Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина
Институт физической культуры, спорта и молодежной политики

В. Л. НАЗАРОВ
Д. В. ЖЕРДЕВ

«БОЛЬШАЯ ИГРА» v. 2.0:
Россия в глобальном информационном пространстве

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА РОССИИ Б. Н. ЕЛЬЦИНА

В. Л. Назаров, Д. В. Жердев

«БОЛЬШАЯ ИГРА» v. 2.0:
Россия в глобальном информационном пространстве

Екатеринбург
Издательство Уральского университета
2018

УДК 316.343
ББК С033.2
Н192

Рецензенты:
А. Л. Семенов, доктор физико-математических наук, профессор, академик РАН, академик РАО, лауреат премии Президента РФ, Правительства РФ, ЮНЕСКО;
С. А. Рогожин, проректор по учебно-методической работе и качеству образования Уральского государственного экономического университета, кандидат физико-математических наук, доцент

Назаров, В. Л.

Н192 «БОЛЬШАЯ ИГРА» v. 2.0: Россия в глобальном информационном пространстве : монография / В. Л. Назаров, Д. В. Жердев ; вступ. ст. А. Л. Семенова. Екатеринбург : Изд-во Урал. ун-та, 2018. — 304 с.

ISBN 978-5-7996-2494-1

Исследуется процесс взаимодействия между субъектами инфосферы в условиях формирования новой системы общественно-экономических отношений глобального информационного общества, и в частности специфика развития ситуации в реалиях России. Отдельное внимание уделяется различным формам агрессивного взаимодействия в инфосфере, в том числе кибер- и информационным войнам.

Книга адресована широкому кругу специалистов, а также преподавателям и студентам разных направлений подготовки.

УДК 316.343
ББК С033.2

ISBN 978-5-7996-2494-1

Выбранное авторами «журналистское» название в книге приобретает серьезное содержание, далеко не ограничивающееся рамками противоборства «сверхдержав» на ограниченном плацдарме в XIX веке или популярной телепередачей. Игровая интерпретация глобальных, прежде всего информационных, процессов XXI века становится, пожалуй, центральной сегодня. Замечательно, что понятия информации, игры, вероятности, случайности и хаоса (в амбивалентном смысле) соединяются сегодня в самых разных исследованиях, включая, например, работы А. Н. Колмогорова (основателя наиболее перспективного сегодня подхода к понятию количества информации).

Начиная свое рассмотрение с наиболее общих, даже абстрактных понятий, авторы в современном стиле переходят к проблематике становления и развития информационного общества в Российской Федерации с учетом глобального контекста, а затем — к разностороннему рассмотрению проблем «информационных игр» — «информационных войн» современного мира.

Авторы подчеркнуто воздерживаются от прогнозов, а факты истории и философские концепты привлекаются лишь в той степени, в которой они необходимы для анализа ключевых проблем

современности. В работе использованы данные официальной и неофициальной статистики, фундаментальные научные исследования и произведения публицистов и философов, выступления политиков и документы инструктивного характера, наконец, широко привлекается современная интернет-публицистика разных направлений: таким образом, современная инфосфера представляется читателю как живое и изменчивое пространство коммуникативной активности с небезусловными на данный момент перспективами. Особое внимание уделяется исследованию форм агрессивного взаимодействия в информационном пространстве, обычно именуемую «информационными войнами», и наиболее распространенных концепций, описывающих эту агрессию.

А. Л. Семенов,
доктор физико-математических наук,
профессор, академик РАН, академик РАО

ПРЕДИСЛОВИЕ

В предлагаемой монографии четыре главы, введение и заключение. Введение поясняет читателю выбранный нами аспект исследования. В первой главе анализируется функционирование и развитие концепции «информационного общества» в академической науке, в медиасфере, а также в государственных и межгосударственных документах. Вторая глава описывает становление информационного общества в Российской Федерации в его социальных, экономических, юридических и образовательно-культурных аспектах в сопоставлении с текущей ситуацией в мире. Третья глава посвящена феноменам киберпреступности и кибервойн как проявлениям частной и/или государственной агрессии в киберсфере. Наконец, четвертая глава содержит комплексный анализ информационной агрессии, информационных войн и информационной безопасности в наиболее частотных интерпретациях этих феноменов — интерпретациях, имеющих определяющее значение в функционировании инфосферы и служащих базой для стратегических управленческих решений, в том числе государственного и межгосударственного уровня. Наконец, заключение подводит итоги исследования, констатируя переходный характер ситуации в инфосфере и доказуемую

неопределенность экономических, политических и социокультурных перспектив глобального сообщества.

Помимо собственно исследовательского материала, мы сочли целесообразным разместить как отдельный раздел список литературы, ориентированный не столько на демонстрацию материала, напрямую использованного в тексте, сколько на поддержку комплексного освоения исследовательского, методического и историко-культурного контекста по данному вопросу, что может быть полезным как студентам, получающим образование по специальностям социального профиля, так и широкому кругу заинтересованных читателей.

В. Назаров, Д. Жердев

ВВЕДЕНИЕ

Термин «Большая игра» впервые прозвучал в английской дипломатической переписке в середине XIX в. Тогда под ним подразумевалось столкновение интересов Российской и Британской империй в Средней и Центральной Азии — столкновение, которое не приводило, как правило, к прямому военному противостоянию, но велось посредством агентурной и дипломатической борьбы, опосредованного участия противников в локальных конфликтах, а также посредством противоборства пропагандистских образов и приемов в СМИ. В широкое употребление термин вошел, популяризованный Р. Киплингом в авантюрно-приключенческом романе «Ким», и это не случайная связь: слово «игра» воспринимается как указание на неофициальный, «игровой», «экзотический» (или, как сказали бы сейчас, «виртуальный» — для обитателей метрополии) характер конфликта, но также и на стратегическую значимость результата, на геополитический выигрыш в качестве ставки в игре. Позднее, в конце 90-х гг. прошлого века, в политической публицистике появился термин «Новая Большая игра» — для обозначения «игры на доминирование» в Центральной Азии, на Ближнем Востоке и на Кавказе, с США, Китаем и Россией в качестве основных игроков. Принципиальной разницы со «Старой игрой» тут, впрочем,

не наблюдается — это снова непрямое столкновение ограниченного числа активных сверхсубъектов, империй, в борьбе за территории/торговые пути/ресурсы/экономическое или военно-стратегическое превосходство. Отечественные геополитики, такие как М. Леонтьев, полагают, что «игра» на геополитическом поле (при более-менее сохраняющемся составе и статусе игроков) не прекращается уже более двухсот лет, рассматривая ситуацию через призму цивилизационных, геоэтнокультурно обусловленных столкновений «атлантистов» и «хартленда» — концепции, впрочем, позаимствованной из английской традиции (прежде всего следует вспомнить классическую статью Х. Маккиндера «Географическая ось истории»). Существуют и альтернативные термины с близким смысловым наполнением — например, знаменитая «Великая шахматная доска» З. Бжезинского.

Рубеж XX–XXI вв. стабильно рассматривается современными исследователями как период радикальных изменений в бытовой, социальной, производственной и научной сфере в рамках современной технологической цивилизации. «В их ряду информационная технология, научная парадигма информационных процессов и миропонимание информационной эпохи. Все это говорит о том, что развитие человечества в XXI веке всецело будет зависеть от успехов познания информационного мира»[1]. Поэтому ряд исследователей говорит о вступлении человечества в новую, «информационную» эпоху, о формировании «информационного общества» как принципиально нового типа экономической, социальной, политической общности. Другие видят в этом тезисе скрытую или явную опасность геополитического характера, идеологему, направленную на подрыв традиционного культурного кода. Более того, даже определяющий характер компьютерных технологий и современной коммуникативной сферы не общепризнан. «Развитие и внедрение новейших технологий связаны с неопределенностью и означают, что мы пока не имеем представления, как в дальнейшем будут развиваться преобразования, обусловленные этой промышленной революцией. Сам факт их сложности и взаимозависимости по всем секторам

[1] *Антоненко В. И.* Информационное единство мира : учеб. пособие. Монино, 1996. С. 314.

предполагает ответственность всех участников глобального сообщества — правительств, бизнеса, научного мира и общественности — за работу в тесном взаимодействии друг с другом, необходимом для лучшего осознания формирующихся тенденций»[2]. При этом радикальные изменения в социальной, экономической, политической, идеологической, коммуникативной, военно-стратегической сферах меняют, очевидно, и характер «Большой игры»:

— игра новейшего времени в первую очередь происходит посредством развития и практического применения новейших технологий, прежде всего технологий, связанных с вычислительной техникой, цифровой передачей и обработкой информации, роботизацией, виртуальной реальностью, дистанционным управлением и искусственным интеллектом;

— благодаря развитию и всеохватывающему проникновению компьютерных технологий и средств цифровой коммуникации эта игра приобретает характер всеобщей значимости, превращаясь из экзотического приключения на периферии цивилизации (как изображал ее Киплинг) в ситуацию, ***возможно***, напрямую влияющую на повседневное существование каждого представителя человечества. Война и политика все более виртуализируются, однако виртуальность при этом приобретает характер объективной реальности (см. гл. 4 § 2 о роли цифровых коммуникационных сетей в протестных социальных движениях или об онтологическом статусе 3D-печати) — граница между динамическим образом мира и самим миром, между «игровым» и «серьезным» постепенно теряет актуальность;

— по той же причине (ведущей к фактическому нивелированию возможностей глобальных империй и отдельных пассионарных личностей — см. подробнее гл. 3) происходит мультиплицирование субъекта игры: вместо пары «шахматистов» за «великой доской» мы наблюдаем хаотическое множество взаимодействующих на равных субъектов несопоставимого уровня;

— коммуникация продуцирует активность игроков, и сама является формой активности, поэтому взаимодействие на уров-

[2] *Шваб К.* Четвертая промышленная революция. М., 2016. С. 8.

не контента — обмен мотивировками, ценностями, принципами, концептами и т. п., — а также совместное создание нового контента становятся неотъемлемой (а по мнению части исследователей, даже и определяющей) составляющей игры;

— переходный характер эпохи делает небезусловным любой глобальный выигрыш (и проигрыш) ввиду возможной девальвации любых декларируемых идеологических или общепринятых экономических ценностей (см., например, действия администрации Д. Трампа по разрушению глобальной свободной торговли, дискуссии о экономическом статусе углеводородов или о возможности отказа от долларового эквивалента и многое другое) и, соответственно, возвышения новых, непрогнозируемых исходя из текущего военного, экономического, политического и научно-технического развития цивилизации — таким образом, сами цели Новой игры становятся неопределенными;

— соответственно, весь процесс игры становится хаотичным, непредсказуемым, и это позволяет исследователям и публицистам как аргументированно утверждать существование игры в качестве единственной социокультурной реальности современного мира, так и (не менее аргументированно) отрицать ее существование в принципе или интерпретировать Игру как поп-концепт околополитической журналистики или вообще элемент «теории заговора».

Данное исследование ставит перед собой задачу описать этот хаос в той степени, в которой это возможно, на всех уровнях — от концепций к техническим и экономическим предпосылкам, создающим возможности игры, от возможностей к практике технических и идеологических столкновений информационной эпохи. Существует ли игра как осознаваемая игроками форма социальной активности или как независимый от воли игроков, объективный и неизбежный этап развития человеческой цивилизации, или же, наконец, как иллюзия, антропоцентрическая проекция нашего системного мышления в хаос несистематизируемых обстоятельств, ее закономерности ***в любом случае*** существуют и, как мы намерены показать далее, отслеживаются через процесс развития информационной цивилизации. Наше исследование не может претендовать на безусловную объективность, поскольку исследователи как часть

эпохи и часть ее информационного поля находятся внутри самой эпохи. Это, несомненно, приводит к неизбежному искажению общей картины. В частности, разумеется, исследователей как граждан России интересует прежде всего та партия, которую играет в настоящее время Российская Федерация, что не может не приводить к аберрации восприятия на глобальном уровне. Однако на данный момент это единственный подход, который нам доступен, и, полагая вопрос актуальным в том числе и для нас, мы воспользовались им для того, чтобы систематизировать доступную нам часть информации.

Глава 1
ИГРОВОЕ ПОЛЕ: ИНФОРМАЦИОННОЕ ОБЩЕСТВО И HOMO INFORMATICUS

Предпосылки возникновения понятия «информационное общество» возникли в связи с развитием систем дальней систем электрической связи и попытками описания «информации вообще» (безотносительно к содержанию) посредством математических алгоритмов. Определяющий вклад в исследование проблемы сущности информации внес Клод Шеннон, который в своих исследованиях, начав с решения сугубо технических задач (корректная передача информации в условиях зашумления канала), разработал математические методы количественного определения информационных потоков в рамках процессов, связанных с передачей, приемом, преобразованием и хранением информации[1]. Под «***информацией***» автором понимается все, что может быть передано по каналам связи от источника к получателю. Понятие «***количество информации***» позволяет оценить количество знаков, достаточных для кодирования передаваемого сообщения, при этом содержание сообщения полагается несуще-

[1] См.: *Shannon C. E.* A Mathematical Theory of Communication // The Bell System Technical Journal. 1948. July, October. Vol. 27. P. 379–423, 623–656. URL: http://worrydream.com/refs/Shannon%20-%20A%20Mathematical%20Theory%20of%20Communication.pdf (дата обращения: 25.08.2018).

ственным. Шеннон вводит понятие «***информационной энтропии***», аналогичное энтропии из термодинамики, которое является мерой неопределенности информации. Также Шеннон определил ***бит*** как количество полученной информации (или уменьшенной энтропии) при нахождении ответа на вопрос, в котором возможны только два варианта ответа (например, «да» или «нет»), причем оба — с одинаковой вероятностью. В конечном счете Шеннон выходит к анализу понятия «связь» и «управление» с общефилософских, гуманитарных, по сути, позиций. Так, по Шеннону, «целью всякого управления должно быть уменьшение энтропии как меры неопределенности и беспорядка в системной среде. Управление, которое не решает этой задачи, является избыточным, то есть ненужным <…>. Все в этом мире в каком-то смысле есть „канал связи". Каналом связи является и человек, и коллектив, и целая функциональная среда, и промышленность, и транспортная структура, и страна в целом»[2]. Таким образом, работы Шеннона не только закладывают основы построения современных вычислительных систем и методов цифровой кодировки информации, но и прямо проецируются на общую теорию управления, устанавливая определяющую роль в управленческих процессах коммуникации как процесса обмена информацией и коммуникационных систем различного рода.

Концепция «информационного общества» как новой стадии развития человечества формируется в начале 60-х гг. прошлого века почти одновременно в США и Японии как попытка понять новую роль «знания» в прогрессе человечества. Собственно термин «информационное общество» впервые появился в Японии в 1966 г. Его изобретение приписывается профессору Токийского технологического института Ю. Хаяши[3]. Он стал основным в докладе специальной группы по научным, техническим и экономическим исследованиям,

---

[2] Цит. по: *Ушаков А.* Клод Шенон — создатель теории информации (к 100-летию со дня рождения). URL: http://controlengrussia.com/retrospektiva/klod-shennon-sozdatel-teorii-informatsii-k-100-letiyu-so-dnya-rozhdeniya/ (дата обращения: 25.08.2018) ; см. также: *Шеннон К.* Работы по теории информации и кибернетике. М., 1963. 832 с.

[3] См.: *Алексеева И. Ю.* Информационное общество. URL: https://iphras.ru/page46589323.htm (дата обращения: 25.08.2018).

созданной японским правительством для выработки перспектив развития экономики страны. Специалисты, предложившие этот термин, разъяснили, что он характеризует общество, в котором в изобилии циркулирует высокая по качеству информация, а также есть все необходимые средства для ее хранения, распределения и использования. Информация легко и быстро распространяется по требованиям заинтересованных людей и организаций и выдается им в привычной для них форме. Стоимость пользования информационными услугами настолько невысока, что они доступны каждому.

Т. Стоуньер утверждал, что информация обладает чертами, сходными с классическим капиталом, поскольку ее, подобно капиталу, можно передавать, накапливать и хранить для будущего использования[4]. При этом в постиндустриальном обществе национальные информационные ресурсы — самый большой потенциальный источник богатства. В связи с этим необходимо развивать новую отрасль экономики — информационную экономику. Постиндустриальная экономика — это экономика, в которой промышленность по показателям занятости и своей доли в национальном продукте уступает место сфере услуг, а сфера услуг есть преимущественно обработка информации. При этом информация как ресурс обладает уникальными свойствами как экономического, так и онтологического характера: «Если у меня есть 1 000 акров земли и я из них отдам кому-нибудь 500 акров, у меня останется лишь половина первоначальной площади. Но если у меня есть некоторая сумма информации и ее половину я отдам другому человеку, у меня останется все что было. Если я разрешу кому-нибудь использовать мою информацию, резонно полагать, что и он поделится со мной чем-нибудь; так же, как сделки по поводу материальных вещей ведут к конкуренции, информационный обмен ведет к сотрудничеству. Информация, таким образом, это ресурс, которым можно без сожалений делиться. Другая специфическая черта потребления информации заключается в том, что в отличие от потребления материалов или энергии, ведущего к увеличению энтропии во Вселенной,

[4] См.: *Стоуньер Т.* Информационное богатство: профиль постиндустриальной экономики // Новая технократическая волна на Западе. М., 1986. С. 392–409.

использование информации приводит к противоположному эффекту — оно увеличивает знания человека, повышает организованность в окружающей среде и уменьшает энтропию. В отличие, скажем, от машины, которая изнашивается от работы, книга не уменьшается от того, что ее прочитали»[5].

А. И. Ракитов в своих работах писал, что переход к информационному обществу означает, что важнейшим продуктом социальной деятельности становятся производство, эксплуатация и использование услуг и знаний, причем удельный вес знаний в этом сочетании возрастает, более того, повышается экономическая роль не просто «белых воротничков» по сравнению с «синими», доминировавшими в индустриальную эпоху, — растет прежде всего процентная доля высококвалифицированных специалистов, занятых интеллектуальным трудом[6]. Подлинное информационное общество должно обеспечить правовые и социальные гарантии того, что каждый гражданин общества, находящийся в любом пункте и в любое время, сможет получить всю необходимую для его жизнедеятельности и решения стоящих перед ним проблем информацию. Информационное общество — это общество, где все средства информационной технологии, то есть компьютеры, интегрированные системы, кабельная, спутниковая и другая связь, видеоустройства, программное обеспечение, научные исследования нацелены на то, чтобы сделать информацию общедоступной и активно внедряемой в производство и жизнь[7].

О. А. Финько полагает, что «информационным» можно назвать общество, в котором:

— персональный компьютер, подключенный к трансграничным информационным сетям, входит в каждый дом;

— каждый член общества имеет возможность своевременно получать с помощью трансграничных информационных сетей полную и достоверную информацию любого вида и назначения из любого

---

[5] *Стоуньер Т.* Указ. соч.

[6] См.: *Ракитов А. И.* Постинформационное общество // Философ. науки. 2016. № 12. С. 7–19.

[7] См.: *Ракитов А. И.* Россия в глобальном информационном процессе и региональная информационная // Проблемы информатизации. М., 1993. Вып. 1–2. С. 20–26.

государства, находясь при этом практически в любой точке географического пространства;

— предоставляется возможность оперативной коммуникации как каждого члена общества с каждым, так и с государственными и общественными структурами вне зависимости от места нахождения на Земном шаре;

— трансформируется деятельность СМИ по формам создания и распространения информации, технологически стыкуясь с информационными компьютерными сетями;

— «исчезают» географические и геополитические границы государств в рамках информационных сетей, происходит «столкновение» информационных законодательств стран, возникает необходимость гармонизации законодательств;

— появляются новые формы деятельности с использованием информационных сетей: работа, творчество, воспитание и образование, медицина[8].

В обобщенном виде на этапе философского осмысления и анализа технических и экономических предпосылок концепция информационного общества выглядела следующим образом:

1. Определяющим фактором общественной жизни в целом является научное знание. Оно вытесняет труд (ручной и механизированный) в его роли фактора стоимости товаров и услуг. Экономические и социальные функции капитала переходят к информации. Как следствие, ядром социальной организации, главным социальным институтом становится университет как центр производства, переработки и накопления знания. Промышленная корпорация теряет главенствующую роль.

2. Уровень знаний, а не собственность становится определяющим фактором социальной дифференциации. Деление на «имущих» и «неимущих» приобретает принципиально новый характер: привилегированный слой образуют информированные, в ту пору как неинформированные — это «новые бедные». Соответственно, очаг социальных конфликтов перемещается из экономической сферы

[8] См.: *Финько О. А.* О развитии информационного пространства России // Информ. ресурсы России. 1998. № 1. С. 12–13.

в сферу культуры. Результатом борьбы и разрешения конфликтов является развитие новых и упадок старых социальных институтов.

3. Инфраструктурой информационного общества является новая «интеллектуальная», а не «механическая» техника. Социальная организация и информационные технологии образуют симбиоз. Общество вступает в «технотронную эру» (З. Бжезинский[9]), когда социальные процессы становятся программируемыми.

Начиная с 80-х гг. прошлого века, термин «информационное общество» занимает прочное место в социологических (и особенно социофутурологических) исследованиях, постепенно вытесняя термин «постиндустриальное общество». В середине XX в. ряд западных социологов приходит к идее ожидаемой смены «индустриальной» фазы развития человечества к следующей за ней «постиндустриальной». Основателем современной концепции постиндустриального общества стал американский социолог Даниэл Белл. В вышедшей в 1973 г. книге «Грядущее постиндустриальное общество», он подробно изложил свою концепцию, тщательно анализируя основные тенденции в изменении отношений секторов общественного производства, становлении экономики услуг, формировании научного знания как самостоятельного элемента производственных сил. Концепция постиндустриального общества, по Беллу, включает пять основных компонент:

— в экономическом секторе — переход от акцента на производстве товаров к расширению сферы услуг;

— в структуре занятости — доминирование профессионального и технического классов, создание новой «меритократии», то есть власти «интеллектуального меньшинства»;

— осевой принцип общества — центральное место теоретических знаний в экономике, смещение «центра власти» от корпораций к университетам;

— ориентация на будущее — особая роль технологического развития, в том числе в сфере оценке перспектив развития общества;

---

[9] См.: *Бжезинский З.* Между двумя веками: роль Америки в эру технотроники. М., 1972. 308 с.

— принятие решений на основе «интеллектуальных технологий»[10].

Согласно концепции постиндустриального общества, история цивилизации делится на три большие эпохи: доиндустриальную, индустриальную и постиндустриальную. При переходе от одной стадии к другой новый тип общества не вытесняет предшествующие формы, но делает их второстепенными. Доиндустриальный способ организации общества основан на:

— трудоемких технологиях;

— использовании мускульной силы человека;

— навыках, не требующих длительного обучения;

— эксплуатации природных ресурсов (в частности, сельскохозяйственных земель).

Индустриальный способ основан на:

— машинном производстве;

— капиталоемких технологиях;

— использовании внемускульных источников энергии;

— требующей длительного обучения квалификации.

Постиндустриальный способ основан на:

— наукоемких технологиях;

— информации и знаниях как основном производственном ресурсе;

— творческом аспекте деятельности человека, непрерывном самосовершенствовании и повышении квалификации в течение всей жизни.

«В наступающем столетии, — утверждает Д. Белл, — решающее значение для экономической и социальной жизни, для способов производства знания, а также для характера трудовой деятельности человека приобретет становление нового социального уклада, зиждущегося на телекоммуникациях»[11].

