

Ю.А.Нисневич,
доктор политических наук,
директор Института проблем
либерального развития,
профессор Российского
университета дружбы народов и
Государственного университета –
Высшей школы экономики

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЫЗОВЫ И УГРОЗЫ ПОСТИНДУСТРИАЛЬНОГО РАЗВИТИЯ*

Со второй половины XX века в развитии человеческой цивилизации начался новый этап – этап постиндустриального развития, связанный с тектоническими изменениями во всех сферах жизнедеятельности социума. Начавшийся переход на новый постиндустриальный путь цивилизационного развития предопределил ряд феноменов, проявившихся во второй половине XX века как результат индустриализации. Доминирующей среди этих феноменов представляется информационная революция.

Суть информационной революции состоит в кардинальных, качественных изменениях и конвергенции технологий создания, накопления и распространения информации, которые принято называть информационно-коммуникационными технологиями (ИКТ), и интенсификации на их основе процессов накопления и использования информационных ресурсов. В своей концепции «трех волн» А.Тоффлер указывает на эту революцию, как на последнюю в ряду трех великих технологических революций (аграрная, индустриальная, информационная).¹ При этом информационная революция – это не просто технологическая, но, прежде всего, социально-технологическая революция. Революционные изменения в области ИКТ оказывают кардинальное влияние не только на экономическое и научно-техническое развитие общества, но и на изменение мировоззрения людей, культурные,

морально-психологические и поведенческие аспекты их жизнедеятельности, политические порядки, государственное устройство и функционирование государственного механизма, на инфраструктуру межличностных, общественных, внутри и межгосударственных отношений.

Определяя генезис нового постиндустриального мира, М.Кастельс отмечает: «Информационно-технологическая революция спровоцировала возникновение информационализма, как материальной основы нового общества. При информационализме производство благ, осуществление власти и создание культурных кодов стали зависимыми от технологических возможностей общества с информационной технологией как сердцевиной этих возможностей. Информационная технология стала необходимым инструментом для эффективной реализации процессов социально-экономической реструктуризации. Особенно важна была ее роль в развитии электронных сетей как динамической, саморасширяющейся формы организации человеческой активности. Эта превалирующая, сетевая логика трансформирует все области общественной и экономической жизни».²

Качественная трансформация информационной среды, которая в результате информационной революции из разряда вспомогательных и обеспечивающих, переходит в разряд определяющих в смысле цивилизационного развития, обуславливает не только интенсивное развитие новой экономики, но постепенный переход к новому типу социальной организации общества. Постиндустриальное общество, которое, по мнению большинства отечественных и зарубежных ученых, имеет информационную и сетевую природу, принято называть информационным обществом. Информационное общество строится на всеобщем кодифицированном знании и неразрывно связанной с ним синергетической информации, свободно циркулирующей в открытых информационно-коммуникационных сетях и системах, образующих единую информационно-коммуникационную (инфокоммуникационную) инфраструктуру.

Формирование информационного общества как нового типа социальной организации предопределяет начинающуюся трансформацию социальных и политических коммуникаций и институтов. При переходе к информационному обществу происходит трансформация как социально-экономической, так и в определенной степени политической организации общества, а также структурное изменение властей, в результате которого информационный фактор становится существенно более значимым в социальном и политическом регулировании.³

В качестве системообразующего фактора трансформации человеческой цивилизации на постиндустриальном этапе ее развития выступает формирование на основе использования новейших ИКТ открытой информационной среды с инфраструктурой сетевого типа. Основная задача сетевой инфраструктуры - обеспечение свободы и доступности массового обмена информацией и массовых коммуникаций. А ее транспортная основа - национальные телекоммуникационные сети, которые, соединяя между собой разнообразные множества депозитариев, источников и потребителей информации, образуют инфокоммуникационные системы и сети различного функционального назначения, которые в совокупности и составляют национальные сегменты глобальной сети.

