Rasulev Abdulaziz Karimovich
Adliya vazirligi huzuridagi Huquqiy siyosat tadqiqot instituti direktorining o'rinbosari Yuridik fanlar doktori, professor

AXBOROT TEXNOLOGIYALARI VA XAVFSIZLIGI SOHASIDAGI JINOYATCHILIKKA QARSHI KURASHISHNING HUQUQIY CHORALARI: TAHLIL VA MUAMMOLAR

Rasulev Abdulaziz Karimovich
Deputy Director of the Research Institute of Legal Policy under the Ministry of Justice, Doctor of Law, Professor

LEGAL MEASURES TO COUNTERACT CRIME IN THE FIELD OF INFORMATION TECHNOLOGY AND SECURITY: ANALYSIS AND PROBLEMS

Расулев Абдулазиз Каримович
Заместитель директора Исследовательского института правовой политики при Министерстве юстиции, доктор юридических наук, профессор

ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И БЕЗОПАСНОСТИ: АНАЛИЗ И ПРОБЛЕМЫ

На сегодняшний день широкое использование информационно-коммуникационных технологий, формирование и развитие виртуальных отношений порождает проблему защиты личности, общества и государства и противодействия правонарушениям в киберпространстве.

В мире сейчас Интернетом пользуются более **4,6 миллиардов** человек, в то время как в 2005 году эта цифра чуть превышала одного миллиарда человек. При этом согласно данным Международного Статистического портала по итогам 2020 года 3,81 миллиардов людей или 85 процентов всех пользователей сети Интернет составляют пользователи социальных сетей, что и подтверждает тезис о том, что мы практически не можем представить свою жизнь без виртуального пространства. Пандемия COVID-19 и условия карантина все больше укрепили статус Интернета и социальных сетей. Если обратить внимание на статистику по итогам 2020 года активизировался процесс использования и обмена информации в таких платформах, как *YouTube, WhatsApp, Wordpress, Twitter, Instagram, Facebook*.

По итогам первого полугодия 2021 года наибольшее количество Интернет пользователей проживает в Китае, Индии, США, Бразилии и РФ.

Республика Узбекистан занимает 33 место. Рекордный темп роста числа пользователей сети в Узбекистане наблюдался в последние десять лет. Их количество увеличилось с 16% до 64,57 % населения.

Интернет среда, облачные технологии, программные продукты нового поколения могут как облегчить современную жизнь, так и стать грозным оружием в руках злоумышленников. Это свидетельствует о возникновении феномена киберпреступности, который по своим масштабам и степени общественной опасности намного опережает традиционную преступность. Согласно данным авторитетных мировых экспертно-аналитических кругов вероятность успешного расследования киберпреступлений составляет всего 0,05%! Между тем, предполагаемый ущерб мировой экономике от киберпреступлений по итогам 2021 года составит **6 триллионов долларов США**. Для сравнения, этот показатель в **два раза** больше, чем годовые доходы от наркоторговли, продажи оружия, незаконной проституции, хищений и т.п. В 2020 году объем мирового рынка киберпреступлений составил 1,5 трлн долл. США. Эта цифра сопоставима с ВВП Канады или Австралии в 2017 г., согласно данным World Bank. Лишь в первые 10 месяцев 2020 года в мире зафиксировано около 980 миллионов правонарушений в сети Интернет со стороны **58 миллионов** правонарушителей в сети Интернет, что больше населения Швейцарии, Швеции, Бельгии и Португалии вместе взятых. В целом история событий «Арабской весны», деятельности ИГ показывают злонамеренное использование ИКТ.

Указанные факторы обеспокоили и Республику Узбекистан. Так в Концепции совершенствования уголовного и уголовно-процессуального законодательства Республики Узбекистан, утвержденной постановлением Президента Республики Узбекистан от 14 мая 2018 года № ПП–3723, в рамках обеспечения действенной и надежной охраны прав и свобод граждан, интересов общества и государства была указана необходимость **пересмотра норм, предусматривающих ответственность в сфере информационных технологий с учетом технологического прогресса, в том числе расширение категорий преступлений, связанных с киберпреступностью**.