Одной из наиболее известных разработок концепции информационного общества как принципиально нового способа производ-

---

[10] См.: *Белл Д.* Грядущее постиндустриальное общество. Опыт социального прогнозирования. М., 2004. 790 с.

[11] Цит. по: *Алексеева И. Ю.* Указ. соч.

ства и, соответственно, нового этапа в существовании человеческой цивилизации считается теория «трех волн» Э. Тоффлера, изложенная в книге 1980 г. «The Third Wave: The Classic Study of Tomorrow»[12]. Согласно Тоффлеру, современная цивилизация формируется через ряд последовательных и радикальных изменений доминирующей производственной парадигмы и связанных с ними системах ценностей и социальных структурах. «Первую волну» Тоффлер называет «сельскохозяйственной цивилизацией». Земля как сельскохозяйственный ресурс становится основой экономики, жизни, культуры, семейной организации и политики. В обществе господствует простое разделение труда и существует несколько четко определенных каст и классов: знать, духовенство, воины, рабы или крепостные. Власть носит жестко авторитарный характер, при этом экономика децентрализована и тяготеет к натуральному хозяйству. «Первая волна» развивалась тысячелетия, но в результате «племенной человек» почти глобально превращается в «феодального». Сельскохозяйственная цивилизация, в свою очередь, трансформируется в результате «взрыва» — промышленной революции в Европе, породившей «вторую волну» преобразований. Эта волна формирует индустриальное общество и «человека индустриального». «*Индуст-реальность*», по выражению Тоффлера, предполагает технологизацию всех уровней социального бытия — рождения, образования, медицинского обслуживания, искусства (переход от камерной музыки сельскохозяйственного мира к симфоническому оркестру), государственного управления (концепция «прав человека» и доминирование в индустриальном мире обезличенных демократических институтов власти). В качестве основных систем правил и принципов (кода) второй волны Тоффлер выделяет стандартизацию (в производстве, услугах, обучении, единицах измерения, ценах и т. д.), специализацию (в разделении труда), синхронизацию (труда во времени, обучения во времени, отдыха и т. д.), концентрацию (населения, трудовой деятельности, энергии, экономики, образования и т. д.), максимизацию (гигантомания в архитектуре, плановых показателях и т. д.), централизацию (экономики — например, Центральный банк,

[12] См.: *Тоффлер Э.* Третья волна / пер. с англ. М., 2009. 800 с.

управление государством). Однако именно идея стандартизации, концентрации, всевластие статистики и прямолинейно понимаемой эффективности порождают основной инструмент угрожающей индустриальному миру «третьей волны» — компьютер. Тоффлер описывает общество, построенное вокруг непрерывно варьирующегося глобального потока информации, как децентрализированное, демассифицированное, дестандартизованное, ориентированное на индивидуальное производство и потребление, многообразное по форме организации личного и социального бытия индивидуума. Подобная диверсификация должна наблюдаться в сфере культуры на всех уровнях, от культуры потребления до элитарных образцов «высокого искусства»: Тоффлер доказывает, что в новом обществе она подстраивается под индивидуальные потребительские нужды. Для ее характеристики Тоффлер прибегает к формулировке «приспособление к возрастанию жизненного уровня» и указывает на совершенствование технологического уровня культурного производства. По его мнению, это позволяет снизить себестоимость «культурных продуктов» и одновременно ведет к повышению качества потребительского спроса и, как следствие, повышение гибкости, адаптивности производства. «Поскольку удовлетворяется все больше и больше основных нужд покупателей, — отмечает исследователь, — можно твердо предсказать, что экономика будет еще энергичней идти навстречу тонким, разнообразным и глубоко персональным потребностям покупателя, потребностям в красивых, престижных, глубоко индивидуализированных <…> продуктах»[13]. В результате меняется и механизм «культурного потребления». Массовая культура отчасти теряет характер стереотипности, она становится более гибкой, соответственно, охватывая большие массы населения, в том числе аудиторию культуры «элитарной» как уникальный релаксационно-адаптивный механизм, выработанный индустриальной эпохой; при этом в каждом конкретном случае ее качество возрастает. В свою очередь, элитарная культура теряет значение маркера избранности, свойственного узкому кругу претендентов на роль интеллектуальной верхушки, и занимает

[13] *Тоффлер Э.* Шок будущего / пер. с англ. М., 2002. С. 248.

позицию доступного для широких масс, но при этом абсолютного по качеству культурного эталона — «массовой культуры высшего порядка». Тоффлер называет этот процесс «индивидуализацией личности», подразумевая отказ от тиражируемой, деиндивидуализированной, в собственном смысле массовой культуры. Традиционным громоздким корпорациям Тоффлер противопоставляет «малые» экономические формы — индивидуальную деятельность на дому, «электронный коттедж». Они включены в общую структуру информационного общества с его инфо-, техно- и другими сферами человеческого бытия. Выдвигается проект «глобальной электронной цивилизации» на базе синтеза телевидения, компьютерной службы и энергетики — «телекомпьютерэнергетики» (Дж. Пелтон). «Компьютерная революция» постепенно приводит к замене традиционной печати электронными книгами, изменяет идеологию, превращает безработицу в обеспеченный досуг. Перспектива развития демократии связывается с распространением информационной техники. Тоффлер и Дж. Мартин отводят главную роль в этом телекоммуникационной «кабельной сети», которая обеспечит двустороннюю связь граждан с правительством, позволит напрямую учитывать их мнение при выработке политических решений. При этом индивидуализация коммуникационной сферы, производства, экономических и политических действий фактически означает деконструкцию устоявшихся моделей общности, таких как централизованное политическое управление, корпорация, семья или религиозная макроконфессия. Социальные структуры в обществе технологий подчиняются не иерархическим принципам, они основаны не на линейном соподчинении, но существуют как совокупность узлов, расположенных на самых различных уровнях власти и выполняющих функции центра. «Сегодня строгая вертикальная иерархия, — утверждает Э. Тоффлер, — утрачивает свою эффективность, поскольку исчезают два основных условия ее успешного функционирования. Руководители сталкиваются со все более разнородными проблемами, и им при решении сложных технических и экономических вопросов приходится во все большей степени учитывать также политические, культурные и социальные аспекты. В то же время обратная связь с прежними уровнями становится

все более неадекватной»[14]. Все уровни социокультурного взаимодействия в результате приобретают необязательных и подвижных, а социальные структуры (включая государство) приобретают вместо иерархического функционально-сетевой характер. Соответственно, современные сторонники концепции Тоффлера оценивают борьбу за «традиционные ценности» (в форме исламского, христианского или иного религиозного фундаментализма, национализма, попытки реконструкции государственных сверхорганизмов имперского типа) как борьбу сторонников «второй волны» против наступления «третьей».

В «Homo Informaticus», адекватного условиям третьей волны, Тоффлер видит формирующуюся (в том числе, предположительно, на биологическом уровне) способность к обработке больших и непрерывно растущих и изменяющихся потоков данных. Эта способность порождается насущной социокультурной необходимостью, поскольку сама по себе инфосфера нового типа появляется как логическое следствие развития политических и экономических процессов индустриальной эпохи, которые приобретают глобальный характер, приводят к резкому росту населения, повышению его мобильности и интенсификации процессов обмена, а значит, требуют радикального роста возможностей для систем коммуникации, учета, контроля и обработки информации; в результате объемы накапливаемой информации лавинообразно нарастают. Соответственно, достижение высокого уровня социализации (и «инфосоциализации») потребует от субъекта новой инфосферы непрерывного самообразования, непредставимой для предшествующих эпох социальной, профессиональной, эмоциональной подвижности. В таких условиях, по замечанию Тоффлера, становится реальностью неизбежный в современной ситуации переход к личности нового типа — информационно-адаптированной, основными характеристиками которой могут быть представлены естественное включение

[14] Цит. по: *Костина А. В.* Тенденции развития культуры информационного общества: анализ современных информационных и постиндустриальных концепций // Информ. гум. портал «Знание. Понимание. Умение». 2009. № 4. «Культурология». URL: http://zpu-journal.ru/e-zpu/2009/4/Kostina_Information_Society/ (дата обращения: 25.08.2018).

в информационные процессы, способность к адекватному восприятию полученной информации и настроенность на эффективное ее использование в своей деятельности.

Следует обратить внимание на два существенных момента. Во-первых, концепция «волн» Тоффлера разрабатывалась на рубеже 70–80 гг. XX в., когда уровень компьютеризации общества был достаточно низок, а современные коммуникационные сети глобального характера не существовали даже в проекте. В настоящее время мы наблюдаем ряд явлений экономической, социальной и общественной жизни, по-видимому, близких к прогнозам Тоффлера, однако это не может служить безусловным доказательством правильности его анализа; кроме того, хотя действие каждой из последующих «волн» несопоставимо быстрее, чем предыдущей (аграрная «волна» распространялась в течение тысячелетий, индустриальная охватила человечество за 3–4 столетия), воздействие «третьей волны» еще не завершено, и новая социокультурная парадигма должна находиться в состоянии становления. Причем, по опыту предшествующих «волн», становление «человека информационного» будет происходить в конфликтной и исторически непоследовательной форме.

Во-вторых, борьбу сторонников третьей и второй волны ни в коем случае не следует воспринимать как борьбу добра со злом. Аналог данной ситуации мы можем наблюдать на примере разворачивания второй волны. Индустриализация повсеместно приносила в общество усиление различных форм насилия и угнетения, и выступали против нее в первую очередь социальные низы (см. движение луддитов в Англии), причем в критике новых отношений аграрное сообщество всегда — и небезосновательно — апеллировало прежде всего к этическим, эстетическим и религиозным нормам, которыми «человек индустриальный» систематически пренебрегал. И хотя реформирование общественных отношений породило и новую этику, и новую эстетику, но они появились не сразу, не общеприняты и вряд ли когда-нибудь будут общеприняты (см., например, проблему прав человека в государствах Ближнего и Среднего Востока). С другой стороны, в большинстве случаев разрушение старого мира и не рассматривалось как цель некоей «революции» (большинство известных нам революций вообще решали частные

задачи социального, политического или национального характера и не ставили глобальных целей). Если концепция Тоффлера верна, то победа третьей волны неизбежна не потому, что к ней кто-то целенаправленно стремится, но потому, что выстроенная на ней постиндустриальная экономика окажется существенно эффективнее индустриальной и при этом, как упомянуто выше, вберет ее в себя как частный, управляемый в рамках общих постиндустриальных принципов сегмент. Таким образом, термин «постиндустриальный» не предполагает в собственном смысле отказа от индустриального способа производства, так же как индустриализация привела не к упразднению, но к реорганизации сельского хозяйства, инкорпорировав его в индустриальную сферу.

К постиндустриальному направлению в социологии можно отнести фундаментальную работу М. Кастельса «Информационная эпоха. Экономика, общество и культура». Прежде всего в ней отвергается упрощенное толкование механизмов перехода общества к постиндустриальной стадии. Анализируя соцально-экономическую и производственную конкретику, Кастельс показывает логическую преемственность постиндустриального и индустриального этапов. Это общество в его интерпретации не имеет качественных отличий от индустриального, но превосходит его по технологическому развитию, по скорости обмена информацией, по эффективности используемых источников энергии и, как следствие, по количественным показателям производства. Однако постиндустриальная фаза создает ресурсный и инфраструктурный задел для формирования действительно принципиально новой стадии развития общества, которую Кастельс называет «информациональной»[15]. На этой стадии генерирование, обработка и передача информации становятся определяющими ценностями и источниками власти, поскольку в условиях достаточных ресурсов любого типа и одновременно возросших потребностей населения на первый план выходят вопросы учета, контроля, логистики и обратной связи.

---

[15] См.: *Кастельс М.* Информационная эпоха: экономика, общество и культура. URL: http://www.gumer.info/bibliotek_Buks/Polit/kastel/index.php (дата обращения: 25.08.2018).

Профессор У. Мартин предпринял попытку выделить и сформулировать основные характеристики информационного общества по следующим критериям:

— *Технологический*: ключевой фактор — информационная технология, которая широко применяется в производстве, учреждениях, системе образования и в быту.

— *Социальный*: информация выступает в качестве важного стимулятора изменения качества жизни, формируется и утверждается «информационное сознание» при широком доступе к информации.

— *Экономический*: информация составляет ключевой фактор в экономике в качестве ресурса, услуг, товара, источника добавленной стоимости и занятости.

— *Политический*: свобода информации, ведущая к политическому процессу, который характеризуется растущим участием и консенсусом между различными классами и социальными слоями населения.

— *Культурный*: признание культурной ценности информации посредством содействия утверждению информационных ценностей в интересах развития отдельного индивида и общества в целом.

При этом Мартин особо подчеркивает мысль о том, что коммуникация представляет собой «ключевой элемент информационного общества». Мартин отмечает, что, говоря об информационном обществе, его следует принимать не в буквальном смысле, а рассматривать как ориентир, тенденцию изменений в современном западном обществе. По его словам, в целом эта модель ориентирована на будущее, но в развитых капиталистических странах уже сейчас можно назвать целый ряд вызванных информационной технологией изменений, которые подтверждают концепцию информационного общества. Среди этих изменений Мартин перечисляет следующие:

— структурные изменения в экономике, особенно в сфере распределения рабочей силы;

— возросшее осознание важности информации;

— растущее осознание необходимости компьютерной грамотности;

— широкое распространение информационной технологии;

— поддержка правительством развития компьютерной микроэлектронной технологии и телекоммуникаций.

В свете этих изменений, как считает Мартин, информационное общество можно определить как общество, в котором качество жизни так же, как перспективы социальных изменений и экономического развития, в возрастающей степени зависят от информации и ее эксплуатации. В таком обществе стандарты жизни, формы труда и отдыха, система образования и рынок находятся под значительным влиянием достижений в сфере информации и знания[16].

Отечественный исследователь А. И. Смирнов, анализируя социальные аспекты информационного общества, отмечает тот факт, что информация становится социальным ресурсом. Информация «способна помочь человеку адаптироваться к жизни в условиях постоянных изменений, выработать новые стереотипы поведения, соответствующие новым обстоятельствам. Для человека информационного общества единство мира оказывается уже не теоретической или идеологической абстракцией, а фактом его повседневной жизни»[17]. Для человека информационного общества повышается возможность выбора, но при этом возрастает и ответственность за сделанный выбор. Развитие массмедиа существенно повышает распространения новых знаний и обмена ими, в то же время усиливаются потенциальные возможности манипулирования сознанием с помощью современных информационно-телекоммуникационных технологий. С точки зрения А. И. Смирнова, в силу размывания национальных и политических границ и унификации культур и усиления влияния транснациональных корпораций возникают угрозы экологической политике, труду и социальной защите во всемирном масштабе. Распространение «экранной» культуры и столкновение с виртуальной реальностью создает целый ряд проблем психологического характера. Возникает проблема ограничения экономического роста, социальной дифференциации населения по признаку

---

[16] *Мартин У. Дж.* Информационное общество (Реферат) // Теория и практика общественно-научной информации : ежеквартальник. М., 1990. № 3. С. 115–123.

[17] *Смирнов А. В.* Информационная глобализация и Россия. Вызовы и возможности. М., 2005. С. 41.

доступа к социально опасной информации. Проблема роста информационно-коммуникационных технологий порождает новую проблему так называемого «цифрового неравенства, сохранности персональных данных, соблюдения авторских прав и т. п. Хотя в силу научно-технического прогресса новые информационные технологии в целом становятся дешевле, стоимость информационных услуг в отдельных случаях может возрастать, что способствует возникновению так называемой „информационной бедности“»[18].

В целом все авторы постмодернистских социологических концепций так или иначе выходят на формирование новой социокультурной реальности, в качестве которой выступает общество, ориентированное на знание и информацию как основной ресурс в сферах экономики и политики. Что, собственно, как раз и позволяет рассматривать «постиндустриальное» и «информационное» общество как модусы описания одной и той же социальной реальности. Следует иметь в виду, что постиндустриальная концепция не общепринята и серьезно критикуется рядом исследователей. Критики указывают на то, что «дестандартизация» Тоффлера является иллюзией, поскольку описываемое общество не существует без глобальных коммуникаций и глобальной логистики, а значит, неявных, но приобретающих глобальный и безусловный характер стандартов; на то, что перехода власти «от корпораций к университетам» не наблюдается ни в какой форме; на разрушение «пузырей» на рынке высоких технологий; на тот факт, что индустриальная сфера не столько сокращается в процентном отношении, сколько перераспределяется географически с переводом производства в развивающиеся страны и т. п. Но хотя в экономике, в сфере производства, в сфере социокультурных прогнозов положения теоретиков постиндустриализма можно оспаривать, это не отменяет самого факта наличия радикальных изменений, затрагивающих все сферы развития общества и тесно связанных с внедрением и нарастающим влиянием информационных технологий. Именно поэтому термин «информационное общество» куда в большей степени, чем «постиндустриальное», выходит за пределы академической социо-

[18] См.: *Смирнов А. В.* Указ. соч. С. 42.

логии, переходит в лексикон политиков, журналистов и, наконец, обывателей, то есть становится частью повседневного дискурса, превращаясь в модус самовосприятия, саморефлексии человечества. Таким образом, если существование информационного общества как некоей специфической и объективно неизбежной стадии развития цивилизации достаточно спорно, то его существование как социального феномена становится общепринятым фактом. Обычно под «информационным обществом» понимают:

— развитие компьютерных технологий, их проникновение во все сферы жизни, от автоматизации и роботизации производства и военной техники до бытовых устройств повседневного использования;

— развитие систем коммуникации, в том числе удаленного доступа к рабочему месту; принципиальное значение здесь приобретает возможность широкополосного доступа к глобальной информационной сети Интернет, в том числе в удаленных районах, с помощью мобильных устройств невысокой стоимости; соответственно, развитие беспроводных сетей третьего, четвертого и — в перспективе — пятого поколения, а также магистральных оптоволоконных и спутниковых систем;

— развитие систем искусственного интеллекта, причем как оказывающих влияние на принятие решений тактического и стратегического уровня (концепция *Big Date*), так и сопровождающих повседневную жизнь индивида (концепция «интернета вещей»);

— все возрастающую вовлеченность индивида в процесс потребления и (что крайне важно) производства информации разного рода, причем информации, потенциально претендующей на глобальный охват потенциальной аудитории (социальные сети, микроблоги типа Twitter, селфи, видеохостинги типа YouTube и многое другое) — вне зависимости от социальной значимости данной информации;

— рост числа сфер человеческой деятельности, так или иначе затронутых идеологией обратной связи (от «интерактивного телевидения» до «электронного правительства»);

— формирование новой системы угроз, связанных как с воздействием информационной сферы на сознание индивидов («компьютерная зависимость», Интернет как среда деструктивной пропаганды

(достаточно вспомнить скандалы вокруг предполагаемого влияния России на выборы в США и последовавшие за ними антироссийские санкции), роль интернет-коммуникаций и интернет-СМИ в событиях «Арабской весны» и «Цветных» революций и многое другое), так и с более или менее прямым воздействием инфосферы на материальный мир (кибератаки, кибертерроризм, кибервойны).

Стремительное развитие и распространение новых информационно-коммуникационных технологий в результате научно-технического прогресса приобретает сегодня характер беспрецедентной по своим масштабам информационной революции, которая оказывает возрастающее влияние на политику, экономику, науку и другие сферы жизнедеятельности общества как в рамках национальных границ, так и в мире в целом. Информация и знания становятся одним из стратегических ресурсов государства, масштабы использования которого стали сопоставимы с использованием традиционных ресурсов, а доступ к ним — одним из основных факторов социально-экономического развития. Постоянно усиливающаяся роль этого фактора как средства ускорения темпов глобальной интеграции в экономике и инструмента воздействия на массовое сознание, культуру и международные отношения позволяет говорить о появлении объективных предпосылок для движения к так называемому «глобальному информационному обществу». В начале XXI в. появляются фиксирующие эту тенденцию международные документы, прежде всего принятая 22 июля 2000 г. лидерами стран «Большой восьмерки» Окинавская хартия Глобального информационного общества. 27 марта 2006 года Генеральная Ассамблея ООН приняла резолюцию под номером A/RES/60/252, которая провозглашает 17 мая Международным днем информационного общества.

Набирающая силу информационная революция быстро меняет мир, предоставляя человечеству принципиально новые решения и возможности во многих сферах. Но вместе с очевидными благами, которые она уже дала людям, и еще большими в скором будущем, эта революция несет и принципиально новые проблемы и противоречия. Среди них — цифровое неравенство стран и регионов, проблема правового регулирования сети Интернет, электронной коммерции и налогообложения в этой области, вопросы интел-

лектуальной собственности, проблема обеспечения безопасности и конфиденциальности информации, соблюдение свободы слова, вопросы цензуры в глобальных компьютерных сетях и др.

Нельзя утверждать, что современный человек умнее или информированнее, чем человек Античности или Средневековья. Принципиальная разница заключается в ином — сейчас неизмеримо более развита система коммуникаций. Тиражирование интеллектуального продукта, передача сведений о нем посредством печатных изданий, телеграфа, радио, телевидения, лекций и семинаров в рамках системы всеобщего образования, сети Интернет — вот что коренным образом отличает современное общество как информационное. «Человек информационный»[19] участвует в большем числе коммуникаций, это не ускоряет на данном этапе качество обработки полученной им информации, но несопоставимо упрощает доступ к информации, обработанной и предоставленной в общее информационное пространство другими участниками коммуникации.

Американский ученый Д. С. Робертсон в работе «Информационная революция» рассматривает работу с информацией на разных этапах развития общества и приходит к выводу, что коммуникационные системы, принципы кодирования, передачи и сохранения информации непосредственно влияют на уровень и качество знания, начиная от первой коммуникационной революции, связанной с формированием языка, и заканчивая последней — электронной, сетевой. Доминирующая информационная система, по Робертсону, определяет характер доминирующей на определенном историческом отрезке культуры[20]. Этот подход, однако, верен лишь отчасти, поскольку не учитывает обратного влияния: развитие коммуникационных систем во многом зависит от наличия общественно значимой потребности в их развитии. К примеру, говоря о книгопечатании, нельзя отрицать его громадную роль в формировании современной европейской цивилизации, и в частности в технологической

---

[19] См., напр.: *Курбатов В. И.* «Homo informaticus» — человек информационной эпохи: характерологические черты // Гуманитар., соц.-эконом. и общ. науки. 2017. № 1. С. 46–51.

[20] См.: *Робертсон Д. С.* Информационная революция: Наука, экономика, технология : реф. сб. / отв. ред. А. И. Ракитов. М., 1993. С. 17–26.

и промышленной революции XVI–XVII вв. и далее. Однако в Китае станок для тиражирования иероглифического письма со сменными литерами был изобретен в XI в., между тем это событие не оказало существенного влияния на развитие восточной цивилизации. Таким образом, наличие технической возможности коммуникации само по себе, без потребности в новом коммуникационном канале, не создает ни культурного, ни экономического скачка. В Западной же Европе изобретение Гутенберга стало началом «третьей информационной революции», по значению приравниваемой Робертсоном к первой — формированию речи и второй — изобретению письменности. Но молниеносное распространение типографского дела было обусловлено потребностями в массовом распространении информации, становящейся все более необходимой с ростом городов и развитием промышленного производства. С ее объемами уже не справлялись монастырские и городские скриптории, ответственные за переписку книг, летучие же листки, производимые техникой гравировки, не могли вместить в себя всю актуальную информацию. То есть потребности цивилизации, вступающей в более прогрессивную стадию социального и экономического развития, и обусловили смену способа кодирования сообщения.

