ГОСУДАРСТВО И ПРАВО, 2009, № 2, с. 48–54

ПРАВО И ИНФОРМАТИКА

СУЩНОСТЬ И СТРУКТУРА ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

© 2009 г. А. К. Жарова[1]

В настоящее время, используя современные высокопроизводительные компьютеры, появилась возможность создавать искусственные миры и выдавать их за реальные. Членам гражданского общества стало сложно отделить агрессивное информационное воздействие от неагрессивного, созидательного, направленного на позитивное формирование отношений всего строя жизни. Одна из проблем существования гражданского общества выражается в том, что коммуникация между субъектами современного общества представляет собой борьбу за способы и модели организации информационного пространства.

Средства вычислительной техники вполне позволяют в режиме реального времени создать виртуальную модель объекта и его связей, а затем проецировать ее на окружающий мир. Информацию начали использовать в качестве средства воздействия на реальные системы – государство, бизнес, человека, технико-технологические системы.

Американский социолог и публицист Э. Тоффлер выделяет *три волны* развития науки и техники. *Первая волна* – "сельскохозяйственная цивилизация", прокатившаяся 10 тыс. лет назад. Она сломала первобытно-общинные формы самоорганизации, привела к разделению труда и созданию иерархических организационных структур. *Вторая волна* – индустриальная цивилизация, возникшая в XVII в. Информационные технологии превращают общества второй волны – индустриальные в общества третьей волны – информационные. *Третья волна* – преобразовывающая все без исключения аспекты человеческого существования посредством использования новейших технологических, аппаратно-программных средств. Э. Тоффлер утверждает, что именно анализ динамики, порождаемой противодействием движущих сил второй и третьей волн, поможет объяснить наиболее важные тенденции развития современного общества[2]. В каждой из волн можно вычленить определенные, характерные для данных периодов развития науки и техники цели достижения противоборств и свои стороны противодействия.

До третьей волны развития науки и техники информация как средство воздействия имела второстепенное значение, так как не существовало на тот момент развитых технологий, позволявших ее использовать. Это было определено тем, что предыдущие периоды развития науки и техники не имели технологий, при помощи которых можно было бы быстро распространять информацию и тем самым получать отклик общества, хотя информационное воздействие существовало всегда. В качестве первых информационных атак использовались, например, мифы. В третьей волне появились новые возможности осуществления информационной атаки с использованием информации и информационных технологий для достижения цели противоборства.

Понятия "противоборство", "противостояние" предопределяют, что сторона должна выразить свое отношение к ситуации и ее участникам, определяемое категориями морального права (справедливость – несправедливость) или нравственной истины (правда – ложь), нормативными актами и правовыми обычаями, наследственно-биологическими факторами, техническими нормами. А в информационном противоборстве стимул формирует информационное воздействие, которое принуждает занять ту или иную сторону.

В состоянии противоборства сторона должна совершить выбор своей позиции, притом что она находится в локальном временном пространстве, а обстоятельства, принуждающие к выбору, сохраняются на протяжении всего отрезка времени до тех пор, пока этот выбор не будет совершен. Особенность права состоит в том, что оно находит свое применение во всех видах информационных противоборств. Поэтому рассмотрение структуры противоборства, роли и места права в этих процессах является важной задачей общества.

В настоящее время *информационное противоборство* имеет две плоскости реализации – *информационный конфликт* и *информационную войну*. Общим для них является то, что каждая из сторон стремится занять несовместимую и противоположную позицию по отношению к интере-

[1] Старший научный сотрудник сектора информационного права Института государства и права РАН, доцент Государсвенного университета – Высшая школа экономики, кандидат юридических наук.

[2] См.: *Тоффлер Э.* Третья волна. М., 1999. С. 54.

