****

***Тасбулатов Р.Е.***

магистрант 2 курса научно-педагогической магистратуры факультета послевузовского образования Алматинской академии МВД РК

им М. Есбулатова, капитан полиции

**К вопросу совершенствования уголовно-правового противодействия цифровой преступности на современном этапе**

**\***

**On the issue of improving criminal-legal counteraction to digital crime at the present stage**

В настоящее время Республика Казахстан вступила в эпоху глобальной цифровизации и всесторонне дает большую возможность цифрового развития во всех сферах жизни граждан страны. В современном Казахстане, цифровые технологии развиваются высокими темпами, а платежная система в стране имеет свои особенности, как и система переводов денежных средств. Молодое поколение предпочитает и осуществляет свою жизнь и отношения в цифровом виртуальном пространстве. В связи с этим возникают и совершаются новые цифровые уголовные правонарушения и поэтому законодательные акты требуют совершенства и доработок.

Существуют такие новые способы обмана населения как цифровые преступления. К примеру, кибермошеничество – как один из видов киберпреступлений в цифровом пространстве, целью которого является преступное обогащение за счет обмана пользователей информационно-коммуникативных сетей. Кибербуллинг – где образуется небезопасная цифровая виртуальная среда для несовершеннолетних которая грозит ментальному здоровью, что трактуется в обыденной жизни как «травля в интернете». Всем известно, что подростковая психика не всегда может справиться с таким давлением и нередко заканчивается фактом доведения до суицида посредством использования сетей телекомуникации, в том числе сети Интернет, уголовная ответственность за что предусмотрена действующим уголовным законодательством [1].

Во многих развитых странах имеется система безопасности для контроля виртуального цифрового пространства, позволяющая мониторить законность и правомерность публикуемой информации и создаваемых сайтов и возможность существования независимо от других источников связи. По нашему мнению, совершенствование уголовно-правового противодействия в цифровом пространстве и ужесточение мер принуждения является одним из важных сдерживающих элементов уголовных правонарушений в уголовной политике Республики Казахстан.

Неслучайно в Послании народу Казахстана от 2 сентября 2024 года Глава государства Касым-Жомарт Кемелович Токаев акцентировал внимание на проблемы в деятельности правоохранительных органах: «Широкое проникновение цифровых технологий в повседневную жизнь людей сопровождается ростом количества разного рода мошенничеств. Мы это уже видим. Поэтому в современных реалиях знание основ экономики и финансов, обладание элементарными цифровыми навыками становится особенно важным. В этой связи хочу отметить проект «Қарызсыз қоғам», инициированный партией «Amanat» для повышения финансовой грамотности граждан. В прошлом году проект охватил 65 тысяч человек, и в текущем году он будет значительно расширен.

Правительству совместно с финрегуляторами необходимо внедрить в школах и вузах образовательные программы по основам финансовой грамотности и цифровой гигиены. Это усилит иммунитет казахстанцев к разного рода мошенническим схемам. Всем уполномоченным органам требуется принять решительные меры противодействия мошенничеству и сопутствующим правонарушениям, от которых страдают добропорядочные граждане.

В настоящее время разрабатывается проект нового Закона «О профилактике правонарушений». Его реализация потребует консолидации усилий госаппарата и общества. Только в этом случае можно изменить ситуацию, обеспечить верховенство закона и безопасность граждан.

Во всех обществах, в нашем в том числе, существуют запросы на такие базовые категории, как справедливость и безопасность. Полноценное удовлетворение этих основных потребностей является надежным показателем эффективности государства.

Глубокие социально-экономические преобразования, комплексные меры в сфере защиты прав человека направлены прежде всего на построение справедливого общества как основы для всестороннего прогресса нашей страны. Поэтому мы продолжим реформы и системную работу в данном направлении.

Вместе с тем нашим стратегическим приоритетом остается обеспечение безопасности граждан – фундаментальной ценности для каждого человека и общества в целом.

За последние годы мы уже добились существенного прогресса в формировании безопасной среды.

Одна из моих основных задач – сделать Казахстан территорией комфортной и безопасной жизни. Перед правоохранительными и профильными государственными органами поставлена задача – обеспечить всестороннюю безопасность граждан.

Министерство внутренних дел обязано принимать жесткие меры в отношении всех правонарушений: от мелкого хулиганства и вандализма до незаконной иммиграции и тяжких уголовных преступлений. В правовом государстве нет места криминалитету, поэтому с бандитизмом должно быть покончено. Это же касается деструктивной деятельности экстремистов, включая религиозных радикалов. Правоохранительным органам нужно проявить профессионализм, решительность и принципиальность [2].

