in the article. The subject grounds of physical, biological and socially-historical pictures of the world are determined in the light of humanism requirement of integrity. Integral logic of development of scientific picture of the world is reconstructed as cyclic motion of idea depending on the prevailing factors of space, time and «space–time». The leading role of language is grounded in spiritual development of humanity.

Б. Исабаев

МЕЖДУНАРОДНО-ПРАВОВОЙ УРОВЕНЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глобальный характер информационного обмена и взаимодействия делает актуальным целый ряд проблем информационной безопасности, порождая потребность мирового сообщества в создании средств и международных механизмов минимизации опасных воздействий на общество вследствие формирования и движения информационных потоков.

Рассмотрим международно-правовой уровень обеспечения информационной безопасности.

Возможности регулирования мирового информационного пространства в рамках традиционного законодательства ограничены. К таким законодательным документам относятся:

• правила ведения вооруженного конфликта, определяемые Женевскими и Гаагскими конвенциями;

• основные соглашения в области ограничения и сокращения вооружений;

• Договор о космосе 1967 года;

• Концепция о международной ответственности за ущерб, причиненный космическим объектам;

• Международная телекоммуникационная конвенция 1973 года и ряд других существующих международно-правовых документов.

Это связано с особенностями формирующегося информационного пространства, со спецификой процесса и последствий применения информационного оружия.

Принятый 4 декабря 1998 года консенсусом документ ООН под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», по существу, стал формальным началом создания совершенно нового международно-правового режима, субъектом которого стали информация, информационная технология и методы ее использования [1].

Члены ООН договорились содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, путей их устранения. В практическом плане и с учетом новизны вопроса государствам-членам ООН было предложено сформулировать свои собственные оценки угроз в данной сфере, дать определения таких основных понятий в области информационной безопасности, как «несанкционированное вмешательство» и «неправомерное использование информационных систем и ресурсов».

На 55-й сессии Генеральной Ассамблеи ООН в октябре 2000 года был представлен очередной доклад Генерального секретаря ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». В этом документе было предложено определение таких базовых терминов, как «информационное оружие», «информационная война» и «информационная безопасность».

Основная идея документа сформулирована в положениях Принципа 1, согласно которому деятельность каждого государства в информационном пространстве должна способствовать общему прогрессу и не противоречить задаче поддержания мировой стабильности и безопасности, интересам безопасности других государств, принципам неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. При этом, однако, подчеркивалось, что право каждого на поиск, получение и распространение информации может быть ограничено законом в целях защиты безопасности каждого государства. Кроме того, все члены международного сообщества должны, в соответствии с Принципами, иметь равные права на защиту своих информационных ресурсов и критически важных структур от несанкционированного информационного вмешательства.

В документе приводятся определения основных угроз в сфере международной информационной безопасности и формулируют направления деятельности, которые могли бы способствовать созданию международно-правовой основы ограничения таких угроз. В этом отношении основной идеей такого договора могло бы стать обязательство участ-

ников не прибегать к действиям в информационном пространстве, целью которых является нанесение ущерба информационным системам, процессам и ресурсам другого государства, его критически важным структурам, подрыв политической, экономической и социальной систем, массированная психологическая обработка населения с целью дестабилизации общества и государства.

В целях создания режима коллективной информационной безопасности участники договора также отказываются от:

• разработки, создания и использования средств воздействия и нанесения ущерба информационным ресурсам и системам другого государства;

• несанкционированного вмешательства в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерного использования;

• действий, ведущих к доминированию и контролю в информационном пространстве;

• противодействия доступу к новейшим информационным технологиям, создания условий технологической зависимости в сфере информатизации в ущерб другим государствам;

• поощрения действий международных террористических, экстремистских и преступных сообществ, организаций,

групп и отдельных правонарушителей, представляющих угрозу информационным ресурсам и критически важным структурам государств;

• разработки и принятия планов, доктрин, предусматривающих возможность ведения информационных войн и способных спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационной войны;

• использования информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;

• трансграничного распространения информации, противоречащей принципам и нормам международного права, а также внутреннему законодательству конкретных стран;

• манипулирования информационными потоками, дезинформации и сокрытия информации с целью негативного воздействия на общество;

• информационной экспансии, приобретения контроля над национальными информационно-телекоммуникационными инфраструктурами другого государства, включая условия их функционирования в международном информационном пространстве [2].