Национальные и глобальные инфокоммуникационные системы и сети открытого типа охватывают все сферы жизнедеятельности общества и государства, изменяя не только технологические, но и сущностные основы такой деятельности. Они становятся основным средством использования, обмена и распространения всех видов информационных ресурсов и оперативной информации. Внедрение во все сферы человеческой деятельности современных технологий создания, накопления и распространения информации, средств вычислительной техники и телекоммуникаций, создание принципиально новых и цифровизация традиционных инфокоммуникационных систем и сетей обуславливает качественные изменения и постоянное расширение объемов циркулирующей

в таких системах и сетях информации, которая становится ключевым ресурсом для экономического, социального и политического развития общества и государства. При этом следует учитывать, что информационные ресурсы обладают рядом специфических особенностей.

Во-первых, информационные ресурсы – это продукт интеллектуальной деятельности самих людей, их производителем является все человеческое сообщество. По мере развития цивилизации происходит постоянное возрастание накапливаемых объемов и интенсивности использования этих ресурсов, совершенствование и конвергенция разнообразных форм и способов их представления.

Во-вторых, информационные ресурсы являются существенно неоднородными. Содержание и смысл информации определяют ее ценностные и потребительские характеристики, необходимость свободного распространения или наоборот ограничения доступа, сохранения в тайне для обеспечения защиты прав и интересов человека, общества и государства.

В-третьих, качество информационных ресурсов определяется такими ключевыми показателями как полнота и достоверность информации. Предумышленное или неумышленное искажение полноты и достоверности информации несет существенные угрозы в смысле принятия некорректных управленческих решений с негативными последствиями и манипулятивного воздействия на общественное мнение в узкогрупповых целях.

В-четвертых, информационные ресурсы в смысле права собственности обладают двумя ипостасями: материальной – на них распространяется право вещной собственности и интеллектуальной – на них распространяется право интеллектуальной собственности и авторское право.

Опыт стран, уже вступивших на путь постиндустриального развития, показывает, что в этих странах опережающими темпами происходит развитие новой экономики, основанной не только на непосредственном использовании интеллектуальных и информационных ресурсов для извлечения прибыли, но и на использование качественно новых свойств информационной среды для

оптимизации расходования таких традиционных ресурсов как природные, человеческие, финансовые.

Принципиально важным представляется тот факт, что при переходе на постиндустриальный путь цивилизационного развития уместно говорить уже не столько о новом, современном уровне развития цивилизации, сколько о формировании пространственного коридора постиндустриального развития. Такой коридор формируют траектории постиндустриального развития отдельных стран, совпадающие в основополагающих трендах и образующие в этом смысле единый поток. Но эти траектории не являются абсолютно идентичными в силу различий специфических для каждой страны связей и институционального строения социальных полей, нормативистики, политико-культурных стереотипов, базовых технологий конкуренции и власти, способов политического обеспечения интеграции социума.⁴

Однако, постиндустриальное развитие в направлении перехода к информационному обществу, как и любое глобальное явление, трансформирующее цивилизацию, открывает не только новые перспективы и возможности устойчивого развития и решения глобальных проблем человечества, прежде всего связанных с необходимостью преодоления кризисных явлений, но и порождает новые вызовы и угрозы личности, обществу и государству. Такие угрозы, обусловленные кардинальной трансформацией информационной сферы, называют информационными, а состояние защищенности национальных интересов в информационной сфере как совокупности сбалансированных интересов личности, общества и государства – информационной безопасностью⁵.

Информационные вызовы и угрозы обусловлены онтологическими свойствами открытой информационной среды с сетевой инфраструктурой.

Прежде всего, такая информационная среда обладает свойством инклюзивности, способностью постоянно расширяющегося проникновения во все сферы жизнедеятельности социума, во все социальное пространство. При этом происходят качественные изменения в институциональном

построении социальных полей, экономических и политических порядков и, как следствие, кардинальная трансформация морфологических свойств самого социального пространства и, в первую очередь, его преобразование в более тесно взаимосвязанное пространство сетевого типа.

