РАЗДЕЛ X. ПОЛИТОЛОГИЯ

Сидорова А.П.

Понятие цифрового пространства и его характеристики. Возможности и угрозы использования цифрового пространства

*Тюменский государственный университет
(Россия, Тюмень)*

doi:10.18411/spc-22-05-2020-11

idsp: sciencepublic-22-05-2020-11

С теоретической и с практической точки зрения понятие «информационное пространство» изучено в контексте разных сфер деятельности. В зависимости от сферы деятельности применяется различная терминология для создания семантического поля данного термина.

В философии лексема «пространство» представляет собой основополагающее определение в такой науке как философия. А.А. Ивин дает следующую коннотацию в своем исследовании: пространство является фундаментальным понятием человеческого мышления, которое раскрывает многосторонний характер существования мира как единого целого, а также его ликвацию. Наиболее распространен термин “пространство” в реальных науках, но в связи с ускоренными темпами глобализации данное понятие получило свое распространение в других сферах. Например, на данный момент с понятием “цифровое пространство” могут использоваться такие уточняющие компоненты как семантическое, гносеологическое и другие пространства. В зависимости от точной характеристики наук, употребление термина “пространство” делает ссылку на взаимодействие между двумя или более точными дисциплинами. Исходя из определения цифрового пространства, которое воспринимается как новая среда для существования современного общества, оно имеет свои показательные характеристики. Ключевая характеристика – виртуальность, которое уже давно вышло из рамок области компьютерных наук. В настоящее время актуальными становятся выражения, которые связаны с понятием “виртуальность”: виртуальные денежные средства, виртуальная кампания, виртуальная должность. Исходя из этого виртуальность становится конкретной и достаточно осязаемой истинностью. В настоящее время термин “цифровое пространство” может быть рассмотрено как одна из сторон киберпространства.

Следует отметить, что понятие пространство является широко употребляемым в различных науках, в некоторых из них, например, в гуманитарных науках, оно является таким средством выразительности как метафора.

Дэвид Белл, философ, доцент в университет в западном Кентукки, определяет цифровое пространство как отдельную единицу, которая может быть рассмотрена не как составляющая киберпространства, а как определенный исход взаимодействия между реальностями.

В работах известных петербургских учёных С.Н. Иконниковой и В.П. Большакова дается толкование «цифровое пространство» - это абсолютно новый тип реальности, который во многом уподобляется термину «виртуальная реальность». В этих исследованиях цифровое пространство изучается, прежде всего, с точки зрения культурного и аксиологического подходов. Отличительной характеристикой цифрового пространства, как отмечают авторы, является его постоянная трансформация и распространение на новые социальные группы и территории, поэтому мы можем прийти к выводу, что цифровое пространство определенно носит транснациональный характер.

По мнению И.А. Добровольской, понятие цифровое пространство созвучно с понятием информационное пространство. Проведем анализ разных подходов[2].

В экономической сфере сформировано определение цифрового пространства, которое было положено С.Э. Зуевым – экономистом, изучающим информационное пространство как платформу и давший также ему другое название – информационная действительность. С. Э. Зуев под информационным пространством понимал информационную действительность, выраженную в правилах игры, новом типе субъектов деятельности в информационном поле[6]. С его точки зрения, информационное пространство выступает фактором глобальных изменений на всех уровнях социальной модернизации для выстраивания стратегии деятельности и политики в информационном поле. Цифровое пространство рассматривается как цепь ключевых элементов, взаимодействующие между собой в информационной реальности, а также технологии, обеспечивающие это взаимодействие. Необходимо учитывать важный фактор для формирования коннотации данного термина, что информационное пространство – исход взаимодействия информационных ресурсов, методов информационного взаимодействия и инфраструктуры. В рамках данного подхода к элементам информационного пространства относятся тип знаний, коммуникаций и субъектов, формирующих особую политику в информационном поле.

С.А. Модестов под информационным пространством понимал процесс конкуренции специфической среде, тесно связанной с сегментами международного экономического, политического, военного, социального сообщества[6].

В работах Г.М. Ниязовой, Т.Ф. Берестовой, А.И. Ненашева информационное пространство является сложной и поле функциональной системой стратификации языковых и неязыковых знаков в рамках функционального подхода[7]. По их мнению, информационное пространство многомерно. Это процесс динамичного формирования информационных барьеров в культуре.