Настроенность индивида внутри информационного общества на постоянное потребление информации вполне оправданно, так как качество социализации определяется именно количеством получаемой информации. Однако рост коммуникационной активности означает также и рост психологического напряжения. «Картина мира современного человека лишь на 10–15 % состоит из знаний, приобретенных посредством собственного опыта. Основным же источником информации любого рода — теоретических и практических знаний, данных о ситуации в ближнем и дальнем окружении, культурных кодов и навыков, языковых и поведенческих стереотипов, а также важнейшим фактором в трансформации системы духовного производства, являются средства массовой коммуникации, образующие в своей совокупности глобальную „инфосферу“, приобретающую универсальный и тотальный характер и фактически воспринимаемую субъектом как его основная

среда обитания»[21]. Стоит заметить, что тотальность инфосферы уже сейчас воспринимается как актуальная угроза. Популярная антиутопия Д. Эггерса «Сфера» («The Circle») описывает человечество, буквально поглощаемое глобальной социальной сетью. При этом все формы приватности, независимости частной жизни личности с помощью средств онлайн-мониторинга уничтожаются самим обществом, воспринимающим их как источник общественной опасности и проявление эгоизма и социопатии[22].

Однако специфическим качеством самой *информации* (в отличие от систематизированного и функционального *знания*) является ее избыточность и фрагментарность. Обилие информации неизбежно приводит к поверхностности сначала восприятия, затем, возможно, и мышления. Ощущение потерянности и удрученности, охватывающее современного человека, имеющего доступ к многотомным энциклопедическим изданиям, причем и в цифровом формате ко всем художественным феноменам, пусть и в электронном виде, П. Валери сравнивает с тем, которое охватывает человека в музее. Здесь «продукция бесчисленных часов, потраченных столькими мастерам и на рисование и живопись, обрушивается в несколько мгновений на ваши разум и чувства». Под влиянием «этого бремени» «мы становимся поверхностными. Или же делаемся эрудитами»[23]. Человек, вынужденный постоянно осуществлять переходы из одной информационной системы в другую, находится под угрозой дезориентации, причем как чисто физической, так и ментальной. Утрата способности осуществления коммуникации с Другим в рамках реальности, с миром, утрата самоидентичности — все это симптомы «фундаментальной потери ориентации», когда бытие человека выступает как постоянная смена в рамках коммуникативного пространства стратегий человека — приемника сообщения и его отправителя, человека — объекта коммуникации и создателя собственной субъективности. Этот новый

---

[21] *Костина А. В., Карпухин О. И., Макаревич Э. Ф.* Основы рекламы. URL: https://www.intuit.ru/studies/courses/3597/839/lecture/30233 (дата обращения: 25.08.2018).

[22] См.: *Эггерс Д.* Сфера. М., 2014. 448 с.

[23] *Валери П.* Проблема музеев / П. Валери. Об искусстве. URL: http://www.sklad.cc/article/27/ (дата обращения: 25.08.2018).

субъект культуры лишен традиционных внутригрупповых связей, так как изменения в сфере коммуникаций умножают эффект объективных социальных сдвигов, в результате чего социум утрачивает возможность «сообщать личности свою специфическую групповую культуру». Таким образом, «сетевую структуру» общества, теоретически описанную Кастельсом в оптимистическом ключе, Валери уже в 1923 г. анализирует как состоявшуюся и видит в ней не источник не столько нового уровня свободы личности, сколько растерянности, утраты ориентиров, психологического дискомфорта.

Лавинообразное нарастание потока обрабатываемой нами случайной информации повышает прежде всего уровень семантической зашумленности сознания, что ведет к размыванию критериев истины, неспособности отличить истину от лжи. Однако для человека это состояние множественности смыслов, значений, ценностей, которые принадлежат разным культурным мирам, является психологически сложным. Человек утрачивает прочные основания своей жизни и начинает испытывать трудности с определением собственной самотождественности. Э. Тоффлер задается вопросом относительно пределов тех изменений в социокультурной среде, к которым человек может приспособиться. Это состояние дезадаптации автор называет «шоком будущего», трактуя его как «страдание, физическое и психологическое, возникающее от перегрузок, которые физически испытывают адаптивные системы человеческого организма, а психологически — системы, отвечающие за принятие решений. Проще говоря, шок будущего — это реакция человека на запредельное нервное раздражение». Как причину этого шока, Тоффлер описывает явление, известное в психологии как «информационная перегрузка» — термин, описывающий трудности понимания проблемы и принятия решений, причиной которых является избыток информации. Тоффлер пишет: «Когда человек погружается в быстро и нерегулярно меняющуюся ситуацию или новый насыщенный контекст, его предсказательная точность падает. Он больше не может сделать достоверную оценку, от которой зависит рациональное поведение»[24].

[24] *Тоффлер Э.* Шок будущего. С. 352.

Оценка избыточной и неструктурированной информации как угрозы встречается уже в древнекитайских и ветхозаветных текстах. Однако именно цифровая эпоха, с Интернетом, мессенджерами, виртуальным присутствием и мобильной связью, делает проблему по-настоящему массовой. В качестве характерных элементов ситуации информационного давления выделяют:

— стремительный рост производства новой информации;

— простота дублирования и передачи данных через Интернет;

— увеличение доступных каналов входящей информации (например, мобильная телефония, электронная почта, системы мгновенного обмена сообщениями);

— противоречия и неточности в имеющейся информации, утрата СМИ качества обработки данных;

— низкое соотношение сигнал/шум (то есть наличие в любой входящей информации большого количества заведомо лишенных ценности, избыточных, раздражающих либо просто дублирующих уже полученную информацию элементов при отсутствии функциональных способов отсеять существенную часть избыточной информации — см. спам как явление);

— отсутствие метода сравнения и обработки различных видов информации;

— отсутствие связи между фрагментами информации, невыявленность когнитивных структур, случайность их размещений в глобальном информационном пространстве (и, соответственно, рост побочной информации, которую обрабатывает индивид в процессе поиска нужных фрагментов).

В 1989 г. в своей книге Information Anxiety («Информационная тревога») Р. С. Вурмен написал: «Один из самых настораживающих побочных эффектов информационной эры — ощущение, что мы обязаны все знать. Понимание своей ограниченности необходимо, чтобы выжить в информационной лавине. Нельзя и не следует впитывать все или даже реагировать на все»[25]. Тридцать лет спустя мы можем утверждать, что убедительная на словах рекомендация Вурмена наталкивается на неспособность масс, и в этом числе лиц,

[25] *Wurman R. S.* Information Anxiety. N.Y. ; L., 1989. P. 34.

ответственных за принятие решений стратегического уровня, руководствоваться этой максимой на практике. Соответственно, установка на абсолютную информированность становится не только потребностью, но и социально значимым требованием. Именно в этом ключе, например, представляет свой идеальный результат концепция непрерывного образования. Таким образом, индивид может ограничить свой контакт с возрастающим информационным потоком, только маргинализуя собственное социальное бытие, в противном случае информационная перегрузка и сопутствующие ей психологические проблемы становятся для него повседневной нормой. Ощущение психологического дискомфорта, боязни мира приводит к намеренному ограничению человеком реальных социальных контактов, выработке особых способов «справляться с завтра», начиная от наркотиков, беспорядочных знакомств и заканчивая сильными эмоциональными переживаниями, связанными с информационной виртуализированной реальностью. При этом сама возможность удерживаться «в тренде» мира развлечений, то есть ощущать себя комфортно в зоне отдыха от возрастающего информационного давления, также требует от индивида использования непрерывно возрастающих вычислительных мощностей. Опять-таки в порядке компенсации информационного давления наблюдается стремление к стабильности на работе, в семье, сохранению связей с родителями, друзьями по колледжу, школе, университету. Такими зонами стабильности могут стать постоянный режим дня, неизменные вкусы, приверженность определенной моде и т. п. (хотя возможно и обратное — см. ниже о «блип-культуре»). С другой стороны, подобные модели приобретают случайный, биографически или локально обусловленный характер, а следовательно, здесь мы также можем говорить и о дроблении общего культурного пространства на субкультуры, что возвращает нас к концепции сетевого общества.

Технологическая специфика коммуникативных потоков «третьей волны», их множественность, взаимозаменяемость и мультимедийная составляющая порождают феномен «клипового сознания», или, по Тоффлеру, «блип-культуры». Образы и ассоциации, создающие «ментальную модель действительности», скрепляющие

нашу картину мира и помещающие нас в пространство и время и определяющие «наше место в структуре личностных взаимоотношений», так или иначе формируются посредством преобразования воспринимающим сознанием посступающей информации. При этом жизнь субъекта традиционного общества «первой волны» протекает, по современным оценкам, в условиях информационного голода: он получает минимум новой информации в единицу времени, воспринимая мир как цикл, неизменно воспроизводящий предвечную схему. Соответственно, он оперирует минимумом базовых «образов мира» и жестко ориентирован на оценку входящей информации по параметру «свое/чужое», маркируя чужое=новое по преимуществу негативно. «Вторая волна» увеличивает информационную нагрузку через средства тиражирования информации (СМИ и книгопечатание, затем телекоммуникации и электроннные медиа), ускоряя обновление информационного фона и предоставляя субъекту одновременный доступ к множеству значимых сообщений, паттернов, «имиджей». Некоторые из них стереотипизировались, трансформировались в иконические изображения, и задачей человека стал выбор и манипуляция этими имиджами, каталогизированными в «картотеке файлов»[26]. Количество этих имиджей существенно возросло по сравнению с эпохой «Первой волны», однако они тиражировались индустриальным способом — унифицированно и централизовано, генерализуя сознание масс: именно эти «централизованно разработанные образы, впрыснутые в массовое сознание средствами массовой информации, способствовали стандартизации нужного для индустриальной системы поведения»[27]. Третья же волна не просто ускоряет темп инноваций, она трансформирует глубинную структуру информации, и человек теряет способность адекватно времени обновлять эту «имиджевую базу данных». Отсюда — разовые предметы потребления, одноразовое искусство, разрушение концепта семьи (особенно традиционной «вертикальной») как системы постоянных отношений, виртуализация системы эмоционального взаимодействия, предполагающая

[26] См.: *Тоффлер Э.* Третья волна.

[27] Там же.

множественность и необязательность контактов, культ туризма и профессиональной мобильности. Показательно распространение интернет-сервисов типа Magic Door, которые позволяют пользователю Сети совершить виртуальную прогулку по случайно выбранному региону планеты непредсказуемого пространственного объема и непредсказуемой культурной насыщенности (в качестве материала для подобных «прогулок» могут использоваться, например, данные видеосъемки Google). То есть индивид получает доступ к случайному блоку впечатлений, претендующему на достоверность, и при этом не требующему от индивида каких бы то ни было социальных контактов и социальной ответственности.

Формируется новый тип культуры, который Тоффлер обозначает как блип-культуру: он основан на «блипах» информации — объявлениях, командах, обрывках новостей, которые не поддаются классификации, в первую очередь по причине того, что они не укладываются в старые категории, или имеют странную, текучую, бессвязную форму. При этом потребители информации не имеют возможности заимствовать готовую модель реальности, а должны сами конструировать ее, непрерывно увеличивая объем поступающей информации и одновременно критически сокращая время на ее обработку. В эпоху господства многоканального телевидения эта тенденция проявилась в феномене «зиппинга» — безостановочного переключения каналов; в эпоху Интернета аналогом зиппинга становится веб-серфинг. Этот образ непрерывно обновляется, в момент «переключения канала» незамедлительно утрачивая свое значение и «перезагружаясь», механически конструируясь заново, что не предполагает ни осмысления, ни критической оценки. При этом он оказывает комплексное воздействие на эмоциональную сферу субъекта, чему способствует его мультимедийный характер, присутствующий как в традиционном телевидении, так и в Интернете. Блип-культура, по Тоффлеру, становится не просто аспектом новой информационной культуры, но и важным социокультурным фактором, ускоряющим разрыв между поколениями второй и третьей волн.

Дело не в том, что «человек информационный» должен обязательно отказываться от устоявшихся традиций, мнений, и норм оценки ситуации, а, скорее, в отказе от принципа последовательно-

сти, системности, от поиска раз и навсегда выбранной, единственно правильной и при этом универсальной точки зрения, призванной тотализировать инфосферу. Современный формат средств массовой коммуникации предлагает информацию в виде коротких модульных вспышек — новостей, фрагментов фильмов и передач, рассекаемых рекламой и имеющих «странную, скоротечную и бессвязную форму». Носитель новой информационной культуры отказывается от восприятия этих модульных данных в рамках предлагаемых извне готовых целостных структур и категорий и стремится формировать из них собственный уникальный контент. Соответственно, между «традиционным» потребителем информации, ориентированным на линейное, концептуализированное и последовательное представление материала, и субъектом инфосферы нового типа возникает «полоса информационного отчуждения», поскольку привычный для одного из них информационный контент принципиально не пригоден для другого.

По Тоффлеру, новая информационная культура требует формирования новой, «метакультурной» индивидуальности, нормой для которой должна стать способность выходить за рамки привычных матриц интерпретации данных и поведенческих паттернов прежде всего потому, что эти матрицы и паттерны утратят свое значение инструментов обработки данных в ситуации, когда сбор и хранение информации представляли для субъекта критически сложную и затратную по времени и вниманию задачу. Компьютеризация и создание электронных систем хранения и поиска данных радикальнейшим образом с момента появления языка и затем письменности меняют структуру «социальной памяти», избавляя человека от необходимости запоминания фактов, но смещая акцент его деятельности на сознательный поиск и преобразование информации в практически безграничном и непрерывно разрастающемся информационном пространстве[28]. В быстро меняющемся мире прошлый опыт реже может служить надежным компасом, необходимы гораздо более быстрое освоение нового, большая реактивность Я, подвижность,

[28] См.: *Тоффлер Э.* Третья волна.

умение действовать методом проб и ошибок[29]. Заметим, однако, что Тоффлер опять-таки идеализирует этот коммуникационный формат, поскольку рассматривает информационное давление как необходимый и продуктивный эволюционный фактор. Если это и так, то на данный момент о сформированности «информационного человека» и тем более «информационного человечества», говорить не приходится, в то время как «информационная тревога» приобретает все более выраженные черты острой проблемы глобального масштаба. Само погружение в бесконечный информационный поиск уже на заре новой информационной эпохи осознавалось как возможное болезненное состояние, род информационной наркомании, ведущий к социальной беспомощности индивида и в конечном счете саморазрушению. (См.: *Лем С.* «Кибериада: путешествие шестое, или Как Трурль и Клапауций Демона Второго Рода создали, дабы разбойника Мордона одолеть» ; *Борхес Х.-Л.* «Алеф», «Книга тысячи страниц», «Вавилонская библиотека».) Однако и балансирование «на границе» глобального океана информации, не исключающее социальной адаптированности, порождает психологическое напряжение.

В 1995 г. американский нейрофизиолог Дэвид Льюис вводит в научный обиход понятие «синдром информационной усталости», обозначающий специфическое психологическое состояние человека, возникающее в условиях лавинообразного потока неструктурированной информации и ведущее к неверным оценкам реальности, ложным умозаключениям и к принятию неудовлетворительных, ошибочных решений. Синдром информационной усталости приводит к таким психологическим и физиологическим проблемам, как ослабление концентрации; стресс (и связанные с ним проблемы); усталость; агрессивность к окружающим.

Кроме того, происходит снижение интереса индивида к сути вещей при гипертрофии значения образа. Человек удаляется от реальности. Происходит доминирование визуального над смысловым. Облегченное компьютерными возможностями воспроизведение фрагментов чужого культурного кода придает бытию индивида ореол культурной ценности, создает иллюзию того, что приобще-

[29] Там же.

ние к массовой культуре делает человека частью культуры. При этом глобальную популярность приобретают авторы, в достаточно упрощенной форме предлагающие массовому реципиенту некие (обычно вымышленные или искаженные) культурные концепты, которые, однако, преподносятся с установкой на принадлежность к элитарному, обычно «тайному» или «запретному» знанию (Дэн Браун, Паоло Коэльо, историки школы А. Фоменко и др.). Массовая культура становится доминирующим типом культуры, а ожидаемое Тоффлером сращение между элитарной и массовой культурой если и происходит, то либо как иллюзия массового сознания, либо как снижение уровня элитарной культуры.

Еще одним важным следствием информационной усталости становится актуальность такого социокультурного феномена, как «политика ***постправды***» (англ. *post-truth politics*). Под постправдой принято понимать тип политической культуры, в которой дискурс в основном формируется через обращение к эмоциям и личным убеждениям аудитории (при этом подробности политической реальности остаются без внимания), повторение одной и той же аргументации и упорное игнорирование объективных фактов, противоречащих заданной концепции. Определяющей чертой политики постправды является то, что участники кампании продолжают повторять свои тезисы, даже если те получили опровержение в СМИ или через независимых экспертов. Это происходит из-за того, что раздробленность источников новостей создает ситуацию, в которой ложь, сплетни и слухи распространяются с необычайной скоростью. Ложь, которую распространяют политики или их сторонники в Интернете через сеть пользователей, может очень быстро подменять правду. В качестве типичного примера политики постправды обычно приводят предвыборные выступления Дональда Трампа. Действующий президент США Дональд Трамп во время предвыборной кампании неоднократно делал резкие заявления категорического толка, не нашедшие впоследствии какого-либо подтверждения. Так, он заявлял, что его противник на выборах Хиллари Клинтон является преступником и должна быть предана суду, а его предшественник Барак Обама родился за пределами США и, следовательно, не имел права баллотироваться на пост президента. Более 70 % заявлений

Дональда Трампа были оценены проектом Politifact как ложь или сознательное искажение фактов. Тем не менее, по опросам населения, Трамп считался более честным и заслуживающим доверия, чем его оппонент Хиллари Клинтон.

Для достижения максимального эффекта от политики постправды используется также конспирология. Согласно мнению Микаэля Дикона, парламентского представителя в The Daily Telegraph, Интернет и социальные сети сделали распространение теорий заговора максимально эффективным и быстрым. Поэтому теории заговоров парадоксальным образом не только вызывают гнев у людей, но и успокаивают, заявляя, что наши проблемы не наша вина, а во всем виноваты истеблишмент, массмедиа, новый мировой порядок и сионисты[30]. Поэтому в «эру постправды» такие конспирологические теории, как, например, заявление Дональда Трампа в 2008 г., что Барак Обама не был рожден на территории США, становятся главными новостными повестками. Согласно опросу, в 2008 г. 20 % населения Америки верили, что Барак Обама — мусульманин.

Стоит отметить, что концепция постправды как некоей специфической политтехнологической методики неоднократно и обоснованно критиковалась. Так, Тоби Янг в журнале «The Spectator» называет термин «политика постправды» идеологическим клише, использованным в основном левыми комментаторами, чтобы нападать на то, что на самом деле является универсальными идеологическими механизмами, заявляя, что «мы все живем в эру постправды и, вероятно, всегда жили»[31]. Но, как и в случае с термином «информационное общество», критика с позиций онтологической достоверности в данном случае неактуальна, поскольку символически ориентированное общество информационной эпохи склонно более ориентироваться на слова, чем на соответствующие или не соответствующие им факты реальности. Соответственно, неважно,

---

[30] *Deacon M.* In a world of post-truth politics, Andrea Leadsom will make the perfect PM // The Telegraph. 9 july 2016. URL: https://www.telegraph.co.uk/news/2016/07/09/in-a-world-of-post-truth-politics-andrea-leadsom-will-make-the-p/ (дата обращения: 25.08.2018).

[31] *Young T.* The truth about «post-truth politics» // The Spectator. 16 july 2016. URL: https://www.spectator.co.uk/2016/07/the-truth-about-post-truth-politics/.

существует ли постправда как осознанно применяемая технология или же это просто новое название для традиционной в политической сфере лжи. Существенно то, что постправда становится универсальным ориентиром в глобальной инфосфере в ситуации, когда иные глобальные ориентиры теряют актуальность. Не случайно слово post-truth («постправда» или «постистина») Оксфордский словарь английского языка назвал словом 2016 г. «Человек информационный» парадоксальным образом одновременно предельно доверчив (для информации, которую он получает из ограниченного референтного круга источников) и предельно циничен, поскольку внутренне убежден, что информационных хаос, с которым он сталкивается, — либо отражение хаоса намерений и перспектив, десакрализующего и дискредитирующего любые ценности, либо (в конспирологическом ключе) есть проявление заговора враждебных по отношению к нему и его референтной группе могущественных сил, сознательно трансформирующих инфосферу таким образом, чтобы добиться своих неведомых, но, очевидно, угрожающих благополучию или даже существованию данного индивида целей.

Частным проявлением постправды можно считать так называемый *фейк*, то есть сознательное распространение через СМИ (а в последние годы также посредством социальных сетей) заведомо ложной информации в формате и на материале, способном привлечь повышенное внимание аудитории, обычно для получения финансовой или политической выгоды. Следует отметить, что этот прием активно используется с момента появления СМИ (традиционный термин — газетная утка). Существует даже специфическая традиция контрфейка, так называемого *грубенхунда*, предполагающего предоставление новостным агентствам абсурдной или демонстративно ложной информации с целью продемонстрировать некритичное отношение СМИ к источникам и погоню за дешевыми сенсациями. Однако специфика современной инфосферы, минимизирующая затраты на создание и распространение фейка (и упрощающая его воздействие — например, в ряде случаев создатель фейка добивается только перехода на нужную страницу в Интернете, для чего может быть достаточно привлечь внимание пользователя Сети броским заголовком, минимально связанным с содержанием самой публи-

кации), привлекает к этому явлению повышенное внимание. Так, британское издательство Harper Collins, выпускающее толковый словарь английского языка Collins English Dictionary, 2 ноября 2017 г. объявило словосочетание fake news («фейк-ньюс») «словом года», ориентируясь на многократно выросшую частоту его употребления[32]. Соответственно, постулируется лавинообразное нарастание объема фейк-публикаций (традиционно в западных СМИ их источником считаются околоправительственные круги РФ[33], а собственно фейк-ньюс — едва ли не основным инструментом предполагаемого воздействия России на внутреннюю политику США[34]; российские источники, соответственно, говорят о «мировой фейк-империи» как инструменте антироссийской/антикитайской/антииранской/антисирийской/антисербской и т. п., прозападной/проатлантической и т. п. пропаганды[35]). Американские аналитики, к примеру, всерьез утверждают, что распространение фейк-ньюс стало одной из главных причин поражения Х. Клинтон на президентских выборах 2016 г.[36] Во всяком случае, можно констатировать, что речь идет о явлении общемирового масштаба[37].

Всеобщая распространенность электронных СМИ позволила президенту корпорации SONY в США Г. Стингеру объявить, что

---

[32] См., напр.: Названо слово года. URL: https://lenta.ru/news/2017/11/02/fakenews/ (дата обращения: 25.08.2018).

[33] См., напр.: Фейки года: кто и как нас обманывал в 2017-м. URL: https://www.bbc.com/russian/features-42421898 (дата обращения: 25.08.2018).

[34] См., напр.: *Беглы С.* Резкая речь Саманты Пауэр о России. URL: https://inosmi.ru/politic/20170119/238557834.html (дата обращения: 25.08.2018).

[35] См., напр.: *Мараховский В.* Мировая фейк-империя и борьба с ней. URL: https://ria.ru/analytics/20170705/1497870947.html (дата обращения: 25.08.2018).

[36] См., напр.: *Schor E.* Clinton decries fake news «epidemic». URL: https://www.politico.com/story/2016/12/hillary-clinton-fake-news-fight-232381 (дата обращения: 25.08.2018).

