Абдулазиз Расулев,
и.о. профессора кафедры «Профилактика правонарушений»
Академии МВД Республики Узбекистан,
доктор юридических наук

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ПАНДЕМИИ КОРОНАВИРУСА

***Аннотация**: в данной статье были проанализированы вопросы обеспечения информационной безопасности в сети Интернет в условиях широкого распространения пандемии коронавируса. Автором были исследованы основные проблемы, являющиеся угрозой информационной безопасности личности, общества и государства. На основе анализа ситуации в Республике Узбекистан автором были разработаны соответствующие практические рекомендации и предложения.*

***Ключевые слова**: информационная безопасность, преступление, информационное пространство, коронавирус, ахборот таҳдидлари, виртуальный мир, блогер.*

Абдулазиз Расулев,
Ўзбекистон Республикаси ИИВ Академияси
“Ҳуқуқбузарликлар профилактикаси” кафедраси профессори в.б., юридик фанлар доктори

КОРОНАВИРУС ПАНДЕМИЯСИ ШАРОИТИДА АХБОРОТ ХАВФСИЗЛИГИ

***Аннотация**: мазкур мақолада коронавирус пандемияси кенг тарқалиши шароитида интернет тармоғида ахборот хавфсизлигини таъминлаш масалалари таҳлил қилинган. Муаллиф томонидан шахс, жамият ва давлат ахборот хавфсизлигига таҳдиди ҳисобланувчи асосий муаммолар тадқиқ этилган. Ўзбекистон Республикасидаги ҳолатнинг таҳлили асосида муаллиф томонидан тегишли амалий таклиф ва тавсиялар ишлаб чиқилган.*

***Калит сўзлар**: ахборот хавфсизлиги, жиноят, ахборот макони, коронавирус, информационные угрозы, виртуал дунё, блогер.*

Abdulaziz Rasulev,
Acting professor of «Prevention of offences» Department at Academy of MIA of the Republic of Uzbekistan,
Doctor of Science in Law

INFORMATION SECURITY IN THE CONTEXT OF THE CORONAVIRUS PANDEMIC

***Abstract**: This article analyzes the issues of ensuring information security on the Internet in the context of a widespread coronavirus pandemic. The author has studied the main problems that are a threat to the information security of the individual, society and the state. Based on the analysis of the situation in the Republic of Uzbekistan, the author has developed appropriate practical recommendations and proposals.*

***Key words**: information security, crime, information space, coronavirus, information threats, virtual world, blogger.*

На сегодняшний день сеть повсеместное использование сети Интернет стало ключевым фактором формирования и развития отношений в виртуальном пространстве. Особую актуальность стали приобретать вопросы защиты информации в сети Интернет, а также самих пользователей сети от неправомерного информационного воздействия. Сейчас, когда в мире выявлено 5.803.416 случаев (на состояние 29 мая 2020 года) заболевания коронавирусом, весь мир вынужден проводить большую часть своего времени дома. В Узбекистане указанная цифра приближается к 4 тысячам, в республике находятся под наблюдением на домашнем или стационарном карантине свыше 40 тысяч граждан. В этих условиях, как никогда, именно Интернет остается самым распространенным и действенным механизмом проведения досуга. Следовательно, на повестке дня возникает очень актуальный вопрос – взаимосвязь сети Интернет и информационной безопасности в условиях пандемии коронавируса. На наш взгляд, негативные аспекты в отношении информационной безопасности можно проследить в следующем:

1. Распространение в сети Интернет ложных и порочащих других лиц сведений.

Вследствие распространения пандемии коронавируса именно сеть Интернет стала тем ресурсом, благодаря которому люди начали оперативно получать информацию. Во время пандемии коронавируса поток информации усилился в виртуальном пространстве, вследствие увеличился поток необработанной и ложной информации в сети Интернет. Фейки стали трудно различимыми вследствие следующих причин:

указанные новости зачастую маскируются под обычные новости и потому легко вызывают панику;

пользователи верят источнику с большим количеством подписчиков, так основная масса, а точнее каждая пятая фейк-новость подпадает под существующие веб-сайты, которые легко можно найти в Google [1];

наличие огромного массива фейков, в связи с чем трудно определить правомерную информацию. Так в по статистическим данным ВШЭ, каждый десятый россиянин уверен, что пандемия – это «выдумки заинтересованных лиц» и не верят официальной статистике [2]. Все это доказывает, что люди больше доверяют фейкам, чем официальным источникам.

