Вестник Восточно-Сибирской открытой академии

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ

Филиппов Андрей Анатольевич – аспирант
Научный руководитель – ***Козлов А.П.***, профессор, доцент ЮИ ФГБОУ ВПО Красноярского аграрного государственного университета

Аннотация: целью этой статьи является исследование вопросов использования информационных технологий организованной преступностью, определение основных направлений деятельности организованных преступных групп в сфере информационных технологий и формулирование основных направлений политики противодействия организованной преступности в данной сфере.

The aim of this article is to investigate the issues of the use of information technology by organized crime, identify criminal groups' main spheres of activity in the field of information technology and formulate the basic directions of reactive policy in this area.

Глобализация, получившая мощный импульс практически во всех сферах жизни, превратилась в важнейший фактор мирового развития в XXI веке. В ее основе лежит новый - информационный - этап научно-технической революции, который внес кардинальные перемены в современный миропорядок. Особенность проходящей научно-технической революции состоит в том, что она вторгается в информационную сферу, затрагивая такие основополагающие для всех видов человеческой деятельности процессы, как создание и обработка, хранение и передача информации. Это ведет к коренным социальным трансформациям в области экономики, политики, культуры, к изменениям в сознании людей, к возникновению нового постиндустриального типа общества. При этом глобализация побуждает все государства адаптироваться к новым

реалиям, задействовать все свои правовые, интеллектуальные, технические и экономические потенциалы, чтобы не оказаться на обочине мировой цивилизации. Именно с развитием глобализации, понимаемой как увеличение экономической международной кооперации и интеграции, возникшей благодаря возрастанию мобильности товаров, услуг и факторов производства, становятся все более очевидными социально-политические аспекты развития информационного общества.

Первой осознала в конце XX века наступление нового этапа развития человечества Европа и немедленно начала действовать. За кратчайшее время были разработаны и реализованы стратегии и программы перехода от прошлого к будущему.За Европой последовали "азиатские тигры" - Япония, Тайвань, Китай, Южная Корея, которые в последствии выбились в лидеры.

В России сформировался и успешно функционирует основанный на современных технологиях коммерческий информационный сектор экономики, производящий современные продукты и услуги. Бизнес информационных технологий стал одним из самых процветающих, заняв пустовавшую на российском рынке нишу. Производство коммерческих консультативных услуг, услуг по созданию различных информационных ресурсов, рекламной продукции, аудио и видеоразвлечений пользуется большим спросом.

Отмеченное, относится как к методологическим категориям социального и правового знания, так и к конкретной преступной практике современности. Так, сам факт выстраивания однополярного мира порождает факт сопротивления периферии, что выражается в протестных движениях, от экологии до политического терроризма. Силовое коммуникативное навязывание западного стандарта мышления и образа жизни формирует пространство информационных войн. Потенциал технологических возможностей виртуальных коммуникаций превращается в источник новых форм криминогенности.

Темпы развития преступных технологий таковы, что сегодня уже ни одна

страна мира не может быть защищена от угрозы разорения. Речь идет уже об искусственном, преступном разорении. Зачастую этим действиям нет адекватного определения ни в национальном, ни в международном законодательстве. Примерами мирового масштаба могут быть события последних десятилетий в Югославии. Афганистане, Ираке, на Африканском континенте, в Украине, кризисные ситуации в экономике и политической жизни ряда стран третьего мира.

К числу наиболее важных в теоретическом и методологическом аспектах выводам можно отнести и тот факт, что преступность, выражая глобальные закономерности собственной динамики, стала приобретать новые качества.

Среди таких качеств в их последовательном ряду следует назвать транснациональность преступности, ее популяризацию в средствах массовой информации, криминализацию экономической и политической сфер, а также правоохранительной системы, формирование виртуальных форм и развитие преступности в параметрах глобального компьютерного киберпространства, появление тенденции не только профессионализации определенных форм преступной деятельности, но превращение ее идеально и реально - в образ жизни, криминальную норму социального поведения.Результатом криминализации экономики стало проявление тенденций подчинения экономической, а в перспективе и всей государственной политики специфическим экономическим интересам криминальных структур, что, в свою очередь, исключает потенциал реформирования материально-производственной базы производства в направлении формирования современной техноструктуры и ведет к соответствующим социально-политическим последствиям для социума в целом. В этой связи проблема преодоления криминализации экономики становится одной из ключевых проблем современной национальной и международной экономической политики и требует неотложных мер по реализации. Постоянно расширяется ареал распространения такого феномена как "теневая экономика". Программы и рекомендации западных специалистов

