ПОНЯТИЕ И ОСОБЕННОСТИ ПРЕСТУПЛЕНИЙ КИБЕРТЕРРОРИЗМА

Аминов Шариф Насимович
доцент Академии МВД Республики Узбекистан, PhD

Аннотация: *В данной статье изложены понятие преступлений кибертерроризма, их признаки и классификация. Также проанализированы понятия, связанные с совершением актов кибертерроризма в информационном пространстве, и особенности совершения данных преступлений.*

Ключевые слова: *Информация, банк, ответственность, преступление, персональные данные, киберпреступления, кибертерроризм, регулятор, понятия.*

Как известно, распространение киберпреступлений в мировом масштабе стремительно развивается с каждым днём. В связи с этим вопросы понимания проблемы киберпреступности становятся одними из важнейших для современного общества. В разные периоды киберпреступления получали различные доктринальные и официальные определения в зависимости от уровня развития информационно-коммуникационных технологий.

Развитие научно-технического прогресса стало причиной появления киберпреступлений, которые сегодня рассматриваются как одна из глобальных проблем человечества. К ним относятся распространение вредоносных программ, взлом паролей, хищение средств с кредитных карт и других банковских реквизитов, присвоение денежных средств, а также распространение незаконной информации через интернет — в частности, клеветы, морально разлагающих материалов, что представляет серьёзную угрозу для общества и безопасности жизни людей.

С целью предотвращения таких угроз в Уголовный кодекс введена совершенно новая глава, устанавливающая ответственность за компьютерные преступления, и регулирующая уголовно-правовые аспекты совершения связанных с ними деяний.

В частности, говоря об анализе законодательства, регулирующего расследование киберпреступлений, нельзя не отметить, что основой соответствующего законодательства по праву считается Конституция Республики Узбекистан — наш основной закон. В соответствии с Конституцией, каждый имеет право свободно искать, получать, изучать, распространять, использовать и хранить информацию. Ограничение получения информации допускается только в соответствии с законом и исключительно с целью охраны прав и свобод человека, основ конституционного строя, моральных ценностей общества, духовного, культурного и научного потенциала страны, а также обеспечения её безопасности.

В нормативно-правовой базе, регулирующей расследование подобных преступлений, предусмотрен ряд документов. В частности, 11 декабря 2003 года был принят Закон Республики Узбекистан "Об информатизации", в котором даны определения таким понятиям, как "информатизация", "информационный ресурс", "информационные технологии".

Данный закон регулирует государственную политику в области информатизации, государственное регулирование этой сферы, порядок использования информационных ресурсов, распространение информации общего пользования в сети Интернет, подключение к национальным и международным информационным системам и сетям.

В киберпреступлениях компьютер или информация могут выступать как цель, объект преступления, либо как средство совершения правонарушения, предоставляя необходимые данные для такого преступления. Все эти виды деяний подпадают под широкое определение термина "киберпреступление".

Киберпреступления — это преступления, основанные на технологии, при которых компьютер или сам интернет используются в качестве орудия или средства для совершения таких преступлений. Они относятся к числу организованных и «беловоротничковых» преступлений и включают кибермошенничество, хакерство, кражу данных, фишинг, похищение идентификаторов и другие подобные деяния.

Киберпреступления совершаются преступниками, глубоко понимающими технологию, с использованием её возможностей. По сути, киберпреступники — это технократы, разбирающиеся в тонкостях информационных технологий.

Кроме того, через компьютерную систему, сеть или иные подключаемые к ним средства либо при их помощи, а также в киберсреде против компьютерной системы, сети или компьютерной информации совершаются общественно опасные деяния, которые квалифицируются как киберпреступления; при этом указанные выше правонарушения часто противопоставляются понятиям «киберпреступление» и «иные преступления».

Действительно, целесообразно признать, что преступления в сфере информационных технологий являются частью киберпреступлений, а само понятие «киберпреступления» имеет более широкий смысл.

Следует также отметить, что понятие преступности в глобальной сети не полностью совпадает с ранее употреблявшимся понятием «компьютерная преступность», поэтому в настоящее время этот вид преступлений чаще обозначается термином «киберпреступность».

