

**Азим Шухрат** – доктор философии  
по юридическим наукам (PhD)  
заместитель начальника  
Исследовательского института  
криминологии Республики  
Узбекистан

**Международное сотрудничество - необходимое условие  
эффективности обеспечения кибербезопасности  
на национальном уровне.**

Тенденции преступности сложны и противоречивы, что особенно наглядно выявляется при исследовании ее динамики за значительные промежутки времени. Влияние оказывают многие факторы. Одним из таких факторов выступает научно-технический прогресс и происходящие в его рамках интеллектуально-промышленные поистине революционные изменения, влекущие как появление новых сфер общественных отношений, так и усложнение уже функционирующих. При этом, что уже подтверждено практикой, научно-технический прогресс и все его составляющие обладают сильной деликтогенностью, постоянно вызывая к жизни всё новые и новые составы правонарушений, усложняя и делая более опасными уже традиционно известные. Это напрямую относится и к киберпространству, в котором с геометрической прогрессией происходят постоянные трансформации, причем не только положительного свойства, но и отрицательно влияющие на функционирующие в социальной жизни общественные отношения. Всё это актуализировало проблему необходимости обеспечения охраны, профиликтирования и предупреждения посягательств, осуществляемых в киберпространстве, общепризнанно обозначаемых большинством ученых и практикующих юристов как самостоятельное явление современности – киберпреступностью.

Об усложнении криминогенной обстановки в киберпреступности и нарастании криминальных проявлений в этой сфере, свидетельствует значительный рост жертв от кибератак, причем как физических, так и юридических лиц, не говоря уже об имиджевых потерях государственных и других структур власти, суммы как прямых, так и косвенных финансовых потерь и убытков.

В опубликованных источниках приводятся сведения об атаках на организации по континентам за 2021 год в процентном отношении по

количеству: Азия - 26%; Европа - 24%; Северная Америка - 23%; Ближний Восток и Африка -14%; Латинская Америка-13%.

Для полноты криминологической характеристики киберпреступности важно акцентировать внимание на профессиональном характере преступных посягательств, на безопасность в сфере информационных технологий. Основываясь на этом предварительном замечании следует констатировать, что с криминологической, и с уголовно-правовой позиций, мы имеем дело с таким явлением современности, как организованная преступность.

С позиции нашего анализа важно подчеркнуть, что киберпреступность в обязательном порядке характеризуется и международными связями.

Представляется правильным выделить двух разновидностей организованной преступности: общеуголовной и хозяйственно-экономической, последняя из которых, образуя разновидность профессиональной преступности непосредственно и должна характеризовать киберпреступность.

В качестве правовой основы международного сотрудничества в сфере борьбы с киберпреступностью может служить Конвенция Совета Европы о преступности в сфере компьютерной информации (ETS №185), подписанная 23 ноября 2001 года в Будапеште. Она открыта для подписания как государствами-членами Совета Европы, так и странами, которые не являются членами, но которые приняли участие в составлении и во вступлении других стран не членом.

Конвенция Совета Европы о компьютерных преступлениях (ETS №185) подразделяет преступления в киберпространстве на четыре группы.

В Республике Узбекистан сформирована правовая основа борьбы с киберпреступностью. В соответствии с Законом Республики Узбекистан от 25 декабря 2007 года (ЗРУ-137) Уголовный кодекс был дополнен самостоятельной главой XXI, предусматривающей ответственность за преступления в сфере информационных технологий, а в некоторые другие статьи Особенной части были включены в качестве квалифицирующих и особо квалифицирующих признаков, преступления, совершаемые с использованием средств компьютерной техники, сетей телекоммуникаций, а также всемирной информационной сети Интернет.

В современном, постоянно меняющемся мире, в условиях постоянного совершенствования технологий, необходим постоянный мониторинг как со

стороны технических специалистов, так и со стороны правоведов. Совершенствующиеся методы криминальных проявлений в сфере кибербезопасности требуют своевременного реагирования и в первую очередь на законодательном уровне.

Общепризнанно, что преступления в сфере информационных технологий очень часто являются международными. Учитывая это, следует обратить внимание на такой институт Общей части УК, как действие уголовного закона в пространстве. В международной законотворческой практике наряду с территориальным, гражданства и универсальным принципами действия уголовного закона в пространстве, которые присущи и законодательству Узбекистана, предусматривается также и реальный принцип. Как отмечается в литературе, сущность реального принципа действия уголовного закона в пространстве состоит в том, что государство признаёт возможным привлечение к уголовной ответственности иностранных граждан и лиц без гражданства или без гражданства, постоянно не проживающих на его территории, за преступления, направленные против интересов этого государства, даже если эти преступления не совершены на его территории и не предусмотрены международными договорами. Поскольку при киберпреступности нередки случаи совершения посягательств на интересы республики Узбекистан и его граждан вне пределов нашего государства, необходимо распространить действия УК РУз и на такие криминальные проявления.

Основываясь на реальном принципе действия УК в пространстве считается целесообразным изложить редакцию ч.3 статьи 12 УК РУз следующим образом: «иностранные граждане и лица без гражданства, не проживающие постоянно на территории Республики Узбекистан, подлежат уголовной ответственности по настоящему Кодексу в случаях, если преступление направлено против интересов Республики Узбекистан, и в случаях, предусмотренных международным договором Республики Узбекистан, если они не были осуждены в иностранном государстве и привлекаются к уголовной ответственности на территории Республики Узбекистан».