Противодействие преступлениям в сфере информационных технологий и безопасности в Республике Узбекистан на современном этапе

Counteracting crimes in the field of information technology and security in the Republic of Uzbekistan at the present stage

Расулев А.К.
Д-р юрид. наук, доцент, и.о. профессора кафедры «Профилактика правонарушений» Академии МВД Республики Узбекистан
e-mail: law@tadqiqot.uz

Rasulev A.K.
Doctor of Juridical Sciences, Associate Professor, Professor of the Department "Crime Prevention" of Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
e-mail: law@tadqiqot.uz

Аннотация
В данной статье были проанализированы вопросы совершенствования уголовного законодательства и государственной политики в области противодействия преступлениям в сфере информационных технологий и безопасности на основе существующей практики и проблем в данной сфере. На основе анализа были сделаны соответствующие выводы в части расширения круга преступлений, создания соответствующих институтов в целях проведения эффективной государственной политики по противодействию указанным преступлениям.
Ключевые слова: преступление, информационные технологии, информационная безопасность, блогер, электронная коммерция, хакеры, киберпреступления, противодействие, уголовное законодательство, защита информации.

Abstract
This article analyzes the issues of improving criminal legislation and state policy in the field of combating crimes in the field of information technology and security on the basis of existing practices and problems in this area. On the basis of the analysis, relevant conclusions were drawn regarding the expansion of the range of crimes, the creation of appropriate institutions in order to conduct an effective state policy to counter these crimes.
Keywords: crime, information technology, information security, blogger, e-Commerce, hackers, cybercrime, counteraction, criminal legislation, information protection.

Стремительный рост информационных технологий в различных сферах человеческой деятельности, с одной стороны, позволил обеспечить высокие достижения и результаты, а, с другой стороны, стал источником самых непредсказуемых и вредных последствий для человеческого общества. В результате можно говорить о появлении принципиально нового сегмента международного противоборства, затрагивающего как вопросы безопасности отдельных государств, так и общую систему международной безопасности на всех уровнях.

Сегодня на международной арене проблема борьбы с преступностью в сфере информационных технологий и безопасности приобретает все более глобальное значение. В частности, Генеральной Ассамблеей ООН, Советом Европы, ШОС, СНГ, Лигой арабских государств и иными организациями были приняты специальные акты, касающиеся информационно-коммуникационных технологий, противодействию и профилактике преступного использования информационных технологий, предупреждению преступности в данной сфере на региональном и международном уровне. Согласно статистическим данным на сегодняшний день подвижными сетями электросвязи было охвачено около семи миллиардов человек (95% мирового населения), размер ущерба от киберпреступности составляет 1% ВВП мира в год.

В Республике Узбекистан осуществляются программные меры в целях правового обеспечения информационной безопасности, предупреждения и борьбы с правонарушениями и преступлениями в сфере информационных технологий. В Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017–2021 гг. предусмотрены вопросы «совершенствования уголовного законодательства, совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере» [4]. В этой связи установление ответственности за распространение информации, представляющей угрозу правам и свободам личности, интересам общества и государства, охрана информационной безопасности в качестве объекта уголовно-правовой охраны, разработка комплекса мер по противодействию информационным преступлениям являются актуальными задачами.

На наш взгляд, противодействие преступлениям в сфере информационных технологий и безопасности в Республике Узбекистан на современном этапе должно осуществляться по следующим приоритетным направлениям:

1. Совершенствование уголовного законодательства.

Следует отметить, что с момента обретения национальной независимости в Республике Узбекистан ведется последовательная работа по охране отношений в сфере информационных технологий уголовно-правовыми мерами. В частности, в УК Республики Узбекистан уже присутствовали нормы об уголовной ответственности в указанной сфере, что, безусловно, говорит о его современном характере, поскольку в УК УзССР не было нормы, предусматривающей ответственность за преступления, совершенные с применением компьютерной техники или ЭВМ.

Так, в Уголовном кодексе Республики Узбекистан [1] 1994 г. была предусмотрена ответственность за рассматриваемый вид преступлений. В ст. 174 УК Республики Узбекистан была предусмотрена ответственность за нарушение правил информатизации. Законодатель охарактеризовал данный вид преступления как «несанкционированный доступ в информационные сети или санкционированный доступ в такие сети без принятия необходимых мер защиты, или незаконное получение из них информации, а равно умышленное изменение, утрата, изъятие или уничтожение информации при санкционированной работе с информационной системой, повлекшее значительный ущерб».

