DOI:10.26104/NNTIK.2023.44.68.052

Саниязова Е.К.

КЫЛМЫШ-ЖАЗА КИБЕР УКУК БУЗУУЛАРДЫН ТҮШҮНҮГҮ ЖАНА АЛАРДЫН КРИМИНАЛИСТТИК КЛАССИФИКАЦИЯСЫ

Саниязова Е.К.

ПОНЯТИЕ УГОЛОВНЫХ КИБЕРПРАВОНАРУШЕНИЙ И ИХ КРИМИНАЛИСТИЧЕСКАЯ КЛАССИФИКАЦИЯ

E. Saniyazova

THE CONCEPT OF CRIMINAL CYBER VIOLATIONS AND THEIR FORENSIC CLASSIFICATION

УДК: 343.9

Макала Кылмыш-жаза кибер укук бузуулар жана алардын криминалисттик классификация түшүнүгүн карап чыгуу максатында аткарылган. Белгилей кетүүчү нерсе, изилдөөлөрдүн кеңири чөйрөсүнө карабастан, бул көйгөйдүн айрым аспектилери жетиштүү иштелип чыккан эмес жана андан аркы илимий издөөлөрдү талап кылат. Казакстан Республикасынын Кылмыш-жаза мыйзамдарына жана көз карандысыз Мамлекеттер Шериктештигине катышкан мамлекеттердин Казакстан Республикасында жана Кыргыз Республикасында ратификацияланган маалыматтык технологиялар чөйрөсүндөгү кылмыштарга каршы күрөшүүдөгү кызматташтыгы жөнүндө макулдашууга салыштырмалуу укуктук талдоо жүргүзүлдү. Иштин натыйжалары кылмыштуу кибер укук бузуулар түшүнүгүн изилдөө жана алардын криминалисттик классификациясы болуп саналат. Автор Казакстан Республикасында жана Кыргыз Республикасында ратификацияланган маалыматтык технологиялар чөйрөсүндөгү кылмыштар менен күрөшүүдө Көз карандысыз Мамлекеттер Шериктештигине катышкан мамлекеттердин кызматташтыгы жөнүндө макулдашуулар ар бир өлкө үчүн өзүнчө кибер укук бузууларга каршы күрөшүүдө мыйзамдарды иштеп чыгуунун пайдубалы болуп сана лат деген пикирге келет.

Негизги сөздөр: *кибер укук бузуулар, соттук классификация, маалымат тутумдары, телекоммуникация тармагы.*

Статья выполнена в целях рассмотрения понятии уголовных киберправонарушений и их криминалистическая классификация. Необходимо отметить, что несмотря на достаточно широкий круг исследований, отдельные аспекты данной проблемы остаются разработанными недостаточно и требуют дальнейших научных поисков. В качестве методов работы проведен сравнительно-правовой анализ уголовного законодательства Республики Казахстан и Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, ратифицированных и в Республике Казахстан и Кыргызской Республике. Результаты работы заключаются в исследовании понятии уголовных киберправонарушений и их криминалистическая классификация. Автор приходит к мнению, что Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий ратифицированных и в Республике Казахстан и в Кыргызской Республике, являются фундаментом для разработки законодательства в борьбе с киберправонарушениями для каждой страны в отдельности.

Ключевые слова: *киберправонарушения, криминалистическая классификация, информационные системы, сеть телекоммуникаций.*

The article is made in order to consider the concept of criminal cyber-violations and their criminalistic classification. It should be noted that despite a fairly wide range of studies, certain aspects of this problem remain insufficiently developed and require further scientific research. As methods of work, a comparative legal analysis of the criminal legislation of the Republic of Kazakhstan and the Agreement on Cooperation of the member states of the Commonwealth of Independent States in combating crimes in the field of information technology, ratified both in the Republic of Kazakhstan and the Kyrgyz Republic, was carried out. The results of the work consist in the study of the concept of criminal cyber-violations and their criminalistic classification. The author comes to the conclusion that the Agreements on cooperation of the member states of the Commonwealth of Independent States in combating crimes in the field of information technology, ratified both in the Republic of Kazakhstan and in the Kyrgyz Republic, are the foundation for the development of legislation in the fight against cyber violations for each country separately.

