

КИБЕРПРЕСТУПНОСТЬ И НАРКОБИЗНЕС КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН

Нурпеисова А.К., Феткулов А.Х., Койлыбаева А.Е., Молдабеков А.Т.
гор. Караганда, РК

Аннотация: рассматриваются вопросы национальной безопасности, а также механизмы защиты прав и законных интересов объектов в информационной сфере, в соответствии с действующим уголовным законодательством, связанных с киберпреступностью и наркобизнесом.

Ключевые слова: национальная безопасность, информационная безопасность, киберпреступность, наркобизнес, интернет, информационные технологии.

Как известно, 19-ый век называли веком производства, 20-ый веком управления, а 21-ый век по праву именуют веком информации.

Сегодня мы все являемся очевидцами повышения значимости информации как для себя лично, так для государства и общества в целом. Важную роль в сознательном проектировании информационных процессов играет право, с помощью которого не только регулируются сложившиеся отношения, но и происходит расширение сферы информационной деятельности, которая связана с общественными потребностями.

Под информационной безопасностью следует понимать защиту интересов субъектов информационных отношений, складывающихся во всех сферах жизнедеятельности общества: экономической, административно-политической, социальной. Впрочем, речь идет о состоянии защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Стремительное внедрение цифровых технологий во все сферы человеческой жизни в конце XX - начале XXI вв. предопределило возникновение новых общественных отношений. В связи с развитием компьютерных технологий, прежде всего всемирной электронной сети Интернет, в международном законодательстве появился новый термин «киберпреступность». Киберпреступность на сегодняшний день является одной из наиболее серьезных угроз для национальной безопасности страны в информационной сфере.

Под преступлениями, совершенными в сфере информационных технологий, следует понимать предусмотренные уголовным законом виновные общественно опасные деяния, направленные на нарушение неприкосновенности охраняемой законом электронной информации и ее материальных носителей, совершаемые в процессе создания, использования и распространения электронной информации, а также направленные на нарушение работы информационной системы или сетей телекоммуникаций, причиняющие вред законным интересам собственников или владельцев, жизни и здоровью личности, правам и свободам человека и гражданина, национальной безопасности, где предметом выступает компьютерная информация.

В свое время на X Конгрессе ООН по предупреждению преступности и обращению с правонарушителями компьютерные преступления были подразделены на две категории: 1) любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем (сетей) и обрабатываемых ими данных (в узком смысле); 2) любое противоправное деяние, совершенное посредством или связанное с компьютерами, компьютерными системами

или сетями, включая незаконное владение и предложение или распространение информации посредством компьютерных систем или сетей (в широком смысле — как преступление, связанное с компьютерами).

Надо сказать, что общий объем рынка телекоммуникаций, связанных с глобальной компьютерной сетью Интернет стремительно растет, но, как и любое прогрессивное техническое явление, Интернет привнес в нашу жизнь, сколько позитивного, столько и негативного.

С сожалением приходится констатировать, что и мировой наркобизнес использует в своих целях «всемирную паутину».

Речь идет об эксплуатации Интернета с целью незаконного расширения возможностей наркобизнеса. Эксперт ООН, координатор Программы ООН по контролю над наркотиками Сандип Шоула сделал заявление, что Интернет стал тайной лабораторией для изготовления синтетических наркотиков. Согласно приведенным им сведениям, сеть Интернет оказалась засорена рецептами производства и потребления наркотиков, главным образом синтетических препаратов новых поколений. По сравнению с другими государствами, такое использование Интернета в нашей стране еще только разворачивается, но имеется российская специфика распространения негативной информации о наркотиках на веб-страничках русскоязычной сети Интернет. Репрезентативный анализ веб-страничек, отведенных под рубрику «наркотики», показывает, что свыше 80 процентов отводится информации негативной. При этом подавляющая доля информации - 77,8 процента - касается так называемых тяжелых, или жестких, наркотиков типа амфетаминов, галлюциногенов и прочих. Этот показатель для русскоязычного Интернета в 1,5 раза выше, чем для Интернета в глобальных масштабах. А «жесткие» наркотики - одни из самых опасных, и привыкают к ним быстрее, и последствия значительно тяжелее. Еще более удручает картина, которая складывается с информацией о полусинтетических наркотиках (героин, морфий и другие). В русскоязычных файлах о наркотиках, информация о героине и морфии встречается почти в 5 раз чаще, чем в Интернете в целом. Содержательный анализ рекламы о наркомании и незаконном обороте наркотиков показывает, что, к примеру, в российской информационной системе Интернет она носит крайне разнузданный характер и отличается откровенным нигилизмом по отношению к закону, не говоря уже об общественной нравственности.

Использование Интернета как инструмента незаконного распространения наркотиков, их рекламы также относится к разряду киберпреступлений, поэтому киберпреступления в наркобизнесе, это проблемы, которые приходится решать правоохранительным органам и спецслужбам в борьбе с ними [1].

Современные компьютерные технологии способствовали интеграции экономики в единую глобальную систему, состояние которой в значительной степени определяется функционированием фондовых бирж и рынков капитала. Однако технический прогресс и глобализация в сфере торговли и финансовой деятельности открыли возможности не только для социального развития, но и для появления новых и развития традиционных форм преступности.

Во всех регионах мира создаются механизмы для изучения преступлений, связанных с использованием высоких технологий, и принятия соответствующих ответных мер. В некоторых регионах основное внимание уделяется борьбе с мошенничеством, детской порнографией и хакерством, а в других основными проблемами считаются отмывание денег и экономическая преступность. В свете

событий, произошедших в последнее время, особое внимание уделяется теперь проблеме использования террористическими организациями новых технологий.