В этом случае такой договор должен содержать:

• определения признаков и классификации информационной войны, информационного оружия и средств, которые можно отнести к информационному оружию;

• меры по ограничению оборота информационного оружия;

• режим запрещения разработки, распространения и применения информационного оружия;

• меры предотвращения угрозы возникновения информационной войны; положение о признании опасности применения информационного оружия в отношении критически важных структур, сравнимой с опасностью применения ОМУ;

• условия для равноправного и безопасного международного информационного обмена на основе общепризнанных норм и принципов международного права;

• меры предотвращения использования информационных технологий и средств в террористических и других преступных целях;

• разработку процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;

• условия создания системы международного мониторинга для отслеживания угроз, проявляющихся в информационной сфере, и механизма контроля выполнения условий режима международной информационной безопасности;

• механизм разрешения конфликтных ситуаций в сфере информационной безопасности;

• условия создания международной системы сертификации технологий и средств информатизации и телекоммуникации (в том числе программно-технических) в части гарантий их информационной безопасности;

• мирное развитие системы международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве;

• рекомендации по гармонизации на основе добровольности национального законодательства в части обеспечения информационной безопасности.

Эксперты ряда развитых стран, включая США, исходят из приоритета рассмотрения и разработки мер информационной безопасности применительно к угрозам террористического и криминального характера. При этом угроза создания информационного оружия и возникновения информационной войны сторонниками такого подхода рассматривалась больше как теоретическая.

Дальнейшее обсуждение этой проблематики предлагалось рассредоточить по региональным и тематическим форумам (Европейский Союз, «восьмерка», Организация азиатских государств, Организация экономического сотрудничества и развития и т.д.), а в рамках ООН перевести из Первого комитета во Второй (экономические вопросы) и Шестой (правовые вопросы).

Другая группа экспертов (в основном представители развивающихся стран) поддерживает концепцию рассмотрения проблемы международной информационной безопасности в комплексе, с выделением в качестве приоритетной задачи ограничение потенциальной угрозы развязывания информационной войны. В этой связи подчеркивалась необходимость безотлагательно приступить к обсуждению и практической разработке международно-правовой основы универсального режима международной информационной безопасности. Выдвигалось, в частности, предложение о создании специального международного суда по преступлениям в информационной сфере.

Принципиально важно, что проблематика международной информационной безопасности была закреплена за Первым комитетом Генеральной Ассамблеи ООН. Тем самым, был подчеркнут ее политический аспект, подтверждена ее непосредственная связь с общим состоянием международной безопасности.

Важным шагом на пути создания международно-правового режима информационной безопасности стала Окинавская хартия глобального информационного общества, принятая на саммите стран «большой восьмерки», прошедшем в июле 2000 года на Окинаве.

В Хартии признается революционное воздействие ИКТ на все сферы жизнедеятельности общества. Необходимо, подчеркивается в Хартии, чтобы ИКТ служили достижению взаимодополняющих целей обеспечения устойчивого экономического роста, повышения общественного благосостояния, стимулирования социального согласия и полной реализации их потенциала в области укрепления демократии, транспарентного и ответственного управления международного мира и стабильности.

Особое внимание в рамках данного документа уделяется поиску правовых решений проблемы информационного неравенства. Доступность информационных технологий для людей во всем мире была провозглашена в Окинавской хартии в качестве одного из основополагающих принципов.

На том же Окинавском саммите «большой восьмерки» было принято решение об учреждении специальной международной комиссии «Группы по возможностям цифровых технологий» (Digital Opportunity Task Force, DOT Force), целями которой являются активное содействие диалогу с развивающимися странами, международными организациями и неправительственными организациями по проблеме «цифрового разрыва», курирование программ и проектов в области информационных технологий, координация инвестиций в данную область.

В 2001 году был сделан следующий шаг на пути международно-правового регулирования информационного пространства: экономический и социальный совет ООН поручил Генеральному секретарю ООН создать Рабочую (нелепую) группу по информационным и коммуникационным технологиям (United Nations Information and Communication Technologies Task Force, UNICTTF). Эта инициатива была призвана «перевести на поистине глобальный уровень всю совокупность действий по преодолению мирового цифрового разрыва, развить цифровые возможности и тем самым прочно поставить ИКТ на службу, развития для всех». 29 апреля 2002 года в Женеве состоялась рабочая встреча, на которой была организована региональная сеть Целевой группы для стран Европы и Центральной Азии с рабочими узлами в Москве и в Женеве. До конца мая 2002 года были созданы 6 аналогичных рабочих групп и Бюро региональной сети, которые начали работу по формированию согласованной политики развития информационного общества для всего региона с участием ведущих экспертов.