по выводу из тени производственных мощностей и товарной массы даже в совокупности с усилиями национальных государств в современных условиях результатов не показывают. Проблема действительно глобальна, так как ее проявления имеют место практически в любой из форм современного государственного устройства и политического режима, геополитического и экономического пространства. Государство как социальный институт не успевает реагировать на происходящие изменения и в определенном смысле слова способствует тем самым формированию новой реальности: правовой, социальной, экономики. Необходимо обратить внимание еще на одно обстоятельство. Впервые за всю историю существования человечества появилась виртуальная экономика, которая ничего не производит и генерирует только саму себя. Дело в том, что экономика всегда была производящей, и только в последние 15 - 20 лет появилась виртуальная экономика, которая не только ничего не производит, но и в принципе не может этого делать. Пока она существует, как и все в этом мире, исключительно за счет инерции движения производящей экономики, но продолжаться вечно это не может, тем более, что запросы пользователей результатами виртуальной экономики растут в геометрической прогрессии. Банк после себя не оставляет ничего: стоит ему перевести активы в другое место, как на месте остается пустыня - виртуальная реальность торжествует над материальной. Происходят качественные изменения в таких сферах деятельности человека, которые складывались тысячелетиями. Так, в конце минувшего века деньги стали стремительно утрачивать свою функцию всеобщего эквивалента и перестали стимулировать все иные виды человеческой деятельности. Они сами стали ходовым товаром. По экспертным оценкам, годовая торговля валютой приближается к 500 триллионам долларов, что в 80 раз превышает объем мировой торговли товарами.

Развитие новых рынков потребления связано в немалой степени с революцией в области коммуникаций, которая способствовала развитию

системы обмена информации на глобальном уровне, высветив различие между странами в формах потребления товаров и услуг. Стремление к потреблению мирового уровня, существующему в экономически развитых странах, привело к возникновению новых рынков для таких товаров и услуг. Сложился глобальный мировой рынок, на котором потребители получили доступ к информации о товарах и услугах практически из любой точки земного шара, а деловые круги получили возможность для организации сбыта в общемировых масштабах.

То же можно сказать и о транснациональных преступных организациях, которые поставляют свои товары и предоставляют услуги по всему миру. Наиболее ярким примером деятельности мирового нелегального рынка можно назвать незаконный оборот наркотиков, которые стали мировым товаром исключительной важности и превратились в глобальный товар. По некоторым оценкам, мировая торговля наркотиками превышает масштабы мировой торговли нефтью и достигает уровня 400 млрд. долларов в год.

Кроме того, современные системы коммуникаций обеспечивают передачу информации в киберпространстве, практически не оставляя следов, что позволяет сделать ее полностью закрытой и поступающей по назначению из любой части света за считанные минуты. Помимо этого, современные технологии и глобальные информационные системы создают невиданные доселе возможности для транснациональной преступной деятельности и дают преступным группам новые способы для более легкого и успешного проведения незаконных операций.

Компьютерные технологии и сопровождающий их рост сложности методов и масштабов глобальных финансовых операций сделали возможным увеличение объемов, скорости и закрытости международных финансовых расчетов, что повысило возможности транснациональной организованной преступности и уменьшило вероятность ее выявления и пресечения. Это позволяет без проблем легализовать доходы от различных видов незаконной деятельности. Ежедневно 1 млрд. криминальных долларов вливается в оборот

мировых финансовых рынков. Количество и объем сделок, проходящих через международные межбанковские электронные системы составляет следующие величины: каждый день через них осуществляется более 465 тысяч электронных переводов на сумму более 2 триллионов долларов и 220 тысяч сделок. Процесс развития такой финансовой системы опережает темпы законотворчества. Существует настолько много точек проникновения в мировую финансовую систему, что введение в тех или иных странах ограничений в отношении оборота денежных средств, полученных в качестве дохода от незаконной деятельности, совсем не означает, что операции по пресечению отмывания денег будут пресекаться, это лишь заставит преступников искать другие каналы получения доступа к этой системе.