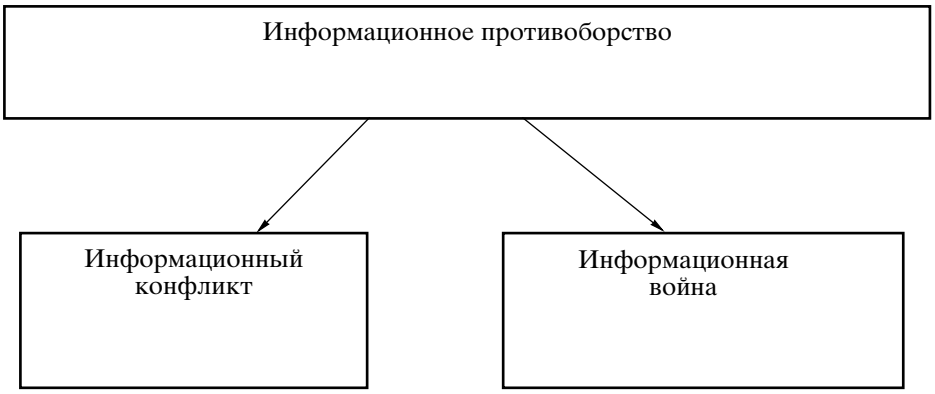

Рис 1. Стадии информационного конфликта и информационной войны.

сам другой стороны и одержать победу путем достижения цели противоборства.

Таким образом, первоначальной стадией информационного конфликта или информационной войны является информационное противоборство. Данные отношения схематично можно представить на *рис. 1*.

Информационное противоборство условно можно рассматривать на *трех уровнях* – противоборство между государствами, конкуренция в сфере бизнеса и борьба интересов на человеческом уровне. Данные уровни взаимосвязаны. Сторонами в противоборстве могут быть государства, общественные группы, технические системы, что, в свою очередь, определяет вид и масштаб противостояния.

Настоящий период развития истории А.А. Зиновьев определяет так: "Теперь история не происходит по своему капризу, стихийно. Она… делается сознательно, можно сказать – по заказу сильных мира сего"[3].

К причинам, характеризующим нынешнее состояние информационного развития общества, он относит следующие:

1) прогресс средств сбора, обработки и передачи информации;

2) прогресс средств коммуникаций;

3) прогресс средств манипулирования людьми, надзора за ними, пресечения массовых движений;

4) влияние массовой культуры на стандартизацию образа жизни людей.

Сила стороны стала выражаться в наличии у нее новейших информационных технологий и возможности использования информации, что оказывает влияние на степень предсказуемости и запланированности развития истории.

Информационное противостояние определяется следующими состояниями:

поведение сражающихся субъектов определяется имеющимися у них моделями мира, области интересов;

используются специфические методы ведения противостояния, основанные на использовании знаний и информации;

средство ведения противостояния – информационный поток;

применяется информационное оружие;

субъекты ведения противостояния – самообучающиеся системы (человек, системы искусственного интеллекта);

борьба осуществляется исключительно путем целенаправленного информационного воздействия на субъектов;

объекты противостояния – смысловые модели противника;

цель – нарушение внутренних и внешних связей самообучающейся системы (т.е. связей, предназначенных для функционирования системы, ее взаимодействия с окружением и ее обучения).

Информационное противоборство возникает тогда, когда более сильные стороны желают воздействовать на другую сторону, используя информационное оружие с целью поделить информационное пространство, контролировать и управлять происходящими в нем процессами. С уверенностью можно сказать, что любое информационное воздействие на субъектов осуществляется во взаимосвязи технико-технологических, аппаратно-программных средств и информации, которую они распространяют. Такие средства позволяют создавать, передавать, уничтожать, модифицировать и похищать информацию.

В какой мере информационное оружие относится к информационным технологиям, к информации или к синтезу технологии и информации? Федеральным законом "Об оружии" от 13 декабря 1996 г.[4] к оружию отнесены *устройства* и

[3] *Зиновьев А.А.* Русская трагедия. М., 2007. С. 90.

[4] См.: Собрание законодательства РФ. 1996. № 51. Ст. 5681.

предметы, конструктивно предназначенные для поражения живой или иной цели, *подачи сигналов*. Информация не может быть отнесена к устройствам, так как по Закону РФ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г.[5] информация – это сами сигналы (сообщения, данные), которые могут производить устройства или предметы. Взяв для примера техническое определение информации, представляющее ее как абстрактную величину, выраженную посредством конкретного сообщения, и основываясь на данном определении, информацию также нельзя отнести ни к предметам, ни к устройствам – информация есть величина. Исходя из этого, приходим к следующему заключению: технико-технологические и аппаратно-программные средства в информационном противоборстве относятся к информационному оружию, а информация – к предмету отношений, т.е. к процессу воздействия на субъектов с использованием информации.

