делает неопределимым само правонарушение.

На наш взгляд, под киберпреступлением стоит понимать преступление, совершаемое исключительно в сети интернет либо с применением удаленного доступа к данным.

В ряде работ [4, 5] отмечается, что в процессе слияния IT и операционных технологий приложения и платформы предприятий попадают под риски манипуляций и уязвимостей. Киберпреступники используют так же блокчейн и машинное обучение для маскировки своей деятельности от традиционных методов защиты информации.

Помимо перечисления самих видов преступлений, совершаемых киберпреступниками, в литературе также можно найти работы, посвященные вопросам повышения безопасности финансовых сделок [6].

В силу этого финансовый сектор в последние несколько лет обсуждает возможности и целесообразность применения технологии блокчейн [2]. Одним из полей применения данной технологии выступает борьба с киберпреступностью, ведь привлечение денег в любой ситуации приводит к увеличению шансов на мошеннические действия. А для всего сектора безопасность имеет первостепенное значение.

Введение блокчейн, безопасной, не подверженной коррупции технологии работающей на системе распределенных баз данных может стать правильным решением. Ведь каждая транзакция хранится в виде блока с криптографическим механизмом, который чрезвычайно сложно взломать. Более того, все блоки связаны друг с другом и благодаря этому механизму

связывания, если один блок нарушен, все остальные блоки в цепочке блоков немедленно отражают данное изменение. Это, в свою очередь, помогает отследить нарушение и не дает хакеру времени внести изменения в общую систему. Имея защищенную систему блокчейн, можно устранить киберпреступления и атаки на банковский и финансовый сектора.

Таким образом, мы можем сделать вывод, что киберпреступления совершаются с завидной постоянностью, более того порядка 70% атак совершается в целях получения финансовой выгоды, в то же время, как и любой другой вид преступлений, киберпреступления совершенствуются и выходят на новый уровень, несмотря на то, что понятия «кибепреступник» или «киберпреступление» в УК РФ не существует.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рейтинг стран мира по уровню развития информационно-коммуникационных технологий. – Режим доступа: https://gtmarket.ru/ratings/ict-development-index/ict-development-index-info.
2. Коханова В.С., Бохон К.С.Влияние технологии блокчейн на финансовый сектор: современное состояние и сферы применения // Научный вестник южного института менеджмента. – 2019. – № 4(28). – С.84-90.
3. Клоков А. Не рискует тот, кто ничего не делает // Банковское обозрение. – 2019. – № 2. – С. 84-85.
4. Ференец В. Все совершенно иначе // Банковское обозрение. – 2018. – № 1. – С. 76 - 80.
5. Пинчук А. Использование методов Deep Learning в задаче выявления мошенничества // Банковское обозрение. Приложение "BEST PRACTICE". – 2018. – № 2. – С. 30-35.
6. Кондрашин М. Security by design как основа // Банковское обозрение. – 2018. – № 11. – С. 69.