В международной научной и правовой практике первоначально использовались понятия «компьютерная преступность», затем — «преступления, связанные с компьютером», «совершение преступления через компьютер», «электронная преступность», «преступность высоких технологий»,

«виртуальная преступность», а сегодня применяются термины «киберпреступность» или «преступность глобальной сети».

Здесь также важно подчеркнуть, что масштабы кибертерроризма и угрозы, которые он представляет для общественной жизни, растут. Кибертеррористическое действие (кибернападение) — это политически мотивированное деяние, осуществлённое с помощью компьютеров и средств информационно-коммуникационных технологий, которое прямо или потенциально может угрожать жизни и здоровью людей, наносить значительный материальный ущерб или привести к таковому, а также иметь целью или приводить к возникновению социально опасных последствий.

Для современных террористов привлекательность использования киберпространства связана с тем, что проведение кибератак не требует больших финансовых затрат. По мнению экспертов, под предлогом содействия развитию развивающихся стран и утверждения общечеловеческих демократических принципов, осуществляется влияние на сознание граждан с целью подчинения их своей воле различными способами.

К сожалению, в этом процессе всё чаще наблюдаются попытки организовывать кибератаки, эффективно используя безграничные возможности глобальной интернет-сети. Роль социальных сетей, существующих в интернете, их разработчиков и спонсоров во «вмешательстве» во внутренние дела суверенных государств до конца не изучена, в результате чего такое «вмешательство» до сих пор официально не признаётся как направленное против этих государств. Не разработаны международные правовые основания для привлечения к ответственности владельцев социальных сетей за размещение на их страницах призывов к свержению государственного строя.

Между тем каждое совершённое преступное деяние или бездействие по своей сути и содержанию не должно оставаться безнаказанным. Интернет-сайты могут внезапно появляться, затем часто менять формат или адрес. Поэтому некоторые эксперты предлагают отказаться от изначальной концепции полной открытости интернета и перейти к его новой модели. Суть этой новой модели заключается в отказе от анонимности пользователей сети, что позволит обеспечить большую защищённость от преступных посягательств.

Кроме того, необходимо принимать соответствующие решения по расследованию и выявлению киберпреступлений и киберправонарушений, их предотвращению и устранению. Также важно участвовать в разработке проектов нормативно-правовых актов по борьбе с киберпреступностью, кибертерроризмом, киберэкстремизмом и организованной преступностью, а также в выявлении и противодействии киберугрозам, направленным против интересов государственных органов и кибербезопасности. Следует проводить доследственные проверки и предварительное расследование киберпреступлений, осуществлять оперативно-розыскную деятельность,

выявлять и устранять причины и условия, способствующие совершению киберпреступлений, угрожающих правам и свободам граждан.

Кибертерроризм — это применение насилия, силы, либо совершение иных действий с использованием кибертехнологий, угрожающих личности или имуществу, либо угроза их совершения в целях:

- дестабилизации международных отношений;
- нарушения суверенитета и территориальной целостности государства;
- подрыва его безопасности;
- развязывания войны и вооружённых конфликтов;
- дестабилизации социально-политической обстановки;
- запугивания населения.

Целями также являются принуждение государственных органов, международных организаций, их должностных лиц, физических или юридических лиц к совершению или отказу от определённых действий, попытки дестабилизировать ситуацию, повлиять на принятие решений государственными органами или воспрепятствовать политической или иной общественной деятельности, в том числе покушения на жизнь государственных или общественных деятелей в связи с их деятельностью.

В уголовном законодательстве Республики Узбекистан преступления в области информационных технологий условно можно разделить на общие и специальные виды.

К специальным преступлениям в области информационных технологий отнесены нормы, включённые в Главу XX1 Уголовного кодекса, тогда как положения, содержащиеся в прочих статьях, признаются общими преступлениями в сфере информационных технологий.