А.И. Ненашев формулирует определение информационного пространства в философской науке как аспект по распространению информации в сложившемся обществе, имеющий отражение на культурные, экономические, политические, технологические и другие факторы[8].

В.Д. Попов, сторонник научного направления социальной информатиологии, под информационным пространством понимает неопределенное количество потоков, взаимодействующих с воспроизводством, восприятием, оценкой, выработкой, отношениями, диспозицией и позицией к информации, формирующие в целом социальное поведение и мотивацию личности[9].

Цифровое пространство включает в себя цифровое инфраструктуру и цифровые ресурсы. К цифровой инфраструктуре относятся: аппаратные средства, программное обеспечение, телекоммуникации, сети. К цифровым ресурсам относятся базы данных, оцифрованные образы физических объектов. К средствам цифрового взаимодействия относятся: процессы, технологии, методы управления.

Ключевыми стратегическими целями развития цифрового пространства являются[3]:

1. Усиление конкурентоспособности экономики во всех субъектах государства.
2. Экономическая стабильность.
3. Включение стран ЕАЭС в глобальные и региональные трансформационные процессы, формирующие цифровую экономику рынков.
4. Совершенствование и развитие человеческих ресурсов в ходе прогрессии цифрового пространства.
5. Повышение жизненного уровня населения.
6. Усовершенствование существующих систем.

В свою очередь, в качестве тактических целей цифрового пространства выступают: мобилизация экономических процессов и сферы сервиса в результате их оцифровки; оцифровка физических объектов и территории, необходимых для реализации цифровых экономических процессов.

Существует две структуры информационного пространства. Согласно первой структуре, в качестве элементов информационного пространства можно выделить: реквизит, составная единица информации (СЕИ), показатель, база данных и хранилище данных[10].

Реквизит – это информационное описание ключевых характеристик предмета или информационного проявления. Это означает, что элементарная единица информации формируется из совокупности подходящих реквизитов и затем представляет собой отображение в виде информации определенного объекта или его составляющей.

Показатель - термин, характеризующийся своей многозначностью. С одной стороны, показатель рассматривается как существенный элемент, привязанный к предметной области, в частности экономической. С другой стороны, исходя из формально-структурного подхода, показатель - законченное высказывание, которое состоит из названия переменной величины, конкретного количественного значения со всеми качественными признаками, необходимыми для идентификации последнего.

Другой важной характеристикой цифрового пространства является связь между ним и сетью. Цифровое пространство ни в коем случае не должно соотноситься с понятием “сеть” или описываться как совокупность данных, но одновременно должно являться зависящей единицей осуществляющей работы информационно-коммуникационных сетей. Цифровое пространство - пространство, контролирующее реализацию и функционирование сетей компьютеров. Из этого исходит вывод, что любая деформация между взаимосвязанными компьютерами (например, потеря мощности), будет отражаться на формат работы и взаимодействия в цифровом пространстве.

Все сферы социума, связанные с процессами жизнедеятельности, функционируют посредством виртуальных коммуникаций. Социум в зависимости от формирования условий приходят к приобретению и адаптации новой формы, но не отделяются от социальной реальности.[4]

Рассмотрев второй вариант структуры цифрового пространства, она включает в себя следующие составляющие:

- структура (Интернет, корпоративные сети, одноранговые сети, программные платформы);
- ультраструктура (иносфера - различные виды данных, которые человек способен воспринимать).

Анализируя развитие сети Интернет как структуры цифрового пространства, можно выделить следующие этапы его становления:

1. web 1.0. - правительственные, корпоративные, онлайн-блоги, сайты - они доступны абсолютно для каждого пользователя и легко ищутся в поисковых системах;
2. web 2.0. - охватывает все социальные платформы, поэтому многие называют его «социальным вебом»;
3. web 3.0. - эта составляющая сети Интернет растет с большой скоростью, которая позволяет устанавливать соединение между Интернетом и пользователями облегченно;
4. WEB 4.0. (нейронет) – характеризуется ускорением работы массивно-параллельных цепей, использованием интеллектуальных виртуальных агентов, формирование полного хранилища человеческих знаний;

5. невидимый Интернет - сервисы, которые не обнаруживаются поисковыми машинами. Они отображаются только при специальном разрешении к доступу (то есть, это данные финансового, научно-технического, экономического, государственного контента);
6. «Интернет вещей» - соединенные между собой встроенные блоки, которые предоставляют информационные данные, являющиеся частью Всемирной сети технологических линий.