Еще одна важная задача – борьба с наркотиками. По сути, это вопрос сохранения генофонда нации.

Необходимые законодательные меры мы уже приняли. Однако каких-то конкретных результатов пока не видно. Нельзя сказать, что государственные структуры, в том числе правоохранительные органы, работают эффективно. Проблема наркотиков усугубляется.

Мы должны построить общество, основанное на законе и порядке, знаниях и прагматизме. Залог успеха нации заключается в культурности, солидарности и созидательности граждан, в особенности молодежи. Чтобы стать цивилизованной страной, нам нужно избавляться от разрушительных моделей поведения. Приняты законы, призванные поставить заслон вандализму и лудомании, запрещены так называемые вейпы.

В Казахстане нет и не может быть никаких притеснений по какому-либо признаку, будь то языковому, конфессиональному, этническому или социальному. Отдельные случаи, провокации, конечно, имеют место, но они происходят из-за безответственности, невежества некоторых граждан, такие факты пресекаются и будут пресекаться правоохранительными органами по закону.

Мы – прогрессивная нация и поэтому должны смотреть дальше и шире, быть выше разного рода провокаций, показывать реальные примеры благоразумия, полагаться на силу закона.

Поэтому повторяю: в нашем обществе должны царить закон и порядок. Это базовое условие обеспечения как общественной, так и индивидуальной безопасности. Только так мы создадим Справедливый, Чистый и Безопасный Казахстан. Чтобы достичь этой стратегической цели, необходимо создавать благоприятные внешние условия для мирного, устойчивого развития страны. Это задача дипломатии, которая в нынешних сложнейших геополитических реалиях должна быть высокопрофессиональной [2].

В настоящие время, мы можем сказать, что многие преступления, которые ранее были только в реальной жизни, в действующий момент перешли в виртуальное цифровое пространство. Существуют уголовные правонарушения как привлечение посредством социальных сетей несовершеннолетних лиц к незаконной деятельности по распространению наркотических средств. Нередки случаи нанесения морального вреда и переход к личным границам прав граждан страны. Распространение ложной информации, которая может в дальнейшем повлиять на жизнь и психологического здоровье граждан. Имеются проблемы различного рода реклам в социальных сетях, что привлекает население Казахстана, к азартным играм и создает эффект быстрого обогащения без приложения особого труда и привлекает негативную привычку и порождают болезнь как лудомания. К сожалению, к уголовной ответственности за распространения рекламной информации или пропаганде лудомании блогеры и организаторы не привлекаются, поэтому в данном направлении необходимы изменения в Уголовный кодекс РК.

Мир глобальной сети не стоит на месте, как и кибермошенники осуществляющие преступные деяния в цифровом пространстве. С каждым днём изобретаются новые методы и способы совершения мошеннических действий в сетях интернета в целях хищения чужого имущества, покушаясь на права человека. В большинстве случаев совершающие преступления – это люди, имеющие какие-либо познания в сфере информационных технологий. Несложно найти любую информацию во всемирной паутине и прокачать свои навыки для применения в криминальной среде. Для этого методы борьбы и предотвращения должны быть на соответствующем уровне [3].

Ответственность за обеспечение правопорядка и безопасности в киберпространстве должна лежать не только на плечах государства, но и на юридических и физических лицах.

В результате анализа текущей ситуации по правонарушениям, совершенным в цифровом пространстве, можно предложить следующие рекомендации:

1. Государственным органам и юридическим лицам, осуществляющим масштабную работу с персональными данными и безопасностью систем сбора и хранения таких данных (базами данных) необходимо:

a. Усилить контроль за безопасным использованием корпоративных локальных сетей и беспроводной связи: большую роль играют сами сотрудники компаний и государственных органов. Нужно обязать сотрудников при корпоративном уровне пройти курсы по информационной безопасности и ввести ответственность за несоблюдение и умалчивание фактов информационных угроз.

б. Усилить контроль по установке обязательных необходимых антивирусных программ, а также внедрить четкую систему отслеживания установки протоколов защиты на официальных сайтах организаций.

Для этого ввести правовое регулирование и обозначить ответственность за нарушение или просрочку установки необходимых программ для сохранения безопасности.

2. На основе проведенного анализа и определения потенциальных причин кибермошенничества выявляется явная необходимость в организации систематических курсов повышения квалификации для сотрудников правоохранительных органов в сфере цифровой криминалистики.

