УДК 004.056

Ерошова Екатерина Алексеевна
студентка
Институт магистратуры и заочного обучения
Саратовская государственная юридическая академия
Россия, Саратов
e-mail: panther02102000@mail.ru

Научный руководитель: Варламова Елена Владимировна
кандидат педагогических наук, доцент
Саратовская государственная юридическая академия
Россия, Саратов

МЕЖДУНАРОДНАЯ ЦИФРОВАЯ БЕЗОПАСНОСТЬ, КАК УСЛОВИЕ УСТОЙЧИВОГО РАЗВИТИЯ СОВРЕМЕННОГО ОБЩЕСТВА

Аннотация: *В статье автор рассматривает международную цифровую безопасность экономики. Также рассматриваются различные способы совершения киберпреступлений. Рассматриваются причины развития угроз для цифровой экономики, анализируются мнения разных учёных. Производится анализ зарубежного опыта. Даются некоторые советы для защиты цифровой экономики.*

Ключевые слова: цифровая безопасность, киберпреступления, реформация, киберугрозы.

Yeroshova Ekaterina Alekseevna
student
Institute of Master's Degree and Distance Learning
Saratov State Law Academy
Russia, Saratov

Scientific adviser: Varlamova Elena Vladimirovna,
candidate of pedagogical sciences, associate professor
Saratov State Law Academy
Russia, Saratov

INTERNATIONAL DIGITAL SECURITY AS A CONDITION FOR THE SUSTAINABLE DEVELOPMENT OF MODERN SOCIETY

Abstract: *In the article, the author examines the international digital security of the economy. Various ways of committing cybercrimes are also being considered. The reasons for the development of threats to the digital economy are considered, and the opinions of various scientists are analyzed. The analysis of foreign experience is carried out. Some tips are given to protect the digital economy.*

Key words: digital security, cybercrimes, reformation, cyber threats.

Бурное развитие цифровой экономики и ее проникновение во все общественные отношения сопряженно с изменением классических инструментов регулирования и трансформации общества несёт с собой не только плюсы, но и новые угрозы для общества [1]. Поэтому на первый план выходит такая вещь как цифровая безопасность она же кибербезопасности все участников цифровой экосистемы.

Про важность кибербезопасности еще в 2018 году на международном конгрессе по кибербезопасности говорил Владимир Владимирович Путин, на данном конгрессе он сказал следующее «Мы убеждены, что обеспечение кибербезопасности — это государственная задача». Важно понимать, что слова президента можно рассматривать, как отправной момент в реализации программы кибербезопасности, ведь от того, как расставятся акценты в данном вопросе и будет зависть результат решения задачи по кибербезопасности, а вместе с этим и успешность работы цифровой экосистемы.

Отталкиваясь от слов Путина В.В., можно сделать вывод о том, что обеспечение кибербезопасности является государственной задачей и для ее решения необходимо вовлечения всех сил, ресурсов и средств. Однако важно понимать, что решение этой задачи зависит не только от правового регулирования данной сферы, но и от технических возможностей государства. Необходимо обсуждать вопросы о кибербезопасности, как с правоведами, так и с приглашенными специалистами в IT-сфере. Специалисты могут рассказать при помощи, каких технических средств возможно обеспечить кибербезопасности. На данный момент защита от киберугроз носит сугубо оборонительный характер, так как никто не пытается решить данную проблему комплексно, а только предлагают локальные способы борьбы с данными угрозами путём установки нового оборудования, модернизации антивирусных программ, увеличения штата IT-специалистов, которые могут выстроить барьеры для кибератак. Однако надо давать отчёт, что такая борьба с киберугрозами

представляет собой лечение симптомов болезни, не саму болезнь, и она не сможет обеспечить надёжную работу цифровой экосистемы и защитить ее от всех угроз. Быстрые темпы развития технологий будут только способствовать наращиванию масштабов проблемы кибербезопасности.

Эксперты уже выдвигают прогнозы о бурном распространение кибератак и с каждым годом их будет становится все больше и больше [2]. Киберпреступления тоже выходят на новый уровень за счёт улучшения вредоносного программного обеспечения и противостать таким преступлением с каждым годом становится сложение.