Неотъемлемым онтологическим свойством сетевой информационной среды является ее пространственность (топологичность). Она представляет собой физическую объемно-пространственную среду, которая неравномерно разворачивается как в социальном, так и в географическом пространстве. Такая пространственная неравномерность обуславливает возникновение напряженностей нового типа по границам социальных, экономических и политико-административных локалитетов.

Постоянно нарастающая интенсификация инновационного развития информационной среды как следствие соответствующего развития ИКТ и формируемых на их основе инфокоммуникационных систем и сетей определяет трансформационную динамику как онтологическое свойство этой среды. Ключевыми тенденциями такой трансформационной динамики являются повышение пространственной инвариантности, снижение временных затрат и расширение контентных объемов информационно-коммуникационных взаимодействий. Это, очевидно, предопределяет наблюдаемое темпоральное ускорение всех политических, социальных и экономических процессов и явлений, существенное сокращение их историко-временной протяженности.

Как следствие онтологических свойств новой информационной среды наиболее общий вызов постиндустриального развития как перехода к информационному обществу представляет процесс «информационного расслоения», который обуславливает многоаспектную проблему «цифрового или информационного неравенства». Эта проблема стала предметом специального рассмотрения стран «Большой восьмерки» на саммите в Японии в 2000 году, по итогам которого была принята Окинавская хартия⁶.

В геополитическом аспекте данная проблема в документах Всемирной встречи на высшем уровне по вопросам информационного общества (ВСИС), которая проходила в Женеве в декабре 2003 года, определяется как проблема разрыва в цифровых технологиях⁷, т.е. неравенства в оснащенности и качестве используемых ИКТ между странами с разными уровнями развития. Поляризация мира и растущий разрыв между богатыми и бедными, технологически передовыми и отсталыми странами создают новые источники нестабильности, сегодняшних и будущих конфликтов, в том числе глобального характера. В мировом сообществе эта проблема оценивается как приоритетная в виду того, что она представляет собой значимое препятствие на пути построения ориентированного на интересы людей, открытого для всех и направленного на развитие информационного общества. В качестве основной меры для ее разрешения участники ВСИС рассматривают формирование международных финансовых механизмов преодоления разрыва в цифровых технологиях и принимают на себя соответствующие обязательства.

В национальном аспекте проблема «информационного неравенства» определяется как проблема неравенства в возможностях доступа к использованию современных ИКТ для граждан, проживающих в разных регионах страны и населенных пунктах различного типа.

Особенно ярко и значимо этот аспект проблема «информационного неравенства» проявляется в России, в которой еще со времен СССР процесс распространения и внедрения всех инноваций протекает существенно неравномерно как во времени, так и в географическом пространстве. Сначала инновации в приоритетном порядке внедряются в Москве и Санкт-Петербурге, затем постепенно с заметными временными задержками распространяются в крупные научно-промышленные и региональные центры, а затем процесс распространения инноваций резко затухает и зачастую вообще не достигает многих удаленных от столицы и региональных центров административно-территориальных образований и населенных

пунктов. Так, например, в России до сих пор не телефонизированы сорок шесть тысяч населенных пунктов.

Подобный процесс распространения и внедрения современных ИКТ и инфокоммуникационных систем и сетей становится существенным препятствием на пути трансформации экономики индустриального типа и тем более в основном ресурсно-ориентированной экономики России в экономику нового типа, основанную на информации и знаниях. При этом возникает реальная угроза не просто административно-территориального «информационного неравенства», а еще более значимого не только в экономическом, но и в социально-политическом плане технологического разрыва информационного пространства страны.