На наш взгляд, указанные проблемы требуют последовательных и нерепрессивных мер, в частности создания **Информационно-аналитических центров по мониторингу СМИ и социальных сетей, а также иных ресурсов в сети Интернет** при Общественном фонде поддержки и развития национальных масс-медиа, созданного в конце января 2020 года [3].

2. Контент в сети Интернет явно свидетельствует о наличии низкого уровня правосознания, а также способствует снижению уровня доверия в сети Интернет.

В последний месяц в сети Интернет можно наблюдать определенный спад уровня правосознания населения. Этому можно привести примеры неподчинения представителям власти, выражающиеся в нарушении правил карантина, установленных запретов, а также общественного спокойствия и безопасности. Так, с сожалением можно отметить, что за первый месяц карантина в Республике Узбекистан было совершено 51182 административных правонарушений [4], что свидетельствует о не восприятии или игнорировании установленных запретов со стороны отдельных категорий правонарушителей. Такого рода правонарушения кажутся незначительными, однако в будущем могут провоцировать намного серьезные преступления. Также вызывает озабоченность низкая культура и нигилизм отдельных лиц, являющихся знаменитостью. Своими действиями указанные лица не только подают дурной пример, но формируют у население чувство коллективной безответственности.

Доказательством низкого правосознания является также недостаточный уровень знаний и кругозора. Анализ текстов в сети Интернет показал, что с каждым годом растет количество случаев использования неграмотных и порой текстов с глупыми ошибками. По данным сайта https://hype.tech практически каждый пользователь допускает ошибки, включая сокращения и иные ошибки. Около 2 процентов пользователей не могут правильно определить окончания слов. Также стоит отметить, что публичная критика их безграмотности порой вызывает недовольство, большое негодование Интернет-сообщества, в связи подавляющим их количеством [5]. Подобного рода случай может свидетельствовать о том, что Интернет определенным образом «поощряет» неграмотность.

Одной из больших проблем доверия в сети Интернет стало и кибермошенничество. В последние два-три года количество мошенников в сегменте Интернета сильно возросло по ряду причин. Так, с появлением и ростом популярности такого явления, как социальные сети, увеличилось количество интернет-пользователей [6], пришедших в Интернет для того, чтобы осуществить поиск своих друзей и знакомых, чем активно пользуются сами мошенники, завлекая «жертв» в виртуальные отношения. С другой стороны, распространение социальных сервисов стало плохим примером для доверия, особенно в тех случаях, когда имеются случаи распространения спама и фишинга, которые нарушают информационную безопасность и способствуют вымогательству электронных денег в сети Интернет. Особую тревожность вызывают факты активизации виртуальных мошенников во время пандемии коронавируса, когда мошенники используют тему коронавируса как «приманку» и просят переходить по ссылке в письмах, якобы отправленных из банка. В этих письмах может оказаться «сайт-ловушка». Так, в РФ за время пандемии увеличилось число доменов со словом «коронавирус» - сразу на 4 тысячи. Помимо этого, на 30% выросло число фишинговых рассылок. Цель таких рассылок – выведать пароли, логины, данные карты за счёт подделки сообщений от доверенного источника. Фишинговые страницы очень похожи на оригинальные страницы сайта банков, вследствие чего люди становятся жертвами преступников [7].

На наш взгляд, одной из причин подобного уровня низкого правосознания и доверчивости пользователей является недостаточное образовательное сопровождение. Отсутствие необходимых знаний в области Интернет и информационно-коммуникационных технологий создает благоприятную почву для снижения общего уровня правосознания. В этой связи следует сформировать трехступенчатую систему образования соответствующим навыкам в информационно-коммуникационном пространстве:

1) на сегодняшний день навыки пользования информационно-коммуникационными технологиями в общих чертах преподаются в рамках информатики, однако специального предметного изучения вопросов информационной безопасности в общих чертах не имеется, в связи с чем следует ввести в общеобразовательных школах специальную дисциплину касательно понятия и сущности сети Интернет, данная дисциплина также должна предусматривать обучение навыкам первичного пользования и поведения в виртуальном пространстве;

2) в системе высшего образования подготовка технических кадров в области информационных технологий и информационной безопасности осуществляется в Ташкентском государственном университете информационных технологий, юридических кадров общей специализации в таких вузах, как Ташкентский государственный юридический университет, Академия МВД Республики Узбекистан, Институт СГБ Республики Узбекистан, при этом современная тенденция в области кадровой политики требует подготовки специалистов в междисциплинарном русле, то есть кадров, обладающих как правовыми, так и техническими навыками обеспечения информационной безопасности;

3) следует создать программу повышения квалификации и переподготовки кадров, осуществляющих оперативно-розыскные мероприятия, дознание или следствие по преступлениям, связанным с информационной безопасностью, в правоохранительных органах.

