ARTICLE HISTORY: Received: September 12, 2022 Accepted: November 08, 2022 Published: November 13, 2022

МЕЖДУНАРОДНЫЙ ОПЫТ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ЭКОНОМИЧЕСКИМ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Бархановв Рахим Бекханович
Магистрант 1 курса, Высшая школа государственного аудита (факультет) МГУ имени М.В. Ломоносова

INTERNATIONAL EXPERIENCE IN COUNTERACTING ECONOMIC CRIMES COMMITTED IN THE FIELD OF INFORMATION TECHNOLOGY

Rahim Bekhanovich Barkhanov
First-year Master's student,
The Higher School of State Audit at Moscow State University

Аннотация. Противодействие экономическим преступлениям, которые совершаются в сфере информационных технологий, имеет большое значение не только на государственном уровне, но также и на международном. Это обусловлено тем, что совершение данных преступлений никак не ограничено границами государства. В связи с тем, что данные преступления распространяются по всему миру, в каждом государстве имеется свой опыт противодействия им. В данной работе мы предлагаем рассмотреть особенности сформировавшегося международного опыта противодействия экономическим преступлениям в сфере информационных технологий.

Abstract. Combating economic crimes committed in the field of information technology is important not only at the state level, but also at the international level. This is due to the fact that committing these crimes is in no way limited by borders of the state. Due to the fact that these crimes are spread around the world, each state has its own experience in dealing with them. In this work we suggest analyzing peculiarities of existing international practices of counteraction to economic crimes in the sphere of information technologies.

Ключевые слова: информационные технологии, дистанционное мошенничество, киберпреступления, киберпространство, информационно-телекоммуникационные сети, компьютерная информация, анонимность, трансграничность.

Keywords: information technology, remote fraud, cybercrime, cyberspace, information and telecommunication networks, computer information, anonymity, cross-border.

Формирование опыта противодействия данным преступлениям в зарубежных странах стоит по временным рамкам отнести к моменту их возникновения, то есть к 70-м, 80-м годам прошлого века. Отметим, что к этому времени во многих странах уже было сформировано законодательство, которое предусматривало уголовную и административную ответственность за киберпреступления, например, США, Италия, Германия и другие. Тем не менее, законодательство указанных государств имело совершенно разрозненный характер не только в области назначения наказания, но и в области понятийного аппарата, то есть одно и то же преступление могло трактоваться совершенно по-разному. Для устранения указанных проблем, 13 сентября 1989 года на заседании Комитета министров Совета Европы была принята Рекомендация №(89)9, которая включила в себя перечень преступлений в компьютерной сфере [1].

В соответствии с установленными списками, было поручено странам ЕС сформировать единую уголовную стратегию противодействия преступлениям данной направленности [2].

Представленная Рекомендация рассматривается как первый факт реагирования на киберугрозу. Главным преступлением в сфере информационных технологий, в соответствии с установленными списками, стало компьютерное мошенничество.

В последствии на 93-м пленарном заседании 56-ой сессии Генеральной Ассамблеи ООН, была принята Резолюция №56/261 от 31 января 2002 года, которая была создана для того, чтобы нормализовать область борьбы с киберпреступлениями и усилить данное направление. Данный документ предлагал странам-участникам ООН создать определенный комплекс мер, которые способствовали бы противодействию данным преступлениям [3]. Представленные предложения и рекомендации способствовали тому, что киберпреступность вышла из государственных приделов и стала мировой проблемой.

Большая роль в противодействии преступлениям в сфере информационных технологий отводилась «Большой восьмерке» (G-8). Так, 26 июня 1996 года во Франции состоялась встреча «G-8», в результате которой был принят Регламент №16. Данный документ предполагал определенные законодательные гарантии криминализации и наказуемости за преступления рассматриваемого вида, посредством установления тесных

связей между правоохранительными органами разных государств. Для исполнения данных гарантий была сформирована «Леонская группа», которая на постоянной основе осуществляла борьбу именно с киберпреступлениями. Создание данной группы положило начало формированию специальных правоохранительных органов, которые осуществляли определенные мероприятия по развитию международного сотрудничества в области расследования киберпреступлений [4].