Для России угроза разрыва ее информационного пространства усугубляется еще и тем, что такой разрыв наметился не только в технологическом, но и в контентном аспекте. Угроза контентного разрыва информационного пространства России порождается использованием в основном манипулятивных и агитационно-пропагандистских методов массового информирования, формирующих вместо реальной виртуальную, целенаправленно конструируемую картину жизнедеятельности общества и государства и препятствующих тем самым формированию единой для всех граждан политической, социальной и экономической повестки дня.

В условиях постиндустриального цивилизационного развития единство открытого информационного пространства страны является одним из краеугольных условий обеспечения ее государственной и территориальной целостности, успешной интеграции в мировое сообщество с учетом национальных особенностей и интересов, обеспечения информационной безопасности на внутригосударственном и международном уровнях. Поэтому формирование и развитие открытого информационного пространства страны как единого и целостного пространства должно рассматриваться в качестве стратегического приоритета ее государственной информационной политики.⁸

В рамках такой государственной информационной политики наиболее эффективным инструментарием для преодоления регионального «информационного неравенства» и купирования угрозы технологического разрыва единого информационного пространства страны представляется национальная целевая программа, ориентированная на интенсификацию развитие единой национальной инфокоммуникационной инфраструктуру. Примерами подобных программ являются программа администрации США Клинтона – Гора по созданию Национальной информационной инфраструктуры (National Inform Infrastructure)⁹ и программа Совета Европы по созданию общеевропейской «информационной автомагистрали», сформулированная в Белой книге Европейской комиссии «Рост, конкуренция, занятость, цели и пути в XXI век»¹⁰. Как показывает мировой опыт, успешная реализация таких программ базируется на партнерском и взаимовыгодном участии в их осуществлении как центральной и региональной власти, так и негосударственного сектора экономики.

Противодействие угрозе контентного разрыва информационного пространства страны представляет собой сугубо политическую проблему. Для ее адекватного разрешения в рамках государственной информационной политики должна быть проявлена политическая воля, направленная на сознательный отказ от манипулятивных методов массового информирования и обеспечение постоянного открытого инфокоммуникационного диалога с обществом, в результате которого только и может формироваться реальная общенациональная повестка дня по развитию страны. При этом одним из стратегических направлений государственной информационной политики должно стать формирование множества альтернативных источников информации - одного из основополагающих политических институтов современной полиархической демократии¹¹.

В социальном плане возникновение проблемы «информационного неравенства» обусловлено тем, что существенные преимущества получает те члены общества, которые имеют возможности, знания и навыки в

использовании современных ИКТ, что позволяет им свободно действовать в новой информационной среде и активно использовать ее для удовлетворения своих потребностей и достижения успеха. В странах, вступивших на путь постиндустриального развития, количество таких членов общества, составляющих его наиболее активную, продвинутую и преуспевающую часть, постоянно возрастает, и постепенно преобладающей в обществе становится сетевая логика социальных взаимодействий и коммуникаций, основанных на индивидуальном использовании инфокоммуникационной инфраструктуры сетевого типа. Однако, даже при увеличении количества людей, успешно адаптировавшихся в новой информационной среде, наблюдается процесс «информационного расслоения» общества и проблема «информационного неравенства» обостряется как социальная. Суть в данном случае состоит в том, что разные социальные слои и группы по различным и не только экономическим причинам получают неравные возможности доступа к использованию информационных ресурсов и информационно-коммуникационных технологий, сетей и систем.

Решение этой качественно новой социальной проблемы также лежит в плоскости государственной информационной политики и такого основного инструментария ее реализации как национальные целевые программы. При этом противодействие угрозе «информационного расслоения» общества как социальной проблеме следует рассматривать в контексте комплексной задачи повышения качества человеческого ресурса страны. Трансформация этого ресурса в самый значимый в условиях постиндустриального развития человеческий капитал требует модернизации форм и методов образования на основе широкомасштабного использования ИКТ и дистанционного обучения, создание общегосударственной системы повышения информационной (компьютерной) грамотности населения, непрерывного информационного образования и переподготовки кадров, высвобождающихся при структурных изменениях экономики. Очевидно, что для успешного и эффективного решения такой масштабной социальной задачи общенационального уровня

необходимо партнерское участие в этом процессе не только государственных институтов и негосударственного сектора экономики, но и самого общества, практически всех его институциональных структур и, в первую очередь, научного и образовательного сообщества страны.