В целом проблема правосознания и доверия в сети Интернет является комплексной проблемой. В этой части необходимо **формировать своеобразную Интернет-культуру** со стороны пользователей виртуального пространства путем проведения **курсов и ознакомительных уроков (включая видео-уроки, которыми можно ознакомиться в режим офлайн), брошюр и иных интересных материалов**.

3. Разжигание конфликтов в сети Интернет.

Свобода слова и расширение возможностей всеобъемлющего использования информационно-коммуникационных технологий не в полной мере обеспечивают достоверность и общественную полезность распространяемой информации. Ни для кого не секрет, что сегодня любое лицо, особенно блогер, имеет более импульсивное и действенное воздействие на сознание общества, чем к примеру, СМИ. При этом блогеры могут неограниченно размещать информацию различного рода. Согласно статистическим данным пользователи предпочитают больше всего использовать Интернет для доступа к политической (54%), медицинской (46%) или информации органов власти (42%). Больше всего политической информации из Интернета получают в арабских странах: Тунис (72%), Ливия (70%) и Египет (68%) [8]. При этом не исключается размещение информации о деятельности террористических организаций. Главные пропагандисты Исламского государства эффективно использовали западные технологии коммуникации – YouTube, соцсети Facebook, Twitter, Instagram, Friendica, для освещения зоны боевых действий и вербовки иностранных граждан. Тысячи аккаунтов, использование Twitter Storm во время боевых операций для создания паники в тылу врага, тысячи видео сторонников движения и десятки миллионов просмотров свидетельствуют о разрушительной силе воздействия информации. Данные медиа-ресурсы в основном осуществляют свою деятельность во Всемирной сети ввиду ее доступности.

Коронавирус создал почву для манипулирования общественным мнением и сознанием. Например, контент-анализ деструктивных текстов пропаганды во время пандемии коронавируса и сравнение этих текстов с текстами журналистов и экспертов, пишущих статьи на тему противодействия экстремизму в то же время, продемонстрировали, что уровень воздействия деструктивных текстов намного сильнее и убедительнее [9]. В Сирии Президент Башар Асад, пользуясь случаем коронавируса, обвинил США в попытке использовать коронавирус в своих интересах, также выразил соболезнования гражданам Ирана, пострадавшим от пандемии COVID-19, вызванной коронавирусом, следовательно, показав свою лояльность Ирану. Однако политические враги Асада наоборот использовали данный случай как хорошую возможность дискредитировать руководителя страны и призвать людей к саботажу [10]. В РФ условия коронавируса стали поводов для различного рода митингов и шествий. Так, во Владикавказе 20 апреля текущего года прошел народный сход нескольких тысяч граждан против режима самоизоляции с требованием отставки главы региона и роспуска республиканского парламента [11].

Подобного рода случаи нарушения общественного порядка и безопасности требуют своевременной ответной меры и слаженных действий со стороны правоохранительных органов. На наш взгляд, борьба с указанным негативным проявлением возможна лишь при соответствующей квалификации сотрудников правоохранительных органов, что требует создания специфического **Центра по противодействию киберугрозам в качестве специального подразделения Службы государственной безопасности Республики Узбекистан**, на который будут возложены задачи по проведению мер в целях пресечения и предупреждения виртуальных угроз в отношении безопасности личности, общества и государства.

Самым важным условием, способствующим нарушению информационной безопасности, является несоответствие законодательства в части регулирования отношений по обеспечению информационной безопасности.