[37] См., напр.: *Safi M.* Fake news: an insidious trend that's fast becoming a global problem. URL: https://www.theguardian.com/media/2016/dec/02/fake-news-facebook-us-election-around-the-world (дата обращения: 25.08.2018) ; *Голубицкий С.* Торжество послеправды. Почему авторами «фейк-ньюс» стали мы сами. URL: https://www.novayagazeta.ru/articles/2018/04/08/76112-torzhestvo-poslepravdy (дата обращения: 25.08.2018).

в эту эпоху «каждый дом становится полем битвы»[38]. Шоу-бизнес выступает в качестве такой же производственной сферы, как и тяжелая индустрия. К началу двухтысячных медиарынок был более-менее поделен транснациональными корпорациями (Alphabet, Walt Disney, Comcast, Viacom, News Groop, Time Warner, Facebook и т. д.), по факту определяющими мировую информационную повестку. В результате они получили возможность влиять на политику всех иных уровней культурной индустрии — дистрибуцию контента через спутниковое, кабельное и эфирное вещание, стандартизацию форматов медиаданных, вопросы издательской деятельности и авторского права. Кроме того, через принадлежащие этим компаниям крупнейшие голливудские киностудии, они одновременно выполняют функцию «фабрики идей» для массового потребителя. Гиганты медиаиндустрии ведут глобальную борьбу за право формировать собственный дискурс для собственных референтных групп.

Этот принцип существования информации как производственной сферы и производительной силы общества, описанный еще Э. Тоффлером, рассматривающим информацию в цивилизациях третьей волны в качестве одного из главных видов сырья становится главным аргументом в таком виде межнационального противостояния, как ***информационные войны***. В своей типологии информационных войн Тоффлер, которому принадлежит приоритет в описании этого феномена, принципиально различает войны аграрные, которые велись за территорию, а также войны индустриальные, разворачивавшиеся вокруг средств производства, от войн третьей волны, от войн информационного века, которые могут вестись за средства обработки и порождения знаний и информации. Современные войны, отмечает Поль Вирильо, существуют как виртуальные кибервойны, ведущиеся в Интернете. Под влиянием новых требований к технологиям изменяется и мышление, функционирующее в предельно функциональном режиме, и модели социального управления, где особенно перспективной становится

[38] Цит. по: *Абдигалиева Г. К., Токтаров Б.* СМИ как фактор манипуляции массовым сознанием. URL: https://articlekz.com/article/8154 (дата обращения: 25.08.2018).

социополитическая кибернетика. Сфера политического представляется исследователю исчезающей, так как в перспективе единственным достоверным источником вариантов стратегических решений, касающихся возможностей мирного и военного развития, будут спутниковые и компьютерные системы. Проблему политики Вирильо увязывает с проблемой скорости. В работе «Скорость и политика» исследователь отмечает, что современная демократия скоро уступит место иному виду политического устройства — «дромократии» — «власти скорости», где диктатура власти основывается на диктатуре скорости, породившей революционные изменения в системах вооружения, преодолевшей границы геополитических образований — культур и цивилизаций и превратившей их в «глобальную деревню»[39].

Вирильо считает, что генетической предпосылкой развития не только современных технологий, но и современной культурной индустрии является милитаризм, так как основными составляющими успеха любой военной кампании выступают информация и скорость ее получения. Военная необходимость трансформирует сферу восприятия субъекта и его способность обрабатывать информацию, используя радары, приборы ночного видения, датчики движения, спутниковое наблюдение и т. п., то есть выходя за пределы собственно человеческих возможностей восприятия. Военные технологии, прежде всего средства визуальной военной разведки, Вирильо считает и генетической первоосновой такой формы массовой культуры, как кино, объединяемой с войной общей «эстетикой исчезновения» и способностью технологического продуцирования образов.

Соответственно, любые каналы сбора, накопления, распространения и интерпретации информации (например, СМИ) толкуются как военно-стратегическая инфраструктура, а собственно информация — как военно-политический ресурс: «Информация никогда не была более значимой. Необходимо оценить уязвимость и чувствительность медиа, американской общественности, наших политиков

[39] См., напр.: *Вирильо П.* Если время — деньги, то скорость — это власть. URL: http://almanax.russculture.ru/archives/1960 (дата обращения: 25.08.2018).

к информационным операциям в форме обмана, психологических операций и компьютерных атак, ежедневно ведущихся против Соединенных Штатов»[40]. Американский военный аналитик Т. Томас упоминает новые методы манипуляции сознанием, эмоциями, восприятием, выбором и интересами как одну из критических угроз человечеству, порожденных техническим прогрессом, наряду с упрощенной доступностью и тиражируемостью любой, в том числе социально опасной, информации (например, доступность знаний о производстве оружия или ОМП для антисоциальных субъектов и организаций, доступность персональных данных потенциальной жертвы для преступника и т. п., см. гл. 3 § 1) а также отсутствие общепринятых в международной практике норм легитимного обеспечения информационной безопасности.

«Общественное мнение, имидж публичного деятеля, приоритеты, которые формируют характер политики, — все это поддается корректировке с помощью стратегий масскульта и свидетельствует о том, что массмедиа выступают в информационном мире в качестве равноправного субъекта политики и образуют эффект, который принято называть „эффектом CNN". Характерно, что из трех блоков угроз — A (угроза выживанию), B (угроза западным интересам) и C (косвенное воздействие на сферу западных интересов) — на откуп СМИ отдается последний»[41]. Медиавойны последних десятилетий (информационное сопровождение балканских войн 90-х и начала тысячных годов, медиакампания против Саддама Хусейна, фактически обусловившая принятие решения об оккупации Ирака проамериканской коалицией, медиавойны против Каддафи и Асада) убедительно продемонстрировали эффективность воздействия новых медиа на политизированную аудиторию, причем в том числе и на решения субъектов мировой политики. В рамках модели информационной войны разворачивается в настоящее время обсуждение возможного вмешательства «российских хакеров» в президентские и парламентские выборы в США. «Сторона обвинения» последова-

---

[40] Цит. по: *Почепцов Г. Г.* Теория коммуникации. URL: https://studfiles.net/preview/2142041/ (дата обращения: 25.08.2018).

[41] *Костина А. В.* Тенденции развития культуры… .

тельно действует в рамках технологии постправды, повторяя одни и те же обвинения, градус которых нарастает по мере опровержения достоверности тех или иных фактов. При этом очевидно, что:

а) апелляция официальных лиц России и российских СМИ к отсутствию доказательств сама по себе не является доказательством (несомненно, что если бы вмешательство было реальным, звучало бы то же самое);

б) критика обвинений с позиции здравого смысла выглядит как проявление слабости, в то время как напор обвинителей воспринимается публикой как проявление силы (поскольку соответствует конспирологическим ожиданиям публики);

в) подтверждение обвинений в рамках обычной судебной аргументации невозможно, поскольку предполагает использование аргументов, доступных только специалистам высокого уровня (например, методы контроля национального информационного пространства спецслужбами США, прежде всего АНБ). Предъявление этих аргументов стало бы утечкой информации, поскольку авторитетным можно было бы считать только мнение независимых, то есть неподконтрольных спецслужбам и правительству США, специалистов; кроме того, многие из этих методов, вероятнее всего, незаконны, и даже ограниченное обнародование факта их использования, вероятно, привело бы к скандалу;

г) наконец, объективное подтверждение обвинений, по-видимому, контрпродуктивно для элит и спецслужб США, поскольку целью проводимой кампании является не проведение расследования (оно если и проводится, то вне всякой связи с выступлениями СМИ и политиков), но воздействие на сознание собственных избирателей, а здесь куда важнее убежденность политиков, чем выстроенная и подкрепленная фактами система аргументов; как раз второй случай в рамках цинического мировосприятия «человека информационного» воспринимается как конструкт, подтасовка данных и попытка скрыть правду.

Характерным примером действий в формате информационной войны можно также считать реакцию политического истеблишмента стран «коллективного Запада» на инцидент с отравлением семьи Скрипалей в Солсбери. Что бы ни произошло на самом деле,

во всяком случае мы наблюдаем: а) бездоказательность и безапелляционность обвинений в адрес РФ[42]; б) постоянное повышение градуса агрессии в высказываниях политиков; в) отклонение любых возражений оппонента как «смехотворных и незаслуживающих внимания» (опять же без какой-либо аналитики); г) призывы к сплочению перед лицом «российской угрозы» по принципу «кто не с нами, тот против нас»[43]; д) эскалация конфликта, перевод ситуации в сферу прямого экономического, политического и (потенциально) военного воздействия на оппонента непосредственно после инцидента, до появления каких-либо официальных выводов, полученных следствием или экспертным сообществом и доказательно подтверждающих участие или хотя бы заинтересованность правительства РФ в совершении рассматриваемых преступных действий.

Следует, однако, иметь в виду, что феномен информационной войны, во-первых, не связан исключительно с цивилизацией информационной эпохи и, во-вторых, как раз в эту эпоху оказывается чрезвычайно сложным явлением, дающим возможности для множественных интерпретаций. Детальному анализу феномена будет посвящена глава 4 настоящего исследования.

---

[42] См., напр.: Инцидент в Солсбери. Версия британского МИДа. URL: https://colonelcassad.livejournal.com/4080413.html (дата обращения: 25.08.2018).

[43] См., напр.: Глава МИД Британии обратится к ЕС с призывом усилить санкции против РФ. URL: https://rg.ru/2018/08/21/glava-mid-britanii-obratitsia-k-es-s-prizyvom-usilit-sankcii-protiv-rf.html (дата обращения: 25.08.2018).

Глава 2
РАССТАНОВКА ФИГУР: ИНФОСФЕРА РФ В МИРОВОМ КОНТЕКСТЕ

Одним из первых в нашей стране, кто ввел понятие «информационная сфера (инфосфера)», был академик А. П. Ершов — в 1988 г., в статье «Информатизация: от компьютерной грамотности учащихся к информационной культуре общества»[1]. В понятие «инфосфера» он включал три элемента: средства телекоммуникации, компьютерные средства и информационные ресурсы, которые в них хранятся, обрабатываются и с их помощью распространяются. Инфосфера рассматривалась им как глобальная целостность, в которой приведены в действие управляющие программы; оконечная аппаратура, вовлеченная в постоянную связь с пунктами возникновения и потребления информации, которые, в свою очередь, рассеянны по всем сферам мира Земли, людей и машин. Информатизация рассматривалась как деятельность, направленная на создание инфосферы. При этом в понятие «инфосфера» не включались все сущности, осуществляющие производство, обработку и потребление информации, информационные объекты (изделия, продукты), информационные процессы, которые реализуются в этом пространстве, а также система общественных отношений, связанная с производством, обработкой и потреблением информации. Информационная сфера

[1] См.: *Ершов А. П.* Информатизация: от компьютерной грамотности учащихся к информационной культуре общества // Коммунист. 1988. № 2. С. 82–92.

по Ершову — это параллельная по отношению к традиционному информационному миру реальность, где обращается информация, преобразованная в форму, удобную для электронной обработки.

Дальнейшее развитие содержания понятия «инфосфера» привело к появлению формулировки, вошедшей в Доктрину информационной безопасности Российской Федерации, утвержденную Президентом РФ в 2000 г. Инфосфера определялась как «совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений»[2]. Инфосфера объявлялась системообразующим фактором жизни общества, активно влияющим на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Понятие «инфосфера» здесь связывается с некоторым логическим пространством, в котором реализуются информационная инфраструктура и деятельность субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также отношения между ними в рамках страны. Причем в определение инфосферы включалась вся информационная инфраструктура страны вне зависимости электронная она или традиционная бумажная, а также вся информация, обращающаяся в стране.

В 2005 г. в результате обобщения работы по регламентации правоотношений, связанных с производством, распространением и потреблением информации, В. А. Копылов предложил понимать под информационной сферой сферу производства, преобразования и потребления информации. При этом информационную сферу предлагалось декомпозировать на пять предметных областей:

1) предметная область реализации права на поиск, получение, передачу и применение информации;

2) предметная область производства, передачи и распространения исходной и производной информации;

---

[2] См.: Доктрина информационной безопасности Российской Федерации № Пр-1895 от 9 сентября 2000 г. URL: https://studfiles.net/preview/4396571/ (дата обращения: 11.08.2018).

3) предметная область формирования информационных ресурсов, подготовки информационных продуктов, предоставления информационных услуг;

4) предметная область создания и применения информационных систем (АИС, БД, баз знаний), других информационно-телекоммуникационных технологий;

5) предметная область создания и применения средств и механизмов информационной безопасности[3].

Г. А. Воробьев называет следующие компоненты информационного пространства:

— система средств массовой информации;

— территориально распределенные государственные и корпоративные компьютерные сети, телекоммуникационные сети, а также средства коммутации и управления информационными потоками;

— система обеспечения информационной защиты;

— система информационного законодательства;

— система взаимодействия информационных пространств различного уровня[4].

Инфосфера, таким образом, предстает как сложное, многогранное явление, одновременно задействующее различные области общественного бытия и общественного сознания: персональную и массовую коммуникацию, образование и просвещение, производство, финансы, политические и административные процессы и процедуры, вопросы правового регулирования и новую сферу возможных угроз и правонарушений.

Говоря о функционировании глобальной инфосферы, мы должны иметь в виду, что ее развитие проходит неравномерно: оно ограничено как технологическими возможностями существующих коммуникационных систем, так и политико-экономическими факторами: неравномерностью экономического, образовательно-культурного и технологического потенциала различных государств, в ряде случаев также географическими и климатическими условиями, а также спецификой взаимодействия инфосферы и политической воли тех

---

[3] См.: *Копылов В. А.* Информационное право. М., 2005. 283 с.

[4] См.: *Воробьев Г. Г.* Твоя информационная культура. М., 1988. 303 с.

или иных субъектов политического процесса (государств, элит, общественных групп, активных индивидуумов). Здесь важно отметить, что спецификой инфосферы является ее развитие «сверху», зачастую по прямой инициативе государственных органов, поскольку инфосфера требует как серьезных инфраструктурных изменений, так и установления правил взаимодействия с существующими правовыми нормами. С другой стороны, некоторые ключевые проекты могут создаваться коммерческими структурами по собственной инициативе, в ориентации на существующие технические возможности и потребности рынка, хотя их реализация и требует взаимодействия с государственными структурами. В качестве примера можно рассмотреть развитие в России систем широкополосного беспроводного доступа в Интернет (мобильные сети третьего и четвертого поколения). Тем не менее данные проекты не могут функционировать без наличия спутниковых и/или кабельных магистральных каналов, которые по большей части находятся в России в собственности телекоммуникационных компаний с государственным участием (АО «Ростелеком» и компании «большой тройки»).

Одним из факторов, негативно влияющих на уровень распространения информационных технологий и развитие информационного общества в России, является недостаточно высокий уровень социально-экономического развития многих субъектов Российской Федерации. Так, сохраняется высокий уровень различия в использовании информационных технологий в домашних хозяйствах регионов. В рейтинговой оценке российских регионов по их готовности к информационному обществу индекс лидера в 22 раза превышает показатель региона-аутсайдера[5]. Остаются проблемы организации широкополосного доступа для конечных пользователей. На конец 2008 г. только около 21,5 % всех российских домашних хозяйств (11,4 млн домашних хозяйств) имели широкополосный доступ в сеть Интернет, а средняя скорость доступа в регионах ва-

[5] См. Распоряжение Правительства Российской Федерации № 1815-р от 20 октября 2010 г. Москва «О государственной программе Российской Федерации „Информационное общество (2011–2020 годы)“». URL: https://rg.ru/2010/11/16/infobschestvo-site-dok.html (дата обращения: 11.08.2018).

рьировалась от 128 Кбит/с до 1 Мбит/с, что существенно ниже, чем в Москве (7,5 Мбит/с) и Санкт-Петербурге (6 Мбит/с). В последнее время эти показатели существенно выросли. Так, в 2014 г. средняя скорость фиксированного доступа в Интернет в России составила почти 24 Мбит/с. Уровни проникновения широкополосного доступа (ШПД) и платного телевидения составили 52 и 62 % соответственно. К началу апреля 2014 г. в России насчитывалось 27,6 млн абонентов ШПД. По данным OpenSignal, на конец 2017 г. Россия занимала 73-е место в мире по охвату беспроводным широкополосным Интернетом формата LTE (65,08 %) и 65-е место по средней скорости передачи данных (15,77 Мбит/с), что выглядит явно недостаточным даже на фоне стран бывшего СССР, таких как Литва, Эстония или Казахстан[6].

Еще одним фактором, препятствующим ускоренному развитию в России информационного общества, является недостаточный уровень распространения в обществе базовых навыков использования информационных технологий. Это касается как населения в целом, так и государственных и муниципальных служащих.

Следует отметить высокий уровень зависимости российского рынка от зарубежной продукции в сфере информационных технологий. В подавляющем большинстве создаваемых информационных систем в России сегодня используются в основном зарубежные разработки. Можно выделить еще ряд барьеров, препятствующих успешному развитию отечественной промышленности в сфере информационных технологий, среди которых критически значимым является низкий уровень правовой защиты интеллектуальной собственности.

Основные направления, по которым наша страна включается в процесс функционирования глобального информационного пространства:

— формирование сферы IT-технологий как самостоятельного сегмента российской экономики и его включение в глобальный технологический процесс;

---

[6] См.: OpenSignal: The State of LTE (February 2018). URL: https://opensignal.com/reports/2018/02/state-of-lte (дата обращения: 11.08.2018).

— взаимодействие российской инфосферы с зарубежными медийными институтами (где Россия с конца 80-х гг. XX в. выступает в роли реципиента информации, а в последнее десятилетие также и активного игрока на информационном поле);

— подключение к глобальной сети Интернет (первые международные контакты посредством аналоговых телефонных модемов через сеть «Релком» — с 1990 г.), формирование и развитие национальной системы доступа к глобальным информационным сервисам, в том числе для частных лиц, и российского сегмента Интернета (так называемого «Рунета»);

— формирование среды постоянного информационного взаимодействия на всех уровнях, охватывающей большинство граждан России, затрагивающей все сферы жизни (от частных интересов индивида до общероссийской и международной политики, а также внедрение элементов системы «электронного правительства»), включая активное воздействие граждан России (как частных лиц, так и субъектов политического процесса) на глобальную инфосферу;

— трансформация характера традиционных СМИ и формирование СМИ нового поколения, развитие социальных сетей и блогосферы;

— развитие системы правового регулирования инфосферы, оценка инфосферы как источника угроз нового поколения, формирование концепции информационной безопасности;

— формирование государственной политики в информационной сфере, в том числе серии основополагающих документов, определяющих стратегические приоритеты и направления развития информационного общества в России.

§ 1. Российская инфосфера и российская экономика

Переход к информационному обществу представляет собой достаточно сложный и многогранный процесс, развитие которого тесным образом связано с определенной перестройкой общественного сознания. В России такая перестройка началась существенно позднее, чем в передовых странах Запада. И причина здесь кроется

не столько в технологическим отставании России, сколько в гуманитарной сфере. Марксистско-ленинская идеология не воспринимала концептуальные идеи глобальной информатизации и формирования информационного общества, которые появились на Западе в конце 70-х и начале 80-х гг. XX в. Концепция построения информационного общества была объявлена в нашей стране антинаучной, хотя и рассматривалась академическими кругами в контексте других постиндустриальных учений. IT-экономика находилась в зачаточном состоянии, компьютерные технологии и информационные сети применялись по преимуществу в военных либо научно-исследовательских проектах; рынка персональных компьютеров практически не существовало. Только в 90-е гг. XX в., после распада СССР, формируется рынок информационных продуктов и услуг, компьютерных и телекоммуникационных технологий. В этот же период происходит разрушение государственной монополии на формирование информационных потоков и либерализация рынка СМИ. Однако в первую очередь это означало доступ западных компаний к российскому потребителю, поскольку наработанные в нерыночных условиях отечественные компьютерные технологии оказались экономически неконкурентоспособными, хотя их разработка в узких сегментах (разработка безопасных сетей и систем обработки данных правительственного и военного назначения) продолжалась.

Отрасль информационных технологий — один из самых динамично развивающихся сегментов российской экономики. В 2015 г. на фоне падения ВВП на 3 % ИТ-отрасль продемонстрировала высокий темп прироста добавленной стоимости (28 %). В ретроспективе последних 10 лет наиболее благоприятными для развития отрасли стали докризисные 2005–2007 гг., а также 2012 г. К провальным можно отнести 2009 и 2013 гг., когда произошло снижение добавленной стоимости соответственно на 7 и 3 % (рис. 1). Причем если в 2009 г. негативную роль сыграл общеэкономический фактор, то стагнация 2013 г. стала следствием сокращения спроса со стороны бизнеса и завершения крупных инфраструктурных проектов. До 2015 г. индустрию отличали высокие темпы развития — прирост добавленной стоимости в постоянных ценах в 2015 г. по сравнению с 2010 г. почти на четверть (при росте ВВП на 7 % — рис. 1). В 2016 г.

достигнутый уровень развития удержать не удалось: произошло сокращение на 5 %[7].

Рис. 1. Динамика валовой добавленной стоимости ИТ-отрасли (в процентах к предыдущему году; в постоянных ценах)

В 2015 г. отмечались структурные изменения в объеме реализованной собственной продукции ИТ-компаний (рис. 2). Скачок продаж (в 1,9 раза по сравнению с 2014 г.) наблюдался в организациях, осуществляющих разработку программного обеспечения и консультирование в этой области. На 18 % повысили продажи организации, деятельность которых связана с обработкой данных. При этом в сегментах консультирования по аппаратным средствам вычислительной техники, создания и использования баз данных и информационных ресурсов удалось достичь лишь соответственно 80 и 72 % от уровня 2014 г.[8]

В 2015 г. впервые за пять лет наблюдалось сокращение внешнеторговых операций по ИТ-услугам. Экспорт компьютерных услуг (услуги, связанные с аппаратным и программным обеспечением, услуги по обработке данных, техническому консультиро-

[7] Информационная индустрия в России : материалы по проекту «Мониторинг информационного общества и цифровой экономики» // Высшая школа экономики: Мониторинговые исследования. URL: https://issek.hse.ru/news/209633223.html (дата обращения: 11.08.2018).

[8] См.: Развитие отрасли информационных технологий за последние 10 лет : материалы по проекту «Мониторинг информационного общества и цифровой экономики» // Центр развития: Мониторинговые исследования. URL: https://issek.hse.ru/news/196240096.html (дата обращения: 11.08.2018).

ванию и внедрению аппаратных и программных средств и другие ИТ-услуги), по оценкам Банка России, снизился на 7 % по сравнению с 2014 г., импорт — на 23 %. Их объемы составили соответственно

Рис. 2. Объем реализованных организациями ИТ-отрасли товаров собственного производства, выполненных работ и услуг собственными силами по видам экономической деятельности, 2015 (млрд руб.)

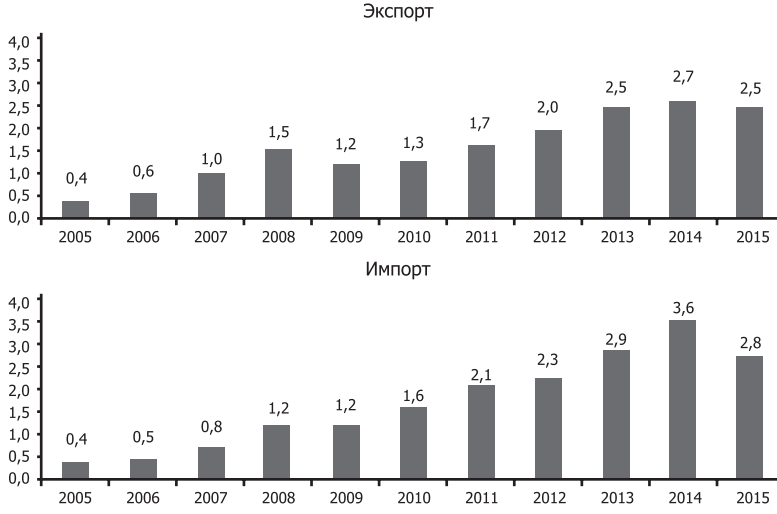

Рис. 3. Динамика экспорта и импорта компьютерных услуг (млрд долл. США)

2,5 и 2,8 млрд долл. США против 2,7 и 3,6 млрд долл. США в 2014 г. (рис. 3)[9].