На наш взгляд, проблемами уголовно-правового противодействия киберпреступности в Республике Узбекистан являются:

1. Слабая гармонизация норм УК Республики Узбекистан в части ответственности за киберпреступления нормам законодательства в сфере информационных технологий и безопасности.

Законодательство Республики Узбекистан в сфере информационных технологий и безопасности представлено 29 Законами, 51 актами Президента и 96 решениями Правительства Республики Узбекистан. Следует отметить, что нормы некоторых этих нормативно-правовых актов не нашли свое подкрепление в части ответственности в КоАО или УК Республики Узбекистан. Так, несмотря на потенциальную

опасность и угрозу сети Интернет для молодежи ответственность за распространение среди детей негативной информации, наносящей вред их здоровью, согласно Закону Республики Узбекистан «О защите детей от информации, наносящей вред их здоровью» не предусмотрена. Аналогично в действующем законодательстве отсутствует специальная правовая норма, устанавливающая ответственность блогера за нарушение требований Закона Республики Узбекистан «Об информатизации».

2. Недостаточная имплементация норм международного права.

Международные акты в этой сфере определяют противодействие нарушениям конституционных (личных) прав и свобод личности в информационных системах и глобальной сети Интернет; защита частной собственности в информационной среде, противодействие киберпиратству, нарушающему авторские и смежные права собственников и товарных знаков; противодействие изготовлению, распространению негативного контента в информационном пространстве государства; защиту информационно-коммуникационных технологий и инфраструктуры от негативного внешнего воздействия; противодействие информационным войнам; борьбу с кибертерроризмом. Эти нормы могут быть использованы в совершенствовании норм УК Республики Узбекистан. Например, Решение Совета Евросоюза от 28 мая 2001 года «Противодействие мошенничеству и подделке безналичных средств оплаты» (2001/413/JHA) указывают на криминализацию мошеннических действий, совершенных в виртуальном пространстве. С учетом схожести хищений в виртуальном пространстве предлагается объединить все киберхищения в единую статью. Договор ВОИС по авторскому праву требует осуществления эффективных действий против любого акта нарушения прав, включая срочные меры по предотвращению нарушений, и меры, являющиеся сдерживающим средством от дальнейших нарушений авторов, что может быть использовано для совершенствования статьи 149 УК Республики Узбекистан.

3. Использование устаревшего понятийного аппарата в структурировании диспозиции статей УК Республики Узбекистан, обобщенность объекта уголовно-правовой охраны киберпреступлений.

Следует отметить, что по действующему УК Республики Узбекистан преступления в сфере информационных технологий указаны в разделе преступления против общественной безопасности и общественного порядка. Однако киберпреступления могут наносить вред не только общественной безопасности, но и безопасности личности или государства. Поэтому указанный родовой объект является недостаточно точным.

Определенная проблема возникает и при квалификации преступлений в этой сфере с учетом терминологии. Так статьи 278^1-278^7 используют понятия компьютера, электронно-вычислительных машин, в

то время как эти понятия не соответствуют современным реалиям динамики развития преступлений в сфере информационных технологий и безопасности. Так не представляется возможным определить мобильное устройство в качестве компьютера. То же самое можно указать про компьютерную информацию.

4. Несоответствие действующей главы XX[1] УК Республики Узбекистан современным вызовам и угрозам кибербезопасности.

Действующая редакция главы XX[1] УК Республики Узбекистан не предусматривает четкое подразделение статей объекту уголовно-правовой охраны. В свою очередь, отсутствие ответственности за нарушение требований размещения информации в сети Интернет, несанкционированный доступ к компьютерной информации, составляющей охраняемую законом тайну не позволяет обеспечить принцип неотвратимости ответственности.

При решении указанных проблем следует обратить внимание на следующее. Исходя из динамики развития и «арены» совершения преступлений в сфере информационных технологий и коммуникаций, можно условно выделить три различных типа киберпреступлений:

• *информационно-коммуникационные технологии, сети, программы и технологические средства как цель* – нападение на компьютеры, программы, сети с помощью вредоносных программных обеспечений или другие разрушительные нападения (например, компьютерный саботаж).