Попытки развязывания «информационного узла» международной безопасности осуществляются не только на уровне ООН. На уровне Совета Европы предпринимаются серьезные усилия по борьбе с киберпреступностью и кибертерроризмом. Опыт уголовно-правовой классификации преступлений в сфере компьютерной информации, накопленный в ведущих промышленно развитых странах мира, был обобщен в разработанном членами Европейского сообщества «Руководстве Интерпола по компьютерной преступности». 23 ноября 2001 года в Будапеште большинством стран-членов Совета Европы, а также Японией и США было подписано, по сути, первое международное соглашение, посвященное регулированию отношений в сети Интернет – Конвенция по компьютерной преступности (Convention on Cybercrime), призванное унифицировать законы, связанные с компьютерными преступлениями [3].

Нерешенным пока остается вопрос о

разделении компетенции в области обеспечения информационной безопасности между различными международными организациями.

В настоящее время проблемы, связанные с развитием информационного общества, рассматриваются как в рамках различных международных политических организаций и объединений (ОЭСР, ЕС, АТЭС, ООН, G8, ВТО, Всемирного Банка, ЕБРР и др.), так и в рамках профильных международных организаций (Международного союза электросвязи, Всемирного альянса информационных технологий и услуг (WITSA), Европейской ассоциации индустрии ИКТ (EICTA), Международного совета по информационным технологиям в государственном управлении (TCA), Международного общества по телемедицине (ISFT), Международного совета по открытому и дистанционному обучению (ICDE).

Основное внимание эти организации уделяют, прежде всего, социально-экономическим проблемам глобальной информатизации, в том числе проблеме цифрового неравенства, при этом многие другие проблемы информационной безопасности остаются без должного внимания.

Именно поэтому многие специалисты считают, что международное регулирование Интернета и решение проблем информационной безопасности должно осуществляться комплексно специализированными международными организациями. Активная позиция мирового общественного мнения может способствовать скорейшему созданию таких институтов и выработке необходимых международно-правовых норм.

Специалисты также выдвигают идею создания постоянно действующих международных механизмов мониторинга информационных угроз, центров информационно-технической помощи странам – жертвам военно-информационной агрессии или любого другого неправомерного применения информационных средств, интернациональных групп специалистов по быстрому реагированию на инфотеррористические выпады. Эта идея приобрела особую актуальность после событий 11 сентября 2001 года.

В современном обществе обостряется проблема возникновения параллельных официальной власти информационных структур, которые могут вести пропаганду в сетях, формировать политические предпочтения (в том числе и экстремистские, радикальные). Поэтому необходимо искать способы противодействия данному явлению, не путем грубого запрета, а через обеспечение правового коммуникационного взаимодействия власти и общества. Известный российский специалист в области правового обеспечения Интернета В.Б. Наумов видит следующие возможные пути решения проблемы юрисдикции использования Интернет: «В первую очередь, это международные договоры, определяющие статус международного информационного пространства и фиксирующие коллизионные нормы использования законодательства различных государств. Не панацеей, но временным выходом могут служить региональные многосторонние соглашения, а также двусторонние договоры о правовой помощи. В идеале необходима унификация норм национальных законодательств относительно использования Сети» [4].

Параллельно с выработкой международно-правового режима информационной безопасности необходимо проводить согласование национальных законодательств, регулирующих информационную деятельность государств. Тем более, что за последнее десятилетие во многих странах мира проделана большая законотворческая работа по выработке правовых документов, направленных на борьбу с компьютерной преступностью и на другие аспекты использования глобального информационного пространства.

В целом можно заметить, что имеющихся на настоящий момент эффективных международно-правовых механизмов обеспечения информационной безопасности пока недостаточно. Во многом это связано со спецификой информационного противоборства и особенностями формирующегося информационного пространства, которые не позволяют напрямую применять существующие международно-правовые документы (правила ведения вооруженного конфликта, соглашения в области ограничения и сокращения вооружений).