Оружием информационного противоборства могут являться любые каналы связи, аппаратно-программные средства, технико-технологические системы, средства массовой информации, носители информации. Таким образом, по законодательству к информационному оружию следует относить только технико-технологические или аппаратно-программные средства и иные устройства и предметы, позволяющие передавать сигналы, информацию, информационный поток с целью нанести ущерб гражданскому обществу, государству; различным системам взаимодействия. Этому оружию присущи универсальность, скрытность, многовариантность форм реализации, широкие возможности в выборе времени и места применения.

Большинство авторов придерживаются позиции, что информационное оружие – это технико-технологические и аппаратно-программные средства. Например, Д.С. Черешкин, Г.Л. Смолян и В.Н. Цыгичко считают, что информационное оружие – это средства уничтожения, искажения или хищения информации; преодоления систем защиты; ограничения допуска законных пользователей; дезорганизации работы технических средств, компьютерных систем. К атакующему информационному оружию они относят:

компьютерные вирусы;

логические бомбы (программные закладки);

средства подавления информационного обмена в телекоммуникационных сетях, фальсификацию информации в каналах государственного и военного управления;

средства нейтрализации тестовых программ;

различного рода ошибки, сознательно вводимые в программное обеспечение объекта[6].

А.А. Стрельцов и Г.В. Емельянов под информационным оружием понимают *«специальные средства, технологии и информацию*, позволяющие осуществлять "силовое" воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства»[7]. Данные авторы отнесли к оружию и информацию, хотя по Закону "Об оружии" это не предусмотрено.

Что же такое информация в информационном противодействии?

К информации (лат. *information* – разъяснение, изложение) относятся:

1. Информирование.

2. Сообщение о положении дел где-либо, о каких-либо событиях и т.п.

3. Сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами[8].

Исходя из того, что информация должна иметь количественные и качественные характеристики, попробуем дать ее определение и предназначение в информационном противодействии. Количество и качество совокупности информации определяют область, масштаб и глубину возможного воздействия. Качество выражается структурой совокупности информации и определяет возможные стороны воздействия, а также возможность деления информационного противостояния на информационный конфликт и информационную войну. Количество определяет область и масштаб охватываемого воздействия, а также объем информации, передаваемый от одной стороны к другой, выступает мерой информационной агрессивности. При этом возникает вопрос о *возможности распространения нормативного регулирования на информационную агрессивность, регламентации, фиксации и определения данной меры. Причем в этом случае неважно, какой характер имеет передаваемая информация*. Величина, характеризующая информацию, определяет величину информационного противостояния и результат такого противостояния.

Исход информационного противостояния зависит от количественных и качественных характеристик информации и не зависит от типа (аппа-

[5] См.: Собрание законодательства РФ. 2006. № 31 (Ч. 1). Ст. 3448.

[6] См.: *Черешкин Д.С., Смолян Г.Л., Цыгичко В.Н.* Реалии информационной войны // http://www.politic.donetsk.ua/terror/terror016.shtml

[7] *Емельянов Г.В., Стрельцов А.А.* Информационная безопасность России. Учебное пособие / Под ред. А.А. Прохожева. М., 2000, С. 34.

[8] См.: Большой толковый словарь русского языка / Сост. и гл. ред. С.А. Кузнецов. СПб., 1998. С. 397.

ратно-программных, технико-технологических систем) применяемого информационного оружия. Одну и ту же информацию можно применять в различных типах информационного оружия, например используя каналы связи, СМИ, программное обеспечение. Уникальность состоит в том, что информационное оружие вторично используемой, распространяемой, модифицируемой информации. Изначально создается информация, а далее ее распространяют аппаратно-программные и технико-технологические системы. Отсюда следует, что информация является средством ведения противостояния, предметом информационных отношений.