В ст. 167 (хищение путем присвоения и растраты), 168 (мошенничество), 169 (кража) УК Республики Узбекистан также были предусмотрены обстоятельства совершения рассматриваемых преступлений с применением средств компьютерной техники.

Так же в принятый в том же году Кодекс об административной ответственности была включена ст. 155 (нарушение правил пользования информацией), устанавливающая административную ответственность за правонарушения в сфере информационных технологий.

Следует отметить, что специфической особенностью построения Особенной части УК Республики Узбекистан является выделение разделов по признаку родового объекта. Это также требовало выделения рассматриваемых преступлений в отдельную категорию

преступлений. Поэтому справедливо можно отметить, что следующим прорывным этапом по обеспечению защиты информации, информационной безопасности явилось принятие в 2007 г. новой отдельной главы XX[1] «Преступления в сфере информационных технологий». В ней предусмотрено семь статей:

ст. 278[1] – нарушение правил информатизации;

ст. 278[2] – незаконный (несанкционированный) доступ к компьютерной информации;

ст. 278[3] – изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций;

ст. 278[4] – модификация компьютерной информации;

ст. 278[5] – компьютерный саботаж;

ст. 278[6] – создание, использование или распространение вредоносных программ;

ст. 278[7] – незаконный (несанкционированный) доступ к сети телекоммуникаций.

Указанные статьи объединены общим родовым объектом преступного посягательства, под которым следует понимать общественные отношения, связанные с охраной законом информации, базы данных и информационных систем их обработки в рамках более общих понятий – общественная безопасность и общественный порядок. Вместе с тем, если провести анализ главы XX[1] «Преступления в сфере информационных технологий», то его родовым объектом выступают общественные отношения по обеспечению общественной безопасности и общественного порядка, однако, исходя из сущности статей предусмотренной главы, родовым объектом является обеспечение информационной безопасности личности, общества и государства. В связи с этим представляется целесообразным расширение круга составов преступлений, указанных в главе XX[1] УК Республики Узбекистан, создав на ее базе Раздел под названием «Преступления в сфере информационных технологий и безопасности, средств телекоммуникаций и связи». При конструировании статей указанного раздела необходимо включение новых статей с учетом имеющихся угроз и рисков. Эта задача также вытекает из Концепции совершенствования уголовного и уголовно-процессуального законодательства, в которой указана необходимость пересмотра норм, предусматривающих ответственность в сфере информационных технологий с учетом технологического прогресса, в том числе расширение категорий преступлений, связанных с киберпреступностью.

Так, информатизация тесно связана с понятием доступа к информации (стэ 278[1]–278[3] связаны с неправомерным доступом к информации). Фундаментальным законом, регулирующим основы реализации конституционного права свободно и беспрепятственно искать, получать, исследовать, передавать и распространять информацию является **Закон Республики Узбекистан «О гарантиях и свободе доступа к информации»,** который определяет, что каждому гражданину гарантируется право доступа к информации, и государство защищает права каждого на поиск, получение, исследование, передачу и распространение информации [2]. Особо указано, что государственные органы, органы самоуправления граждан, общественные объединения, предприятия, учреждения, организации и должностные лица не могут предоставлять информацию, содержащую государственную или иную охраняемую законом тайну.

Поэтому злоумышленники могут предпринимать меры по взлому сайтов или других информационных ресурсов государственных органов и организаций. К примеру, 19 ноября 2013 г. хакерская группировка Bangladesh Grey Hat Hackers взломала веб-сайты газеты «Народное слово» и ее узбекской версии «Халқ сўзи». Аналогичный случай с республиканской газетой имел место и 27 марта 2016 г. Тогда на главных страницах сайтов была размещена заставка группы, называющей себя Anonplus. В результате взлома главные страницы газет были изменены. 20 ноября 2017 г. были недоступны сайты Министерства юстиции, хокимията Ташкента, Государственного центра тестирования и другие сайты государственных учреждений и организаций. При поиске адресов этих

сайтов в Google в результатах можно было увидеть фразу «Hacked By Skidie KhaN : TeaM Cyber CommandOs», что говорит об их дефейсе (замена главных страниц). Однако, к сожалению, в Уголовном кодексе не предусматривается специальная норма, устанавливающая ответственность за несанкционированный доступ к государственным информационным ресурсам и системам. Поэтому установление ответственности за подобные деяния является разумным шагом.