Не обошла данная проблема и Европейский союз, так была создана определённая сеть правоохранительных органов, которые занимались расследование и противодействием киберпреступлениям - «Европейский центр киберпреступлений» (European cybercrime centre), или «EC-3». EC-3 состоит из 10 подразделений, которые осуществляют конкретную работу, например, исследуют статистические данные, формируют определенные способы выявления данных преступлений и т.д. [5]

Так же стоит обратить внимание на Будапештскую Конвенцию Совета Европы «О киберпреступности» от 23 ноября 2001 года [6]. Данная конвенция определяется как самая строгая в области противодействия киберпреступлениям. Данная конвенция не была подписана Российской Федерацией, мы можем предполагать, что именно из-за ее сверхстрогого характера, так как определенные ее положения не соответствуют законодательству России.

Далее в 2010 году в Бразилии прошел двенадцатый Конгресс ООН, на котором были рассмотрены вопросы относительно разработки Глобальной Конвенции по борьбе с ней [7].

Помимо международного регулирования данного вопроса, каждое государство пытается решить его в пределах своей территории, при этом создавая государственные стратегии, которые имеют большое значение для определения особенностей киберпреступлений в той или иной стране.

Определено, что не каждое государство располагает стратегией кибербезопасности, в некоторых странах она вовсе отсутствует, а в некоторых находится в стадии разработки, например, в России [8].

Государственная политика в первую очередь направлена на защиту стратегически важных областей от киберпреступлений. Таким образом, принимая стратегии кибербезопасности, зарубежные страны воспринимают угрозу таких преступлений, как угрозу национальной безопасности. Мы считаем, что при принятии стратегии в Российской Федерации необходимо учесть данный факт.

Как мы видим, главной мерой противодействия киберпреступлениям является именно нормативно-правовая база, а именно уголовное, административное и информационное законодательство. Так же большое значение в области противодействия имеет криминализация новых преступлений, ужесточение ответственности за те преступления, которые уже криминализированы.

Считаем, что целесообразно в ст. 63 УК РФ внести дополнение, которое будет касаться отягчающего обстоятельства, так необходимо дополнить статью пунктом следующего содержания: «совершение преступления в отношении лиц старше 60 лет, а также лиц, относящихся к социально незащищенным категориям граждан». Внесение дополнения в ст. 63 УК РФ обусловлено тем, что ежегодно от действий кибермошенников страдают пожилые люди.

Как мы уже отмечали, законодательство зарубежных стран имеет разрозненный характер, но имеются и общие положения, которые закреплены в Уголовных кодексах многих государств.

Так, например, в Уголовном кодексе РФ в ст. 159^6 есть «Компьютерное мошенничество» или «хищение с использованием средств компьютерной техники». Уголовный кодекс Белоруссии [9] определяет, что хищение, которое совершено с применением компьютерной техники, стоит расценивать как самостоятельную форму хищения (ст.ст. 212, 327, 323, 294 УК Белоруссии).

Так же, в ст. 216 УК Белоруссии определен способ хищения, при котором используется модификация компьютерной информации [10].

Уголовный кодекс Дании в статье 279 «а» определяет компьютерное мошенничество (дат. - databedrageri) как: «незаконное изменение, дополнение или стирание информации либо программы, используемой для электронной обработки данных с целью получения для себя или для других лиц незаконной выгоды» [11].

В Уголовном кодексе КНР [12] определена ответственность за хищение денежных средств при помощи компьютерной техники (ст. 287). Статья носит ссылочный характер, так как ответственность назначается по иным статьям УК КНР, а максимальное наказание – смертная казнь.

В Японии на законодательном уровне не выделено компьютерное мошенничество в отдельный вид преступления, но в данном государстве действует Закон «О несанкционированном проникновении в компьютерные сети» 2000 года [13], который определяет ответственность в данной области.

Итак, проанализировав законодательство нескольких зарубежных стран, мы можем отметить, что в некоторых государствах компьютерное мошенничество выделено в отдельный вид хищения или вовсе такое выделение не происходит, а другие страны компьютерное хищение определяют как цель. Исходя из представленного анализа, мы считаем, что для Российской Федерации, наиболее приемлемым является законодательство Белоруссии, так как уголовное законодательство Республики является наиболее близким к уголовному законодательству России.

Далее рассмотрим получение сведений, составляющих коммерческую тайну путём неправомерного доступа к компьютерной информации, по-другому данный вид преступления называют «компьютерный коммерческий шпионаж».