По мнению экспертов, этот процесс сильно стимулировал секс-индустрию, торговлю радиоактивными материалами на черном рынке, наркотиками и огнестрельным оружием, человеческими органами, отмывание грязных денег и многие другие виды деятельности преступных транснациональных организаций. Поэтому значительные трудности государственного мониторинга преступной деятельности, облегчение контактов между транснациональными преступными организациями и общий рост транснациональной организованной преступности явились отрицательным результатом успехов в технологии и развитии коммуникаций.

Преступления, совершаемые организованными преступными группами с использованием информационных технологий, можно разделить на две большие группы:

1. Преступления ненасильственного, как правило, экономического характера;
2. Преступления насильственного характера.

К преступлениям ненасильственного, экономического, характера,

совершаемым организованными преступными группами путем использования информационных технологий, можно отнести:

- отмывание денег, добытых преступным путем;
- мошенничество с платежными пластиковыми карточками;
- хищение денег с банковских счетов;
- кибератакис целью хищения информации;
- фальшивомонетничество;
- компьютерноемошенничество;
- распространение детской порнографии;
- распространение наркотиков.

Организованная экономическая преступность – это глобальная социальная проблема практически всех экономически развитых государств и крупных международных субъектов. По оценкам МВФ масса «грязных денег» составляет от 590 до 1500 млрд. долларов, то есть от 2 до 5 % суммарного ВВП всех стран мира. Закономерная цель организованной группы – получение криминальных капиталов и их легализация, т.е. введение их в сферу легальной предпринимательской деятельности. «Отмывая грязные деньги», организованные преступные группы все чаще используют всемирную компьютерную сеть Интернет.

Отмывание денег с помощью Интернет подразумевает использование всемирной паутины для того, чтобы скрыть происхождение денег, полученных нелегальным путем. Отмывание денег – давно известное преступление, однако анонимность Интернета облегчила преступникам осуществление махинаций с “грязными деньгами”, помещение их в легальные активы и инвестиции. Можно назвать следующие способы отмывания денег через Интернет: проведение азартных игр; использование Интернет-банков. С помощью проведения азартных игр в Интернете незаконно полученные доходы используются для заключения сделок в играх на деньги. Интернет–банки также предоставляют возможности для преступников, которые могут открыть счет, не общаясь

“лицом к лицу” с работниками банка. Деньги могут быть депонированы на секретный оффшорный счет в банке или перемещены с помощью электронных переводов из одного банка в другой, и так далее, пока след найти станет трудно или практически невозможно. Хотя все еще остается трудность с помещением большой суммы наличных денег на счет, но если уж эта сумма помещена, то перемещать ее и управлять ею намного быстрее и легче чем раньше – посредством электронного перемещения.

Большое распространение получил такой вид преступления, как мошенничество с платежными пластиковыми карточками. Этот вид преступлений отличается простотой и тем, что потерпевшие – банк и законный собственник карты, как правило, никогда не видят преступника. Данный вид мошенничества также широко используется организованной преступностью. По данным Генерального секретариата Интерпола, почти 60% всех мошенничеств, связанных с использованием кредитных карточек, совершены организованными преступными группами азиатского происхождения, а на преступные группы из Нигерии, Болгарии, Ирана и стран бывшего Советского Союза приходится 40% совершения этого вида преступлений. Очень часто организованная преступность в своей деятельности использует работу хакеров, которые с помощью специального программного обеспечения достают, а потом продают номера действующих счетов кредитных карточек, а также распространяют пароли, идентификационные номера, кредитную и другую персональную информацию через компьютерные системы, чем помогают преступникам получать незаконный доступ к кредитным бюро и компьютерным системам финансовых учреждений.

Следующий способ хищения денег с помощью банкоматов. Когда данные с магнитной полоски кредитных карточек и PIN-комбинация доступа к счету похищаются не только всякими хитроумными приспособлениями-считывателями, накладными панелями к банкоматам, скрытыми телекамерами и пр. Есть гораздо более эффективный путь: члены организованных преступных

групп приобретают собственные банкоматы, заряжают наличными и выставляют в людных местах, переделывая банкоматы таким образом, что все нужные данные фиксируются. На основе полученной информации изготавливаются карточки-клоны, с помощью которых снимаются наличные деньги через официально установленные банкоматы. Похищенные суммы исчисляются десятками и сотнями миллионов.