Key words: *cyber-violations, criminalistic classification, information systems, telecommunications network.*

Киберправонарушения в Республике Казахстан и в мире имеют быструю динамику развития, их количество и число пострадавших от действий киберпреступников постоянно увеличивается. Но общество не выработало против такого вида преступлений эффективных мер борьбы. Следует отметить, понятие киберправонарушения некоторые ученые трактуют как различные виды (группы) преступлений в сфере информационных технологий, классификация которых осуществлялась по разным признакам. При этом признаком для «отнесения» отдельных преступлений в сфере информационных технологий в общем виде является орудие совершения преступления – компьютерная техника, а признаком для выделения киберпреступности – специфическая среда совершения преступлений – киберпространство (среда информационных систем и сетей) [1].

Безусловно, если рассматривать группу преступлений, объединенную в отдельную главу Уголовного кодекса Республики Казахстан (далее - УК РК) – «Уголовные правонарушения в сфере информатизации и связи» [2] в отрыве от других форм проявления преступного поведения с использованием информационный техники и сети связи, то данная классификация имеет смысл. Проблема киберправонарушений,

хоть и взаимосвязана с относительно недавно возникшей сферой жизнедеятельности человека, по сравнению, например, с организованной или служебной, однако неоднократно находила отражение в работах отечественных и зарубежных ученых юристов [3].

Цель данной статьи заключается в том, что несмотря на достаточно широкий круг исследований, отдельные аспекты данной проблемы остаются разработанными недостаточно и требуют дальнейших научных поисков. Прежде всего это касается выделения киберправонарушений как самостоятельного вида преступности, определения ее специфических особенностей, круга деяний, характерных для данного вида преступных проявлений, криминалистическая классификации киберправонарушений и объектов преступных посягательств данного вида.

Задача состоит в формировании определения данной категории преступлений и выделения ее характеристики. На сегодня в казахстанском законодательстве отсутствует определение понятия «киберправонарушение», есть лишь обобщенное понятие преступлений и правонарушений, совершаемых с использованием информационных систем или сеть телекоммуникаций, в частности:

- Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205 УК РК);
- Неправомерные уничтожение или модификация информации (206 УК РК);
- Нарушение работы информационной системы или сетей телекоммуникаций (ст. 207 УК РК);
- Неправомерное завладение информацией (ст. 208 УК РК);
- Принуждение к передаче информации (ст. 209 УК РК);
- Создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК РК);
- Неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211 УК РК);
- Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК РК);
- Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213 УК РК) [2].

Вместе с тем, необходимо отметить, что согласно главе 6 Уголовного кодекса Республике Казахстан [2], который называется «Уголовные правонарушения против собственности», также закреплены нормы регламентирующие «киберправонарушения»: кража, то есть тайное хищение чужого имущества, – путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций (п.4 ч.2 ст.188 УК РК); мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, – путем обмана или злоупотребления доверием пользователя информационной системы (п.4 ч.2 ст.190 УК РК).

Вопрос поиска путей противодействия преступлениям с использованием сетей телекоммуникационных систем уже длительное время находится в сфере внимания международного сообщества. В настоящее время Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (далее – Соглашение СНГ) ратифицированных и в Республике Казахстан и в Кыргызской Республике, которые является фундаментом для разработки законодательства в борьбе с киберправонарушениями для каждой страны в отдельности [4].

В соответствии с настоящим Соглашением СНГ, было принято решение:

- о сотрудничестве в целях обеспечения предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере информационных технологий в рамках национального законодательства и международными договорами, участниками которых они являются;
- принимать все необходимые организационные и правовые меры для выполнения положений настоящего Соглашения СНГ;
- стремятся к сближению национальных законодательств в области борьбы с преступлениями в сфере информационных технологий [4].