Наглядно показывает рост преступности в своей научной статье «Международная цифровая безопасность: миф или реальность?» кандидат юридических наук Крайнова Надежда Александровна, в данной работе она провела статистический анализ преступности в киберпространстве. Исходя из этого анализа следует, то, что в период с января по август 2020 г. в РФ было зарегистрировано 272 737 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий это на 94,6% больше, чем за данный период в 2019 году. Среди выявленных преступлений большинство с использованием и применением сети Интернет (155 745, увеличение на 86,9 %) и средств мобильной связи (115 996, увеличение на 103,7 %). Хоть и почти все преступления были раскрыты органами внутренних дел и Федеральной службой безопасности. Анализ статистики даёт неутешительные прогнозы роста преступности в 1Т-сфере. А с условием, что за последние пять лет процент раскрываемости данных преступлений с каждым годом становится меньше можно сделать вывод о недостаточной подготовленности правоохранительных органов, как с технической стороны оснащённости, так и с профессиональной подготовкой кадров, готовых работать в сфере кберпреступлений. Следует отметить, что вина лежит не только на правоохранительных органах, которые не могут раскрывать все преступления в данной сфере, но и на законодательных органах, которые не могут внести определённость в данной сфере.

Предпосылкой для увеличения киберпреступлений, можно считать переход на полную цифровую деятельность крупных компаний [3]. Они стараются таким образом повысить свою эффективность с одной стороны, при этом с другой стороны становятся более уязвимыми для кибератак. Усугубляет ситуацию с преступностью в данной сфере, и активизация киберпреступников которые используют возможности машинного обучения искусственного интеллекта, тем самым создавая новые вредоносные программы так называемые чат-боты, которые помогают мошенникам совершать кибератаки. Новым способом кражи личных данных является криптография, ее особенность состоит в том, что жертва даже не догадывается о том, что ее учетную запись взломали и выкрали конфиденциальные данные. Получается то, что современный технологичный мир сам делает себя все более небезопасным, подвергая рискам и угрозам саморазрушения.

Решить проблему кибербезопасности, путём сдерживания киберпреступлений на социально терпимом уровне, возможно только путём международного взаимодействия по обеспечению четкого правого регулирования в цифровой сфере предусмотрев гибкие возможности защиты цифровой экосистемы от киберпреступлений. В таком случае государство выступает гарантом цифровой безопасности и ему отводится широкая роль в данном вопросе.

Важно понимать, что решения вопросов, связанных с цифровой безопасностью государства и международной цифровой безопасностью невозможно без привязки к вопросам права. Это связанно с тем, что изначально на первый план в вопросах цифровой безопасности выходит безопасность людей, социума, а она возможна только в рамках, которые закреплены законном. Поэтому все обсуждения цифровой безопасности, которые происходят без правовых специалистов изначально недопустимы.

Главной проблемой правового регулирования цифровой международной безопасности является, то что классическое материальное право, построенное на обозначение правонарушение и преступление, и вместе с ним процессуальное

право, регламентирующее правовые механизмы воздействия на правонарушителей в цифровой сфере работает в аналоговом режиме. Это связанно с тем, что она изначально было создано для регулирования общественных отношений типа человек-человек, так как когда право только зарождалось субъектами правоотношений выступали исключительно люди. Все нормы права и правовые институты, которые регулируют правоотношения в обществе на данный момент относятся к традиционным нормам, и обязаны существовать в реальном мире взаимодействия. В этом заключается главная проблема регулирования общественных отношений, возникающих в цифровой сфере, ведь они могут находится в нереальном, а виртуальном мире и в данном случае традиционные нормы могут давать сбой или не работать вовсе. В следствии чего становится более понятна позиция некоторых ученых, которые говорят о неготовности нашего законодателя и, главное, правоприменителя адекватно реагировать на происходящие в мире технологические перемены [4].

Учтя вышесказанное возникает один главный вопрос, на который необходимо ответить раньше, чем проводить масштабное реформирование уголовное законодательство в целях обеспечение цифровой безопасности и этот вопрос звучит сующим образом: нужна ли это реформация?

Для ответа на данный вопрос обратимся к изменениям, которые произошли в Гражданский кодекс РФ, в связи с реализацией Национальной программы «Цифровая экономика Российской Федерации». Данные изменения вступили в силу с октября 2019 г., и их уже ученые проанализировали и сделали вывод о их декларированном характере и необходимости внесения в них срочных дополнений. При этом эти новеллы законодатель принял со значительным опозданием опираясь на сложившиеся на практике отношения и даже это не помогло дать нужный результат. Главным же отличием гражданско-правового регулирования от уголовно-правового регулирования состоит в том, что в нем можно использовать принцип аналогии права, что в свою очередь даёт плацдарм для введения новел в ГК РФ с возможностью их постоянной доработки и изменения. В уголовно-правовом регулирование такая ситуация априори

нереализуема, так как принципы уголовного права запрещают применения аналогии права.