На сегодняшний день растет количество преступлений, связанных с электронной коммерцией. Поэтому необходимо также обратить внимание на уголовно-правовую охрану отношений, возникающих в электронной коммерции. Правовой основой электронной коммерции является Закон Республики Узбекистан «Об электронной коммерции». Использование в качестве пространства информационных систем с учетом особенности заключения договора в электронной коммерции (путем осуществления акцепта в виде электронного документа или электронного сообщения), является предпосылкой возможной потенциальной угрозы киберпреступности в данной сфере. На практике основная часть киберпреступлений, а именно 90% экономических преступлений в киберпространстве связаны с электронной коммерцией [6]. Именно в электронной торговой площадке могут возникнуть всевозможные кибератаки. В частности, по данным МВД РФ, отмечается устойчивый рост общих объемов потерь российских компаний от мошеннических и других действий при осуществлении сделок в электронной коммерции, так за последние три года для кредитно-финансовой отрасли в совокупности данный показатель увеличился на 26,8%, что в рублевом эквиваленте превышает 8,9 млрд руб.

Сегодня каждый человек может создать аккаунт, стать блогером и сообщать новости. Это огромная проблема, потому что эти люди нивелируют информационное поле. В странах арабской весны большинство активистов использовали социальную сеть в качестве ключевого инструмента в выражении своего недовольства правящим режимом. Активисты использовали Facebook для организаций протестов, Twitter для распространения информации, а YouTube, чтобы показать это всему миру. Такие понятия как «твиттер-революция» и «революция через социальные сети» прочно вошли в научный оборот именно после событий арабской весны. С учетом этого в 2014 г. было внесено изменение в законодательство Республики Узбекистан, устанавливающее ответственность блогера. Блогер – физическое лицо, размещающее на своем веб-сайте и (или) странице веб-сайта всемирной информационной сети Интернет общедоступную информацию общественно-политического, социально-экономического и иного характера, в том числе для ее обсуждения пользователями информации.

Согласно ст. 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.

При этом указано, что нарушение данных требований влечет за собой ответственность в соответствии с законодательством. Но, к сожалению, в действующем законодательстве Республики Узбекистан отсутствует специальная правовая норма, устанавливающая ответственность блогера.

2. Совершенствование государственной политики в области противодействия преступлениям в сфере информационных технологий и безопасности.

В настоящее время кибератаки представляют собой наиболее опасные угрозы, наносящие ущерб не только экономического характера, но и влияющие на сознание массы людей, особенно молодежи. Поэтому особую важность приобретает осуществление мер по предупреждению правонарушений среди молодежи, пропаганде здоровой атмосферы при использовании информационно-коммуникационных технологий, защите детей от негативного воздействия информационного пространства. Ни для кого не секрет, что Интернет в последнее время становится «площадкой» для вербовки и подготовки хакеров. К примеру, администрация сайта iso27000.ru «Искусство управления информационной безопасностью» приводит ссылки на сайты хакеров (hackzona.ru, inattack.ru, cracklab.ru), которые посвящены хакерским технологиям, вопросам взлома компьютерных систем и защите от взлома. На сайте http://hack-academy.ru/ приводятся рекомендации и советы начинающим хакерам для использования при взломе и несанкционированному доступу к приложениям и сайтам.

Свободное пользование средствами информационно-коммуникационных технологий и сетью Интернет может повлечь за собой определенные негативные последствия. К примеру, получив доступ к различным сайтам террористических и экстремистских организаций, пользователи (особенно молодежь) могут быть завербованы для участия в различных преступлениях, протестах или акциях.

К примеру, с начала своего существования ИГ создало мощную пропагандистскую структуру. С 2006 г. еще в период ИГИЛ было учреждено медиаагентство «Аль-Фуркан» («Различение добра и зла»), которое стало основным центром производства широкого спектра медиапродукции для распространения в сети Интернет. Данные медиаресурсы в основном осуществляют свою деятельность во Всемирной сети ввиду ее доступности.