Следует отметить, что Соглашения СНГ, как основополагающий документ в сфере борьбы с киберправонарушениями, предоставляет условную классификацию киберправонарушений, разделяемых на следующие категории: «уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации; создание, использование или распространение вредоносных программ; нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия; хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной ин-

формации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации; распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего; изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети; незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб; распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма» [4].

Согласно данным правоохранительных органов особое внимание выделяется преступлениям, в сфере мошенничества совершаемых с использованием информационных технологий:

Способы совершения киберправонарушений очень разнообразны. Преступниками используются методы социальной инженерии, направленные на получение денег в виде предоплаты, оформление онлайн-займов, завладевая персональными данными граждан для доступа к банковским счетам, электронной почте, аккаунтам в социальных сетях и т.д. Похищенные деньги выводятся через сервисы международных переводов либо переводятся в криптовалюту. Популярны фишинговые Интернет-ресурсы, а также хакерские программы, позволяющие осуществлять подмену звонящего номера, искажать голос звонящего. Постоянно изобретаются новые преступные схемы [5].

Таким образом, стремительное развитие информатизации в Казахстане несет за собой потенциальную возможность использования компьютерных технологий из корыстных и других мотивов, что в определенной степени ставит под угрозу национальную безопасность государства [6].

Вместе с распространением внедрения современных информационных технологий в Казахстане постоянно растет угроза как для государственных информационных систем, так и для частных организаций и отдельных граждан. Данные статистической отчетности свидетельствуют о негативных тенденциях мошенничества в сети Интернет и малой возможности по поимке Интернет - мошенников. Так, если в 2017 году произошло около 600 вышеуказанных преступлений, то в 2022 году уже более трех тысяч [7].

Таким образом, современный уровень информатизации общества требует от законодательства Республики Казахстан обеспечить надлежащий и эффективный механизм борьбы с киберправонарушениями как одной из серьезных угроз национальной безопасности государства. Такая потребность становится еще более очевидной, учитывая транснациональный характер исследуемых преступлений, что требует от правоохранительных органов Казахстана еще более качественных технического обеспечения и компетентности для осуществления качественного сотрудничества как в рамках международного сотрудничества во время уголовных производств данной категории, так в целом в вопросах противодействия киберправонарушениям.

Также необходимо отметить, что в рамках Соглашения СНГ были регламентированы следующие понятии и терминологии:

- вредоносная программа – созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы информационной (компьютерной) системы;

- информационные технологии – совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу, распространение и защиту информации;

- информационная система – организационно упорядоченная совокупность средств, реализующих определенные технологические действия посредством информационных процессов, предназначенных для решения конкретных функциональных задач;

- компьютерная система – комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации;

- компьютерная информация – информация, находящаяся в памяти компьютерной системы, на машинных или на иных носителях в форме, доступной восприятию компьютерной системы, или передающаяся по каналам связи;

- несанкционированный доступ к информации – доступ к защищаемой информации с нарушением прав или правил, установленных ее обладателем, владельцем и (или) законодательством Сторон [4].

Проанализировав теоретические и практические исследования в области определения понятия киберправонарушения, можно прийти к выводу, что среди современных казахстанских ученых нет единого подхода к определению понятия киберправонарушения. Причем подходы достаточно существенно отличаются, что может быть причиной неправильной трактов-

ки, а это в свою очередь может привести к неправильной квалификации преступных действий, что создаст проблемы не только на теоретическом, но и на практическом уровнях.

В действующем законодательстве Казахстана на сегодня отсутствует нормативно-правовое закрепление ключевых терминов как «киберправонарушение», что вызывает многочисленные научные дискуссии среди исследователей современности. Ученые юристы уделяют много внимания исследованию указанной проблематики и предлагают собственные определения этих понятий.

Так, киберправонарушением следует считать вмешательство в работу телекоммуникационных сетей, компьютерных программ, функционирующих в их среде, или несанкционированную модификацию компьютерных данных, дерзкую дезорганизацию работы критически важных элементов инфраструктуры государства, создающую опасность гибели людей, задачи значительного имущественного ущерба или наступления других общественно опасных последствий, осуществляемые с целью нарушения общественной безопасности, запугивания населения или влияния на принятие органами власти выгодных преступникам решений, удовлетворение их имущественных или иных интересов [8].