При анализе данных видов преступлений целесообразно прежде всего рассмотреть преступления в области информационных технологий, входящие в Главу XX1 Уголовного кодекса. Эта глава состоит из семи статей. Статья 2781 направлена на регулирование преступлений, связанных с нарушением правил информатизации. За совершение такого преступления — то есть за нарушение правил информатизации, а также за создание, внедрение и использование информационных систем, баз данных и банков данных, систем обработки и передачи информации без принятия установленных мер защиты, а также за использование информационных систем с разрешения (рухсат билан фойдаланиш) — если это повлекло причинение значительного ущерба либо серьёзного вреда правам граждан или охраняемым законом интересам, либо государственным или общественным интересам, — предусмотрена соответствующая уголовная ответственность.

Кроме того, статья 2782 Уголовного кодекса Республики Узбекистан посвящена противоправному (несанкционированному) использованию компьютерной информации. Под этим понимается незаконное

(несанкционированное) использование информации, содержащейся в информационно-вычислительных системах, их сетях и структурных элементах; если такие действия приводят к уничтожению, блокированию, модификации информации, созданию её копий или её похищению, либо нарушению работы электронных вычислительных машин, системы ЭВМ или их сетей, за это предусмотрена уголовная ответственность в установленном порядке.

В Уголовном кодексе Республики Узбекистан статья 278^3 посвящена подготовке, передаче и распространению специальных средств, предназначенных для противоправного (несанкционированного) использования компьютерной системы. Под этим понимается создание, передача и распространение программных или аппаратных средств с целью несанкционированного доступа к защищённым компьютерным системам.

Статья 278^4 УК посвящена преступлению, связанному с модификацией компьютерной информации. Это включает в себя противоправное изменение информации, хранящейся в компьютерной системе, её повреждение, удаление, а также умышленное внесение ложной информации. Если такие действия повлекли причинение значительного ущерба правам граждан, охраняемым законом интересам либо государственным или общественным интересам, наступает уголовная ответственность.

Статья 278^5 УК Республики Узбекистан касается компьютерного саботажа и предусматривает ответственность за умышленное выведение из строя чужого компьютерного оборудования, в том числе используемого в служебной деятельности, а также за нарушение работы компьютерной системы (компьютерный саботаж).

Статья 278^6 УК регулирует ответственность за создание, использование или распространение вредоносных программ, то есть за общественно опасные деяния, связанные с такими действиями.

Статья 278^7 УК касается противоправного (несанкционированного) использования телекоммуникационных сетей, в частности, за использование таких сетей в обход установленных систем защиты и за проведение международного трафика без соответствующего разрешения.

Статья 278^8 УК предусматривает уголовную ответственность за незаконное приобретение, передачу или обмен криптоактивов, а также за осуществление деятельности в сфере оборота криптоактивов без получения лицензии в установленном порядке или за проведение операций с анонимными криптоактивами провайдерами таких услуг после применения к ним административного взыскания.

Статья 278^9 УК охватывает деяния, связанные с незаконным осуществлением майнинговой деятельности. В частности, сюда относятся майнинг анонимных криптоактивов или нарушение установленного порядка при ведении майнинга после применения административной ответственности.

В качестве предложения следует отметить необходимость совершенствования главы XX[1] Уголовного кодекса. В частности, целесообразно пересмотреть диспозицию статьи 278[2]. Вместо формулировки:

«Незаконное (несанкционированное) использование компьютерной информации, то есть информации, содержащейся в информационно-вычислительных системах, сетях и их составных частях, если такие действия привели к уничтожению, блокированию, модификации, копированию или завладению информацией, нарушению работы ЭВМ, их систем или сетей»,

предлагается использовать формулировку: «Незаконное (несанкционированное) использование данных цифровых информационных систем, если такие действия повлекли уничтожение, блокирование, модификацию, копирование или завладение информацией, либо нарушение функционирования цифровых технологических систем».

Учитывая уровень современного технологического развития, включая расширение видов преступлений, связанных с киберпреступностью, можно отметить, что глава XX[1] УК не охватывает весь спектр киберпреступлений. С учётом опыта развитых зарубежных государств, рекомендаций, содержащихся в международно признанных конвенциях, а также анализа текущих глобальных информационных атак, представляется целесообразным дополнить Уголовный кодекс положениями, предусматривающими уголовную ответственность за отдельные виды киберпреступлений.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Указ Президента Республики Узбекистан № ПФ-209 от 21 декабря 2023 года «О мерах по коренному повышению роли института махалли в обществе и обеспечению его функционирования в качестве первичного звена по решению проблем населения».