Период карантина в связи с коронавирусом показал, что хуже коронавируса может быть только паника из-за коронавируса. Ежедневно в различных мессенджерах или на веб-сайтах в Интернете появляются новости о массовом заражении и гибели людей, об исчерпании запасов продовольственных ресурсов, о введении комендантского часа или чрезвычайного положения. Правоохранительным органам приходится в режиме онлайн 24 часа в сутки бороться с этой проблемой. Уже несколько месяцев Правительства всех стран напоминает об ответственности за распространение ложной информации. Так, Премьер-министр Республики Узбекистан А.Арипов уже в начале 2020 года провел совещание по вопросам профилактики коронавируса и указал, что государство принимает меры по профилактике и предупреждению распространения болезни [12]. В свою очередь, как глава Специальной республиканской комиссии по подготовке Программы мер по предупреждению завоза и распространения коронавируса в Республике Узбекистан, Премьер-министр принимает ряд важных мер и правил, соблюдение которых направлено на предупреждение распространения коронавируса, в первую очередь, смягчения последствий на экономику. Согласно данным Bloomberg из-за

эпидемии нового коронавируса мировая экономика может потерять до $2,7 трлн [13], в связи с чем профилактические меры со стороны государства приобретают особую важность как факторы, снижающие темпы расходов и ущерб от пандемии. С учетом прогноза возможных больших потерь, Республика Узбекистан приняла важные меры по стабилизации экономики, так был создан Антикризисный фонд, из которого были израсходованы 3,306 триллиона сумов (326 миллионов долларов США). Больше 40% расходов, или 1,4 трлн сумов, пришлось на поддержку секторов экономики [14] в виде субсидий и ссуд.

Ряд Интернет-ресурсов и социальных сетей запустил собственные информационные кампании по доведению до пользователей сведений о ситуации, которые подтверждены официальными источниками. Так, в целях доведения до населения официальной информации о коронавирусе в Узбекистане Министерство здравоохранения Республики Узбекистан запустил сайт coronavirus.uz и его канал в мессенджере Telegram «Koronavirus Info». Все это свидетельствует о приоритетности насыщения населения достоверной информацией о состоянии дел во время пандемии коронавируса.

Несмотря на наличие официальных источников, в сети Интернет увеличились случаи распространения фейков касательно коронавируса. Так, в Австрии разошлась аудиозапись, на которой женщина взволнованным голосом говорит, что находится в больнице, и все, у кого обнаружены тяжелые симптомы коронавируса, принимали ибупрофен. Женщина представляется как Полин, мама некоей девочки по имени Полди. Это фейк: медики не называли ибупрофен причиной активизации коронавируса, но пользователи охотно делились записью, [15] вводя в заблуждение своих близких.

Коронавирус для Узбекистан стал также своеобразным толчком в сторону критического пересмотра законодательства. Так, за период коронавируса было принято 16 указов и постановлений Президента, направленных на смягчение воздействия пандемии на экономику.

Одной из проблем во время коронавируса стало отсутствие законодательных норм, устанавливающих ответственность за распространение не соответствующих действительности сведений о коронавирусе, а также невыполнение без уважительных причин в условиях возникновения и распространения карантинных и других опасных для человека инфекций требований о прохождении медицинского обследования, лечении и прибытии в места, определенные для прохождения карантина и непокидании данных мест в установленный период, разглашении сведений о лицах, с которыми был контакт и местах посещения в период риска заражения заболеванием, а также других законных требований органов государственного санитарного надзора. Решением этой проблемы, хоть и запоздалым, стало внесение изменений в статью 54 КоАО и статью 257^1 УК Республики Узбекистан, а также установление уголовной ответственности распространение не соответствующих действительности сведений о распространении карантинных и других опасных для человека инфекций в условиях возникновения и распространения карантинных и других опасных для человека инфекций.

Следующей проблемой является вольность и безответственность блогера. Свободное пользование средствами информационно-коммуникационных технологий и сетью Интернет может повлечь за собой определенные негативные последствия. К примеру, особое негативное влияние это оказывает на обыденных пользователей. Как и любое государство Республика Узбекистан также намерена решить вопрос предупреждения распространения негативного контента. Так, в начале апреле 2020 года Министерство внутренних дел Республики Узбекистан выставило на обсуждение проект постановления Президента Республики Узбекистан «О мерах по дальнейшему совершенствованию системы профилактики правонарушений среди несовершеннолетних и молодежи». Пункт 9 части Дорожной карты по реализации проекта предусматривает создание виртуальной группы блогеров-патриотов из числа членов Союза молодежи, студентов Ташкентского государственного университета информационных технологий и добровольцев, на которых возлагаются задачи по предупреждению негативного контента, фильтрации Интернет ресурсов и т.д. Однако указанная мера является не полноценной, а лишь помогает определить одну из сторон проблемы. Рассматривая проблемы негативного воздействия сети Интернет на сознание людей можем отметить, что нами в рамках докторской диссертации и опубликованных в ее рамках научных статьях было указано на комплексный подход в решении проблем. В этих целях считаем целесообразным принять Государственную программу по формированию Интернет культуры, включающий в себя комплекс мер – проведение тренингов, специальных курсов в образовательных учреждениях, подготовку и распространение в СМИ и Интернете пропагандистских материалов (флаеров, стендов, презентаций). В этих условиях важное значение приобретают меры социального характера, которые направлены на формирование у людей, в частности, молодежи, осознания опасности и негативных последствий преступлений в сфере информационных технологий и безопасности.