Что касается расходов организаций на приобретение программных средств, то большая их часть приходится на импортную продукцию. В 2015 г. доля расходов организаций на приобретение программных средств отечественного производства в общем объеме затрат на ИТ не превысила 21 %. Наименьшую зависимость от поставок из-за рубежа демонстрируют органы государственного управления и организации здравоохранения: в них рассматриваемый показатель составил 44 и 46 % соответственно. Самая низкая доля закупок российского программного обеспечения наблюдается в отраслях транспорта и связи — менее 8 %[10]. Основные причины наблюдаемого спада, помимо сложной экономической ситуации, — это сокращение затрат компаний на ИТ, насыщение корпоративного и розничного сегментов; отсутствие прорывных российских ИТ-решений, а также кадровый голод. В целом на конец 2017 г. базовые рейтинги развития ИКТ-технологий ставят РФ на 45 место при общей тенденции на снижение сравнительных показателей[11].

Необходимо подчеркнуть, что ИТ-сектор достаточно чувствителен к политическим и экономическим изменениям. По данным аналитической компании Gartner, снижение мировых расходов на ИТ (ИТ-устройства, ИТ-услуги, ПО, системы для data-центров, услуги связи) наблюдается начиная с 2012 г. (на 5–7 % в год), что обусловлено замедлением темпов развития глобальной экономики[12].

---

[9] Развитие отрасли информационных технологий за последние 10 лет…

[10] Там же.

[11] См.: Взлет России в мировых ИТ-рейтингах сменился застоем и падением. URL: http://www.cnews.ru/news/top/2018-04-09_podem_rossii_v_klyuchevyh_iktrejtingah_smenilsya (дата обращения: 11.08.2018) ; Рейтинг стран мира по уровню развития информационно-коммуникационных технологий: информация об исследовании и его результаты: ICT Development Index // Индекс развития информационно-коммуникационных технологий. URL: https://gtmarket.ru/ratings/ict-development-index/ict-development-index-info (дата обращения: 11.08.2018).

[12] См., напр.: ИТ (мировой рынок). От 18.06.2018 г. URL: https://tinyurl.com/ybfb5l9j (дата обращения: 11.08.2018).

Спрос на ИТ-решения сократился как со стороны государственных структур, так и со стороны корпоративного сектора. В 2016 г. негативное влияние на глобальный рынок оказал Brexit (объем рынка в 2016 г. — 3,4 трлн долл.). Однако в 2017–2020 гг. эксперты ожидают положительную динамику при среднегодовых темпах роста, равных 3 %. Что касается сегмента ПО, то он является самым быстрорастущим на мировом ИТ-рынке (+6 % в 2016 г. до 333 млрд долл.).

С географической точки зрения, по оценкам аналитиков, крупнейшим потребителем ИТ-решений является Северная Америка, на этот регион приходится около 30 % мировых ИТ-расходов. Доля Западной Европы составляет более 20 %; доля Азиатско-Тихоокеанского региона (исключая Японию) — менее 30 %[13]. Рыночная доля РФ на глобальном рынке на конец 2016 г. не превышала 1 %[14].

Существенное отставание российской промышленности в сфере высокотехнологического производства, прежде всего электроники и компьютерной техники, привело к тому, что отечественная продукция представлена по преимуществу в сферах военной техники, промышленного и научного оборудования, а также в сфере госуслуг; на внешнем рынке эта техника практически не востребована. Что касается географии продаж российского ПО, то, по данным Руссофт, более 90 % продаж осуществляется на развитых рынках — в США и странах Западной Европы, а около 10 % — в прочих странах дальнего зарубежья[15]. При этом в настоящий момент в мире развивается достаточно много перспективных ИТ-рынков, где российские компании или представлены точечно или вообще не представлены (например, Латинская Америка, Африка и др.).

В течение нескольких последних лет доля зарубежных продаж российского ПО увеличивалась опережающими темпами по сравнению с темпами роста совокупного объема российского экспорта (2,7 % в 2016 г., 1,9 % в 2015 г., 1,2 % в 2014 г.). Однако здесь суще-

---

[13] См.: *Седых И. А.* Рынок компьютерных услуг 2017 // Центр развития: Мониторинговые исследования. URL: https://tinyurl.com/yby9kzpv (дата обращения: 11.08.2018).

[14] Там же.

[15] Там же.

ственную роль сыграло сокращение всего отечественного экспорта в стоимостном выражении по причине падения цен на нефть. При этом средние темпы роста экспортных поставок ПО начали замедляться с 40–50 % в 2002–2007 гг. до 15–20 % в 2008–2016 гг. Это можно объяснить в большей степени созреванием рынка и эффектом высокой базы, чем сокращением внешнего спроса. В денежном выражении, по данным Руссофт, экспортные объемы ПО, увеличились с 2,8 млрд долл. в кризисном 2009 г. до 7,6 млрд долл. в 2016 г. Позитивные результаты были достигнуты фактически без господдержки, которая активизировалась только в 2015–2016 гг.[16]

Среди наиболее успешных российских игроков на мировом рынке можно отметить прежде всего представителей сегмента ИТ-безопасности: Kaspersky Lab, InfoWatch. Также достаточно популярны продукты для финансовых организаций от Diasoft; решения в сфере облачных вычислений — от Acronics; системы виртуализации и автоматизации хостинговых услуг — от Parallels; услуги по индвидуальной разработке ПО — Epam, Luxoft, Mera, First Line Software.

Несмотря на тот факт, что российский рынок относят к категории формирующегося, на нем присутствует существенное число компаний, которые являются состоявшимися и активноразвивающимися организациями (не стартапами) и могут привлекать инвестиции посредством других инструментов (например, IPO), нежели венчурное финансирование.

Для отечественного ИТ-рынка в настоящее время характерно наличие ряда стимулирующих и сдерживающих факторов. К наиболее серьезным сдерживающим факторам можно отнести слабую диверсификацию экономики России, зависимость от сырьевых ресурсов и их экспорта. На фоне западных санкций и снижения цен на энергоносители, снижается и объем доступных для инвестирования в экономику средств.

Другой негативный фактор — неэффективность крупных государственных инвестиционных проектов. Слабое взаимодейст-

---

[16] См. подробнее: Четырнадцатое ежегодное исследование российской индустрии экспортной разработки программного обеспечения. URL: http://www.russoft.ru/report/4304 (дата обращения: 11.08.2018).

вие федеральных и региональных властей приводит к увеличению стоимости ИТ-проектов, нарушению сроков их реализации и раздуванию бюджетов.

К стимулирующим факторам можно отнести увеличение объема перерабатываемых данных и необходимость автоматизации процесса переработки. Многие предприятия стремятся автоматизировать бизнес-процессы, что ведет к модернизации ИТ-инфраструктуры.

Росту рынка способствует также проникновение Интернета. Несмотря на то, что по показателям проникновения Россия отстает от развитых стран, степень проникновения в стране все же на достаточно высоком уровне. Это увеличивает популярность услуг, оказываемых через Интернет. В период 2014–2016 гг. доля пользователей электронной торговли среди населения России в возрасте 15–72 лет выросла на 5 процентных пунктов и достигла 23 %. Среди пользователей Интернета — 30 % заказывают товары и услуги. Особенно активно через Интернет приобретают товары, относящиеся к категориям «Одежда, обувь, спорттовары» (востребованы у 48 % онлайн-покупателей), «Предметы домашнего обихода» (26 %), «Электронное оборудование» (14 %). Наименьшую популярность получила покупка через сеть важных товаров для жизнеобеспечения: продуктов питания (9 %) и медицинских товаров (10 %). В сфере услуг лидируют финансовые: доля их пользователей увеличилась с 2014 г. на 10 процентных пунктов (максимальный рост среди категорий товаров и услуг, приобретаемых через интернет) — до 29 %. Кроме того, население активно пользуется Интернетом для организации путешествий, покупки билетов на развлекательные мероприятия, а также телекоммуникационными услугами (по 18 %)[17].

При этом уровень развития российского IT-рынка с трудом соответствует среднемировым показателям и серьезно отстает от лидеров. По данным за 2016 год, доля информационной индустрии в России составила 3,3 % ВВП. В большинстве развитых стран этот показатель находится на уровне 5 %, в Великобритании, Венгрии, Ирландии,

[17] См.: Электронная торговля в России // Высшая школа экономики: Мониторинговые исследования. URL: https://issek.hse.ru/news/206444153.html (дата обращения: 11.08.2018).

Республике Корея, США, Японии достигает 7 %[18]. Однако по показателю объема рынка интернет-торговли Россия в 2016 г. входила в десятку стран-лидеров[19] и демонстрировала устойчивый рост в 2017 г.[20]

Присутствие иностранных инвесторов на ИТ-рынке России также положительно сказывается на его развитии. Приоритетное направление для иностранных инвесторов — облачные технологии. Однако степень присутствия зарубежного капитала в последние годы стабильно снижается, что вызвано экономической и политической неопределенностью. По данным Центрального банка России, чистый вывоз капитала из РФ частным сектором в 2017 г. составил 31,3 млрд долларов США что означает рост в сравнении с показателями 2016 г. в 1,5 раза[21].

Положительно на развитии рынка может сказаться также закон о хранении и обработке персональных данных внутри страны. Это позволит повысить востребованность систем хранения данных. Стимулировать рост может и политика импортозамещения в области разработки отечественных ИТ-продуктов, в том числе процессоров, что повлечет также расходы и на ИТ-услуги.

Еще один потенциальный драйвер роста для рынка — меры, направленные на импортозамещение в программной сфере, прежде всего в деятельности органов государственной и муниципальной власти. Так, с 1 января 2016 г. государственные органы обязаны закупать отечественное программное обеспечение, вошедшее в Единый реестр российских программ для электронных вычислительных

---

[18] См.: Информационная индустрия в России // Высшая школа экономики: Мониторинговые исследования. URL: https://issek.hse.ru/news/209633223.html (дата обращения: 11.08.2018).

[19] См.: *Седых И. А.* Рынок интернет-торговли в РФ: 2017 // Центр развития: Мониторинговые исследования. URL: https://tinyurl.com/yclfbxny (дата обращения: 11.08.2018).

[20] См.: *Сергеева Ю.* Интернет 2017–2018 в мире и в России: статистика и тренды // По данным агентства We Are Social и платформы Hootsuite. URL: https://www.web-canape.ru/business/internet-2017-2018-v-mire-i-v-rossii-statistika-i-trendy/ (дата обращения: 11.08.2018).

[21] URL: https://www.rbc.ru/rbcfreenews/5a5f7e569a79473c169d0c4b (дата обращения: 11.08.2018).

машин и баз данных[22], при этом покупка ПО иностранного производства разрешена только в случае отсутствия российских аналогов.

К наиболее неоднозначным по части воздействия на IT-индустрию событиям можно отнести расширение мер по обеспечению государственной безопасности, таких как «закон Яровой»[23]. Критики данного комплекса законодательных актов указывают на непроработанность его концепции в организационной и экономической сфере, на неоправданные расходы, которые должны лечь на предприятия IT-сферы и в конечном счете резко повысить расходы конечного потребителя[24], наконец, на возможность возникновения в результате его реализации новых стратегически значимых уязвимостей в российской инфраструктуре. Так, директор отдела анализа и контроля рисков, информационной безопасности компании PwC в России Роман Чаплыгин отмечает, что исполнение закона может привести к созданию хранилищ данных с большим объемом накопленной информации, которые могут стать привлекательной целью для злоумышленников и спровоцировать рост числа кибератак. При этом угрозой конфиденциальности могут стать недобросовестные

---

[22] URL: https://reestr.minsvyaz.ru (дата обращения: 11.08.2018).

[23] См.: Федеральный закон Российской Федерации «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» № 374-ФЗ от 6 июля 2016 г. URL: https://duma.consultant.ru/documents/3711655 (дата обращения: 11.08.2018) ; Федеральный закон Российской Федерации «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» № 375 от 6 июля 2016 г. URL: https://duma.consultant.ru/documents/3711654 (дата обращения: 11.08.2018).

[24] См., напр.: «Почте России» придется потратить 500 млрд рублей на исполнение «закона Яровой». URL: http://www.forbes.ru/news/324549-pochte-rossii-pridetsya-potratit-500-mlrd-rublei-na-ispolnenie-zakona-yarovoi (дата обращения: 11.08.2018) ; Закон Яровой с 1 июля 2018 года спровоцирует повышение цен на Интернет. URL: http://www.1rre.ru/130778-zakon-yarovoj-s-1-iyulya-2018-goda-sprovociruet-povyshenie-cen-na-internet.html#i (дата обращения: 11.08.2018) ; Операторы не могут исполнить закон Яровой. URL: https://regnum.ru/news/2441627.html (дата обращения: 11.08.2018) и др.

сотрудники, обладающие доступом к данным[25]. Российский союз промышленников и предпринимателей предупредил, что закон может привести к «общей деградации интернет-отрасли в России»[26]. В любом случае, законопроекты приняты Государственной думой РФ в июле 2016 г.; соответственно, поправки, дающие Правительству РФ полномочия обязывать операторов связи хранить записи телефонных разговоров, SMS и интернет-трафик пользователей сроком шесть месяцев, вступили в силу 1 июля 2018 г.

К числу оспариваемых инициатив Правительства РФ относят также понижение с 1 июля 2018 г. порога стоимости облагаемых таможенной пошлиной онлайн-покупок за рубежом с перспективой дальнейшего снижения этого порога после 2020 г. Закон, лоббируемый Ассоциацией российских компаний интернет-торговли (АКИТ), опять-таки повышает расходы конечного пользователя и при этом усложнение процедуры для зарубежных трейдеров, что может привести к их отказу от работы с российскими пользователями либо возникновению и распространению теневых схем[27].

Д. А. Мирошниченко, эксперт в области управления сбытом и стратегического менеджмента портала Openbusiness, предлагает следующую оценку основных тенденций развития IT-сферы в РФ:

— «закат» серверной виртуализации: рост рынка на сегодняшний день обеспечивается только за счет обслуживания уже интегрированных решений;

— облачные решения перестают быть трендом и выходят в плоскость мейнстрима;

— рост популярности модели SaaS (ПО как услуга);

— развитие сетей устройств, «интернета вещей»;

---

[25] См.: *Виноградова Е., Кантышев П., Серьгина Е.* Кто может заработать на законе Яровой. URL: https://www.vedomosti.ru/technology/articles/2016/08/22/653895-kto-zarabotaet-zakone-yarovoi (дата обращения: 11.08.2018).

[26] См.: *Шамина О.* Как подорожает сотовая связь из-за «закона Яровой» // Русская служба BBC. URL: https://www.bbc.com/russian/features-44376641 (дата обращения: 11.08.2018).

[27] См. напр.: URL: https://nalog-expert.com/oplata-nalogov/nalog-na-internet-pokupki-2018.html; http://mybrendtop.ru/pokupki-v-zarubezhn-int-mag (дата обращения: 11.08.2018) и др.

— развитие технологий 3D-печати со среднегодовым темпом роста 64,1 % до 2019 г.;

— появление новых типов данных, например сенсорной информации;

— дальнейшее развитие нейронных компьютерных сетей и популяризация и их использования;

— машинное обучение ведет к росту популярности роботов, автономных транспортных средств, виртуальных персональных ассистентов;

— существенно усложняется защита информации на фоне активизации хакеров и усложнения цифровых систем (усложнение делает их более запутанными для самих пользователей);

— рост данных потребует значительных вычислительных ресурсов, вследствие чего получат распространение архитектуры на базе программируемых вентильных матриц и графических ускорителей;

— разработка программных платформ для «интернета вещей»[28].

В последние несколько лет государство стало уделять повышенное внимание регулированию и поддержке российской отрасли информационных технологий. На данный момент уже принят ряд законодательных документов (Стратегия развития информационного общества в РФ на 2017–2030 г.; Стратегия развития отрасли информационных технологий РФ на 2014–2020 гг.; федеральные и региональные нормоакты, касающиеся налоговых льгот для ИТ-компаний и др.), которые напрямую или косвенно регулируют отечественную ИТ-отрасль. Кроме того, осуществляется стимулирование таких инфраструктурных элементов, как технопарки, особые экономические зоны, территории передового развития.

Отдельно стоит остановиться на Стратегии развития отрасли информационных технологий правительства РФ[29], основная цель которой — улучшение условий для ускоренной трансформации российской

---

[28] См.: *Мирошниченко Д. А.* Обзор рынка информационных технологий. URL: https://www.openbusiness.ru/biz/business/obzor-rynka-informatsionnykh-tekhnologiy/ (дата обращения: 11.08.2018).

[29] Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года. Утверждена Распоряжением Правительства РФ от 01.11.2013 № 2036-р. URL: http://mins-

ИТ-отрасли. В частности, под этим понимается комфортный фискальный режим; наличие квалифицированных специалистов на рынке; наличие инфраструктуры для развития; качественные механизмы защиты интеллектуальной собственности; доступность источников финансирования. Согласно целевым показателям документа, объем производства российской ИТ-продукции в РФ должен к 2020 г. достичь 450 млрд руб. (по данным некоторых экспертов, на 2017 г. этот уровень уже пройден). Наконец, План мероприятий предполагает увеличение объема экспорта ИТ-продукции до 9 млрд долл. (в 2015 г., по данным Руссофт, объем экспортных поставок составил 6,7 млрд долл., в 2016 г. — порядка 8 млрд долл.)[30]. Государственная стратегия «Информационное общество» предполагает, что к 2020 г. Россия должна будет войти в первую десятку международного рейтинга по индексу развития информационных технологий, в двадцатку рейтингов — по развитию электронного правительства и сетевого общества.

Реализация процесса перехода к информационному обществу в России в определенной мере учитывает накопленный отечественный и зарубежный опыт программно-целевых методов организации работ. Стратегия перехода, как и отдельные, принятые позже программы ее реализации, имеют в какой-то степени интегрирующий характер, способный объединить различные ведомственные и коммерческие проекты. Стратегия имеет, таким образом, как бы надведомственный общегосударственный статус, обеспечивающий возможность координации усилий всех участников процесса перехода.

Согласно стратегии, основой российского пути перехода к информационному обществу должны явиться:

— информатизация всей системы общего и специального образования — от детского сада до окончания высшей школы и последующих форм подготовки и переподготовки специалистов;

— повышение роли квалификации, профессионализма и способностей к творчеству как важнейших характеристик человеческого потенциала;

---

vyaz.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014-2020_2025.pdf (дата обращения: 11.08.2018).

[30] См.: *Седых И. А.* Рынок компьютерных услуг. 2017.

— формирование и развитие индустрии информационных и телекоммуникационных услуг, в том числе домашней компьютеризации, ориентированной на массового потребителя;

— обеспечение сферы информационных услуг духовным содержанием, отвечающим российским культурно-историческим традициям, в том числе организация мощного русскоязычного сектора в Интернете.

Решение этих вышеназванных масштабных, исторических для России задач будет означать реальное превращение информации и знаний в подлинный ресурс социально-экономического и духовного развития. Оно будет также означать укрепление институтов гражданского общества, реальное обеспечение права граждан на свободное получение, распространение и использование информации, расширение возможностей для саморазвития личности[31].

Таким образом, историческая преемственность, национальная идентичность, восстановление нравственного сознания, образование единого духовного пространства страны — таковы основные особенности вероятного пути России к информационному обществу.

Осознание важности развития информационно-телекоммуникационных технологий стало, по сути, только первым шагом в формировании новых российских приоритетов. И политические дебаты, и интеллектуальные дискуссии последних лет подтверждают, что идея телекоммуникационной политики как важнейшей сферы деятельности современного российского государства находит все более масштабную поддержку в общественном мнении страны. Но России нужна новая коммуникационная политика, где три важнейшие силы российского рынка: частный бизнес, государство и пользователи — выработали бы определенные соглашения о том, как, в каком направлении будут развиваться ИТТ с тем, чтобы использовать мировой опыт и одновременно учитывать национальную специфику.

«Отрасль информационных и телекоммуникационных технологий в России с 2000 г. развивалась высокими темпами, ежегодный

[31] Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года.

прирост составлял около 25 %, что существенно выше среднегодовых темпов роста валового внутреннего продукта и роста отдельных отраслей. Информационные технологии и информационные услуги стали существенной статьей российского несырьевого экспорта. Однако сводные индексы и межстрановые сопоставления до сих пор характеризуют Россию не лучшим образом, что говорит о недостаточном уровне развития отрасли информационных технологий, об отставании от мировых лидеров, а также о нереализованности потенциала уже существующих инфраструктур и технологий. С другой стороны, по ряду параметров Россия не отличается от европейских стран, где доля сектора информационных технологий составляет около 5 % валового внутреннего продукта, около 30 % населения никогда не пользовались сетью Интернет и только 38 % граждан использовали сеть Интернет при получении государственной услуги (в основном для получения формы заявления)»[32].

Отмечавшиеся в указанный период достаточно высокие темпы роста были продемонстрированы во многом благодаря новым открывшимся рынкам, новым продуктам и услугам (сотовая связь, компьютерное оборудование, консалтинг и другие услуги) на фоне низкого начального уровня развития информационных технологий в России. В настоящее время становится очевидным, что для сохранения набранных темпов роста необходимо устранить целый ряд существующих барьеров. Одним из таких барьеров является недостаточное развитие системы электронного документооборота и взаимодействия граждан с государственными структурами в онлайн-режиме. В декабре 2009 г. впервые в РФ был утвержден «Сводный перечень первоочередных государственных и муниципальных услуг, предоставляемых органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления в электронном виде, а также услуг, предоставляемых в электронном виде учреждениями субъектов Российской

[32] См.: Государственная программа Российской Федерации «Информационное общество (2011–2020 годы)». URL: https://rg.ru/2010/11/16/infobschestvo-site-dok.html (дата обращения: 11.08.2018).

Федерации и муниципальными учреждениями»[33]. В июле 2015 г. Госдума РФ приняла Федеральный закон № 263-ФЗ, направленный на уравнивание в правах электронных и бумажных документов[34], причем номенклатура государственных и коммерческих документов, действительных в электронном виде, постоянно расширяется[35]. Тем не менее в 2016 г. наша страна заняла 35-е место в рейтинге электронного правительства Департамента экономического и социального развития ООН, потеряв с 2014 г. восемь позиций, хотя динамика показателей Индекса развития электронного правительства позволила РФ сократить разрыв со страной-лидером на 1 % — с 27 до 26 %; при этом по целевым показателям стратегии во II квартале 2018 г. ожидалось вхождение РФ в первую двадцатку индекса[36]; фактический показатель на июль 2018 г. — 32 место[37]. Таким образом, на данный момент действия Правительства РФ

---

[33] См.: «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления в электронном виде, а также услуг, предоставляемых в электронном виде учреждениями субъектов Российской Федерации и муниципальными учреждениями (с изменениями на 28 декабря 2011 года)». Распоряжение от 17 декабря 2009 года № 1993-р. URL: http://docs.cntd.ru/document/902191383 (дата обращения: 11.08.2018).