2. Таштемиров А. А. и др. Зўравонлик билан боғлиқ ҳуқуқбузарликлар профилактикаси тушунчаси ва ўзига хослиги //Innovative achievements in science 2024. – 2025. – Т. 4. – №. 37. – С. 82-90.

3. Tashtemirov A., Raxmonqulov S. Profilaktika inspektorining yashash manzillaridan uzoq muddatga ketgan shaxslar bilan ishlash faoliyatining tushunchasi //Общественные науки в современном мире: теоретические и практические исследования. – 2024. – Т. 3. – №. Maxsus son 12. – С. 62-67.

4. Tashtemirov A., Sadullaev M. Huquqbuzarliklar profilaktikasini amalga oshirishda iiolari profilaktika inspektorlarining bojxona xizmati bilan xamkorligining tashkiliy-huquqiy asoslari //Общественные науки в современном мире: теоретические и практические исследования. – 2024. – Т. 3. – №. Maxsus son 12. – С. 50-53.

5. Tashtemirov A., Baxtiyorov S. Profilaktika inspektorining jinoyat ishlar bo ‘yicha sudlar bilan hamkorligining o ‘ziga xos xususiyatlari //Общественные науки в современном мире: теоретические и практические исследования. – 2024. – Т. 3. – №. Maxsus son 12. – С. 38-42.

6. Аминов Ш. Н., Мирсалихова Г. А. Ёшларда экстремизмга қарши иммунитетни шакллантириш йўналишлари //Innovation in the modern education system. – 2025. – Т. 6. – №. 49. – С. 215-225.

7. Tashtemirov A., Usmonova Y. Profilaktika inspektorining yashash manzillaridan uzoq muddatga ketgan yoshlar bilan ishlash faoliyatining o ‘ziga xos xususiyatlari //Общественные науки в современном мире: теоретические и практические исследования. – 2024. – Т. 3. – №. 12. – С. 51-52.

8. Tashtemirov A., Usmonova Y. Profilaktika inspektorining yashash manzillaridan uzoq muddatga ketgan shaxslar bo’yicha ishlash faoliyatini huquqiy ta’minlash //Наука и технология в современном мире. – 2024. – Т. 3. – №. 12. – С. 59-61.

9. Асракулов М. М., Машарипов Т. Э. Ёшлар-келажак бунёдкори //Journal of new century innovations. – 2022. – Т. 18. – №. 5. – С. 293-300.

15. Асракулов М. М., Машарипов Т. Э. Сущность оперативной техники и правовая основа ее использования в борьбе с преступностью. – 2022.

10. Аминов Ш. Н. Терроризм ва экстремизмнинг жамият барқарорлигига таҳдиди //Journal of innovations in scientific and educational research. – 2025. – Т. 8. – №. 2. – С. 15-22.

11. Аминов Ш. Н. Возникновение терроризма, а также факторы, его вызывающие //Международная конференция академических наук. – 2024. – Т. 3. – №. 10. – С. 167-173.

12. Мирзахмедов А. М., Аминов Ш. Н., Холматов Ғ. М. Таълим сифати–ижтимоий тараққиёт омили //Academic research in educational sciences. – 2023. – Т. 5. – №. NUU Conference 2. – С. 424-432.

13. Холматов Ғ. М., Аминов Ш. Н. Фарғона водийсида жадидлик: миллий маданият муаммолари //Academic research in educational sciences. – 2023. – Т. 5. – №. NUU Conference 2. – С. 848-856.

14. Асракулов М. М., Мирсалихова Г. А. Ички ишлар органлари тезкор-қидирув фаолиятининг вазифаларини ҳал этишда овоз ёзиш воситаларини қўллаш тартиби //Models and methods for increasing the efficiency of innovative research. – 2025. – Т. 4. – №. 44. – С. 268-276.

15. Таштемиров А. А. и др. Жамиятда фуқароларнинг хуқуқий онги ва маданиятини юксалтиришда иио профилактика инспекторларининг асосий вазифалари //Scientific approach to the modern education system. – 2025. – Т. 3. – №. 35. – С. 91-96.