Также Интернет становится очень удобной средой для различных обманщиков и мошенников, распространяющих различные неправдоподобные сообщения и идеи, фейковые новости. Можно привести знаменитый пример Уба Батлера, который с помощью фейковых комментариев сделал свой сад во дворе дачи лучшим рестораном на популярном портале. Идея журналисту пришла после того, как он написал несколько отзывов для других рестораторов на TripAdvisor за 10 €. В мае 2017 г. он разместил на TripAdvisor несуществующий ресторан. Перед этим он зарегистрировал название «Усадьба в Дульвиче», сделал сайт с меню и выложил туда фото блюд, сделанных из пены для бритья, губок и краски на столе во дворе своего дома. Уже в мае фиктивный ресторан был принят на TripAdvisor и «стартанул» с 18 149 места. Далее «шеф-повар» попросил всех своих знакомых с разных компьютеров написать рецензии на «сарай» и с легкостью обошел технологию Anti-scammer, которой портал защищается от фейков. К 1 ноября «Усадьба в Дульвиче» (у которой, к слову, даже не указан адрес) стала лучшим рестораном Лондона по версии TripAdvisor, получив 89 тыс. просмотров за день. Поэтому, среди социальных мер важное значение имеет пропаганда среди молодежи своеобразной «виртуальной культуры и этики» (культура поведения в сети Интернет). В противном случае, молодежь будет перенимать негативный опыт использования сети Интернет. В этих целях считаем целесообразным принять Государственную программу по формированию Интернет-культуры, включающей 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.

На наш взгляд, наступил момент для 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.

Одним из ключевых вопросов организации борьбы с информационной преступностью является формирование в системе правоохранительных органов специальных подразделений, обученных и подготовленных к эффективному решению задач противодействия исследуемым явлениям. В качестве примера подобной организации дела можно привести Национальный отдел по борьбе с преступностью в сфере высоких технологий (National Hi-Tech Crime Unite), созданный в Великобритании, Центр управления по борьбе с преступлениями в области информатики и коммуникаций (Франция), Национальный центр защиты инфраструктуры США (USA National Infrastructure Protection Center), созданное в 1998 г. Управление компьютерной и информационной безопасности ФСБ Российской Федерации. В Республике Узбекистан в 2005 г. в соответствии с постановлением Президента Республики Узбекистан от 5 сентября 2005 г. №167 «О дополнительных мерах по обеспечению компьютерной безопасности национальных информационно-коммуникационных систем» была создана Служба реагирования на компьютерные инциденты Центра UZINFOCOM, в свою очередь, на основании постановления Кабинета Министров Республики Узбекистан «О мерах по организации деятельности Центра информационной безопасности и содействия в обеспечении общественного порядка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан» от 17 октября 2017 г. № 838 ведет свою деятельность Центр информационной безопасности и содействия в обеспечении общественного порядка. При этом деятельность данных подразделений направлена на сбор и анализ информации по компьютерным инцидентам, консультативную и техническую поддержку пользователям в предотвращении угроз компьютерной безопасности. Обнаружив инциденты или угрозы информационной безопасности, указанные подразделения обращаются в правоохранительные органы, следовательно, не в полной мере участвуют в правоохранительной деятельности. Поэтому, важное значение имеет создание специального подразделения по борьбе с киберпреступлениями. Мы считаем целесообразным создать специализированный Центр по борьбе с киберпреступлениями и обеспечению информационной безопасности при Службе государственной безопасности Республики Узбекистан.

Безусловно, специализация данного подразделения повысит эффективность борьбы с киберпреступлениями за счет адекватной концентрации мер уголовно-правового воздействия. Целесообразно, наряду с центральным координирующим и руководящим ведомством, создавать соответствующие службы, специализирующиеся в борьбе с киберпреступлениями на принципе территориальной концентрации (на уровне регионов и областей).