[34] См.: Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части отмены ограничений на использование электронных документов при взаимодействии физических и юридических лиц с органами государственной власти и органами местного самоуправления» № 263-ФЗ от 13.07.2015. URL: http://www.consultant.ru/document/cons_doc_LAW_182652/ (дата обращения: 11.08.2018).

[35] См.: Электронные и бумажные полисы ОСАГО законодательно уравняют в правах. URL: https://rg.ru/2018/06/28/elektronnye-i-bumazhnye-polisy-osago-zakonodatelno-uravniaiut-v-pravah.html (дата обращения: 11.08.2018).

[36] См.: *Абдрахманова Г. И., Ковалева Г. Г., Коцемир М. Н.* Россия в рейтинге развития электронного правительства / Информационное общество : мониторинг. Информационный бюллетень. 2016. № 5 (10) // Центр развития: Мониторинговые исследования. URL: https://tinyurl.com/ybdnbyj5 (дата обращения: 11.08.2018).

[37] См.: Рейтинг электронного правительства ООН. URL: https://tinyurl.com/y8zcpvn6 (дата обращения: 05.08.2018).

по реализации Стратегии развития отрасли ИТ следует оценить как недостаточные, даже с учетом объективных трудностей, с которыми сталкивается российская экономика на фоне кризисных явлений в мировой экономике и под действием санкционной политики государств коллективного Запада.

§ 2. Медиасфера и коммуникации

По образному определению американского медиолога Дугласа Рашкоффа, «единственная среда, в которой наша цивилизация еще может расширяться, наш единственный настоящий фронтир — это эфир, иными словами — медиа. Вследствие этого власть, которой сегодня обладает тот или иной человек, определяется уже не количеством собственности, находящейся в его распоряжении, а скорее тем, сколько минут „праймтайма“ на телевидении или страниц новостной печати он может заполучить. Непрерывно расширяющиеся медиа стали настоящей средой обитания — пространством, таким же реальным и, по всей видимости, незамкнутым, каким был земной шар пятьсот лет назад…»[38].

В конце XX — начале XXI в. в мировом информационном пространстве появилось новое явление — глобальное новостное телевещание. Оно стало одним из наиболее ярких проявлений и проводником глобализации. Интенсивное развитие технических средств передачи информации (спутниковых, кабельных, компьютерных систем и коммуникационных средств связи, сети Интернет) позволяет оперативно распространять новостные программы в течение 24 часов в сутки (так называемый феномен CNN). Это привело к созданию глобального коммуникационно-информационного пространства, в орбиту которого вошли практически все страны и народы — так называемой глобальной инфосферы или медиасферы.

---

[38] *Рашкофф Д.* Медиавирус. Как поп-культура воздействует на ваше сознание. М., 2003. С. 8.

Для описания функционирования медиасферы М. А. Буряк[39] предлагает брать за основу характерные черты так называемого медиатекста как основного продукта медиасферы:

— особый тип и характер информации — информация рассматривается отправителем как существенная, важная или даже необходимая обществу как массовому ее потребителю. Информация, вращающаяся в медиасфере, должна представлять интерес для какой-либо аудитории: это может быть небольшая группа, а может быть подавляющее большинство, то есть массовая аудитория. Чем большее количество людей воспринимают получаемую информацию как значимую, тем дольше она будет сохраняться в медиасфере, тем большими обрастет деталями и подробностями (соответственно, мы должны отметить изменчивость и динамический характер как определяющие особенности медиасферы. — *Прим. авт.*);

— массовая аудитория, вступающая в опосредованное, социально ориентированное общение и соответственно обретающая категориальные признаки, такие как рассредоточенная, неопределенная, разнородная аудитория, объединенная «только элементарным знанием языка»; представляющая собой социальные группировки, не связанные целями и интересами (массовая аудитория является характерной аудиторией для медиасферы, однако не единственной);

— производство на поток, одноразовость, сиюминутность, быстротечность информации. В эпоху современных технологий этот критерий стал наиболее актуален. Информация очень быстро может получить статус значимой и важной для общества и так же быстро его потерять;

— смысловая незавершенность, открытость для многочисленных интерпретаций; интертекстуальность — тексты СМИ представляют собой совокупность фраз бесконечных гипертекстов, где все является ссылкой друг на друга и бесконечным цитированием;

— поликодовость текста — текст может включать видео и комментарии к нему, графики или схемы. В современном медиапростран-

---

[39] См.: *Буряк М. А.* Медиасфера: концептуализация понятия. URL: https://cyberleninka.ru/article/n/mediasfera-kontseptualizatsiya-ponyatiya.pdf (дата обращения: 05.08.2018).

стве практически невозможно встретить информацию, подающуюся в каком-то одном заданном формате, чаще всего она мультимедийна;

— медийность — информация попадает в медиасферу через медиаканалы: это СМИ, как традиционные (печатные, аудио-, видео, онлайн-издания), так и новые социальные медиа. Например, переписка в «Твиттере» между двумя собеседниками может стать достоянием аудитории и тиражироваться далее в других СМИ; при этом, к примеру, твиттер-активность президента США Д. Трампа становится заметным фактором мировой политики[40].

Доминирующее положение на мировом информационном рынке занимают мегакомпании, созданные по типу вертикальной интеграции: America Online — Time Warner, Walt Disney Co, Vivendi Universal Viacom, Bertelsmann, News Corporation и др.; эти компании занимают высокие позиции популярного рейтинга Fortune Global 500[41], составляемого по показателю среднегодовой выручки. Медиамагнатами, то есть субъектами, контролирующими заметную долю глобального медиаконтента, считаются, например, глава News Corporation Руперт Мэрдок (150 медиакомпаний во всем мире), президент компании Viacom Самнер Редстоун, владелец медиакорпорации Bloomberg Майкл Блумберг.

Коммуникационная революция в конце XX в. была отмечена не только появлением сети Интернет и мобильной связи, но и развитием нового феномена концентрации транснациональных и мультимедийных СМИ. Глобальные медиакомпании взаимодействуют между собой, образуя картели и концерны.

Деятельность глобальных медиакомпаний включает в себя: создание медиапродуктов, то есть традиционных и электронных СМИ, графического, видео- и аудиоконтента (изображений и фотоматериалов, музыкальных роликов, фильмов, сериалов, телепрограмм),

---

[40] См., напр.: «Это его оружие»: как Трамп ведет войны в «Твиттере». URL: https://www.gazeta.ru/politics/2018/07/08_a_11830435.shtml (дата обращения: 05.08.2018).

[41] См. данные за 2018 г. на сайте исследования. URL: http://fortune.com/global500/ (дата обращения: 20.11.2018) ; см. также бесплатно данные рейтинга за 2006–2013 гг. на сайте CNN. URL: https://money.cnn.com/magazines/fortune/global500/2013/full_list/?iid=G500_sp_full (дата обращения: 20.11.2018).

книг, статей и т. д.; дистрибуция, аккумуляция, импорт и экспорт контента медиаканалов.

Крупнейшим производителем и экспортером медиапродукции в мире являются Соединенные Штаты Америки.

Следует отметить, что глобальные медиахолдинги учитывают не только общемировую повестку, но и локальную специфику потребителя на местах, его вкусы и интересы, создавая в ряде случаев адаптированный к ним информационный контент. Эта тенденция считается частным случаем процесса ***глокализации*** (glocalization) — то есть сосуществования разнонаправленных тенденций в едином информационном пространстве. «Глокализация в корпоративных стратегиях медиакомпаний способствует сведению к минимуму финансовых рисков и получению максимальных прибылей. Глокализация одновременно приспосабливает и продвигает локальные медиапродукты на глобальном рынке и служит адаптации глобальных продуктов на местных информационных рынках»[42]. Примером могут служить каналы MTV, наполнение которых меняется в зависимости от региона трансляции; аналогичным образом действуют глобальные новостные сети, включающие в повестку освещение региональных новостей. Таким образом, «глокальная» аудитория получает доступ к интересующему ее медиапродукту под брендом и в стилистике глобального — и в контексте популярного глобального контента. «Наряду с приспособлением локальных культур к вторжению западных ценностей, образцов и стандартов массовой культуры, глокализация способствует росту мультикультурализма (сосуществования и частичного взаимопроникновения различных культур), наиболее полно проявляющемуся в многонациональных мегаполисах. <…> К проявлениям глокализации относятся дальнейший рост национального самосознания народа, <…> их стремление к участию в глобальных процессах. Данная тенденция проявляется в рамках процесса европейской интеграции»[43].

---

[42] См. *Орлова В. В.* Глобальные телесети новостей на информационном рынке. М., 2003. URL: http://zavantag.com/docs/427/index-2016694.html (дата обращения: 11.08.2018).

[43] *Ефременко Д.В.* БРЭ. Т. 7 // Большая Российская энциклопедия, 2007. С. 250.

Еще одной важнейшей особенностью современных СМИ является их **конвергентность.** Конвергентная журналистика — это результат слияния, интеграции информационных и коммуникативных технологий в единый информационный ресурс. Сегодня современные медиакомпании расширяют свой спектр информационных и развлекательных продуктов и используют при этом «новые» формы подачи медиапродукта: онлайн-газета, радио в Интернете, веб-телевидение и др.

Важной особенностью современной медиасферы является **депрофессионализация** журналистики. Специфика сети Интернет позволяет организовывать регулярное информационное вещание на широкую аудиторию без специального развертывания особой технической инфраструктуры — соответственно, любой желающий получает возможность создавать собственные средства массовой информации. На рубеже веков стала развиваться и завоевывать популярность **блогосфера**, зачастую заменяющая традиционные СМИ. Профессиональная журналистика и блогосфера конкурируют между собой и в то же время дополняют друг друга. Важнейшими характеристика интернет-журналистики являются ее мультимедийный характер, интерактивность и диалогичность.

Параллельно со сменой предпочтений в выборе коммуникационных каналов происходит и трансформация интересов в области содержания информации. Майк Рэгсдейл, исследователь, предприниматель и основатель 30A.com, отмечает: «Люди больше не обращаются к основным СМИ для получения новостей — они обращаются к ним только для того, чтобы услышать свое собственное мнение, отраженное в них. Консерваторы смотрят консервативные новостные каналы, в то время как либералы предпочитают либеральные новостные каналы. При этом сами СМИ искренне верят в то, что они предлагают „нейтральные“ новости, но на самом деле журналистики в чистом виде уже давно не существует». «Люди, измученные ежедневным информационным стрессом и приводящими в ужас историями и политическими комментариями, будут рады отдохнуть от всего этого», — резюмирует М. Рэгсдейл и прогнозирует рост интереса к «позитивным» новостям и увели-

чение роли пользовательских трансляций, обмена фото- и видеоинформацией[44].

Еще в конце «нулевых» исследователями отечественного и мирового медиарынка были отмечены: а) устойчивое снижение общезрительского интереса к информационным программам; б) дифференциация внимания аудитории по социальным группам и микрогруппам (так, специалисты топ-уровня, ответственные за принятие решений, были заинтересованы в существовании специализированных информационных каналов); в) устойчивое перераспределение в медиасфере: отмирание печатных СМИ, падение интереса к эфирному радио (при росте внимания к интернет-радио), переключение внимания среднего и старшего поколения (30–70 лет) на телевидение и, наконец, устойчивое снижение интереса молодежи к так называемым традиционным медиа вообще и полное переключение на новые медиа, завязанные на Интернет. Показательным здесь является возникновение промежуточных форм — интернет-телевидения или видеотрансляции в Интернете эфирных радиопрограмм (так называемые «стримы» — например, передач «Эхо Москвы»). Таким образом, трендом можно назвать размывание устоявшихся технологических границ между каналами коммуникации. Так, Хью Шардт, генеральный директор компании AIR, считает, что в ближайшем будущем границы между различными каналами размоются окончательно: «К 2020 г. мы придем к полной и окончательной победе мультиплатформенного контента. Новая медиасистема — это выход за пределы традиционных видовых характеристик печати, радио, телевещания или цифрового вещания. Новости будут выходить на тех платформах, которые в наибольшей степени соответствуют их сути»[45].

При этом определяющими становятся принципы таргетирования, дробления целевой аудитории вплоть до подбора медиаобъектов в соответствии с индивидуальными предпочтениями потребителя (это уже практикуют социальные сети и ряд информационных порталов типа «Рамблера», причем определяющим моментом ста-

---

[44] Дивный новый медиамир: Какими будут медиа в 2020 году. URL: https://www.cossa.ru/trends/157072/ (дата обращения: 11.08.2018).

[45] Там же.

новится неявный сбор персональной информации и индивидуализация рекламы). Макроэкономическое значение социальных сетей и мессенджеров определяется распространением высокоскоростных эфирных каналов, обеспечивающих беспроводной широкополосный доступ в Интернет, и возрастающая доступность эффективных мобильных платформ (смартфоны и планшеты).

Современные исследователи описывают систему новых медиа четырьмя ключевыми взаимосвязанными процессами: *конвергенцией, дигитализацией, интерактивностью и принадлежностью данных медиаресурсов к сетевому пространству.* При этом в широком смысле к новым медиа можно отнести вообще Интернет, а также компьютерные игры, цифровые фильмы и фотографии, мобильную телефонию, «Википедию», явление гражданской журналистики и даже электронную почту. Другими словами, речь идет о самом широком перечне новых медиаформатов, которые могут включать в себя: интернет-представительства (порталы) онлайновых СМИ; интернет-СМИ; интернет-ТВ (вебкастинг); интернет-радио (подкастинг); мобильное ТВ; блогосферу; мессенджеры и интернет-телефонию; кино, рассчитанное на интернет-аудиторию; социальные сети (включая детские социальные сети); twitter; виртуальные сообщества; виртуальные игры; другие ресурсы Веб 2.0.

Таким образом, расширение пространства журналистской коммуникации происходит за счет включения новых видов сетевых коммуникативных практик, таких как блоги и социальные сети. Зачастую такие новые медиа именуют уже новейшими.

Упомянутые тенденции носят глобальный характер, но подключение России к глобальной медиасфере сделала их актуальными и для нас. Рассмотрим данные ВЦИОМ по медиапотреблению на конец 2017 г.[46]

---

[46] Здесь и далее данные до 2016 г. см.: Медиапотребление сегодня: пять основных фактов // Всероссийский центр изучения общественного мнения (ВЦИОМ). URL: https://wciom.ru/index.php?id=236&uid=116026 (дата обращения: 11.08.2018) ; на 2017 г. — *Федоров В.* Медиапотребление в России. Доклад на рабочей встрече Клуба деловой репутации «Комсомольской правды» в Страсбурге. URL: https://wciom.ru/fileadmin/file/reports_conferenc-

1. Главным источником новостей о событиях в стране для большинства наших сограждан по-прежнему остается телевидение, однако его популярность снижается (62 % — в 2015 г., 57 % — в 2016 г., 52 % — на 2017 г.). В то же время Интернет (включая информационные сайты, социальные сети и блоги) на 2017 г. используют для поиска новостных материалов 32 % всех опрошенных (в 2015 г. — 22 %). Однако можно предположить, что в дальнейшем это число будет только расти, поскольку сеть является главным источником новостей для 82 % 18–24-летних, 59 % — 25–34-летних.

2. Оценка воздействия ТВ на зрителей за последние 25 лет ухудшилась. Так, если в 1989 г. 73 % респондентов считали, что телевидение повышает моральный уровень людей, то на 2014 г. об этом говорят 46 %. В то же время в пять раз стало больше тех, кто отмечает ухудшение нравственности общества под воздействием просмотра телеканалов (с 8 до 38 %). Каждый третий россиянин (35 %) уверен: если в течение месяца люди не смогут смотреть телевизор, это пойдет им лишь на пользу (с 18 % в 1989 г.), однако 51 % респондентов думают, что это все же будет значимой потерей.

3. Несмотря на снижение интереса, телепередачи центральных каналов остаются в лидерах рейтинга доверия средствам массовой информации: по данным 2017 г., им доверяют или скорее доверяют 70 % россиян. Показатель региональных ТВ ниже (64 %). Другие же СМИ вызывают доверие менее чем у половины опрошенных, а абсолютными аутсайдерами являются зарубежные телепередачи, газеты, журналы и т. д.: им доверяют только 7–9 %, в зависимости от характеристик фокус-группы. Наиболее высокие показатели — порядка 14 % — отмечены для возрастной группы 18–24 лет, и для Москвы показатели не превосходят 14 %. Интересно, что группа доверяющих традиционным СМИ практически не верит новым медиа, в то время

---

es/2017/2017-10-26_smi_abr.pdf (дата обращения: 11.08.2018) ; на 2018 г. — Восстановление уровня лояльности к рекламе в Интернете: Медиапотребление в России — 2018. URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/research-center/media-consumption-in-russia-2018-ru.pdf (дата обращения: 11.08.2018).

как группа доверяющих новым СМИ при определенных условиях готова верить и традиционным.

4. Объективность освещения информации, по мнению населения, зависит от тематики: если новостные материалы о природных катаклизмах (70 %), а также деятельности главы государства (55 %) и положения России на мировой арене (51 %) более половины граждан считают скорее непредвзятыми, то в отношении других тем (положение дел в экономике, деятельность оппозиции, события на Украине и др.) показатели не превосходят 40 % и устойчиво снижаются.

5. Печатные СМИ читают менее половины наших сограждан (44 % по опросам 2018 г. при нарастающей тенденции к снижению аудитории). Интернет-версии печатных изданий пользуются меньшей популярностью — к ним обращаются 58 % опрошенных (однако доля ежедневной аудитории выше, чем у бумажных аналогов — 18 %). Бумажную прессу чаще читают люди пенсионного возраста — 59 % (против 49 % в группе от 18 до 24 лет), тогда как онлайн-пользователи СМИ — это скорее молодежь — 82 % 18–24-летних (против 25 % старше 60 лет). Большинство наших сограждан (79 %) в 2017 г. утверждали, что не готовы совсем отказаться от бумажных СМИ. Однако доля тех, кто заявил, что может полностью перейти на чтение электронных медиа, составляла 19 % (с незначительным ростом показателя на 1–2 % в год). Представители молодежных групп выражают подобную решимость в два раза чаще, чем в среднем по выборке (36 %), тогда как люди пенсионного возраста, напротив, крайне редко (4 %).

В целом на 2018 г. общий рейтинг пользы медиаисточников распределяется следующим образом: Интернет — 49 % для рабочего и 39 % для выходного дня; радио — 6 и 4 % соответственно, печатные СМИ: –1/–2 % и телевизор: –11 и –4 %[47].

В послереволюционный период Россия длительное время находилась в ситуации информационной изоляции — взаимодействие

[47] См.: Восстановление уровня лояльности к рекламе в Интернете: Медиапотребление в России — 2018. URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/research-center/media-consumption-in-russia-2018-ru.pdf (дата обращения: 11.08.2018).

с мировой медиасферой осуществлялось либо через контролируемые государством каналы разного рода, либо через «вирусное» воздействие западных СМИ типа радиостанций «Голос Америки» или «Свобода», либо, наконец, частным порядком, зачастую негласно и опосредованно, в том числе через нелегальное тиражирование информационных объектов разного рода (преимущественно произведений массового искусства — «музыка на костях», подпольные видеосалоны и т. д., — а также текстов, так или иначе попадавших под цензурный запрет — феномен самиздата). Соответственно, государственные медиа и контролируемая государством система массовых и частных коммуникаций развивались в условиях отсутствия конкуренции, без учета экономической составляющей и в ряде случаев — потребительского качества информации. Перед медиасферой ставились в первую очередь пропагандистские, затем культурно-просветительские задачи; передача информации как таковой по преимуществу была подчинена пропагандистским задачам. В результате при либерализации медиарынка, в условиях отсутствия или недостаточности господдержки отечественные медиа длительное время демонстрировали недостаточную конкурентоспособность. Фактически основной целью медиа становится трансляция рекламы, обеспечивающей экономическую состоятельность медиапроектов; соответственно, основным содержанием медиа становятся развлекательные программы разного рода (фильмы, сериалы, программы-состязания, юмористические шоу, спорт): так, в эфире Первого канала на 2012 г. развлекательный контент составлял порядка 70 % эфира, в эфире канала «Россия 1» — 72 %. На 2015 г. общий процент развлекательных программ составил 57 %, даже с учетом существования в эфире сугубо информационных («Россия 24») или просветительских («Культура») телеканалов. Следует при этом учитывать, что существенная часть развлекательного контента является трансляцией либо калькой западных медиаобъектов, либо, наконец, трансляцией международных медиасобытий (международные спортивные соревнования разного уровня, «Евровидение» и пр.).

Медиапространство диктует свои ролевые модели и статусы. Соответственно процесс социализации индивида в информаци-

онном обществе имеет свои особенности. К классическому пониманию понятия социализации добавляется «процесс и результат усвоения, а также готовность к воспроизведению и анализу личностью актуальной составляющей информационного опыта человечества, включающего работу с информацией и информационно-коммуникационными технологиями»[48]. Этот процесс получил название **инфосоциализации** (информационной социализации). Стремительные изменения в современной общественной жизни и рост информационных коммуникативных технологий позволяют утверждать, что инфосоциализация по своему содержанию есть процесс информационного становления личности, который начинается с первых минут жизни человека.

Процесс инфосоциализации характеризует не только то, как медиапространство воздействует на человека, но и то, как информационная деятельность индивида влияет на само информационное пространство. Современная медиасфера ставит читателя и СМИ в равные условия. Человек перестает быть пассивным зрителем и получателем информации, он получает возможность влиять на медиапространство, собственно, именно это и происходит, когда мы говорим о недостаточной таргетированности традиционных СМИ и о политике перехода от максимально широкого охвата к просчитанному (в том числе с подключением технологии искусственного интеллекта) индивидуальному воздействию на потребителя. Подобный подход невозможен без наличия информационной активности самого потребителя, позволяющей оценить его вкусы и предпочтения. Именно возможность информационой активности субъекта и определили параметры медиареволюции XXI в., которая снизила роль традиционных информационных каналов в пользу сети Интернет.

В 2004 г. издательство O'Reilly Media, специализирующееся на информационных технологиях, впервые употребило термин **Web 2.0.** Позднее термин концептуализировал руководитель изда-

---

[48] *Бодрунова С. С.* Медиакратия. Атлантические подходы к определению термина // Медиафилософия. Границы дисциплины : материалы междунар. науч. конф. СПб., 2013. С. 91–105.

тельства Тим О'Рейлли (Tim O'Reilly) в статье «Что такое Веб 2.0». До настоящего времени содержание и обоснованность применения термина является предметом дискуссии, однако он фиксирует важный этап эволюции сети Интернет. Если на первом этапе Глобальная сеть рассматривалась как средство передачи информации, созданной пользователями за ее пределами, и мыслилась, соответственно, как среда открытого хранения данных и система каналов обмена данными, то идеология Веб 2.0 фиксирует момент превращения Интернет в среду активной коммуникации, предполагающей создание информации непосредственно в Сети, в том числе в результате совместной деятельности нескольких удаленных пользователей (идеология и технология вики, то есть разработка сайтов, содержимое которых пользователи могут самостоятельно изменять с помощью инструментов, предоставляемых самим сайтом, с появлением изменений в режиме реального времени и поддержкой многопользовательского режима[49]).