Интенсивное смещение человеческой активности в экономической и социальной сферах в качественно новую информационную среду, глобальная инфокоммуникационная инфраструктура которой становится преобладающей сетевой формой самоорганизации и расширения такой активности, требует адекватного ответа на этот вызов информационной эпохи не только непосредственно в указанных сферах, но и в поле политики.

Следует отметить, что сегодня даже в странах, уже вступивших на путь постиндустриального развития, выражается озабоченность тем, что необходимая реорганизация государства как высшего политического института запаздывает по отношению к начавшейся информационной трансформации экономической и социальной сфер жизнедеятельности общества. Такое запаздывание чревато нарастанием негативных тенденций во взаимоотношениях государственной власти и общества.

Из исторического опыта известны два основных пути преодоления нарастающих разногласий между обществом и властью: внутренние революционные преобразования и внешнее силовое воздействие. Постиндустриальный этап развития, порожденный информационной революцией, открывает альтернативный путь разрешения извечной проблемы - необходимости изменения взаимоотношений между обществом и государственной властью в лице системы ее органов для приведения их в соответствии новым социально-экономическим условиям. Современная информационная среда, функционирующая на основе всеохватывающего использования ИКТ и сетевой инфокоммуникационной инфраструктуры, позволяет без революционных взрывов и потрясений поэтапно перераспределить властные полномочия в пользу общества и передать ряд регулирующих функций его политическим, экономическим, социальным и

иным институциональным самоорганизующимся структурам.¹² Эта среда обеспечивает также возможности эволюционного преодоления консерватизма органов государственной власти в организации своей деятельности и взаимодействий с гражданами и их объединениями.

Однако для того, чтобы реорганизация системы государственного управления, адекватная вызовам информационной эпохи, не осталась бы только декларацией о намерениях, а начала реально воплощаться в жизнь необходимы, во-первых, политическая воля правящей элиты и, во-вторых, практически реализуемая концепция такой реорганизации, учитывающая сложнейшие экономические, социальные, административные и правовые проблемы, возникающие при внедрении новых организационных моделей.

В качестве такой концепции ведущими странами мирового сообщества сегодня предлагается идея создания «электронного правительства», суть которой заключается в следующем. Во-первых, вся система органов государственной власти и государственных учреждений, обобщенно называемая правительством, рассматривается как единая сервисная организация, предназначенная для оказания услуг населению. Во-вторых, деятельность правительства должна быть открытой и информационно прозрачной для граждан и оно должно быть доступно каждому члену общества в любой момент времени и из любого места его расположения. В-третьих, для совершенствования и повышения качества оказания услуг населению и повышения эффективности функционирования правительства в его деятельности используется виртуальное пространство или, точнее, его деятельность переносится в современную сетевую информационную среду.

Таким образом, электронное правительство следует рассматривать не только как современное организационно-технологическое построение системы государственного управления, основанное на использовании ИКТ и сетевой инфокоммуникационной инфраструктуры, но и, прежде всего, как постиндустриальную философию государственного управления.¹³ В таком контексте электронное правительство представляется также дальнейшим

качественно новым развитием на основе использования постиндустриальных ИКТ механизма связей с общественностью (public relations), признанного неотъемлемой частью современного института государственного управления и одной из его ключевых функций, способствующей установлению и поддержанию общения, взаимопонимания и сотрудничества между государственной властью и обществом.