• *информационно-коммуникационные технологии, сети, программы и технологические средства как орудие преступления* – совершение «традиционных» преступлений, которые могут быть совершены с помощью компьютера, посредством компьютерных программ или средств (например, кибермошенничество, или распространение порнографии через социальные сети и т.д.

• *информационно-коммуникационные технологии, сети, программы и технологические средства как место или вспомогательный атрибут совершения преступлений* – совершение преступления в сети Интернет (клевета, оскорбление в социальных сетях), а равно использование технологических средств и программ, чтобы хранить незаконную или похищенную информацию либо иным способом облегчить совершение преступлений.

Считается возможным определить **родовой объект** киберпреступлений (или преступлений в сфере информационных технологий и безопасности) как *общественные отношения, обеспечивающие безопасность личности, общества и государства в сфере информационной безопасности и технологий.*

Следует отметить, что в мировой практике наблюдается тенденция снижения возраста субъекта преступлений в сфере информационных технологий и безопасности. Этому способствуют, на наш взгляд, две причины:

1) Интернет стал важным и значимым ресурсом в жизни молодежи, практически незаменимой средой коммуникации;

2) в последнее время стали распространяться атаки со стороны юных хакеров – школьников и подростков.

К примеру, в Беларуси снижен до 14 лет возраст привлечения к уголовной ответственности за хищение путем использования компьютерной техники и уклонение от отбывания наказания в виде ограничения свободы. По данным Национального центра правовой информации это обусловлено ростом числа таких преступлений, совершенных несовершеннолетними.

По некоторым данным в США группа юных хакеров (школьников), которая называет себя CWA, в 2015 году взломала личную электронную почту директора ЦРУ Джона Бреннана и министра национальной безопасности Джея Джонсона.

Специалисты одного из крупнейших российских медиа об IT и IT-безопасности «ХАКЕР» утверждают, что большинство хакеров – просто скучающие дети, у которых слишком много свободного времени. Только 10% хакеров отдают отчет в своих действиях. 90% актов вандализма в Интернете осуществляют 13-ти летние подростки, которым просто нужно «хорошо провести время».

С учетом широкой вовлеченности молодежи в информационно-коммуникационное пространство, совершения различных правонарушений и преступлений подростками и молодежью необходимо снизить возраст уголовной ответственности за преступления в сфере информационных технологий и безопасности **до 14 лет**.

На наш взгляд, кардинального пересмотра требует отдельная глава XX[1] «Преступления в сфере информационных технологий», являющаяся единственной главой, предусматривающей ответственность за уголовные деяния в сфере информационных технологий и безопасности (т.е. за киберпреступления). Исходя из предложенной нами классификации преступлений в данной сфере (информационных преступлений), мы полагаем целесообразным вместо главы XX[1]

«Преступления в сфере информационных технологий» включить в УК Республики Узбекистан концептуально новый **раздел VI[1] «Преступления в сфере информационных технологий и безопасности, средств телекоммуникаций и связи»**, предусматривающий три главы.

В первой главе XX[1] «Преступления против информационной безопасности» будут предусмотрены преступления, характеризующиеся посягательствами на безопасное создание, хранение, владение, использование и распространение компьютерной информации, находящейся под уголовно-правовой охраной. В данную главу предлагается включить следующие четыре статьи:

Статья 278[1]. Нарушение правил эксплуатации информационных ресурсов

В статье 278[1] УК Республики Узбекистан предлагается внести изменения в части названия и диспозиции, предусмотрев замену слова «информатизация» на слова «эксплуатация информационных ресурсов». Согласно Закону Республики Узбекистан «Об информатизации» под информатизацией понимается организационный социально-экономический и научно-технический процесс создания условий для удовлетворения потребностей юридических и физических лиц в информации с использованием информационных ресурсов, информационных технологий и информационных систем. При этом сущность статьи 278[1] УК Республики Узбекистан предусматривает нарушение правил использования информационно-коммуникационных или компьютерных сетей, то есть эксплуатацию информационных ресурсов. Поэтому считаем целесообразным представить статью 278[1] в вышеуказанной редакции.