Таким образом, анализ различных подходов к понятию информационное пространство позволил установить, что данная проблема актуальна в разных научных направлениях. Цифровое пространство является предметом изучения представителей разных научных направлений - философии лингвистики, культурологии, экономики, информатики, политологии, математики. При определении цифрового пространства первоначально раскрываются две категории - “пространство” и “цифровизация”, каждое из данных понятий имеет свою коннотацию. При изучении понятий “цифровое пространство” и “информационное пространство” необходимо учитывать разницу между коннотациями этих понятий: информационное пространство представляет собой продукт (результат) деятельности человечества, а цифровое пространство - это виртуальная версия пространства, совокупность информационных ресурсов, пространство, в котором люди могут вступать в цифровое взаимодействие. Цифровое пространство состоит из реквизита, составной единицы информации (СЕИ), показателя, базы данных и хранилища данных, каждая из составляющих имеет свою функцию и свою роль в реализации всей работы пространства. Основываясь на междисциплинарных связях, в ходе написания исследования мы сформулировали собственное определение термина “цифровое пространство” - виртуальная версия пространства, которое включает предоставление специализированной разносторонней информации, осуществление различных видов деятельности при помощи персонализированных автоматических средств, что обеспечивает мобильность, автоматизированность к получению, обработки и передачи информации.

Необходимо отметить, что цифровое пространство включает в себе как положительные, так и отрицательные аспекты, так как оно является площадкой для демонстрации различных ориентиров. На сегодняшний день существуют факторы, которые влияют на распространение сети Интернет, увеличение пользователей и сфер, которые стали вовлеченными в кибер-пространство, массовое распространение агрессивного и деструктивного контента в сети, формируют угрозу унификации и модификации культур.

Цифровое пространство становится неотъемлемой составляющей в происходящих процессах жизнедеятельности социума. С его развитием необходимо отметить улучшение процессов различных видов жизнедеятельности, а также привело к автоматизации и улучшением в таких сферах как экономика, здравоохранение, образование, культура, космическая и военная отрасли. Благодаря цифровизации возникают каждый день новые формы организации управления с применением инновационных средств, которые используются для проведения анализов, аналитики, сбора и обработки информации.

Стремительное развитие цифрового пространства в наше время формирует множество положительных аспектов жизни в виде удобства коммуникации, скорости получения, обработки и передачи информации. Но также стоит отметить, что использование новых цифровых технологий может привести к очень серьезным угрозам и рискам. Расширение цифровых услуг и индивидуализация многочисленных видов услуг повышают риск мошенничества, одновременно снижая контроль над пользователями или поставщиками.

Организация ООН уделяет большое внимание факту цифровизации всех сторон общественной жизни. Цифровые технологии вносят большой вклад в реализацию

повестки дня в Области Устойчивого Развития на период до 2030 года, размытость границ и уникальные сторонники различных социально-экономических и политических взглядов, и поэтому сотрудничество с широким кругом отраслей и стран является неотъемлемой частью цифровых технологий. Для того чтобы реализовать потенциал, снизить связанные с ним риски и смягчить непреднамеренные последствия

Генеральный секретарь Организации Объединенных Наций сформировал группу высокого уровня по цифровому сотрудничеству для содействия выдвижению предложений по укреплению сотрудничества в цифровом пространстве между правительствами. Задача группы состоит в том, чтобы повысить осведомленность о преобразующей силе цифровых технологий в социально-экономическом плане, рассмотреть соответствующие нормы в области прав человека, содействовать всеобщей безопасности и включению в цифровое пространство будущего[12].