Авторы, исследовавшие отношения, возникающие с применением информационного оружия, уходили в плоскость информационных войн. Например, С.П. Расторгуев видит информационную войну как стратегию, "операции, тактические действия, проводимые в мирное время, во время кризиса, конфликта, войны, в период восстановления мира между соперниками, конкурентами, врагами с использованием современных информационных технологий, чтобы достигать своих целей"[9].

Информационная война в различных определениях представлена по-разному. Однако во всех определениях фигурирует очень важная схема – воздействие на систему через информацию с целью внесения хаоса в межэлементные связи системы, вызвав тем самым ее разрушение и достигнув своей цели. Следует отметить, что информационное противостояние – это не только информационная война, но и информационный конфликт. И в том и другом состоянии используется информационное оружие, а цели вовлечения сторон в такое противостояние одинаковы.

В чем же состоит отличие информационной войны от информационного конфликта?

Военный энциклопедический словарь дает определение войны как сложного, специфического общественно-политического явления, продолжение политики насильственными средствами, подчиняющейся своим законам[10]. В начале прошлого века американский конгрессмен Н. Додд четко определил назначение войны как наиболее действенного средства для изменения жизни целого народа. Война имеет две диалектически связанные стороны – социально-политическую и военно-техническую. В настоящее время военно-технический арсенал оружия пополнился новыми средствами информационного воздействия.

Под конфликтом в широком смысле понимается война[11]. То есть в узком смысле под войной можно понимать конфликт, но для этого противостояние должно быть ограничено одним из трех уровней взаимоотношений, указанных выше, например территорией государства. Если ведется информационное воздействие на различные по своей структуре социальные группы, то можно говорить об информационной войне, а не об информационном конфликте, так как под такое воздействие попадает большая и разнообразная по структуре группа, т.е. информационная война вовлекает все три вышеназванных уровня взаимоотношений – государство, сферу бизнеса и человеческие интересы.

При рассмотрении понятия "информационная война", как правило, выделяются две ее составляющие: *наступательная* и *оборонительная*[12]. *Наступательная* информационная война предполагает использование разнообразных средств и методов воздействия на информационные системы противника в целях снижения эффективности их функционирования. *Оборонительная* же включает в себя проведение различных мероприятий с использованием средств и методов противодействия эффективному применению информационного оружия противником. Особенность информационной войны – необходимость одновременного проведения как наступательных, так и оборонительных мероприятий.

Три волны развития науки и техники включили в себя четыре вида прошедших войн и пятую – настоящую. Начиная с третьей войны – это войны информационные. "После 1945 года в мире началась Третья мировая война, которая превратилась в цепь непрерывных операций непрямого действия и которая закончилась блестящей победой Запада и новых кочевников над нашей Империей – Советским Союзом – в декабре 1991 года. После 1991 года началась Четвертая мировая – война за передел мира, война финансовая, но эта война получилась сравнительно короткой, окончательного успеха агрессору принести не смогла"[13]. В 2002 г. началась Пятая мировая консциентальная[14] война, в основе которой лежит уничтожение человеческой способности к свободной идентификации, т. е. способности каждого из нас к самоопределению.

По мнению И.И. Завадского, "информационная война состоит из действий, предпринимаемых

[9] *Расторгуев С.П.* Теория информационной войны. М., 2002. С. 28.

[10] См.: Военный энциклопедический словарь / Гл. ред. Н.В. Огарков. М., 1984. С. 151–152, 354.

[11] См.: там же.

[12] См.: *Гриняев С.Н.* Информационная война: история, день сегодняшний и перспектива. СПб., 2000. С. 240.

[13] *Калашников М., Крупнов Ю.* Гнев орка. М., 2003. С. 23.

[14] Консциентальная война предполагает конкуренцию форм организации сознаний, где ***предметом поражения и уничтожения являются определенные типы сознаний***.

для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой нашей собственной информации и информационных систем"[15].

Противоборство интересов государств оказывает влияние на внутригосударственные и межгосударственные отношения, т.е. на внутреннюю и внешнюю политику государств, а привлечение новых информационных технологий предоставляет возможность более быстрого и дешевого воздействия.