Наиболее значимым на сегодняшний день результатом международного сотрудничества в борьбе с преступностью, связанной с использованием высоких технологий, является Конвенция Совета Европы о киберпреступности. В подготовке текста участвовали 43 государства — члены Совета, а также Канада, Япония, Соединенные Штаты (имеющие статус наблюдателей) и Южно-Африканская Республика. В Конвенции затрагиваются вопросы юрисдикции, выдачи, перехвата сообщений, а также формирования и сохранения данных. В ней перечисляются деяния, которые должны быть признаны уголовно наказуемыми согласно национальному законодательству, в том числе: несанкционированный доступ, незаконный перехват данных, нарушение целостности данных, нарушение целостности систем, связанный с использованием компьютеров подлог, связанное с использованием компьютеров мошенничество, пособничество или подстрекательство к совершению этих преступлений.

В Конвенции подробно рассматривается механизм налаживания эффективного международного сотрудничества и координации при проведении расследований и уголовном преследовании. В частности, стороны этой конвенции должны будут наделить национальные органы полномочиями производить компьютерный поиск и изымать компьютерные данные.

В рамках дел, связанных с наркотиками, конвенция будет применяться в качестве средства обеспечения взаимной юридической помощи. Например, компетентные органы, стремящиеся получить электронные доказательства деятельности торговцев наркотиками и обнаружить их клиентов или их активы в другом государстве, смогут обращаться к такому государству с просьбой о поиске баз данных, которые использовались подозреваемыми в занятии наркобизнесом лицами, или о перехвате их электронных сообщений, например электронной почты.

Тем не менее, частный бизнес и гражданские объединения выступают против некоторых положений конвенции о киберпреступности. Консорциум ассоциаций, объединяющих предприятия по производству информационных технологий, заявил о своих возражениях в связи с тем, что конвенция, по его мнению, возлагает на поставщиков услуг в сети Интернет обременительные обязанности по сохранению данных и ответственность за действия третьих сторон, а также ограничивает масштабы законной деятельности в Интернете. Группы борьбы за гражданские свободы сделали аналогичные заявления о своей обеспокоенности предусмотренными в конвенции мерами, которые, по их мнению, представляют собой посягательство на неприкосновенность частной жизни.

Международный комитет ООН по контролю над наркотиками (МККН) считает, что такой правовой документ может способствовать осуществлению усилий по борьбе с незаконным оборотом наркотиков и злоупотреблением ими.

В Республике Казахстан острой проблемой также является слабое развитие отечественной индустрии информационной безопасности. И этому причиной являются крупные иностранные компании-гиганты. К примеру, когда государственными органами и иными организациями объявляются конкурсы на закуп определенных средств защиты информации, то выигрывают компании, фактически являющиеся партнерами ведущих иностранных производителей. То есть иностранные компании-гиганты через своих представителей в Казахстане не дают возможность встать на ноги отечественным стартап-компаниям. Истинно отечественные разработчики, которым требуется время и

деньги на разработку отечественных средств защиты информации и иных программно-технических продуктов, остаются в проигрыше, так как предоставить готовую продукцию в течение установленного срока в рамках закона о государственных закупках не представляется возможным. Поэтому требуется принятие определенных мер, в том числе законодательных, по стимулированию отечественных стартап-компаний по производству продукции в области защиты информации.

Что касается уголовного законодательства, регламентирующего информационно-правовые отношения, то с января 2015 года введен в действие новый Уголовный кодекс, которым введено понятие уголовное правонарушение, которое состоит из преступления и уголовного проступка [2]. Другими словами, если ранее за употребление наркотических средств была предусмотрена только административная ответственность, то сейчас эта ответственность уголовная. Если человек употребляет наркотики в общественных местах, он подлежит уголовной ответственности, поскольку совершил уголовный проступок, предусмотренный ст.296 ч.1 Уголовного кодекса РК [3].

Более того появилась целая глава в Особенной части УК РК «Уголовные правонарушения в сфере информатизации и связи»[3].

На сегодняшний день существует ряд законов регулирующих информационно-правовые отношения, складывающихся в различных сферах жизнедеятельности общества: Закон РК «Об информатизации», Закон РК «О связи», Закон РК «О средствах массовой информации», Закон РК «О государственных секретах», Закон РК «Об авторских и смежных правах», Закон РК «О рекламе», Закон РК «О персональных данных», Закон РК «О доступе к информации» и др.

Компьютерная преступность в прошлом году обогнала по обороту наркобизнес, и ее масштабы со временем будут увеличиваться, - утверждает Валери Макнайвен (Valerie McNiven), советник Управления США по вопросам криминальной активности в интернете. «Киберпреступность движется с такой большой скоростью, что правоохранительные органы не могут за ней угнаться» - считает советник. Легкими жертвами киберпреступников становятся компьютерные инфраструктуры развивающихся стран [4].

Связанная с наркотиками киберпреступность с использованием высоких технологий по-прежнему является относительно новым явлением, и лишь немногие страны располагают средствами для оценки ее масштабов или последствий, в связи с этим практически отсутствуют конкретные инициативы в области борьбы с такой преступностью.

Список литературы:

1. Наркотики: <http://www.narkotiki/5-5553.htm#1>
2. Уголовный кодекс Республики Казахстан №226-V ЗРК от 3 июля 2014 года (введен в действие с 1 января 2015 года)
3. Борчашвили И.Ш. Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (том 2) / Под общ. ред. Генерального Прокурора Республики Казахстан, Государственного советника юстиции 1 класса Даулбаева А.К. – Алматы: Жеті Жарғы, 2015. – 500 с.
4. Киберпреступность и наркобизнес. http://www.cnews.ru/news/line/kiberprestupnost_pribylnee_narkobiznesa