3. Проводить профилактические мероприятия с населением, информируя о последствиях, по кибергигиене и способах совершения кибермошенничества, повышая компьютерную и правовую грамотность. Объяснять важность сообщения правоохранительным органам о факте преступных деяний в глобальной сети.

4. В целях совместного транснационального и эффективного преступного противодействия группам, которые специализируются на преступлениях в сфере информационных технологий, необходимо наладить международное сотрудничество для обмена опытом и оперативного реагирования на информационные угрозы.

5. Необходимо создать государственную структуру, которая объединит все заинтересованные органы и привлечет лучших специалистов из числа правоохранительных органов, IT специалистов, привлечет «хакеров» и экспертов в области кибербезопасности, которые обладают специальными знаниями и навыками.

В последующем делиться приобретёнными знаниями и взаимодействовать с государственными органами, финансовыми организациями и другими юридическими лицами.

6. Необходимо организовать курсы повышения квалификации для сотрудников правоохранительных органов, которые работают в области информационных технологий. Тем самым повысить качество работы с электронными доказательствами, проведения анализа, экспертиз и других оперативно-розыскных мероприятий. [4]

Помимо сотрудников правоохранительных органов надлежит обязать пройти подготовку и повысить профессиональный уровень судей. Данные практические рекомендации способствуют снижению не только кибермошенничества, но и киберпреступности в целом. Они были разработаны исходя из существующих проблем в правовом поле, практическом применении, а также на основании консультации с действующим экспертом в области кибербезопасности.

Информационные технологии охватывают практически все сферы деятельности человека. Наряду с новыми возможностями, новая среда все чаще становится объектом для противоправных действий. В связи с глобальной цифровизацией борьба с преступностью в киберпространстве становится приоритетным направлением как на национальном уровне, так и международном. Развитие киберпреступности в отличии от других сфер деятельности происходят стремительно быстро.

Распространение технологий в современном обществе меняет образ жизни людей. Интернет-мошенничество и другие цифровые уголовные правонарушения не знают географических границ. Вне зависимости от того, в какой вы стране, в каком часовом поясе и какой деятельностью занимаетесь – злоумышленник удаленно может получить доступ к вашим персональным цифровым данным преступным путем, что в дальнейшем может привести к большим финансовым потерям [5].

Согласно динамике роста раскрываемость мошенничества в Интернете сигнализирует о проблемах в расследовании правоохранительными органами, необходимости усовершенствовании правовых механизмов и методов уголовного противодействия. Предпринимаемые меры по разработке рекомендаций, пособий и методики выявления цифровых преступлений, а также анализируя настоящую ситуацию в цифровом пространстве, можно значительно повысить показатель раскрываемости. Нормотворчество и взгляд прогрессивных, компетентных специалистов в юриспруденции, финансах и в сфере IT технологий приблизят к быстрому и эффективному реагированию на подобные инциденты.

В сентябре 2024 года постановлением Правительства Республики Казахстан «О некоторых вопросах МВД РК» образован Комитет по противодействию наркопреступности, что свидетельствует о постоянном совершенствовании правоохранительной системы и укреплении уголовно-правового противодействия наркопреступлениям, совершенным в цифровом пространстве.

В рамках проводимой научно-исследовательской работы по проблемам выявления и расследования кибермошенничества, мной выявлен ряд проблем:

1 Дефицит следователей обладающих специальными знаниями IT технологий, загруженность сотрудников по расследованию уголовных дел ведущих в электронном формате. Нередко в производстве одного следователя находится одновременно до 50 уголовных дел. Стоит необходимость расширения и придания самостоятельного статуса подразделению противодействия киберпреступности, и в будущем возможно будет необходимость создания в штате МВД подразделения по противодействию киберпреступности на правах Департамента или Комитета.

В данный момент кандидаты желающие работать в правоохранительной системе имеют юридическое образование, о не имеют образование по IT технологиям. Чтобы решить проблемы со специалистами, со спецобразованием IT технологий необходимо ввести парралельно в юридическую сферу образования и образование ITтехнологии.

2 На сегодняшний день имеется проблема материально технической оснащенности подразделений по противодействию киберпреступности. Нередко нет возможности расследовать преступления из-за элементарных специальных электронных программ таких как AIRIS и др. Требуется техническое оснащение в соответствии с современными инновационными технологиями.