Одной из важных задач является также укрепление материально-технической базы подразделений, специализирующихся в борьбе с инцидентами в сфере информационных технологий и безопасности. Практика показывает, что нынешнее состояние технической оснащенности подразделений значительно отстает от киберпреступников, которые на данном этапе используют современные информационно-коммуникационные технологии и специальные средства. Такое «опережение» преступного мира в виртуальном пространстве негативно влияет на раскрытие информационной преступности и привлечение виновных к ответственности. Следовательно, осуществление профилактических функций практически невозможно. Все мировое сообщество акцентирует свое внимание на предупреждении и профилактике компьютерных правонарушений, при этом выделяя огромные средства на укрепление и совершенствование современных, передовых методов упреждения вызовов и угроз. Поэтому, на наш взгляд, в Республике следует создать **специальную лабораторию** при Центре информационной безопасности и содействия в обеспечении общественного порядка для проведения испытательных и исследовательских работ, а также тестирования средств защиты в области информационной безопасности. Данная лаборатория будет осуществлять функции своеобразного «полигона» по испытанию новейших средств защиты от компьютерных вирусов, вредоносных программ, взломов и т.д. К примеру, в России, Беларуси, Венгрии и ряде государств существуют аналогичные компании по обеспечению информационной безопасности, деятельность которых направлена на защиту информации ограниченного доступа в органах государственной власти, государственных учреждениях и предприятиях, организациях банковской системы и коммерческом секторе. Опыт технологий Trend Micro Smart Protection Network позволил заблокировать более 81 миллиардов угроз в 2016 г., что на 56% больше, чем в 2015 г. Во второй половине 2016 г. блокировалось, в среднем, более 3 тыс. атак в секунду на клиентов компании. За этот период 75 миллиардов угроз получено через электронную почту.

Противодействие преступлениям в сфере информационных технологий и безопасности требует от государства проведения действенной и обдуманной политики, свидетельствует о необходимости систематизации и конкретизации основ государственной политики в сфере информационной безопасности. С этой целью считаем целесообразным принять Концепцию информационной безопасности Республики Узбекистан. В Концепции информационной безопасности на основе анализа современного состояния информационной безопасности должны быть определены цели, задачи и выявлены ключевые проблемы обеспечения информационной безопасности.

При этом в ней следует предусмотреть объекты, угрозы информационной безопасности и возможные их последствия, методы и средства предотвращения, парирования и нейтрализации угроз, а также особенности обеспечения информационной безопасности в различных сферах деятельности государства.

Концепция станет основой государственной политики обеспечения информационной безопасности в Республике Узбекистан, в которой будут изложены организационная структура и принципы построения системы информационной безопасности.

Таким образом, на современном этапе развития Республики Узбекистан, на наш взгляд, следует предусмотреть и расширить круг преступлений в сфере информационных технологий и безопасности, предусмотрев новые составы преступлений – преступления в сфере электронной коммерции, «взлом» государственных информационных ресурсов, распространение недостоверной информации блогерами, а также разработать Концепцию информационной безопасности Республики Узбекистан, соответствующие нормативно-правовые акты в сфере информационных технологий и безопасности. В свою очередь, необходимо принять комплекс мер по совершенствованию организационных и технических мер по противодействию преступлениям в сфере информационных технологий и безопасности, в частности создать «Клуб молодых программистов-патриотов», специальную лабораторию при Центре информационной безопасности и

содействия в обеспечении общественного порядка для проведения испытательных и исследовательских работ, а также тестирования средств защиты в области информационной безопасности, а также специализированный Центр по борьбе с киберпреступлениями и обеспечению информационной безопасности при Службе государственной безопасности Республики Узбекистан.

Литература

1. Уголовный кодекс Республики Узбекистан (источник www.lex.uz).
2. Закон Республики Узбекистан «О гарантиях и свободе доступа к информации» от 24 апреля 1997 года № 400-I.
3. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 года № 560-II.
4. Указ Президента Республики Узбекистан «О Стратегии действий по дальнейшему развитию Республики Узбекистан» от 7 февраля 2017 года № УП-4947 (Собрание законодательства Республики Узбекистан, 2017 г., № 6, ст. 70).
5. Постановление Президента Республики Узбекистан от 14 мая 2018 года № ПП–3723 «О мерах по кардинальному совершенствованию системы уголовного и уголовно-процессуального законодательства».
6. *Чупрова А.Ю., Яцеленко Б.В.* Электронная коммерция как вид экономической преступности. Вестник Нижегородской академии МВД России. – 2017. – № 3 (39). – С. 239–240.