Рассматривая информационное противоборство в Интернете, можно говорить только об информационной войне, так как трансграничная реализация сети вовлекает во взаимоотношения все государства; уровень человеческих интересов определен включением всех субъектов, находящихся в государствах, что демонстрирует объединение различных человеческих сообществ и бизнеса. Если противоборство не охватывает различные уровни взаимоотношений, то необходимо говорить о конфликте, например конфликт на границе, отказ в работе системы, конфликт в организации, коллизии.

Таким образом, началом информационной войны и информационного конфликта является информационное противостояние, но разделить эти схожие понятия можно путем учета факторов: локальность территории и массовость участников противостояния.

Основная цель такого воздействия – дезорганизация работы других систем. В связи с подобием отношений, возникающих при информационном конфликте и информационной войне, будем говорить об информационном противоборстве, которое включает в себя и конфликт, и войну.

Информационное противоборство использует различные методы достижения цели. К таким *методам* можно отнести: психологический, нейролингвистического программирования, дезинформационный, компьютерного моделирования. *Цель* таких методов – разрушение структуры системы противника. "Предметом теории информационных войн являются модели, создаваемые информационными субъектами и служащие для управления этими субъектами"[16].

Различные модели воздействия, использующие данные методы, можно классифицировать следующим образом:

невидимая модель – модель, к которой у остальных систем общества не выработано никакого отношения. Цель функционирования такой модели – разрушение системы противной стороны "невидима" или "невоспринимаема" обществом.

Например, передачи, формально определяемые как развлекательные, аналогично воспринимаемые обществом, но по замыслу их создателей подрывающие мораль и нравственность гражданского общества. Основой этой модели разрушения является возможность маскировки под благовидную сущность идеи;

опасная модель – модель, которая (будучи осознанной миром) приведет к частичному или полному разрушению, уничтожению этого мира.

Например, воздействие, направленное на разрушение СССР. Каждое общество для самосохранения использует релевантные информационные режимы. Так, бывший Советский Союз ограничивал возможности внешних коммуникаций, видя в них опасность для сохранения строя. Запад же, напротив, настойчиво требовал культурных обменов, по которым в результате приходила губительная для СССР информация.

Информационное воздействие ведется только на объект (сознание, накопленный опыт, модель моделирования внешнего окружения) субъектов – самообучающихся систем, так как только они могут реагировать на потоки информации, накапливая опыт прохождения стадии обучения. Опыт – это переработанная и усвоенная системой информация, трансформируемая в знания.

Все самообучающиеся системы можно разбить на *два класса*. К *первому* относятся все биологические системы, но из множества элементов биосистемы нас в первую очередь интересует человек как самостоятельный субъект воздействия и как основной элемент более сложной социальной структуры – гражданского общества, общественных организаций, государства и т.п.

Ко второму классу относятся технико-технологические системы – системы искусственного интеллекта, которые изначально формировались как системы, моделирующие деятельность мозга человека. Они должны заменить его в чрезвычайных ситуациях, в коих человек в силу физиологического состояния не может быстро охватить объем поступающих данных и принять решение.

Информационное воздействие может быть оказано на данные классы систем, так как только они оперируют такой категорией, как "сознание" – отношение к миру и самому себе, и являются носителями смысла и сознания. При возникновении информационного противостояния происходят создание, модификация, распространение, уничтожение, навязывание и блокирование носителей смысла – информации. Основная задача такого противостояния – изменение модели внешнего

[15] *Завадский И.И.* Информационная война – что это такое? // http://www.fbr.donetsk.ua/InfoWar/text01.shtmll.

[16] *Расторгуев С.П.* Информационная война. Проблемы и модели. Экзистенциальная математика. М., 2006. С. 9.

окружения, которое окажет воздействие на структуру системы.

Роль права в противоборствах должна заключаться в охранительной, регулятивной и запретительной функциях. Однако существует значительная разница в реализации функции права в противоборствах без использования информационного оружия и с использованием такового.

Ведение информационного взаимодействия, охватывающего формы противоборства, происходит в среде, где действуют определенные законы, международные соглашения, конвенции. Но ведение информационного противоборства, где в качестве средства воздействия выступает информационный поток, не поддается регламентации правом, так как информационное противоборство выходит за рамки классических военных отношений. Это связано с тем, что использование информационного оружия имеет другую среду – сетевую, что позволяет вести противоборство скрытно, без явных физических жертв и сохранять наступательный характер. Информационное противоборство не имеет алгоритма начала и окончания конфликта.