3 Необходимо укрепить взаимодействие с банками второго уровня для своевременного решения о блокировках счетов потерпевших от кибермошенников, создать единую базу(группу) с банками второго уровня и подразделением противодействия киберпреступности для блокировки счетов при поступлении информации о мошеннических действиях хакеров или кибермошенников пользующихся искусственным интеллектом. Законодательно закрепить обязанности для банков второго уровня осуществлять выдачи займов офлайн, отменить регистрацию онлайн кредитов пенсионерам и инвалидам, в связи с тем, что они являются частыми жертвами кибермошенников.

4 Усилить государственный контроль за микрофинансовыми организациями по упорядочиванию займов физическим и юридическим лицам, отменить беспорядочные выдачи кредитов, ужесточив условия выдачи как онлайн займов, так и офлайн.

5 Имеется необходимость применения строгости закона о передаче личных цифровых данных третьим лицам и приравнять их к уголовным правонарушениям, включить в Уголовный Кодекс Республики Казахстан понятие цифровая ответственность. Также имеется пробелы в сфере привлечения к уголовной ответственности дропперов. В основном, дропперы – это молодые люди не имеющие постоянную работу или студенты. Административная ответственность за дропперство не является эффективной мерой противодействия. На наш взгляд, признавать дроппером лиц, имеющих от трех переводов денежных средств и законодательно блокировать счета признанных дропперов и предусмотреть за их преступные деяния наказание в виде лишения свободы сроком от 3 до 5 лет или ограничения свободы на тот же срок.

С учетом изложенного и имеющихся экспертных оценок, мнений специалистов в рассматриваемой нами проблематике, а также в целях совершенствования уголовно-правового противодействия киберпреступлениям необходимо в Главу 7 Уголовные правонарушения в сфере информатизации и связи УК Республики Казахстан ввести следующие статьи: «Кибермошенничество», «Кибербуллинг», «Киберэкстремизм», «Кибертерроризм», «Кибервербовка в преступную деятельность», «Кибервербовка в наркопреступность» и разработать понятийный аппарат соответствующих терминов с обобщением различных интерпретаций данного феномена для правильной квалификации данных преступлений. Кроме этого, имеется необходимость совершенствования действующих статей, в которых имеются квалифицирующие признаки такие как «посредством компьютерных сети или сети интернет» с отсылкой к 7 Главе Особенной части Уголовного кодекса Республики Казахстан.

Наличие жестких санкций изначально препятствуют на подсознательном уровне совершать неправомерные деяния и является сдерживающим фактором. Вместе с уголовно-правовыми основами нужно в совокупности охватывать и техническую составляющую.

Системы могут быть уязвимыми до тех пор, пока стандарты безопасности не будут внедряться во все структуры, в особенности там, где хранится большая база персональных данных. Комплексное рассмотрение данной проблемы как со стороны юриспруденции, цифровой криминалистики и сферы IT поможет эффективному раскрытию и противодействию киберпреступности.

**Список литературы**

1 Мухамеджанова А.Д. «Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы его предупреждения»,) <https://cyberleninka.ru/article/n/osobennosti-dinamiki-kiberprestupnosti-v-respublike-kazahstan-i-ee-vliyanie-na-voprosy-eyo-preduprezhdeniya/viewer(дата> обращения 16.09.2024)

2 Послание Президента РК от 02.09.2024 г. <https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-spravedlivyy-kazahstan-zakon-i-poryadok-ekonomicheskiy-rost-obshchestvennyy-optimizm-285014.(дата> обращения 16.09.2024)

3 Горбунова А. В МВД рассказали о самых популярных видах интернет-мошенничества в Казахстане // ForbesKazakhstan. URL: https://forbes.kz/process/probing/samyie\_populyarnyie\_vidyi\_internetmoshennichestva\_v\_kazahstane\_nazvali\_v\_mvd (дата обращения 16.09.2024)

4 Ханов Т.А., Нуркеев А.Ж., «Современные подходы к определению компьютерной преступности... и особенности компьютерных преступлений» <https://cyberleninka.ru/article/n/sovremennye-podhody-k-opredeleniyu-kompyuternoy-prestupnosti-i-osobennosti-kompyuternyh-prestupleniy/viewer(дата> обращения 16.09.2024)

5 Информационный портал «Zakon.kz» Как интернет-мошенники обманывают казахстанцев. URL: <https://www.zakon.kz/4927774-kak-internet-moshenniki-obmanyvayut.html(дата> обращения 16.09.2024)