«**Статья 278[2]. Незаконный (несанкционированный) доступ к компьютерной информации**

В данную статью, исходя из опыта Франции, Дании, Швейцарии предлагается внесение редакционных изменений, связанных с уточнением понятия «**компьютерная информация**», к которой в настоящее время, с развитием ИКТ следует относить не только информацию, находящуюся в компьютере, но также и в иных устройствах обработки данных (в том числе, новейших смартфонах, планшетах, коммуникаторах, навигаторах и прочих гаджетах), информационных системах, базах и банках данных, системах обработки и передачи информации.

Статья 278[3]. Изготовление с целью сбыта либо сбыт, использование или распространение специальных программных или аппаратных средств для получения незаконного (несанкционированного) доступа к защищенным информационным ресурсам, а равно для негласного получения информации

На наш взгляд, действующая редакция статьи сужает круг предмета преступления, так как сегодня при желании можно без труда найти лиц, занимающихся незаконным (то есть вне специальной регламентации, без применения в правоохранительных целях) изготовлением и распространением приборов и специальных технических средств, предусмотренных **для негласного получения информации**. Зарубежный опыт свидетельствует о возможности совершенствования УК в данном аспекте.

Статья 278[4]. Несанкционированный доступ к компьютерной информации, составляющей охраняемую законом тайну (<u>новая статья</u>)

В УК Республики Узбекистан не предусматривается ответственность за несанкционированный доступ к компьютерной информации, составляющей государственную тайну или иные

охраняемые законом секреты в виде специальной нормы. При этом нынешние киберпреступники взламывают не только информационные ресурсы крупных компаний или организаций, но и сети, информационные системы государственных органов, предприятий оборонной промышленности, транспорта, кредитно-финансовой сферы, энергетики, топливной и атомной промышленности. Поэтому установление уголовной ответственности за несанкционированный доступ к компьютерной информации, составляющей охраняемую законом тайну, имеет особую важность. В свою очередь, установление уголовной ответственности за рассматриваемое деяние послужит реализации норм Закона Республики Узбекистан «О защите государственных секретов».

Во вторую главу XX[2] «Преступления против безопасности стратегической информационной инфраструктуры» включены все преступления, характеризуемые посягательствами на целостность компьютерной информации и одновременно компьютерной техники, наступлением последствий в виде выхода из строя компьютерных технологий, сбоев и нарушений эксплуатации. В данную главу предлагается включить следующие три статьи.

Статья 278[5]. Модификация компьютерной информации

Статья 278[6]. Компьютерный саботаж

Статья 278[7]. Создание, использование или распространение вредоносных программ

Аргументация предлагаемой главы может быть выражена при помощи следующих доводов. Во-первых, во все вышеуказанные статьи вносится редакционное изменение касательно уточнения объекта и предмета преступного посягательства. Это связано с тем, что рассматриваемые преступления **наносят вред (ущерб) не только компьютеру,** но и иным устройствам обработки данных, информационной системы, баз и банков данных, системам обработки и передачи информации.

Во-вторых, зарубежный опыт (США, ФРГ, Франция, РФ, Казахстан) свидетельствует о наличии целого ряда уголовно-правовых норм в части обеспечения охраны и защиты информационной инфраструктуры.

В-третьих, объединение статей в одной главе объясняется тем, что особый акцент делается на обеспечении ***безопасности*** именно ***стратегической (то есть критически важной) информационной инфраструктуры.*** В Докладе Генерального секретаря ООН говорится, что информационная война – противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам, ресурсам, ***критически важным структурам***, подрыва политической, экономической и социальной систем, а также массированной психологической обработки населения с целью дестабилизации общества и государства. Иными словами, речь идет о создании информационного оружия, применение

которого с учетом уровня информатизации общества и уязвимости ***стратегически важных структур*** может иметь разрушительные последствия, сравнимые с воздействием оружия массового поражения. При этом **основной угрозой** в сфере информационной безопасности является создание и использование средств, предусматривающих целенаправленное информационное воздействие на ***критически важные структуры*** другого государства.