В настоящее время многие страны добились определенного прогресса в области построения электронного правительства, хотя темпы развития и качество предоставляемых услуг изменяются в самых широких пределах – от публикации самой общей правительственной информации до подачи налоговых деклараций и платежей в бюджет. В России определенные шаги по построению электронного правительства запланированы в рамках федеральной целевой программы «Электронная Россия (2002-2010 годы)».¹⁴ По мнению ряда российских специалистов эта целевая программа содержит концептуальные недостатки, обусловленные как представляется политико-административными факторами, и даже при ее успешной реализации, к чему имеются серьезные препятствия и, прежде всего, финансового характера, не будет обеспечен полномасштабный переход от традиционного правительства к электронному и в 2010 году Россия по-прежнему будет находиться в состоянии догоняющего развития.

Следует особо отметить, что все страны, приступившие к созданию электронного правительства, объединяет общее понимание того, что реализация такого правительства представляет собой адекватный ответ на вызовы постиндустриального развития в поле политики и, следовательно, является одной из приоритетных внутривластных задач.

Широкомасштабное внедрение ИКТ и инфокоммуникационных сетей и систем во все сферы жизнедеятельности общества и государства создает качественно новые условия для массовых коммуникаций, обработки, передачи и использования различных видов информации и при этом

обостряет уже известные и порождает новые информационные угрозы и проблемы как правового, так и технического характера.

Постиндустриальная информационная среда существенно расширяет потенциальные возможности реализации права на информацию, которое в международном праве определяется как одно из основных прав и свобод человека и гражданина.¹⁵ Это право в аспекте действий с информацией наиболее полно устанавливается Конституцией России (1993) как право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным образом (статья 29), т.е. как право свободно осуществлять весь набор действий с информацией.

Гарантированное соблюдение и защита права на информацию как естественного и неотчуждаемого права человека и гражданина, прежде всего, со стороны государства представляет собой одно из основных направлений обеспечения информационной безопасности как защиты национальных интересов страны и интересов ее граждан в информационной сфере. Отсутствие у граждан полной и достоверной информации обо всех событиях и процессах, происходящих в стране и за ее пределами, всей общественно значимой информации, основным и самым мощным источником которой является государственная власть, цензурирование и манипулирование такой информацией представляет собой существенно значимый фактор социальной и политической дестабилизации обстановки в стране.

Однако право на информацию, как и другие права и свободы, не является безграничным. Любые права и свободы человека действительно являются таковыми лишь до тех пор, пока их осуществление не нарушает те или иные права других людей, а также конституционные права и обязанности иных субъектов общественных отношений, таких как добровольные объединения граждан, субъекты экономической деятельности, органы государственной власти и местного самоуправления.

В связи с этим общепризнанным правовым фактом необходимо является введение на законодательном уровне некоторых ограничений права на

информацию. Смысл таких ограничений состоит не в том, чтобы ограничить право на информацию как таковое, а лишь в том, чтобы, во-первых, запретить использование информации, представляющей реальную угрозу интересам личности, общества и государства и, во-вторых, ограничить в той или иной степени свободу действий с информацией конфиденциального характера. К конфиденциальной информации, работа с которой в целях обеспечения информационной безопасности личности, общества и государства подлежит законодательной регламентации, относится информация, содержащая государственную, коммерческую, служебную, личную и другие виды тайны.

В условиях формирования глобального постиндустриального общества особую остроту и значимость приобретает задача недопущения и пресечения пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды. К сожалению, сетевая инфокоммуникационная инфраструктура открытой информационной среды создает технологические возможности для широкомасштабного распространения такой информации и существенно усложняет задачу выявления, пресечения и определения меры ответственности ее источников. Тем не менее, практическая реализация запрета подобной деятельности, который установлен международными актами и, как правило, национальными конституциями, должна быть объектом постоянного, пристального внимания и ответственности правоохранительных органов и такая деятельность подлежит жесткому преследованию в уголовном порядке.

При переходе к открытому информационному обществу одну из ключевых правовых проблем представляет коллизия между правом на информацию и правами на неприкосновенность частной жизни, личную и семейную тайну, защиту чести, достоинства и доброго имени.