В связи со скрытностью противоборства противник получается неясным и рассредоточенным, его удары очень трудно отражать. Само противоборство превращается в тотальное, сплошное. Нет уже фронтов, есть многомерное пространство противостояния, которое захватывает политику, право, культуру и экономику, технологии, проникает в города и в идеологию. Американский политолог Дж. Аркилла и его коллеги отмечают, что основой такой сетевой войны сегодня становится бурно растущий третий социальный сектор. Это – огромное разнообразие самоуправляемых частных или неправительственных организаций. Несмотря на то что распространение информации фиксируется технологиями, воздействие на субъектов не всегда можно выявить. Результаты такого воздействия могут проявиться через некоторое время.

Дж. Аркилла, приводя многочисленные подтверждения из работ других исследователей, показывает, что социально-сетевые войны ведутся на транснациональной основе. Огромная роль в них принадлежит целевому проектированию и использованию форм коммуникаций и информационных технологий. Однако это не исключает, а как правило, обязательно включает боевые отряды людей как небольшой по количеству, но важнейший элемент сетевых децентрализованных организаций, которые и организуют социально-сетевую войну[17].

[17] См.: *Arquilla J. and Ronfeldt D.* The Emergence Noopolitik. Toward and American Information Strategy. Santa Monica, 1999.

Целью информационного противоборства выступает психологическое состояние человека, общества. Можно говорить о победе, если эти системы (люди, общество), на которые направлено разрушение, стали реагировать на созданную противником модель, сделались зависимыми от такой модели и пытаются исправить ситуацию, бросая на это огромные силы.

Формирование сознания, идей, опыта и целей самообучающихся систем зависит от следующих параметров: *во-первых*, от качества и количества информационного потока, проходящего через такие системы, а также от того, в состоянии ли система противостоять этому потоку, и от возможности информации за определенное время успеть остаться и прорасти в системе; *во-вторых*, от организации самой системы и качества связей данной системы, т.е. от того, какими элементами представлена система и насколько они подвержены воздействию.

Подверженность воздействию зависит от множества факторов, например от *качества накопленного опыта* (известно, что некоторым людям требуется время для усвоения и понимания полученной информации, другие все "схватывают на лету", третьи просто не поймут, и информация пройдет мимо них или войдет и усвоится помимо их воли); *от крепости и зависимости внешних и внутренних связей этого элемента с другими элементами в системе* (т.е. некоторые люди независимы в своих суждениях, не связывают себя с мнением окружающих, другие ориентируются на общественное мнение и формируют свои идеи в непосредственной связи с другими элементами).

Безопасность системы определяется не только знаниями, которые данная система получает о противнике, но и теми из них, от восприятия которых ей удалось уклониться. Все это свидетельствует о специфичности проблематики информационного противостояния, связанной с особенностями ее объектов – смысловыми моделями противника и субъектами ведения противостояния – самообучающимися системами.

Реализация информационного противоборства имеет два измерения: *технико-технологическое*, позволяющее зафиксировать наличие информации, и *правовое*, позволяющее дать правовую оценку качеству и количеству информационного потока. Для оценки воздействия необходимо определить содержание, структуру, объем и направленность информационного потока, что сделать правовыми средствами довольно сложно, так как передаваемая информация с точки зрения нормативной классификации информации может относиться к открытой, но содержание, структура информации могут быть направлены на неявное разрушение структур функционирования другой стороны. Поэтому распространение подобной информации

по формальному признаку запретить нельзя, так как в ст. 29 Конституции РФ определено право на свободу слова.

Право в таких противоборствах должно определить соотношение между свободой слова и секретностью, открытостью глобального информационного пространства и вопросами информационной безопасности государства, защитой информационных систем от внешних атак. Вопросы правового регулирования информационной сферы в России еще ждут своего решения.

Таким образом, разнообразие сторон в информационном противоборстве, его фактическая неявность, сетевая среда и глобализация действий обязывают выработать новые взгляды на роль и место права в регулировании информационных противоборств.