Даже в таком виде преступной деятельности, как продажа наркотиков, организованные преступные группы все чаще используют глобальную компьютерную сеть Интернет. Наркоторговцы и их клиенты заключают сделки в сети. Наркодилеры используют для отмывания доходов интернет-банки. Продажа наркотиков и лекарственных препаратов в Интернете приносит большие прибыли.

К преступлениям насильственного характера, которые совершаются организованными преступными группами, прежде всего, нужно отнести «кибертерроризм». В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии.

Под кибертерроризмом понимают преднамеренную, политически мотивированную атаку на обрабатываемую компьютером информацию, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной опасности, запугивания населения, провокации военного конфликта.

Кибертерроризм использует открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу, и является своего рода дополнением

к традиционному виду терроризма. Эта категория преступлений включает также использование электронной почты для осуществления связи между участниками преступного заговора, передачи информации, используемой для совершения насильственных действий, вербовке новых участников террористических групп через Web–сайты сети Интернет.

Выделяются следующие способы, с помощью которых террористические группы используют Интернет:

1. Сбор с помощью Интернета подробной информации о предполагаемых целях, их местонахождении и характеристике.
2. Сбор денег для поддержки террористических движений.
3. Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени и встрече людей, заинтересованных в поддержке террористов, указаний о формах протеста и т.п., т.е. синергетическое воздействие на деятельность групп, поддерживающих террористов.
4. Вымогательство денег у финансовых институтов, с тем чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.
5. Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов.
6. Использование Интернета для информационно-психологического воздействия, в том числе инициация «психологического терроризма».

С помощью Интернета можно посеять панику, ввести в заблуждение, привести к разрушению чего-либо. Всемирная сеть – благодатная почва для распространения различных слухов, в том числе и тревожных, и эти возможности сети также используются террористическими организациями.

Точно такое же влияние на сознание масс имеется и у информационных ресурсов. Искаженные, или с выгодной точки зрения, преподнесённые новости и факты. Для этого создаются специальные теле и радио программы с публицистическим оттенком.

Всё это может нужным образом может влиять на поведение определённых групп населения и в совокупности с организованными акциями (митинги, демонстрации) направлять их действия

Информационное пространство является основой социально-экономического, политического и культурного развития и обеспечения безопасности России. Эффективное информационное пространство обеспечивает построение информационного общества в стране и вхождение ее в мировое информационное сообщество. Информационное пространство будет эффективным только тогда, когда станет открытым для общества, дающим возможность реализовывать согласованные интересы граждан, общества и государства на комплексной и системной основе. Эффективное информационное пространство может развиваться только на основе целенаправленной государственной информационной политики, обеспечивающей поступательное движение страны к построению информационного общества. Это движение должно опираться на новейшие информационные, компьютерные, телекоммуникационные технологии и технологии связи, развитие которых привело бы к бурному развитию открытых информационных сетей, прежде всего, Интернета, дающих принципиально новые возможности международного информационного обмена и на его основе трансформации различных видов человеческой деятельности. Перспективные информационные, компьютерные и телекоммуникационные технологии многократно усиливают воздействие СМИ на социально-политическую и культурную жизнь людей.

Национальные интересы России в информационной сфере включают в себя интересы личности общества и государства в информационной сфере.

Интересы государства заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества. На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности (ИБ), и в ходе технического прогресса эта зависимость будет возрастать.

Государство должно иметь гибкую, адаптивную, мобильную и эффективную систему ИБ, способную быстро реагировать на возникающие угрозы и новые условия деятельности.

Для этого необходимо:

- организовать постоянный контроль за ситуацией в тех сферах, где могут возникнуть угрозы ИБ, и перманентная проверка возможностей существующих систем обеспечения ИБ по отражению реальных и потенциальных угроз;

- согласование разрабатываемой нормативной правовой базы развития информационного пространства и обеспечения ИБ, в первую очередь, в аспектах интегрирования России в международные телекоммуникационные сети, создания технических средств обеспечения ИБ, закупок зарубежных программно-технических и телекоммуникационных средств и их использования в стратегически важных областях;
- объединить усилия широкой общественности, профессионалов, ученых и представителей органов власти, делового мира для решения исключительно важной в настоящее время для России задачи - надежной защиты ее информационных ресурсов.