При этом объединение молодежи должно носить добровольный и самостоятельный характер, а не быть продиктованным сверху. Нами было указано целесообразность создания «Клуба молодых программистов-патриотов», который будет являться местом сбора талантливой и креативной молодежи, обладающей необходимыми знаниями и навыками в сфере информационно-коммуникационных технологий и кибербезопасности, дискуссионной средой и наглядной площадкой для подбора кадров. На наш взгляд, данный клуб целесообразно создать при Союзе молодежи Узбекистан, а также при поддержке Мининфокома, Минвуза, Министерства по инновационному развитию с привлечением специалистов, экспертов и аналитиков. Создание данного клуба может служить ярким примером открытого диалога с молодежью, своеобразным профилактическим центром по предупреждению и выявлению лиц, имеющих склонность к совершению информационных правонарушений, а также их воспитания в духе патриотизма, уважения к закону и

сопричастности к построению развитого государства и информационного общества. В отличие от инициированного Правительством проекта One Million Uzbek Coders по подготовке миллиона отечественных программистов, направленного на подготовку специалистов по информационным технологиям, предлагаемый клуб будет площадкой для государственно-частного партнерства в целях выполнения важнейших государственных заказов. В свою очередь, данный клуб может содействовать реализации различных стартап-проектов, поэтому его деятельность намного шире от существующей системы подготовки специалистов по проекту One Million Uzbek Coders.

Второй стороной проблемы является отсутствие конкретных мер ответственности. При этом законодательство предусматривает существующие запреты на «использование» Интернет в негативном смысле. Согласно статье 12^1 Закона Республики Узбекистан «Об информатизации» владелец веб-сайта и (или) страницы веб-сайта, в том числе блогер, обязан не допускать использование своего веб-сайта и (или) страницы веб-сайта во всемирной информационной сети Интернет, на которых размещается общедоступная информация, в целях:

– призыва к насильственному изменению существующего конституционного строя, территориальной целостности Республики Узбекистан;

– пропаганды войны, насилия и терроризма, а также идей религиозного экстремизма, сепаратизма и фундаментализма;

– разглашения сведений, составляющих государственные секреты или иную охраняемую законом тайну;

– распространения информации, возбуждающей национальную, расовую, этническую или религиозную вражду, а также порочащей честь и достоинство или деловую репутацию граждан, допускающей вмешательство в их частную жизнь;

– пропаганды наркотических средств, психотропных веществ и прекурсоров;

– пропаганды порнографии;

– совершения других действий, влекущих за собой уголовную и иную ответственность в соответствии с законом [1].

Однако вышеуказанные действия не влекут ответственности ни по КоАО, ни по УК Республики Узбекистан, вследствие чего следует **установить соответствующие меры ответственности**, а именно установить административную и уголовную ответственность за неправомерные действия блогера. **В свою очередь, необходимо предусмотерть возможность закрытия веб-сайтов или иных ресурсов в сети Интернет по решению суда, так как суд является конечной инстанцией, которая осуществляет правосудие.**

Таким образом, можно отметить, что основным шагом, который целесообразно применить, является формирование своеобразной Интернет-культуры, реализация которой должна осуществляться не только мерами репрессивного, но и мерами просветительского характера. Именно благодаря осознанному выбору поведения лица в информационно-коммуникационном пространстве можно обеспечить защиту информационной безопасности в виртуальном пространстве. Также необходимо проведение соответствующих институциональных и организационных мер в целях обеспечения защиты интересов личности, общества и государства в виртуальном пространстве.

Список использованной литературы:

1. Закон Республики Узбекистан «Об информатизации».
2. https://runet.rbc.ru/
3. https://www.kommersant.ru/
4. https://www.gazeta.uz/
5. https://pv.uz/ru/
6. https://hype.tech/
7. https://www.saferunet.ru/
8. www.statista.com
9. https://www.bbc.com/
10. https://crss.uz/
11. https://www.rbc.ru/
12. https://regnum.ru/