Говоря об угрозах цифрового пространства, следует рассмотреть возможности его использования в деятельности экстремистских и террористических организаций. Если рассматривать технологический аспект компьютерного терроризма, то по данным экспертов наибольший интерес для террористов вызывают следующие сферы: энергетическая сфера, военная и ядерная структура государства, сфера транспортных перевозок, в том числе перевозки, осуществляемые воздушным транспортом, а также финансовая сфера государства. Согласно публикациям, в иностранной прессе, хакерские атаки особенно опасны для химических заводов, самолетов и систем энергоснабжения. По последним исследованиям ученых, военные и пассажирские лайнеры, оборудованные чипом со встроенной функцией контроля полета, могут быть взломаны с помощью вируса «Flame»[13], посредством доступа к микрочипу через Интернет. При этом взломщик получит доступ к системе управления движением самолета и запросто сможет вывести машину из строя.

Современный религиозный экстремизм и террористические организации все больше накапливают все имеющиеся возможности для преступных целей, включая широкий спектр возможностей, предоставляемых глобальным информационным пространством, а интернет становится все более важным инструментом пропаганды терпимости и универсальности насилия как способа игнорирования политических проблем, правового нигилизма, основных прав и свобод человека. Необходимо отметить, что количество пользователей сети Интернет увеличивается в постоянной геометрической прогрессии, в октябре 2018 года число пользователей достигло 4,2 миллиарда человек.[11]

В ближайшем будущем, по мнению аналитиков, экстремизм и терроризм в глобальном информационном пространстве станут приемлемой альтернативой традиционным экстремистским и террористическим актам по многим причинам.

Международные эксперты отмечают, что многие вопросы безопасности в глобальном информационном пространстве лежат в основе важнейшей задачи дальнейшего развития киберпространства - "всемирной паутины" современная платформа для ведения "информационных войн", которые могут угрожать жизни людей и нести опасные последствия для общества. Благодаря многочисленным малым группам, которые пытались быть известными через всемирную паутину, а также давним организациям, экстремистские организации и террористические организации все чаще используют многочисленные социальные сети, которыми активно пользуются представители разных возрастов и социальных групп. В качестве примера осуществления террористической атаки от социальных сетей рассматривается теракт группировки «Аль-Шабаб» в торговом центре «Westgate» (21 сентября 2013 года, Кения). На протяжении нескольких дней террористы осуществляли жестокие убийства заложников и комментировали это в режиме в «Twitter» и «Facebook».[14] Теракт, совершенный террористами Царнаевами, которые осуществили террористическое действие 15 апреля 2013 года в городе Бостон (Соединенные штаты Америки). Ими

были заранее опубликованы планы действий, которые были проигнорированы агентам спецслужб.[15]

Большое внимание уделяется оформлению террористических и экстремистских интернет-сайтов, которые, как правило, сочетаются с большим количеством визуальных фотографий, аудио-и небольших статей.[5] Помимо наличия большого количества визуальной информации, облегчающей узнаваемость сайта посетителями, это, как правило, голосование, баннер аналогичных интернет-страниц, сетевое объединение также является важным фактором, обеспечивающим интернет-пропаганду, то есть, одна и также информация может быть распространена на нескольких информационных социальных платформах.

Исходя из анализируемых данных, наиболее популярными социальными сетями, которые активно и постоянно используются террористами для вербовки, распространение пропагандистских взглядов, а также для оповещения о реализации террористических актов, являются «Facebook» (2 млрд.), «YouTube» (1,5 млрд.), «Instagram» (700 млн.), «Twitter» (более 328 млн.).[16]

Следующий риск, который может возникнуть при реализации деятельности в цифровом пространстве - кибер-атака, которая трактуется как преднамеренный и организованный взлом компьютерных сетей или массовое распространение вирусов в компьютерной цепи. Существует большое количество различных средств и ресурсов, с помощью которых кибер-атака может реализовываться: Mailbombing, переполнение буфера, вирусы, sniffеры, руткиты, сетевая разведка, sniffing пакетов, инъекция кода, социальная инженерия, отказ в обслуживании и многие другие. Все эти средства объединены тем, что имеют общую цель - захват контроля и выведение из работы системы и приведение к ее дестабилизации.