Интернет и каналы широкополосного доступа позволили реанимировать идеологию компьютерных терминалов (в формате «тонкий клиент»), что расширило функционал сравнительно маломощных мобильных устройств, расширили возможность удаленной работы, в том числе для специалистов, нуждающихся в существенных вычислительных мощностях, и одновременно предельно упростили процесс сбора первичной информации: расширяющиеся возможности тех же смартфонов радикально повышают не только количество, но и качество любительского фото- и видеоконтента, что ставит под вопрос будущее профессиональной журналистики. Это одновременно повышает статус интернет-дискуссий — от частного обмена мнениями к имеющему социальное значение диалогу между значимыми дискурсами, «интердискурсивности»[50]. Пользователь Сети, таким образом, превращается из пассивного потребителя в создателя

[49] См. проекты фонда «Викимедиа», но также и коммерческие вики-сервисы, такие как «Яндекс-вики», Confluence, PBWorks и др. Ward Cunningham's original description of Wik. URL: http://www.wiki.org/wiki.cgi? WhatIsWiki (дата обращения: 11.08.2018).

[50] См.: *Пастухов А. Г.* Вопросы интердискурсивности и селекция новостей // Дискурс современных масс-медиа в перспективе теории, социальной

информации, в активного игрока на информационном поле, и в этом смысле действительно следует говорить о перераспределении существующих социальных ролей, о некоей новой социализации, новых формах самоутверждения и новой социальной реальности, границы которых должны определиться в ближайшем будущем.

§ 3. Инфосфера в образовании и культуре

В 70-е гг. прошлого века получил распространение термин «параллельная школа»[51]. В Европе так называли эффект получения знаний из общедоступных средств массовой информации. Ребенок мог сформировать представление об исторических фактах по художественным фильмам и телесериалам, изучить язык по мультфильмам, сделать выводы о том, что такое нефть и как ее перерабатывают, из телепередачи про Арабские Эмираты. Разумеется, полученные таким образом знания нередко нуждались в уточнении, а зачастую просто формировали у подростка искаженную картину мира. «Параллельная школа» воспринималась как потенциальная угроза для официального образования; с другой стороны, развитие инфосферы привело к появлению тезиса о принципиальном устаревании традиционного образования как системы линейной трансляции накопленных знаний между поколениями. Лавинообразное нарастание потока информации и стремительные изменения научной картины мира и представления о технических возможностях человечества заставляют предполагать, что:

— процесс линейной передачи знаний («информационно-знаниевая парадигма образования»), который не успевает за прогрессом и не может конкурировать по степени влияния на сознание с «па-

практики и образования : материалы II Международ. науч.-практ. конф. Белгород, 2016. С. 57–67.

[51] См. напр.: Параллельная школа — средства массовой информации (радио, телевидение, кинематограф, пресса), воздействующие на подрастающее поколение и оказывающие огромное влияние на его формирование // Проф. образование : словарь. Ключевые понятия, термины, актуальная лексика. М., 1999. С. 223.

раллельным образованием», должен уступить место обучению процедурам самостоятельного и/или группового поиска, оценивания, освоения и использования информации из доступных источников (на первом этапе обучения) и затем навыкам создания информации как технической, экономической и социальной ценности (то есть нового достоверного знания и новых навыков) в процессе творческого освоения реальности («развивающая парадигма образования», см., напр., требования ФГОС общего образования, по которым уделяется особое внимание компетенциям обучающегося — «…**метапредметным**, включающим освоенные обучающимися межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные), способность их использования в познавательной и социальной практике, самостоятельность в планировании и осуществлении учебной деятельности и организации учебного сотрудничества с педагогами и сверстниками, способность к построению индивидуальной образовательной траектории, владение навыками учебно-исследовательской, проектной и социальной деятельности; ***предметным***, включающим освоенные обучающимися в ходе изучения учебного предмета умения, специфические для данной предметной области, виды деятельности по получению нового знания в рамках учебного предмета, его преобразованию и применению в учебных, учебно-проектных и социально-проектных ситуациях, формирование научного типа мышления, владение научной терминологией, ключевыми понятиями, методами и приемами»)[52];

— во всех сферах индивидуальная работа с информацией постепенно должна уступить место ее коллективной обработке в составе работающих над общим проектом исследовательских или творческих групп (лабораторий, компаний, студий и т. п.) «Чтобы добиться успеха, необходимо создать организацию, способную аккумулировать и ассимилировать собственные знания и опыт,

[52] Федеральный государственный образовательный стандарт среднего общего образования (в ред. Приказов Минобрнауки России от 29.12.2014 № 1645, от 31.12.2015 № 1578, от 29.06.2017 № 613). URL: http://classinform.ru/fgos/1.4-srednee-obshchee-obrazovanie-10-11-class.html (дата обращения: 11.08.2018).

заниматься самообразованием. Это требует от нас, в первую очередь, понимания и признания того, что мы несовершенны. Для создания организации, которая была бы способна аккумулировать знания и учиться, необходимо увеличить скорость трансформации и транспортации знаний. Начинается этот процесс с того, что знания свободно распространяются в организации. Нужно сместить накопление знаний с уровня индивидуального на уровень групповой, уровень всей организации»[53];

— рутинные, воспроизводящиеся операции по поиску, накоплению и черновой обработке информации должны во все возрастающей степени брать на себя обучаемые и самообучающиеся системы искусственного интеллекта, оставляя человеку больше времени для осмысления и преобразования накопленного человечеством культурного опыта[54].

При этом следует иметь в виду, что взаимодействие образовательной среды и инфосферы идет по двум асимметричным направлениям: с одной стороны, мы должны говорить об инфосфере как о об инструменте, позволяющем трансформировать традиционные подходы к образованию, об инфосфере как возможности; с другой — следует говорить о формировании информационных навыков и компетенций как важнейшей задаче образовательного процесса[55].

В качестве основных проблем, возникающих на стыке образования и современной инфосферы, следует отметить:

— упомянутое выше некритическое восприятие информации (в том числе экономически, технически и/или соцокультурно значимой), полученной в результате свободного поиска в медиасфере (приобретает исключительное значение в условиях массовой доступности ресурсов сети Интернет);

---

[53] *Нордстрем К., Риддерстрале И.* Бизнес в стиле фанк. Капитал пляшет под дудку таланта. СПб., 2002. С. 165. URL: http://vitalik.info/pictures/photo/4484.pdf (дата обращения: 11.08.2018).

[54] См. напр.: *Ложечкин А.* Об искусственном интеллекте. URL: https://tinyurl.com/ybs9cd82 (дата обращения: 11.08.2018).

[55] См. напр.: *Васильев В., Сухорукова М.* Информационное общество и образование. URL: https://cyberleninka.ru/article/n/informatsionnoe-obschestvo-i-obrazovanie-2 (дата обращения: 11.08.2018).

— нетворческое, компилятивное использование ресурсов Интернета[56];

— образовательная и эмоциональная некомпетентность представителей старшего поколения, которые зачастую уступают обучающимся в навыках работы в современной информационной среде, отказываясь от ее использования либо используя ее формально-механически (что приводит к усилению социально-психологического разрыва между поколениями и утрате оснований для культурной преемственности)[57];

— наконец, неочевидность результатов организационных и экономических мер воздействия на образовательную среду. Необходимые реформы означают одновременно переподготовку педагогических кадров, повышение информационной компетентности общества в целом, изменения критериев оценки результатов образования, развитие инфраструктуры образовательных учреждений и информационной инфраструктуры и т. д. При этом процесс реформ движется параллельно с процессом технологических и социокультурных изменений, в результате чего реформы приобретают «вечно догоняющий» характер, а их эффективность постоянно оказывается под вопросом[58].

Обратимся к статистике. Согласно данным мониторинговых исследований ВШЭ, в 2015 г. численность ИКТ-профессионалов в России — разработчиков и аналитиков программного обеспечения и приложений, специалистов по базам данных и сетям, специалистов-техников по эксплуатации ИКТ и поддержке пользователей

---

[56] Там же.

[57] См. напр.: *Баранова Е. В.* Образование в информационном обществе. Проблемы образования в России и пути их решения // Науч.-метод. электрон. журнал «Концепт». 2015. Т. 5. С. 41–45 ; *Измагурова В.* Интернет-имидж педагога. Как не наделать ошибок в Сети? URL: http://zviazda.by/ru/news/20171207/1512647246-internet-imidzh-pedagoga-kak-ne-nadelat-oshibok-v-seti (дата обращения: 11.08.2018) ; Личная страница педагога в соцсети: цель, приватность и общие правила поведения. URL: https://rosuchebnik.ru/material/lichnaya-stranitsa-uchitelya/ (дата обращения: 11.08.2018) и др.

[58] См. напр.: *Рябенко В.* Образование и информационное общество. URL: http://magref.ru/obrazovanie-i-informatsionnoe-obshhestvo/ (дата обращения: 11.08.2018).

ИКТ, телекоммуникациям и радиовещанию — оценивалась в 1,2 млн человек (около 2 % занятых), при этом, допустим, в Финляндии, Швеции, Великобритании эта доля достигает 5–6 %; в целом РФ занимает по этому параметру одно из последних мест в Европе[59] (рис. 4).

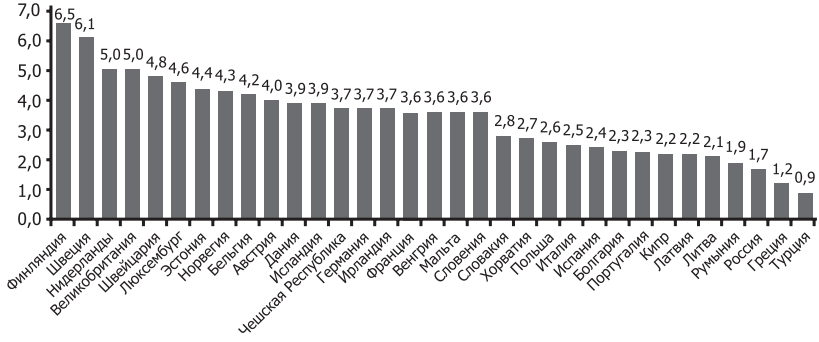

Рис. 4. Удельный вес ИКТ-специалистов
в общей численности занятых по странам, 2015 (%)

С другой стороны, можно говорить о высокой распространенности пользовательских ИКТ-навыков у населения РФ: четыре пятых населения (81 %) в возрасте от 15 до 72 лет когда-либо пользовались персональным компьютером, столько же — Интернетом. Ежедневная сетевая аудитория приблизилась к 60 %.

Обследование населения по вопросам использования информационных технологий и информационно-телекоммуникационных сетей, проводимое Росстатом, показало, что самые распространенные компьютерные навыки связаны с работой с текстовым редактором (применяло 42 % респондентов), передачей файлов между компьютером и периферийными устройствами (29 %), работой с электронными таблицами (23 %). Однако доля продвинутых пользователей, способных изменить параметры или настройки конфигурации программного обеспечения, не превышает 3 %, такой же показатель

[59] См.: Цифровые навыки населения // Высшая школа экономики: Мониторинговые исследования. URL: https://issek.hse.ru/news/207284687.html (дата обращения: 11.08.2018).

касается лиц, обладающих навыками установки или переустановки операционной системы. Решение задач самостоятельного написания программного обеспечения с использованием языков программирования под силу лишь 1 % опрошенного населения[60].

Нельзя назвать благополучной и ситуацию в научно-исследовательской среде. В ходе опроса Росстата владение на базовом уровне терминологией, связанной с наиболее распространенными современными цифровыми технологиями, продемонстрировали от 57,1 (термин Big Data Analysis) до 24,5 (термин Back End and Front End Programming) опрошенных специалистов высшей квалификации — кандидатов и докторов наук. Об использовании этих технологий в своей профессиональной деятельности заявили 29,9 и 10,4 % опрошенных соответственно (с сопоставимыми параметрами убывания показателей от термина к термину)[61].

Более обнадеживающей, на первый взгляд, выглядит ситуация в сфере российской культуры. Понимая культуру в широком смысле как основную форму существования ноосферы, можно выделить различные направления влияния на нее информационного общества через внедрение информационно-коммуникационных технологий. Определяющим и объединяющим этих направлений является перевод культурной информации, культурных смыслов и кодов в цифровую форму. В цифровой форме сейчас представляются как традиционные виды информации — текст, графика, звук, видео, так и совершенно новые, которые могут существовать только в цифровой форме — мультимедиа, гипертекст, виртуальная реальность, цифровая голография, видео 360° и др. При этом не только растут объемы оцифрованной традиционной культурной информации — параллельно создается и оригинальный цифровой контент[62].

---

[60] Там же.

[61] См.: Цифровой кругозор российских ученых / Материалы по проекту «Мониторинг информационного общества и цифровой экономики» // Высшая школа экономики: Мониторинговые исследования. URL: https://issek.hse.ru/news/216441485.html (дата обращения: 11.08.2018)

[62] См.: *Борисов Н. В., Прокудин Д. Е.* Информационное пространство направления научных исследований «Культура и технологии» // Культура и технологии. 2016. Т. 1. Вып. 1. С. 1–14.

Можно выделить несколько основных направлений разработки, внедрения и использования технологий информационного общества в современном пространстве культуры:

Сохранение культурного наследия и техническое обеспечение преемственности в сфере культуры. Человеческое общество за время своего существования создало и аккумулировало через институты культуры огромное число культурных ценностей, представленных в различной форме: архитектурные сооружения, произведения искусства, памятники письменности и пр. Время, деятельность человека, войны и другие факторы пагубно влияют на эти объекты, приводя к их постепенному разрушению. Современные технологии позволяют создавать цифровые копии различных объектов культурного наследия (от текстов до трехмерных моделей скульптур и зданий), тем самым способствуя его сохранению. Тем более эта возможность важна для динамических форм культуры (исполнительские искусства, традиционные формы быта, народные промыслы, праздники, обряды, перформансы и т. п.), которые существуют только в процессуальной форме и даже с помощью современных технологий могут быть задокументированы лишь отчасти. Важно при этом, что цифровые средства записи позволяют не только хранить, но и неограниченное количество раз воспроизводить мультимедийную и текстовую информацию без искажений, не связанных с погрешностями самой записи. Это позволяет упростить доступ к культурному наследию, приблизить его к широкому кругу потенциальных реципиентов и акторов. Изначально записи такого рода распространялись преимущественно на цифровых носителях разного рода (например, на оптических дисках), однако в последнее время все большее распространение получают различные формы виртуального присутствия, в том числе в режиме реального времени, посредством систем широкополосного доступа в интернет (виртуальные экскурсии по музеям, виртуальные коллекции высокого качества обработки, виртуальные библиотеки и др.). Так, в мае 1996 г. по инициативе трех крупнейших московских музеев — Московского Кремля, Пушкинского и Третьяковской галереи — была учреждена Ассоциация по документации и новым информационным технологиям в му-

зеях (АДИТ). Членами АДИТ являются сотрудники учреждений культуры и образования, отвечающие за информационные технологии, и представители компаний-поставщиков оборудования и программного обеспечения. Ежегодные конференции АДИТ, проводимые с 1997 г., содействуют продвижению информационных технологий среди музеев и других учреждений культуры и призваны способствовать развитию музеев и обмену региональным опытом. С 1998 г. конференции АДИТ проводятся в различных регионах страны[63]. В цифровую форму систематически переводятся фонды российских библиотек[64] и музеев разного направления, крупнейшие музеи предоставляют через Интернет возможность виртуального посещения[65]. С другой стороны, на фоне работы мировых культурных центров (например, вошедших в международную инициативы OpenGLAM[66] или Flickr Commons[67]), гигапиксельных коллекций парижских музеев (включая Лувр)[68] или музея Метрополитен и международных проектов виртуального свободного доступа (прежде всего Google Art&Culture[69]) дости-

---

[63] *Борисов Н. В., Прокудин Д. Е.* Информационное пространство…

[64] См.: Проект Национальная электронная библиотека. URL: нэб.рф (дата обращения: 11.08.2018), заявленный как определяюще значимый в Стратегии развития информационного общества (гл. III, раздел «Формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений». URL: http://www.consultant.ru/document/cons_doc_LAW_216363/79898f482ff9dd0f019a0d2149434fa7a8c09e35 ; см. также: Электронные библиотеки открытого доступа: Русскоязычные электронные библиотеки. URL: http://www.shpl.ru/readers/helpful_links/free_ebooks/ (дата обращения: 11.08.2018).

[65] См., напр., виртуальную экскурсию по Государственному Эрмитажу. URL: https://www.hermitagemuseum.org/wps/portal/hermitage/panorama?lng=ru (дата обращения: 11.08.2018) ; «Виртуальный филиал» Государственного Русского музея. URL: http://rusmuseumvrm.ru/ (дата обращения: 11.08.2018) и др.

[66] См. URL: https://openglam.org/ (дата обращения: 11.08.2018).

[67] См. URL: https://www.flickr.com/commons/institutions/ (дата обращения: 11.08.2018).

[68] См. URL: http://parismuseescollections.paris.fr/fr (дата обращения: 11.08.2018).

[69] См. URL: https://artsandculture.google.com/ (дата обращения: 11.08.2018).

жения России выглядят достаточно скромно. Ряд современных музейных трендов[70], таких как геймификация, интерактивность или дополненная реальность, только начинают осваиваться музейным сообществом[71]. Ряд социокультурно значимых федеральных проектов (например, Единая коллекция цифровых образовательных ресурсов, предполагавшая, в частности, онлайн-публикацию объектов культурного наследия из коллекций российских музеев и художественных галерей)[72] вообще заглох в начальной стадии.

Изучение культурного наследия средствами академической науки. С 2001 г. в Санкт-Петербургском государственном университете (СПбГУ) реализуется образовательная программа «Прикладная информатика в области искусств и гуманитарных наук». В 2003 г. в СПбГУ была создана кафедра информационных систем в искусстве и гуманитарных науках. На ее базе были реализованы многочисленные научные проекты в области использования мультимедиа технологий для информационного обеспечения гуманитарных научных исследований и сохранения культурного наследия при поддержке Российского гуманитарного научного фонда (РГНФ), Российского фонда фундаментальных исследований (РФФИ) и СПбГУ. В 2001 г. в Московском государственном университете была создана Лаборатория исторической информатики, преобразованная в 2004 г. в кафедру исторической информатики исторического факультета МГУ. На базе кафедры изучаются проблемы использования информационных технологий в исторических исследованиях, создаются виртуальные реконструкции памятников культуры. В Сибирском федеральном университете в 2010 г. была создана кафедра информационных технологий в креативных и культурных индустриях. В 2016 г. было принято решение о создании в вузе Лаборатории прикладной информатики и современных цифровых технологий в гуманитарных

---

[70] См.: *Рено А.* Музеи и цифровые технологии: как развивается визуальное пространство. URL: https://te-st.ru/2017/10/31/museums-and-digital-technologies/ (дата обращения: 11.08.2018).

[71] См., напр.: *Рыцарева Е.* Русский музей попал в цифровую пучину. URL: http://expert.ru/2011/12/20/russkij-muzej-popal-v-tsifrovuyu-puchinu/ (дата обращения: 11.08.2018).

[72] См. URL: http://school-collection.edu.ru/ (дата обращения: 11.08.2018).

науках. В 2007 г. участниками научного семинара «Визуальные практики» под руководством профессора В. Савчука был сформирован исследовательский Центр медиафилософии[73], ориентированный на исследование феномена медиа, медиареальности, медиакультуры. В 2012 г. при центре была сформирована Лаборатория исследований компьютерных игр (ЛИКИ), занимающаяся анализом компьютерных игр, определением их сущности, медиальной природы, специфических характеристик, особенностей функционирования, влияния на формирование восприятия, телесности, субъективности и изучением их роли в конституировании социальной реальности[74] и т. д. Дать принципиальную общую оценку объему и качеству проводимой работы проблематично в силу отсутствия критериев эффективности, однако можно отметить, что ни один из российских проектов в данной сфере не может быть назван безоговорочно лидирующим в мировом академическом сообществе[75].

Освоение современных технологий создания культурных объектов, событий и процессов, новых социокультурных практик. В сфере социальной политики — ***техническая, финансовая и организационная поддержка*** творческой деятельности населения России, межкультурного взаимодействия, поддержание интереса к современной российской культуре на национальном и международном уровне. Стратегия развития информационного общества оговаривает данные пункты в самом общем виде (за исключением пункта о поддержке Национальной электронной библиотеки, см. выше). Достаточность/недостаточность и эффективность/неэффективность действий государственных органов и частной инициативы в данной сфере в последние годы настолько неоднозначна и дискуссионна, что требует отдельного исследования для минимально объективной оценки. По субъективному мнению авторов, в момент подготовки данной работы Россия в целом не производит впечатления лидера мировой информационной культуры — ни в сфере производства духовных ценностей, ни в сфере создания качественного медиакон-

---

[73] См. URL: http://mediaphilosophy.ru/ (дата обращения: 11.08.2018).

[74] Цит. по: *Борисов Н. В., Прокудин Д. Е.* Информационное пространство…

[75] По: *Борисов, Н.В., Прокудин, Д. Е.* Указ. соч.

тента, ни в области элитарного искусства, хотя о безоговорочном отставании от мировой культуры также говорить нельзя: сознательно выбрав роль активного игрока в процессе генерации цифровой культуры, мы с неизбежностью оказались в пространстве неопределенности и непредсказуемости результатов. Однако доступная статистика по смежным областям — например, приведенные выше данные по образованию и освоению информационных технологий или приведенные в гл. 3 данные о технической вооруженности российской науки и экономики) и наличие негативной динамики по этим показателям заставляет и в области культуры оценивать глобальные перспективы РФ скептически.

§ 4. Инфосфера и вопросы права и правоприменения

С возрастающей ролью информации в современном обществе связано возникновение (начало 80-х гг. XX в.) информационного права как самостоятельной отрасли юриспруденции. Окинавская Хартия глобального информационного общества (г. Окинава, Япония, 22.07.2000) уделяет большое значение организационно-правовому обеспечению (ОПО) внедрения и использования информационно-компьютерных технологий (ИКТ) (только качественное релевантное ОПО может обеспечить эффективность внедрения и использования ИКТ). С другой стороны, ИКТ, реализованные на базе средств телекоммуникаций и компьютерной техники, сами представляют собой базовые элементы информационно-технического обеспечения (ИТО) любой профессиональной деятельности, включая правовую (только качественное релевантное ИТО может обеспечить повышение рациональности организации и эффективности профессиональной деятельности). Потребность в нем была обусловлена прежде всего широким распространением ИКТ и внедрением глобальных телекоммуникационных сетей, создающих принципиально новые возможности и стимулы для развития экономики и изменения общественных отношений, включая появление большого разнообразия новых форм межсубъектного взаимодействия в инфосфере (в том числе между субъектами разного

уровня организации — например, личность/личность, личность/государство, личность/общественное движение или организация и т. п.), что, в свою очередь, приводит к необходимости создания адекватной нормативной правовой базы.

Новая отрасль правовых отношений естественным образом формирует новый круг юридических проблем, таких как правоотношения и правоприменение в сфере компьютерной информации и электронного документооборота (проблема «легитимизации» электронного документооборота, доменные споры, правовой режим функционирования интернет-сайтов и др.). Одновременно обновляются традиционные правовые коллизии, например конфликт между интересами личности и общества (прежде всего, право на доступ/ограничение доступа граждан к информации), проблема достоверности и сохранности привилегированной информации (например, персональных данных); вопросы правового обеспечения работы в Интернете традиционных и интернет-СМИ, легитимное обеспечение информационной безопасности личности, общества и государства.