В качестве способа совершения коммерческого шпионажа в УК Финляндии определен неправомерный доступ к компьютерным системам [14].

УК РФ не предусматривает ответственность за данный состав преступления, квалификация данного общественно опасного деяния осуществляется по совокупности преступлений, предусмотренных статьями 18 и 272 УК РФ.

Далее рассмотрим такой состав преступления, как кибер-вымогательство. Особенность данного преступления заключается в характере угрозы, то есть передача денежных средств, происходит под угрозой уничтожения данных, которые хранятся на компьютере.

Ответственность за такое преступление предусмотрена в УК Нидерландов (ч. 2 ст. 317), Закона №1030 США (п. (A)(7)).

УК РФ так же не предусматривает ответственность за рассматриваемое преступление, но при этом квалифицирует его по совокупности преступлений, предусмотренных статьями 163 и 272 УК РФ. Однако, при такой квалификации возникают проблемы, которые связаны с тем, что данные статьи не предусматривают такой признак, как «угроза повреждения или уничтожения данных, хранящихся на компьютерном устройстве». Соответственно, такая квалификация по совокупности не может считаться правильной, что подтверждает необходимость внесения на законодательном уровне нового квалифицирующего признака.

Рассмотрев уголовно-правовые меры противодействия преступлениям в сфере информационных технологий, обратим внимание и на иные меры. Например, проблема анонимности данных преступлений в определенных странах разрешается на административном уровне. Так, после теракта в Милане в 2004 году, доступ к сети «Интернет» в кафе предоставлялась только после предъявления удостоверяющих личность документов.

Таким образом, нормативно-правовое регулирование стоит считать самой эффективной мерой противодействия преступлениям в киберпространстве.

Проведя анализ международного и зарубежного опыта противодействия киберпреступлениям, мы можем сказать, что он является весьма несогласованным, что не дает ему быть достаточно эффективным. Опыт зарубежных государств в некоторых странах формировался много лет, в других же странах до сих пор данные преступления не криминализированы. Международные конвенции скорее обладают политическим характером, нежели правовым, а их подписание не представляется возможным [15].

Так, эффективность противодействия указанным преступлениям возможна в результате проведения определенной реформы законодательства, которая будет включать в себя криминализацию новых составов, ужесточение ответственности и т.д. Но для Российской Федерации криминализация новых составов – не совсем верное решение. Мы считаем, что необходимо дополнить перечень отягчающих обстоятельств: с применением средств компьютерной техники.

Список использованных источников

1. Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом (по материалам зарубежной печати): Ежем. информ. бюл. ВИНИТИ. - М., 1992. - № 4. - С. 4.

2. Побегайло А.Э. Киберпреступность: лекция. М., Академия Генеральной прокуратуры Российской Федерации. - 2016. - С.13. 41

3. Резолюция Генеральной Ассамблеи ООН от 31 января 2002 № 56/261 «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века» (Принята в г. Нью-Йорке на 93-м пленарном заседании 56-ой сессии Генеральной Ассамблеи ООН) // СПС «КонсультантПлюс». – Последнее обращение: 14.11.2021.

4. Сухаренко А.Н. Современные криминальные вызовы и угрозы информационной безопасности России [Электронный ресурс] // URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (Дата обращения: 14.11.2021).

5. Киселёв А.К. Киберпреступность – взгляд из Европы. // Библиотека криминалиста. - 2018. - №5(10). - С.311 - 312.

6. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // Российская Федерация в настоящей Конвенции не участвует. Текст перевода документа предоставлен Правовым управлением Государственной Думы ФС РФ. / СПС «Гарант». – Последнее обновление: 14.11.2021.

7. Дубко М. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией [Электронный ресурс]// URL:http://www.crimeresearch.ru/articles/Dubko_0001 (Дата обращения: 14.11.2021).

8. Парламентская библиотека. Государственные стратегии кибербезопасности [Электронный ресурс] // URL: http://www.securitylab.ru/ (Дата обращения: 14.11.2021).

9. Уголовный кодекс Белоруссии. [Электронный ресурс]// URL:http://etalo№li№e.by/?type=text&reg№um=hk9900275#load_text_№o№e_1 (Дата обращения:15.11.2021).