Примером одной из многочисленных атак можно отменить кибер-атаку, реализуемую в ноябре 2018 года. Специалистами «Лаборатории Касперского» было обнаружено, что рассылаемые с адреса «Юнистрима» фишинговые письма содержали SCR-файл, который после загрузки устанавливал на компьютер вредоносное программное обеспечение. Ответственность за атаки, предположительно, лежит на группировке Cobalt. По мнению экспертов, новый взлом стал следствием некачественного расследования первого инцидента.

Информационная война является также одной из отрицательных сторон реализации действий в цифровом пространстве. Под данным термином понимается противоборствующий процесс, направленный на достижение результата в политической, экономической, стратегической сферах. Данное понятие было заимствовано из американского языка и с перевода *information and psychological warfare* трактуется как информационное противоборство. Информационная война имеет свои характерные черты такие как модификация моделей поведения людей и мира, реализация действий с целью возникновения информационного шума, навязывание чуждых мнений и концепций. Самое главное различие от других войн - это использование информации как главное военное средство. Примером такой войны может быть информационная операция в Ираке, проводимая Министерством обороны США. Суть информационной трактовки содержит следующую информацию: если частные подрядчики Ирана будут производить политические материалы, развлекательные средства для иракских средств массовой информации для привлечения местного населения к поддержке США, то, соответственно, это будет оплачиваться со стороны США.

Информационная война может являться одним из составляющих компонентов войны между двумя или более государствами. Например, в гражданской войне в Анголе в 1988 году кубинской противовоздушной системой обороны был сбит южно-африканский истребитель, обломки которого выдавались за обломки других самолетов, о сбитии которых было сообщено кубинцами.

Как указано в докладе экспертной группы правительства по развитию в области информатизации и связи в сфере международной безопасности, Генеральная ассамблея обсуждала вопросы международной безопасности 2016 и 2017 годов.[17] Особое внимание уделяется пункту, который гласит о соблюдении государствами-участниками международные обязательства в отношении международного неправомерного поведения в соответствии с международным правом. На случай возникновения инцидента, необходимо предоставить всю информацию о его возникновении в сфере информационно-компьютерных технологий, разрешение вопроса об установлении ответственности (определить степень и характер ответственности). Также было предложено обсуждения для поиска и реализации наилучших путей взаимовыгодного сотрудничества для реализации всех действий для обмена информацией, а также предотвращения преступлений террористами с использованием информационно-компьютерных технологий.

В ходе проведения ассамблеи каждая страна сознательно не допускает делегирования международного неправомерного поведения с использованием ИКТ или использования посредников для посредничества в международном неправомерном поведении на своей территории, а также страны соглашаются на исполнение своих обязательств по международному праву[17]. Страны должны реагировать на соответствующие требования, направленные на смягчение последствий злоумышленных действий в сфере ИКТ, которая является важнейшей инфраструктурой других стран.[17].

Важным аспектом является то, что страны не имеют права использовать уполномоченную компьютерную группу готовности к чрезвычайным ситуациям другого государства, а также государство в области использования ИКТ и ИКТ должно сотрудничать с частным сектором и организациями гражданского общества для реализации правил ответственного поведения государства в информационном пространстве с учетом потенциальной роли.

Цель такой стратегии заключается в постоянном изучении соответствующих международных концепций, направленных на повышение безопасности глобальных информационно-коммуникационных систем, и в том, чтобы все государства-члены учитывали области информации и коммуникации в контексте международной безопасности, информируя Генерального секретаря о своих взглядах и оценках по проблемам информационной безопасности, усилиям, предпринимаемым на национальном уровне для укрепления информационной безопасности, о принятии и реализации мер, которые могли бы содействовать укреплению информационной безопасности на глобальном уровне.[17]

Таким образом, использование информационного пространства влечет за собой принципиально новые качественные изменения в социально-экономических отношениях на государственном уровне и на уровне отдельных составляющих структур. Возможности использования цифрового пространства (киберпространства) сегодня бескрайни, с их внедрением мы наблюдаем большой прогресс в таких сферах как здравоохранение, образование, усовершенствование военной структуры, развитие космической обороны, культуры. Особенное распространение оно получило в области цифровизации экономики. В экономические отношения были внедрены новые информационные программы, появились такие технологии, как блокчейн-система.