Важным шагом к цифровой безопасности является появления ФЗ № 259 от 31.07.2020 «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [5]. Данный ФЗ даёт ясность в вопросе правового регулирования криптовалюты, обозначая ее цифровой валютой и дающий возможность использовать ее как средство платежа, которое не является денежной единицей. При этом неоднозначность, данного ФЗ заключается в том, что Центральный банк РФ внес свои коррективы, через заявления о намерении изучить целесообразность выпуска цифрового рубля. Согласно заявлениям ЦБ РФ, цифровой рубль будет представлять собой код и храниться в специальном электронном кошельке. Основным мотивом введения цифрового рубля является сокращение издержек на проведение транзакций. Цифровой рубль даст новые возможности по использованию и развитию новых инструментов и финансовых услуг. С точки зрения безопасности предполагается. Что благодаря прозрачности расчётных операций с использованием цифрового рубля уменьшиться количество киберпреступлений. Цифровой рубль в теории должен стать цифровой валютой российского Центробанка и будет наделён всеми свойствами, которые необходимы для реализации денег и будет обращаться наряду с наличными и безналичными рублями и все эти три вида рубля будут, равноценными и эквивалентными друг другу. Из этого следует. Что цифровой рубль не является криптовалютой, так как его эмитентом выступает Центробанк.

Раз цифровой рубль, не является криптовалютой, чем же она тогда является. Если опираться на практику уголовно-правового регулирования в данной сферы, то можно сделать вывод о том, что криптовалюту можно считать имуществом и даже взыскать ее по решению суда. Это связанно с изменением которые были внесены 26 февраля 2019 г. ППВС РФ от 7 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или

сбыте имущества, заведомо добытого преступным путем». Важным разъяснением стало расширения предмета преступления таких статей, как ст. 174 и 174.1 УК РФ, согласно данным изменениям в предмет преступления стали входить и денежные средства, преобразованные из виртуальных активов (криптовалюты), которые были приобретены в результате совершения преступления. Из-за этого следует, что законодатель рассматривает криптовалюту, как иное имущество способное быть предметом преступления.

Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем».

Для цифровой безопасности Российской экосистемы, может носить опасность ведение в оборот понятия «цифровой рубль», как альтернативы криптовалюте [6]. Это может создать большую неопределённость в данной сфере правового регулирования из-за, того, что нет ответа, как рассматривать цифровой рубль. Возможно несколько подходов к его рассмотрению:

1. В свете уже сложившихся подходов в качестве имущества и применять соответствующие правила квалификации при совершении преступлений, где предметом будет выступать цифровой рубль.

2. В новом свете в связи с тем, что цифровой рубль будет иметь особый правовой статус, в этом случае действующего уголовно-правового возможно будет недостаточно.

Проанализировав ситуацию, сложившуюся данной сфере, можно согласиться с мнением директора по правовым вопросам «Новых облачных технологий» Константином Кокуриным, который рассуждая на данный вопрос подметил, что практика правоприменения в новых областях регулирования в России на первых этапах зачастую носит хаотичный характер. Он связывает хаотичный характер правоприменения с стремительным развитием технологий, за которыми не успевает правовое регулирование и ему постоянно приходится подстраиваться.

В 2020 году вступил в законную силу, ещё один важный ФЗ № 258 от 31.07.2020 «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [7]. Важность данного ФЗ, с точки цифровой безопасности связанна с тем, что он является некой попыткой по выявлению и закреплению в формате специального регулирования отношений, связанных с применением цифровых инноваций, данный нормативный правовой акт, породил больше вопросов, чем дал ответов.

Подводя итог написанному выше, можно сделать вывод о том, что для обеспечения цифровой безопасности России в сфере уголовно-правовых отношений, необходимо четко разграничивать предмет правового регулирования и инструменты, которые будут применяться для достижения данной цели. Нужно отдавать отчёт тому, что нельзя слепо следовать тенденциям правового регулирования, которые присущи другим отраслям права.

Список литературы:

1. Бут Н.Д., Тихомирова Ю.А. Обеспечение законности в сфере цифровой экономики. М.: Изд-во Юрайт, 2024. 250 с.

2. Зубарев С.М. Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. 2020. № 6. С. 23-32.

3. Савюк Л.К. Правовая статистика: учебник для студентов вузов. М.: Норма, 2019. 640 с.

4. Никитин Е.В. О новых возможностях применения цифровых технологий в правоохранительной деятельности // Правоохранительная деятельность и электронное правосудие. 2018. № 4 (19). С. 55-59.

5. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2020. № 31. Ст. 518.

6. Конягина М. Н. Основы цифровой экономики. М.: Изд-во Юрайт, 2023. 235 с.

7. Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Собрание законодательства РФ. 2020. №31. Ст. 517.