В этих условиях представляется необходимым создание специального международно-правового режима, важными шагами на пути к которому должны стать:

• продолжение важных инициатив, начатых на уровне ООН и других международных организаций и форумов;

• усиление координирующей роли ООН в выработке правовых основ информационной безопасности и более четкое определение компетенции различных международных организаций в этой области;

• учет опыта и практики национального законодательства в сфере информационной политики различных государств и одновременно с этим создание специализированных международных организаций и институтов, постоянно действующих международных механизмов мониторинга информационных угроз.

Важная роль в выработке такого международно-правового режима может принадлежать Казахстану, перед которым сейчас стоит задача сохранения авторитета в области обеспечения информационной безопасности, упрочения своих, позиций в мировом информационном пространстве, проведения эффективной информационной политики.

1. Крутских А.В. Информационный вызов безопасности на рубеже XXI века // Международная жизнь. — 1999. - №2. - С.48.

2. Информационные вызовы национальной и международной безопасности / Под ред. А.В. Федорова, В.Н. Цыгичко. - М: ПИР-Центр, 2001. - С. 193.

3. Convention on Cybercrime (Будапешт, 23 ноября 2001 г.) // http://conventions. coe.int.

4. Наумов В.Б. Право и Интернет: Очерки теории и практики. — М.: Книжный дом «Университет», 2002. - С. 16-17.

К. М. Атымтаева

СОЦИАЛЬНАЯ АДАПТАЦИЯ ЛИЧНОСТИ

Представление социальной адаптации личности в качестве объекта философского анализа требует уяснения принципов (стратегии) социальной адаптации, установления границы исследования между «интерпретативным» и «нормативным» подходами в социологии. Прежде всего, уясним себе следующее. Адаптивно-интерпретативное направление социальной философии охватывает примерно следующий перечень ключевых понятии по рассматриваемой нами проблематике: адаптивная ситуация и установка, интерпретация и идентичность, индивидуальная система значений и информационно-символическое взаимодействие, которые в комплексе с понятием «стратегия социальной адаптации» могут составить понятийный каркас данного исследовательского подхода. Для сведения - анализ «интерпретативной» и «нормативной» парадигм впервые был выполнен американским исследователем Т. Уилсоном [1, С. 560].

Доминирующая методологическая ориентация символического интеракционизма Мида наиболее зримо проявляется при её сопоставлении со структурно-функциональной теорией социального действия Парсонса и его последователей. Вслед за Т. Уилсоном мы начинаем убеждаться, что теоретическая конфронтация социальных концепций Мида и Парсонса явилась основой принципиального противостояния парадигмы - интерпретативной и нормативной. Нормативная парадигма, - отмечает Х. Абельс - постулирует, что «участники социального взаимодействия разделяют общую систему символов и значений, относящихся к социокультурной системе ценностей, которая обладает принудительной силой. Вследствие социализации в общей системе ценностей партнёры по взаимодействию интерпретируют социальные явления и события как соответствующие некоторым «образцам» уже известных из прошлого ситуаций и способов поведения» [2, С. 45-46].

Интерпретативная парадигма, напротив, «исходит из отсутствия заранее заданной общезначимой системы символов в строгом смысле этих терминов. В своей программной статье «Методологические основы символического интеракционизма» Г. Блумер целенаправленно акцентирует внимание на позиции символического интеракционизма - «человек способен приписывать вещам значения, т.е. интерпретировать окружающую среду и тем самым создавать свой символический мир. Если человек намерен действовать, то он должен продемонстрировать себе и другим значения этого символического мира». Мы с интересом обнаруживаем, что проблема социальной адаптации личности практически долго никем не рассматривалась в качестве одного из этих важных феноменов, а интерпретативный подход столь длительное время фактически игнорировался при анализе философских аспектов адаптации личности в социуме. Мы отмечали, что приспособительный процесс - это череда постоянных изменений разнообразных социальных ситуаций, которые непрерывно интерпретируются субъектом социальной адаптации. А раз так, то процесс и результативность социального приспособления не объяснить с помощью анализа одних лишь объективных и субъективных причин этих изменений.

С позиции интерпретативного подхода интерпретация субъектом адаптации социальных ситуации вполне может быть рассмотрена в качестве специфической доминантной стра-