Однако, наряду с огромным спектром возможностей, появляется и более обширный спектр угроз, например, неправомерный доступ к информации киберпреступниками, осуществление процессов над ее модификацией, реализация различных видов хищения. Исходя из статистических данных, из всех перечисленных сфер жизнедеятельности человека сферой, которая является наиболее востребованной для реализации кибер-атак, является финансовая сфера.

Но наиболее опасными угрозы связаны с террористами и экстремистами, которые активизируют свою деятельность в сети Интернет для осуществления своей преступной деятельности, а именно дезинформация общества, распространение паники среди населения того или иного государства, создание психологической атаки.[18] Рассмотрев проявления и виды компьютерного экстремизма и терроризма, мы пришли к заключению, что для противостояния с перечисленными угрозами необходим комплексный подход, который объединяет все формы и методы действий (политико-дипломатические, экономические, гуманитарные), которые также должны действовать в совокупности с антитеррористическими и антиэкстремистскими мерами.

1. Вестник Полоцкого государственного университета. Серия: педагогические науки. 2012. №15. С. 123-127.
2. Добровольская И.А. Понятие «информационное пространство»: различные подходы к его изучению и особенности // Вестник РУДН, серия Литературоведение. Журналистика, 2014, № 4. С. 140-147.
3. Жилкин В.В. К вопросу понимания сущности термина «информационное пространство» [Электронный ресурс] // Центр системного анализа. URL: <http://rosanaliz.ru/Post.aspx?Post=107> (дата обращения: 10.10.2019).
4. Игнатьев В.И., Степанова А.Н. Виртуальное социальное действие и трансформация повседневных практик // Вестник Московского университета. Серия 18. Социология и политология. 2010. № 3. С. 93.
5. Круликовский А.П., Усеинова Л.С. Угрозы киберпространства и их динамика // Проблемы информационной безопасности. - 2016. - С. 114-115.
6. Модестов С.А. Информационное противоборство как фактор геополитической конкуренции. М.: Московский общественный научный фонд : Издательский центр научных и учебных программ, 1999. 64 с. (12.10.2019).
7. Ниязова, Г.М. Современное информационное пространство полиэтнического региона: этнолингвофункциональный подход: автореф. дис. ... д-ра филол. наук: 10.02.19 / Г.М. Ниязова. Краснодар, 2008. 44 с. (12.10.2019).
8. Ненашев, А.И. Информационное пространство современного общества: коммуникационный аспект: автореф. дис. ... канд. филос. наук / А.И. Ненашев. Саратов, 2008. 32 с. (12.10.2019).
9. Попов, В.Д. Информациология и информационная политика / В.Д. Попов. М.: РАГС, 2003. 118 с. (12.10.2019).
10. Сороко С.М. Структура информационного пространства культуры //
11. Интернет в странах мира [Электронный ресурс] // Информационный сайт «Интернет в России и мире». URL: http://www.bizhit.ru/index/polzovateli_interneta_v_mire/0-404# (дата обращения: 27.04.2019)
12. ООН: Группа высокого уровня Генерального секретаря по цифровому сотрудничеству [Электронный ресурс] <https://www.un.org/ru/digital-cooperation-panel/> (Дата доступа: 29.03.2020)
13. Flame – самый сложный вирус, применяемый для шпионажа [Электронный ресурс] // Информационный портал «3D news». URL: <https://3dnews.ru/630129> (дата обращения: 27.04.2019)
14. Теракт в ТЦ в Кении [Электронный ресурс] // Информационное агентство «РИА новости». URL: https://ria.ru/attack_of_insurgents_in_Nairobi_21092013/ (дата обращения: 27.04.2019)
15. Теракт на Бостонском марафоне 15 апреля 2013 года [Электронный ресурс] // Информационное агентство «РИА новости». URL: <https://ria.ru/20180415/1518569022.html> (дата обращения: 27.04.2019)
16. Социальные сети в 2018 году: глобальное исследование [Электронный ресурс] // Информационный ресурс. URL: <https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/> (дата обращения: 27.04.2019)
17. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года Электронный ресурс: <https://undocs.org/pdf?symbol=ru/A/RES/73/27> (Дата доступа: 29.03.2020)
18. Павлов Н.В. Многомерный подход к противодействию киберугрозам // Авиационные системы. - 2016. - № 1. - С. 37