Секция «ВЫЗОВЫ И УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ»

Айдабулова Солтанат Арсланбековна

студентка специальности «Право и организация социального обеспечения» филиала Российской правовой академии Минюста России, г. Махачкала, aydabulovas@bk.ru

РАЗВИТИЕ ЭЛЕКТРОННОГО РЫНКА КАК КРИМИНОГЕННЫЙ ФАКТОР

Аннотация. Становление и развитие системы цифровой экономики сопряжено с рисками преступных хищений и умышленного незаконного получения денежных средств. Развитие киберпреступности позволяет отметить отрицательные тенденции в Российской системе уголовного права как отрасли призванной бороться с такими посягательствами. В исследовании дается общая характеристика, и приводятся средства охраны электронной информации. В конце даны выводы и решения по указанной проблеме.

Ключевые слова: электронная подписка, подделка документа, состав преступления, ответственность.

Aydabulova Soltanat Arslanbekovna

Student of the specialty "Law and Social Security Organization" branch of the Russian Academy of law Ministry of justice of Russia, c. Makhachkala, aydabulovas@bk.ru

DEVELOPMENT OF THE ELECTRONIC MARKET AS A CRIMINAL FACTOR

Abstract. The formation and development of the digital economy system is associated with the risks of criminal theft and intentional illegal receipt of funds. The development of cybercrime allows us to note the negative trends in the Russian system of criminal law as an industry designed to deal with such attacks. The study gives a general description and provides a means of protecting electronic information. At the end, conclusions and solutions to this problem are given.

Keyword. Electronic subscription, forgery of a document, crime, liability.

Становление системы электронного документооборота привело к важнейшему этапу в истории экономики мира – электронной экономике, концепции, предполагающей деятельность рынка на основе электронных товаров и услуг. Признание и закрепление статуса

электронной подписи, и перевод акций в исключительно электронный вариант привели к становлению электронного рынка в России максимально скоростными темпами. Однако где есть оборот денежных средств, там есть место и лицам, намеренным незаконным путем, заполучить себе денежные средства. Именно такие факторы и порождают возвышение количества лиц преступных мотивов. Борьба с ними – фундаментальный этап становления электронного рынка.

Первоначальными способами охраны информации являлось шифрование. Такой способ позволял передавать информацию без риска для ее получателя и отправителя. Однако, чем изощренные становились протоколы шифрования, тем сильнее становились средства вскрытия таких протоколов. Последний и самый сильный протокол шифрования – RSA признается протоколом максимальной крипто стойкости. Именно он является основой банковской и акционерной системы, потому как современные ЭВМ не способны взломать его в короткий период. Именно данный протокол и является основой современного защитного механизма всего рынка ценных бумаг и банковской системы.

С целью воспрепятствования совершению преступлений в сфере компьютерной информации была принята гл. 28 УК РФ, регулирующая преступность в сфере компьютерной информации. Однако данная глава УК является одной из самых маленьких и составляет объем в 4 статьи [1]. При этом сами статьи не предполагают какой-либо защиты электронного рынка, они направлены на общие составы преступлений. При этом в сфере электронного рынка находится, куда большее количество составов. Они включают в себя множество групп, среди которых есть и «неправомерное использование и передача банковской информации» и прочие подобные по своей сути преступные, но не признанные законодателем таковыми действия. При этом преступные деятели своими действиями способны вызвать ужасающие последствия для самого рынка. Эти последствия могут начинаться с самого непосредственного вмешательства в банковскую систему и обнуления счетов вкладчиков, заканчивая полным прекращением работы электронного рынка на длительное время. Схожие действия имели место быть, когда в Швеции была организована крупнейшая в мире DDoS атака, вызвавшая отключение всего Шведского электронного государства [2].

Безусловно, проблематика довольно непроста. Некоторые факты совершения преступлений вовсе могут быть необнаруженными. Подделки документов и сложности их сертификации преследовали электронную сферу постоянно. Однако было создано средство для борьбы с такими подделками – электронная подпись. Данная подпись фактически заменяет собой обыкновенную подпись человека. В соответствие с Федеральным законом от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016 г.) «Об электронной подписи» под электронной подписью понимается информация в электронной форме, которая присоединена к другой

информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [3]. Данная подпись способствует признанию лица в качестве такового и позволяет исключить подлог документов. Такая подпись защищает акции и иные юридически значимые документы. При внесении изменений правонарушителем, электронная подпись перестает быть удостоверяющей и прекращает содержать в себе информацию об издателе.

Фактически средства защиты информации в сфере электронного рынка существуют. Однако уровень государственного регулирования этих отношений оставляет желать лучшего. Развитие уголовно-правовой ответственности позволяет пресекать большее количество правонарушений. Однако составы преступлений не должны дублировать друг друга. При этом уникальность каждого состава должна позволять нам не отделять составы родовых признаков друг от друга с целью дальнейшей их интеграцией не только в систему российского права, но и правосознания.

Мы предлагаем следующее:

1. Внести в статью 272 УК РФ квалифицирующее обстоятельство, в виде неправомерного доступа к информации, защищенной электронной подписью.

2. Внести в главу 28 УК РФ состав преступления «Неправомерное получение, передача и распространение ценных бумаг».

3. Внести в главу 28 УК РФ состав преступления «Неправомерный доступ к банковской информации».

Включение в УК РФ данных составов позволит нам защитить цифровой рынок от дальнейших посягательств. Более того развитие самого рынка напрямую связано вниманием законодателя в этом направлении. Развитие института ответственности за информационные преступления скажется положительно не только на самом институте цифровой экономики, но и на всех уровнях общественной жизни.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2020. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 09.09.2020).

2. Андрусова Т.Б., Гомонова Ю.Г., Багаева А.П. Информационное оружие и информационные войны // Актуальные проблемы авиации и космонавтики. – Красноярск: СибГУ им. М.Ф. Решетнева, 2017. С. 403-404.

3. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ// КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2020. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 09.09.2020).