Интенсивное развитие и повсеместное внедрение современных ИКТ, инфокоммуникационных систем и сетей обеспечивает широкие возможности для создания многочисленных и мощных баз данных, легкость

распространения информации из различных баз, простоту ее копирования, агрегирования и модификации и т.п. При этом существенно возрастают информационные угрозы неприкосновенности частной жизни в смысле «прозрачности» каждого человека, как для государства, так и для других людей, преднамеренного манипулирования информацией персонального характера. Именно действия с информацией персонального характера как со стороны государства, естественно, стремящегося взять своих граждан под максимальный контроль, так и со стороны различных негосударственных организаций и отдельных лиц, стремящихся извлечь ту или иную выгоду от использования и распространения такой информации, представляют наибольшую угрозу информационного вторжения в частную жизнь.

Информация персонального характера или персональные данные представляет собой информацию о конкретном человеке, отождествляемую с конкретным человеком или которая может быть с ним отождествлена, и позволяющую прямо или косвенно идентифицировать этого человека. Распространение такой информации без согласия самого человека может, как способствовать формированию его положительного образа в общественном сознании, так и нанести непоправимый урон, моральный вред, особенно если такая информация недостоверна или преднамеренно искажена.

Поэтому на международном уровне проблеме работы с персональными данными в условиях интенсивной сетевой информатизации уделяется особое внимание и уже принят ряд документов, определяющих правовые принципы преодоления коллизии между правом на информацию и правом на неприкосновенность частной жизни при обеспечении защиты прав частных лиц от информационного вторжения.¹⁶ При этом страны, подписавшие Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, в том числе и Россия, взяли на себя обязательство реализовать содержащиеся в ней правовые принципы в своем национальном законодательстве к моменту ратификации Конвенции. Сегодня специальные законы, основанные на международных

правовых нормах регулирования работы с персональными данными, действуют более чем в 20 странах.

В условиях всепроникающей информационной среды важнейшим аспектом обеспечения информационной безопасности все категорий пользователей инфокоммуникационной инфраструктуры является защита от таких угроз как несанкционированный доступ к информационным ресурсам пользователей и каналам передачи информации; распространение ложной и недостоверной информации; преднамеренное или непреднамеренное искажение информации, включая искажение электронных транзакций; сетевое мошенничество, включая фишинг^{*}; распространение «вредоносного контента» - вирусов, червей, шпионского и рекламного программного обеспечения, спама, а также другие компьютерные преступления.

Несанкционированные вторжения в информационные ресурсы и электронные транзакции, подключения к каналам передачи информации, причем, как извне, так и изнутри организации являются сегодня наиболее распространенным видом преступлений в информационной сфере. Цель таких преступлений – информация, признаваемая стратегически важным товаром, на приобретение которого, в том числе и на теневом рынке, расходуются значительные финансовые средства. За подобные преступления, естественно, необходимо в законодательном порядке устанавливать административную и уголовную ответственность. Но наиболее эффективным средством непосредственной защиты от несанкционированных вторжений являются такие программно-аппаратные средства как межсетевые экраны (firewall), которые защищают периметр сети пользователя или ее отдельные сегменты от подобных вторжений.¹⁷

Сложность организации эффективной законодательной защиты от информационных угроз контентного типа заключается в том, что их генезис

^{*} Фишинг (от англ. fishing – ловля рыбы) – обман пользователя, который, получив по электронной почте или иным способом сфальсифицированное письмо, начинает выполнять какие-либо действия (может указать свой PIN код к банковской карте, ввести пароль доступа к закрытым разделам тех или иных сайтов и т.д.).