10. Простосердов, М.А. Преступления, совершаемые в информационном пространстве стран ЕврАзЭС // Информационное пространство Евразэс: правовые основы интеграции: монография, 2019. – С. 95.

11. Уголовный кодекс Дании. [Электронный ресурс] // URL: https://www.retsinformation.dk/Forms/R0710.aspx?id=152827#Kap28 (Дата обращения: 15.11.2021).

12. Уголовный кодекс Китайской Народной Республики [Электронный ресурс] // URL: http://constitutions.ru/archives/403 (Дата обращения: 15.11.2021).

13. Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста.- 2018. - №5(10). - С.57.

14. Уголовный кодекс Финляндии [Электронный ресурс] // URL:http://www.finlex.fi/en/laki/kaannokset/1889/e№18890039.pdf (Дата обращения 15.11.2021).

15. Простосердов, М.А. Сравнительный анализ зарубежного законодательства в сфере противодействия виртуальным преступлениям / М.А. Простосердов // Актуальные проблемы уголовного права и криминологии: сборник научных трудов кафедры уголовного права. Вып.4 / Под ред. А.В. Бриллиантова. − М.: РАП, 2020. − С. 133.

References:

1. Problems of Combating Computer Crime // Combating Crime Abroad (based on foreign press): Journal of the Russian Academy of Sciences. VINITI. - M., 1992. - № 4. - C. 4. (In Russian).

2. Pobegaylo A.E. Cybercrime: a lecture. Moscow, Academy of the General Prosecutor's Office of the Russian Federation. - 2016. - C.13. (In Russian).

3. UN General Assembly Resolution No. 56/261 of 31 January 2002 "Plans of Action for the Implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the XXI Century" (Adopted in New York City at the 93rd plenary meeting of the 56th session of the UN General Assembly) // ConsultantPlus Information System. - Last accessed: 14.11.2021. (In Russian).

4. Sukharenko A.N. Modern criminal challenges and threats to information security of Russia [Electronic resource] // URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (Last accessed: 14.11.2021). (In Russian).

5. Kiselev A.K. Cybercrime - a view from Europe. // Library of criminalist. - 2018. - №5(10). - C.311 - 312. (In Russian).

6. Convention on Cybercrime ETS No. 185 (Budapest, November 23, 2001) // Russian Federation does not participate in this Convention. The text of the document was provided by the Legal Department of the State Duma of the Federal Assembly of the Russian Federation. / Garant. - Last update: 14.11.2021. (In Russian).

7. Dubko M. International cooperation in the sphere of criminal-legal struggle against the misappropriation of computer information [Electronic resource]// URL:http://www.crimeresearch.ru/articles/Dubko_0001 (Date of accession: 14.11.2021). (In Russian).

8. Parliamentary Library. State cybersecurity strategies [Electronic resource] // URL: http://www.securitylab.ru/ (Date of access: 14.11.2021). (In Russian).

9. Criminal Code of Belarus. [Electronic resource]// URL:http://etalo№li№e.by/?type=text&reg№um=hk9900275#load_text_№o№e_1 (Date of access:15.11.2021). (In Russian).

10. Prostoserdov M.A. Crimes committed in the information space of EurAsEC countries // EurAsEC information space: legal basis for integration: monograph, 2019. - C. 95. (In Russian).

11. Criminal Code of Denmark. [Electronic resource] // URL: https://www.retsinformation.dk/Forms/R0710.aspx?id=152827#Kap28 (Date of reference: 15.11.2021). (In Russian).

12. Criminal Code of the People's Republic of China [Electronic resource] // URL: http://constitutions.ru/archives/403 (Date of reference: 15.11.2021). (In Russian).

13. Khilyuta V.V. Embezzlement with the use of computer equipment or computer fraud? // Library of criminalist.- 2018. - №5(10). - C.57. (In Russian).

14. Criminal Code of Finland [Electronic resource] // URL:http://www.finlex.fi/en/laki/kaannokset/1889/e#18890039.pdf (Date of access 15.11.2021). (In Russian).

15. Prostoserdov, M.A. Comparative analysis of foreign legislation to counteract virtual crimes / M.A. Prostoserdov // Actual problems of criminal law and criminology: collection of scientific papers of the department of criminal law. Vyp. 4 / Ed. by A.V. Brilliantov. - MOSCOW: RAP, 2020. - C. 133. (In Russian).