Стоит обратить внимание, что в научной юридической литературе приведены такие признаки киберправонарушений, отличающие их от «обычных» преступных посягательств и значительно повышающие их общественную опасность.

Во-первых, киберправонарушение не требует физического сближения жертвы и субъекта преступления в момент совершения такового.

Во-вторых, киберправонарушение является «автоматизированным» преступлением (субъект преступления с помощью компьютерных технологий в течение короткого периода времени может увеличить количество противоправных деяний до нескольких тысяч).

В-третьих, субъект киберправонарушение не подвластен ограничениям, которые существуют в реальном, физическом мире. Так, киберправонарушения могут быть совершены моментально, а потому нуждаются в быстрой реакции на них.

В-четвертых, киберправонарушение до сих пор остается новым феноменом, и наука еще не способна устанавливать модели распространения различных видов преступлений географически и демографически, как это возможно в отношении преступлений, совершаемых в реальном, физическом мире [9].

Исходя из приведенного анализа, можно сделать вывод, что киберправонарушение – это противоправное виновное деяние (действие или бездействие), которое предусматривает вмешательство в данные персональных компьютеров, компьютерных программ и компьютерных сетей, или деяние, совершенное с помощью компьютеров и других современных технологий, за которое предусматривается уголовная ответственность и которое может создавать личную опасность для граждан, угрозу национальной безопасности государства и мировой безопасности.

В заключении предлагаем авторскую дефиницию на термин «киберправонарушение» как совокупность правонарушений, совершаемых в виртуальном пространстве с помощью информационных систем или путем использования информационных сетей и других средств доступа к виртуальному пространству в информационных сетях, а также против информационных систем, информационных сетей и информационных данных.

Литература:

1. Бутузов В.М. Соотношение «компьютерная преступность» и «киберпреступность» / [Текст] / В.М. Бутузов // Информаций на безопасность человека, общества, государства. – 2010. – № 1 (3). - С. 18.
2. Уголовный кодекс Республики Казахстан № 226-V ЗРК от 3 июля 2014 года. [Электронный ресурс]. Режим доступа: https://adilet.zan.kz/rus/docs/K1400000226/k226_.htm
3. Имангалиев Н.К., Садыков А.Ж. Криминологический портрет киберпреступника. / [Текст] / Н.К. Имангалиев, А.Ж. Садыков // Журнал «Наука и жизнь Казахстана» № 5(65), 2018. [Электронный ресурс]. Режим доступа: https://academy-rep.kz/item.php?id=233
4. Закон Республики Казахстан от 9 декабря 2019 года №277-VI «О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий». [Электронный ресурс]. Режим доступа: https://-online.zakon.kz/Document/?doc_id=34724841
5. В Астане было зафиксировано 22% всех кибермошенничеств в РК – МВД [Электронный ресурс]. Режим доступа: https://kapital.kz/gosudarstvo/113106/v-astane-bylo-zafiksirovano-22-vsekh-kibermoshennichestv-v-rk-mvd.html
6. Что угрожает национальной безопасности Казахстана? [Электронный ресурс]. Режим доступа: https://www.worldandwe.com/ru/page/Chto_ugrozhaet_nacionalnoy_bezopasnosti_Kazahstana.html
7. Кибермошенничество в Казахстане: факты, тенденции и анализ. [Электронный ресурс]. Режим доступа: https://-er10.kz/read/analitika/kibermos hennichestvo-v-kazahstane-fakty-tendencii-i-analiz/
8. Пилипчук В.Г., Клювань А.П. Теоретические и государственно-правовые аспекты противодействия информационному терроризму в условиях глобализации стратегические приоритеты. / [Текст] / В.Г. Пилипчук, А.П. Клювань // 2011. № 4 (21). - С. 12-17.
9. Европа И.В. Виды противоправных действий в сфере новейших информационных технологий. / [Текст] / И.В. Европа // Вестник Академии адвокатуры. - Украина. 2010. №3 (19). - С. 129-136.