В третьей главе XX[3] «Преступления в сфере телекоммуникаций и связи», следует предусмотреть преступления, совершаемые в сфере незаконной эксплуатации информационно-коммуникационных технологий, глобальной сети Интернет, преступления, связанные с незаконным оборотом (размещением контента) информации в национальном сегменте сети Интернет), а также преступные деяния в сфере предоставления услуг связи, в том числе мобильной. Сегодня мобильные средства становятся отличной средой для совершения киберпреступлений и информационных правонарушений. В предлагаемой главе предусмотрены четыре статьи:

Статья 278[8]. Неправомерное распространение электронных информационных ресурсов ограниченного доступа (новая статья)

Рассматриваемая статья исходит из положений статьи 4 Закона Республики Узбекистан «О принципах и гарантиях свободы информации», которая гласит, что доступ к информации может быть ограничен только в соответствии с законом и в целях защиты прав и свобод человека, основ конституционного строя, нравственных ценностей общества, духовного, культурного и научного потенциала, обеспечения безопасности страны.

Статья 278[9]. Незаконное ограничение права на доступ к информационным коммуникациям и ресурсам (новая статья)

Предлагаемая статья предусматривает своей целью дальнейшую реализацию конституционной нормы, согласно которой ***каждый имеет право искать, получать и распространять любую информацию***, за исключением направленной против существующего конституционного строя и других ограничений, предусмотренных законом (статья 29 Конституции Республики Узбекистан).

Статья 278[10]. Нарушений требований размещения информации в сети Интернет (новая статья)

В качестве аргументации предложенной статьи можно указать, что сегодня каждый человек может создать аккаунт, стать блогером и сообщать новости. Закон Республики Узбекистан «Об информатизации» устанавливает обязанности блогера, однако за из нарушение ответственности нет. Сейчас практика показывает опасность размещения различных пропагандистских идей в сети Интернет, что требует установления ответственности блогеров.

Статья 278[11]. Неправомерное изменение идентификационного кода абонентского устройства мобильной связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (новая статья)

Предлагаемая статья является абсолютной новацией для УК Республики Узбекистан. В настоящее время неуклонно растет уровень преступлений в мобильной среде. В связи с этим следует установить ответственность за неправомерное изменение идентификационного кода абонентского устройства мобильной связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства. Данное деяние может быть совершено в следующем виде:

неправомерный доступ в локальные и глобальные коммуникации под чужими учетными именами и паролями;

доступ к информации на мобильных устройствах для ее копирования, блокирования, хищения денежных средств;

использование телефонов - «двойников» мобильной связи.

Статья 278[11]. Незаконный (несанкционированный) доступ к сети телекоммуникаций

Вместе с тем, считаем нецелесообразным размещать в отдельном разделе (главе) все преступления, совершаемые с использованием информационных технологий, поскольку это не представляется возможным исходя из разнообъектности преступлений и невозможности отражения в единой главе таких разновекторных и разноплановых преступных деяний (копирайтинг, распространение порнографии, цифровая подделка и прочие преступления, совершаемые с использованием информационных технологий, где основным объектом являются не отношения в сфере компьютерной информации, а иные отношения).

Библиографические ссылки:

1. Расулев, А. К. "Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности. д. ю. н.… дис." (2018): 16-18.

2. Расулев Абдулазиз Каримович. "КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ (КОМПЬЮТЕРНЫХ) ПРЕСТУПЛЕНИЙ" Вопросы современной юриспруденции, no. 2 (53), 2016, pp. 28-38.

3. А.Расулев. "ПРОТИВОДЕЙСТВИЕ КИБЕРТЕРРОРИЗМУ: МЕЖДУНАРОДНО-ПРАВОВЫЕ И УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ" Review of law sciences, no. 4, 2018, pp. 92-95. doi:10.24412/2181-1148-2018-4-92-95

4. Расулев, А. К. "Тенденции развития объекта киберпреступлений в англосаксонской правовой системе." Российский следователь 21 (2016).

5. Турсунов, Ахтам Соломович, and Абдулазиз Каримович Расулев. "УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ МЕРЫ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХТЕХНОЛОГИЙ И БЕЗОПАСНОСТИ." Вопросы криминологии, криминалистики и судебной экспертизы 2 (2019): 40-44.

6. Абдулазиз, Р. и Рахмонова, С. 2020. Преступления в сфере информационных технологий и безопасности: детерминанты и предупреждение. Общество и инновации. 1, 1 (авг. 2020), 200–209. DOI:https://doi.org/10.47689/2181-1415-vol1-iss1-pp200-209.