лежит как в форме представления, так и, что самое главное, в самом содержании информационных сообщений, распространяемых по средствам инфокоммуникационных сетей и систем. При этом законодательное регулирование и контроль содержания информационных сообщений является крайне противоречивой и сложной юридико-правовой проблемой. Тем не менее, законодательное установление жесткой административной и уголовной ответственности, определяемой в судебном порядке, за распространение и предоставление недостоверной, неэтичной, заведомо ложной информации, диффамацию и сокрытие общественно значимой информации способно заметно повлиять на повышение уровня информационной безопасности.

Законодательные меры защиты от распространения «вредоносного контента» представляются малоэффективными и плохо реализуемыми в правоприменительной практике. Для противодействия этой информационной угрозе наиболее эффективным и практически полезным является предоставление пользователям широкого спектра таких программных средств защиты как антивирусные программы, системы обнаружения и предотвращения атак, антиспамовое программное обеспечение, средства контроля содержимого web-трафика и электронной почты и другие.

В целом для защиты пользователей инфокоммуникационных сетей и систем от сетевых информационных угроз и компьютерных преступлений различного типа оптимальным следует признать сочетание правовых, программных и программно-аппаратных методов и средств защиты.

В заключении можно констатировать, что обеспечение национальной информационной безопасности как защищенности интересов личности, общества и государства в информационной сфере представляет собой одну из ключевых задач управления современным государством. Системное решение такой задачи должно быть направлением национальной стратегии информационного развития, разработка и реализация которой необходима каждой стране, стремящейся занять достойное место в мировом сообществе в

условиях постиндустриального развития цивилизации как перехода к глобальному информационному обществу.

¹ Тоффлер А. Третья волна. – М.: АСТ, 1999 – с.31-50.

² Кастельс М. Информационная эпоха: экономика, общество и культура. – М.: ГУ ВШЭ, 2000 – с.492-493.

³ Нисневич Ю.А. Информация и власть. – М.: Мысль, 2000 – с.10.

⁴ Нисневич Ю.А. Проблемы транзита в условиях постиндустриального развития цивилизации /Вестник МГУ, серия 12 Политические науки. - М., 2002, №3, - с.95.

⁵ Доктрина информационной безопасности Российской Федерации. Архив Государственной Думы, регистр. №9425 от 26.09.2000 – с.2.

⁶ Окинавская хартия глобального информационного общества (2000).

⁷ Декларация принципов и План действий ВСИС (WSIS-03/GENEVA/DOC/0004, WSIS-03/GENEVA/DOC/0005).

⁸ Нисневич Ю.А. Информация и власть. Указ. соч. – с.46.

⁹ Gore A., vice President of United States, Brown R., secretary of commerce and chairman information infrastructure task force. The Global Information Infrastructure: agenda for cooperation. Peter Max, February 1995.

¹⁰ Бангеманн А. Европа и мировое информационное сообщество //Рост, конкуренция, занятость, цели и пути в XXI век. Бюллетень Европейской комиссии. Приложение №6, 1993.

¹¹ Даль Р. О демократии. – М.: Аспект Пресс, 2000 – с.85.

¹² Совершенствование государственного управления на основе его реорганизации и информатизации. Мировой опыт. – М.: Эко-Трендз, 2002 – с.12.

¹³ Нисневич Ю.А. Электронное правительство как постиндустриальная философия государственного управления //Политическая коммуникация в постсоветской России: проблемы формирования и парадигмы развития.– М.- Улан-Удэ, 2003 – с.225.

¹⁴ Постановление Правительства РФ №65 от 28.01.2002 «О федеральной целевой программе «Электронная Россия (2002-2010 годы).

¹⁵ Всеобщей Декларацией прав человека (1948); Европейской Конвенцией о защите прав человека и основных свобод (1950); Международный пакт о гражданских и политических правах (1966).

¹⁶ Основные положения Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональными данными (1980); Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (1981); Руководство ООН относительно компьютерных файлов персональных данных (1990); Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (1995).

¹⁷ Информационная безопасность /Информ-Курьер-Связь, 2005, №7 – с.31.