При построении систем, регулирующих функционирование инфосферы, учитывается ряд прагматических юридически значимых свойств информации, включая общие (внутренние и внешние) и специальные (правовые) свойства. К общим внутренним (присущим собственно информации) юридически значимым свойствам содержательной информации в настоящее время относятся следующие основные: *пертинентность* (полнота, релевантность), *неисчерпаемость, кумулятивность* (избирательность, гомоморфизм), в совокупности составляющие внутреннее качество содержательной информации или ее актуальность.

Под актуальностью (actuality; от позднелат. *actualis* — деятельный) содержательной информации понимается комплексное свойство, характеризующее степень ее значимости (ценности) для активного потребителя во времени, то есть с учетом «морального старения» этой информации.

Пертинентность (pertinence; от англ. *pertinent* — относящийся к делу, подходящий) информации — свойство, характеризующее степень соответствия совокупности новых сведений, содержащихся в информационных массивах (массивах данных, массивах программ,

сообщениях, фактах), воспринимаемых получателем (информационным деятелем, эргасистемой, функциональной подсистемой и др.), информационным потребностям получателя: в знаниях о конкретном материальном объекте (системе) или процессе (семантический аспект) и использовании их для выработки (с учетом индивидуального или общесистемного тезауруса — накопленных знаний, целей и задач) и принятия управляющего решения-предписания (прагматический аспект).

Полнота (wholeness) *информации* — свойство содержательной информации обеспечивать требуемую осведомленность получателя или принятие им рациональных (оптимальных) управленческих решений-предписаний (при управлении объектом, регулировании отношений и др.).

Релевантность (relevance, от англ. *relevant* — существенный, уместный) информации — свойство содержательной информации соответствовать динамическому состоянию объекта (проблемы, деятельности).

Неисчерпаемость (inexhaustibility) информации — свойство содержательной (в отличие от структурной) информации не подвергаться физическому старению и не изменяться при передаче ее неограниченному числу пользователей.

Кумулятивность (cumulativeness; от лат. *cumulatus* — полный) информации — свойство содержательной информации, заключенной в информационном массиве небольшого объема, достаточно полно отображать действительность.

Избирательность (selectiveness) информации — свойство содержательной информации достаточно полно отображать действительность, представленную информационными массивами большого объема с помощью малого числа информационных единиц (символов) на основе учета квалификации, опыта и др. субъективных качеств личности конкретного лица (информационным деятеля), принимающего решения. Социально-психологическая составляющая кумулятивности информации.

Гомоморфизм (homomorphism; от др.-греч. ὁμός — равный, одинаковый и μορφή — вид, форма) информации — свойство содержательной информации достаточно полно отображать дейст-

вительность, представленную информационными массивами большого объема, с помощью малого числа информационных единиц (символов) на основе соответствующих моделей агрегирования (типа «многое в одном»). Формально-техническая составляющая кумулятивности.

Наличие свойств неисчерпаемости и осмысленности обусловливает возможность неограниченного разнообразного тиражирования содержательной информации (в результате осуществляется постепенное наращивание знаний и передача их от поколения к поколению, что создает предпосылку прогрессу человечества). При этом побочным эффектом является возможность произвольного распространения сведений, одновременного нахождения их в полном объеме в нескольких местах и одновременного использования любым количеством субъектов (в том числе и соперничающими или конфликтующими сторонами). Свойства неисчерпаемости и ценности информации предопределяют конструирование в праве механизмов ограничения доступа и распространения информации, именуемых институтами тайн. С ними также связана проблема установления авторства.

Свойство избирательности содержательной информации, связанное с различными способностью и подготовленностью субъектов воспринимать одну и ту же информацию в зависимости от различных обстоятельств (социокультурного уровня, физического и психического состояния субъекта и др.), определяет необходимость формулирования в законодательстве института документированной информации — зафиксированной путем документирования на материальном носителе информации с реквизитами, позволяющими определить такую информацию или (в установленных законодательством России случаях) ее материальный носитель. В частности, в федеральном Законе об информации[76] (ст. 11, 11.1) содержатся основные положения, касающиеся документирования.

---

[76] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 11.08.2018).

К основным общим внешним (присущим информации в определенной эргасистеме) юридически значимым свойствам содержательной информации в настоящее время относятся достоверность, конфиденциальность, сохранность, которые, являясь конструктивными (сложными), обусловлены, соответственно, свойствами помехоустойчивости и помехозащищенности, доступности, скрытности и имитостойкости; целостности и готовности информации, в совокупности составляющие внешнее качество содержательной информации или ее защищенность[77].

Под *защищенностью* (security) содержательной информации понимается свойство эргасистемы (точнее ее функциональной подсистемы контроля и защиты содержательной информации), характеризующее степень защищенности *информационных массивов* (*ИМ*) и заключающееся в способности не допускать случайного или целенаправленного искажения или разрушения, раскрытия или модификации ИМ в информационной базе эргасистемы.

Достоверность (trustworthiness, tolerance) информации — свойство эргасистемы, характеризующее степень соответствия (в пределах заданной точности) реальных информационных единиц (символов, знаков, записей, сообщений, документов и др.) их истинному значению и заключающееся в способности обеспечить отсутствие ошибок переработки информации, то есть не допустить снижения ценности информации при принятии управляющих решений-предписаний, искажений ИМ, их смыслового значения, замены единичных символов ИМ и др. из-за несовершенства организации (структуры) технологических процессов переработки информации, несовершенства алгоритмов, ненадежной работы и неисправностей комплекса технических средств, сбоев *комплекса средств автоматизации* (*КСА*), ошибок людей-операторов, недостатков в комплексе программных средств и др.

Помехоустойчивость (hindrance-stability) информации — свойство эргасистемы, характеризующее степень устойчивости реальных

---

[77] Характеристики юридически значимых свойств содержательной информации здесь и далее по: *Ловцов Д. А.* Системология правового регулирования информационных отношений в инфосфере : монография. М., 2016. 316 с.

ИМ к действию незначительных помех и заключающееся в способности обеспечить отсутствие трансформации символов (синтаксическая помехоустойчивость на основе контроля преобразований ИМ, рациональных методов телеграфии при использовании простых сигналов-переносчиков и посимвольном приеме ИМ и др.) и искажения смыслового значения перерабатываемых ИМ (семантическая помехоустойчивость на основе логического контроля преобразований, избыточного кодирования ИМ и др.).

Помехозащищенность (hindrance-defense) информации — свойство эргасистемы, характеризующее степень живучести ИМ и заключающееся в способности обеспечить наличие хотя бы минимального установленного объема ИМ для решения целевых и функциональных задач эргасистемы в условиях внешних разрушающих (подавляющих) возмущающих воздействий.

Конфиденциальность (confidence; от лат. confidential — доверие) информации — статус, предоставленный информационным массивам и согласованный между организацией или лицом, предоставляющими ИМ, и организациями, получающими их, то есть это понятие употребляется по отношению к информации. При этом под секретностью (от лат. *secretus* — отделенный) информации понимается право организаций и отдельных лиц решать, какие ИМ они желают разделить с другими, а какие — скрыть от других, то есть это понятие употребляется по отношению к организациям или отдельным лицам.

Доступность (accessibility) информации — свойство эргасистемы, характеризующее степень разграничения действий объектов эргасистемы (людей-операторов, задач, устройств, программ, КСА, подсистем и др.) и заключающееся в возможности использования ИМ по требованию оператора и объектов эргасистемы, имеющих соответствующие полномочия (мандаты).

Скрытность (reticence) информации — свойство эргасистемы, характеризующее степень маскировки информации и заключающееся в способности противостоять раскрытию смысла ИМ (семантическая скрытность на основе обратимых преобразований информации), определению структуры хранимого ИМ или носителя (сигнала-переносчика) передаваемого ИМ (структурная скрытность

на основе плохообратимых преобразований, использования спецаппаратуры, различных форм сигналов-переносчиков, видов модуляции и др.) и установлению факта передачи ИМ по каналам связи (энергетическая скрытность на основе применения специальных (широкополосных и др.) сигналов-переносчиков ИМ, организации периодического маскирующего обмена ИМ в распределительной информационной сети эргасистемы и др.).

Имитостойкость (steadfastness to imitation) информации — свойство эргасистемы, характеризующее степень защищенности информации от инфильтрации (внедрения) ИМ, имитирующих авторизованные (зарегистрированные) ИМ, и заключающееся в способности не допустить навязывания дезинформации и нарушения нормального функционирования эргасистемы.

Сохранность (safety) информации — свойство эргасистемы, характеризующее степень готовности определенных ИМ к целевому применению и заключающееся в способности обеспечивать постоянное наличие и своевременное предоставление ИМ, необходимых для автоматизированного решения целевых и функциональных задач эргасистемы, в процессе эксплуатации информационной базы (хранения, транспортировки и непосредственного использования ИМ), то есть не допускать разрушения ИМ из-за несовершенства носителей, механических повреждений, неправильной эксплуатации, износа и старения комплекса технических средств, ошибок персонала и несанкционированных корректировок, ошибок в комплексе программных средств и др.

Целостность (integrity) — свойство эргасистемы, характеризующее степень физической равнозначности ИМ во внутримашинной (электронной) информационной базе эргасистемы и в исходных документах (сообщениях) и заключающееся в способности обеспечить, насколько это возможно, физическое наличие информационных единиц в информационной базе в любой момент времени, то есть не допустить случайных искажений и разрушения ИМ из-за дефектов и случайных сбоев комплекса технических средств, действия компьютерных «вирусов», ошибок человека-оператора (при вводе информации в информационную базу или обращении к ней),

ошибок в комплексе программных средств (операционных системах, СУБД, комплексах прикладных программ) и др.

Готовность (readiness) информации — свойство эргасистемы, характеризующее степень работоспособности ИМ при выполнении целевых и функциональных задач эргасистемы и заключающееся в способности обеспечить своевременное предоставление необходимых неразрушенных ИМ.

Для содержательной информации в информационном праве разработан особый правовой режим в электронных документах. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» определяет правовые условия использования различных ее видов (простая, усиленная, квалифицированная) в электронных документах, при соблюдении которых ЭП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе[78]. При этом организационно-правовые механизмы удостоверения, квитирования, архивирования и др., использующие соответствующие виды ЭП, должны обеспечить специальные (правовые) свойства информации:

— легитимность (юридическую значимость) циркулирующих в информационной сети электронных документов (ИМ), включающую их аутентичность (содержательная составляющая);

— легальность (формальная составляющая);

— верифицируемость (процедурная составляющая).

Легитимность (legitimacy от лат. *legitimus* — законный, правомерный) информации — специальное (правовое) свойство эргасистемы (подсистемы контроля и защиты информации), характеризующее степень законности (правовой или юридической значимости) ИМ, циркулирующих в *информационно-распределительной сети* (*ИРС*) эргасистемы, и заключающееся в возможности легального (правомочного) использования циркулирующих ИМ абонентами-получателями, имеющими соответствующие полномочия (мандаты).

---

[78] См.: Федеральный закон «Об электронной подписи» № 63-ФЗ от 06.04.2011 (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 11.08.2018).

Аутентичность (authenticity; от др.-греч. αυθεντικό — подлинный) информации — специальное (правовое) свойство эргасистемы, характеризующее степень подлинности ИМ, циркулирующих в ИРС эргасистемы, и заключающееся в способности обеспечить семантическую равнозначность содержания циркулирующих ИМ и исходных массивов-оригиналов, хранимых абонентами-источниками в документальном виде.

Легальность (legality; от лат. *legalis* — правовой, признанный) информации — специальное (правовое) свойство эргасистемы, характеризующее степень соответствия конфигурации (формы) ИМ, циркулирующих в ИРС эргасистемы, регламентированным требованиям (правилам формирования) и заключающееся в способности обеспечить установление абонентами-получателями авторства ИМ, полномочий и других необходимых атрибутов (идентификаторов, реквизитов и др.) абонентов-источников.

Верифицируемость (verifiable; от лат. *verificatio* — сравнение сведений из разных источников) — специальное (правовое) свойство эргасистемы, характеризующее степень осуществимости проверки истинности (легальности и аутентичности-подлинности) ИМ, циркулировавших в ИРС эргасистемы, через неопределенное время и заключающееся в способности обеспечить подтверждение истинности ИМ путем сопоставления массивов из различных архивных источников.

Можно выделить (по критерию доступности к содержательной информации) следующие четыре юридически значимые группы правовых режимов информации:

1) *неограниченного доступа*: литература (нормативная, учебная, научная, справочная, общественно-политическая, а также публицистика и др.), произведения искусства (имеющие информационный, то есть художественно-познавательный, характер), сообщения и материалы массмедиа, таблоиды, реклама, судебные решения и др.;

2) *ограниченного доступа*: тайны, секреты производства (включая ноу-хау), секреты промысла, торговые секреты и др.;

3) *обязательного предоставления* (в соответствии с федеральными законами или с заключенными соглашениями) для доступа:

декларации (налоговые и др.), объявления (о банкротстве, об экологической обстановке и др.), авизо, обвинительные заключения и др.;

4) *запрещенного ограничения доступа*: отчеты (кредитные, финансово-хозяйственные, бухгалтерские; о деятельности государственных органов и органов местного самоуправления и др.), комплекты документов (учредительных, платежно-расчетных и др.), свидетельства (о праве, включая патенты), кадастры (лесной и др.) и др.

Урегулированные нормами права информационные отношения, то есть общественные отношения, возникающие по поводу информации либо юридически значимых результатов действий (бездействия) в отношении этой информации (передача, получение, преобразование, предоставление, неразглашение и др.), принято называть *информационными правоотношениями*.[79]

В связи с тем, что все устанавливаемые в процессе активного взаимодействия информационных деятелей информационные связи и отношения в зависимости от их назначения делятся на целевые (являющиеся средством достижения конкретных целей и одновременно результатом определенной информационной деятельности) и обеспечивающие (являющиеся только средством достижения конкретных целей), соответствующие информационные правоотношения также можно разделить на два больших класса:

1) *целевые* (предметные, отраслевые) — информационные правоотношения в инфосфере;

2) *обеспечивающие* — информационные правоотношения в иных (экономической, политической, социальной, то есть в сфере социального обеспечения и страхования, образования и культуры, охраны здоровья и т. п.; экологической, брачно-семейной, трудовой, нравственной и др.) сферах.

Информационные правоотношения, как и все общественные правоотношения, могут быть:

---

[79] Классификация по: *Ловцов Д. А.* Информационные правоотношения: особенности и продуктивная классификация // Информ. право. 2009. № 3 (14). URL: http://www.center-bereg.ru/h1249.html (дата обращения: 11.08.2018) ; см. также: *Куликова С. А.* Информационное право России : учеб. пособие. Саратов, 2010. С. 22.

— *односторонними и двусторонними* (включая «условно многосторонние») — по числу участников правоотношений;

— *абсолютными и относительными* — по степени индивидуализации сторон;

— *простыми и сложными* — по структуре и количеству взаимосвязей прав и обязанностей сторон (при этом отдельные юридические связи могут иметь не информационную природу);

— *регулятивными* (включая общерегулятивные) и охранительными — по функциональному назначению;

— *активными и пассивными* — по характеру обязанности сторон;

— *материальными и процессуальными* — по характеру правового регулирования.

Они также возникают при наступлении предусмотренных законом юридических фактов (договоры, правонарушения, события, административного акта и др.).

Кроме того, информационные правоотношения в инфосфере (целевые) в зависимости от информационной «насыщенности» их фактического содержания и «чистоты» информационной природы объекта — компонента деятельности (объема информационных действий), то есть от роли и «величины» информационной составляющей, условно можно разделить на следующие три основные группы[80].

1. «*Чисто*» *информационные правоотношения* — то есть с преобладанием информационной природы у объекта (уже сегодня образованные и поддерживаемые относительно самостоятельными комплексами норм права, которые можно рассматривать как подотрасли информационного права) в области:

— средств обеспечения информационной безопасности личности, общества и государства и соответствующей привилегированной содержательной информации, необходимой для удовлетворения информационных потребностей жизнедеятельности (функционирования), развития и обучения — подотрасль «Право информационной безопасности» (включая институт информационных прав и свобод, институт тайны, институты охраны права на частную и публичную информационную деятельность и др.);

---

[80] См.: *Ловцов Д. А.* Информационное право : учеб. пособие. М., 2011. 228 с.

— средств массовой информации и соответствующей «массовой» информации — подотрасль «Медиаправо», или «Право средств массовой информации» (включая институт свободы массовой информации, институт прав телерадиовещателей и др.);

— средств автоматизации (включая автоматизированные информационные системы — АИС, автоматизированные системы управления — АСУ, государственные автоматизированные системы — ГАС), электронно-вычислительной техники и соответствующей машинной («компьютерной») информации — подотрасль «Компьютерное право» (включая институты электронного документооборота, электронной подписи, программно-математического обеспечения и др.);

— средств коммуникаций и соответствующей многоаспектной электронно-цифровой информации — подотрасль «Телематическое право» или «Интернет-право», «Сетевое право» (включая институты телекоммуникаций и связи, институт доменных имен и др.).

2. «*Смешанные*» *информационные правоотношения* (информационно-имущественные, информационно-неимущественные, информационно-хозяйственные, информационно-производственные и др.) в области компьютерной преступности, интеллектуальной собственности (включая промышленную собственность) и собственности на информационные ресурсы, правовой информатизации и др.

3. «*Частично*» *информационные правоотношения*: в области употребления (использования) информационных ресурсов (в частности, в области культуры, библиотечного дела, архивов и др.).

«Исходя из этого, предметом интегрированной (частично самостоятельной и частично комплексной) отрасли права — информационного права логично определить способы и нормы правового регулирования информационных отношений в инфосфере, выделив по значимости и с учетом предметов других отраслей права следующие классы соответствующих целевых информационных:

— *основные* (предметные, отраслевые) — «чисто» информационные правоотношения (регулируются нормами информационного права);

— *дополнительные* (смешанные, многоотраслевые) — «смешанные» информационные правоотношения (регулируются комплексом норм информационного и других отраслей права);

— *факультативные* (смежные, практически других отраслей) — «частично» информационные правоотношения (регулируются нормами других отраслей права, которые могут входить в информационное право только в части, касающейся непосредственно информационно-правового режима).

При этом самостоятельную часть интегрированной отрасли информационного права составляют способы и нормы правового регулирования основных (предметных, отраслевых) — «чисто» информационных отношений в инфосфере, а комплексную — смешанных и смежных.

Таким образом, объективно сложившаяся на современном этапе система информационного права как целостное развивающееся сложное образование, включающее в качестве основных многоаспектно взаимосвязанные компоненты (подотрасли), такие как право информационной безопасности, медиаправо, компьютерное право и телематическое право, ориентирована на правовое регулирование информационных отношений в информационной сфере общественно-производственной деятельности»[81].

При этом информационное право в системе права:

— базируется на ряде конституционных положений (в частности, закрепляющих информационные права и свободы личности, регламентирующих производство таких информационных объектов, как федеральные конституционные и федеральные законы и др.);

— использует методы административного права (например, при регулировании отношений, возникающих при осуществлении органами государственной власти и местного самоуправления обязанностей в области СМИ, по формированию информационных ресурсов и выдаче информации из них широкому кругу информационных деятелей и др.);

— «предоставляет» свои методы и средства отраслям: гражданского права (например, при регулировании имущественных отношений и личных неимущественных отношений в инфосфере по поводу информационных объектов), уголовного права (при регулировании

[81] *Ловцов Д. А.* Системология правового регулирования информационных отношений в инфосфере : монография. М., 2016. С. 53–54.

отношений в области информационно-компьютерной преступности), финансового права (при регулировании финансовых, кредитных, эмиссионных, аудиторских отношений в части контроля и управления), трудового права (при регулировании отношений в области персональных данных работников), земельного права (при регулировании отношений в области публичного информирования) и др.

Необходимым условием обеспечения эффективности правового регулирования информационных отношений в инфосфере на основе продуктивных классификаций и рациональных моделей является учет специфики видов информационных отношений. В связи с этим предполагается наличие у специалистов по информационному праву (законодателей и правоприменителей) определенных концептуальных знаний из смежных научных отраслей, таких как *информология и криптология* (подотрасль право информационной безопасности), *журналистика* (медиаправо), *информатика* (компьютерное право), *телекоммуникации* («Телематическое право»).

Непосредственно правовое регулирование информационных отношений осуществляется путем практической реализации правовых предписаний (норм права), предварительно подвергшихся осмыслению субъектами правоприменения. Это обусловливает необходимость целенаправленного формирования их правосознания. При этом ответственность за информационные правонарушения (преступления, деликты, проступки, ущербы) может быть уголовной (юридический порядок определен УК РФ), гражданско-правовой (ГК РФ), административной (КоАП РФ), финансовой (БК РФ), дисциплинарной и материальной (ТК РФ).

Современный этап новейшей истории развития международно-правовых основ глобального информационного обмена берет начало с 24 октября 1945 г. — даты вступления в силу Устава Организации Объединенных Наций. В статьях 54, 65 и 73 Устава ООН предусматривается добровольное исполнение членами ООН принятых на себя обязательств по информированию Совета Безопасности и Генерального секретаря о деятельности по поддержанию международного мира и безопасности, по предоставлению статистической и другой специальной информации об экономических, социальных и образовательных условиях на территориях, за которые они несут

ответственность. Данные положения Устава ООН инициировали разработку и принятие всеми странами — членами ООН соответствующих национальных нормативных правовых актов.

После распада СССР и создания Содружества Независимых Государств (СНГ) одной из первых возникла проблема межгосударственного информационного обмена. В этой связи в 90-е гг. XX в. в Российской Федерации был принят ряд основополагающих нормативных актов в области международно-правовой информатизации. Среди них Указы Президента РФ: от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации», от 20 января 1994 г. № 170 «Вопросы формирования единого информационно-правового пространства Содружества Государств», от 29 марта 1994 г. № 603 «О взаимодействии федеральных органов власти Российской Федерации в области информационно-правового сотрудничества с органами власти государств — участников СНГ».

С принятием данных нормативных правовых актов, а также благодаря тому, что Россия продолжает согласно Федеральному закону от 15 июля 1995 г. № 101-ФЗ «О международных договорах Российской Федерации» выполнять обязательства, вытекающие из договоров, заключенных СССР, в качестве государства — преемника СССР, наше государство стало участником процесса международного сотрудничества в информационной сфере, создания глобального информационного общества, формирования единого глобального информационного пространства.

В настоящее время переход к информационному обществу осознан как насущная и приоритетная задача развития практически в любом экономически и политически состоятельном государстве. При этом основой для координации усилий мирового сообщества по созданию единой информационно-производственной среды деятельности человечества стала Окинавская хартия глобального информационного общества (2000).

Говоря о правовых основах участия Российской Федерации в международном информационном обмене, необходимо отметить, что для России особое значение имеют вопросы ее эффективного участия в международном информационном обмене в рамках единого мирового информационного пространства. Согласно дейст-

вующей Конституции РФ, «Общепризнанные принципы и нормы международного права, международные договоры Российской Федерации являются составной частью ее правовой системы» (ч. 4 ст. 15).

Проблемы, связанные с созданием условий, способствующих обеспечению граждан, юридических лиц, публичных образований иностранными информационными продуктами и услугами, были решены с принятием Федерального закона от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» (ныне утратил силу), базировавшимся на общепризнанных принципах и нормах международного права в информационной сфере, в том числе предусмотренных Уставом ООН. Согласно этому закону, «международный информационный обмен — это передача и получение информационных продуктов, а также оказание информационных услуг через Государственную границу Российской Федерации» (ст. 2)[82].

В целях обеспечения информационной безопасности России при осуществлении международного информационного обмена посредством информационных систем, сетей и сетей связи, включая международную ассоциацию ГТС «Интернет», Президентом РФ были подписаны: Указ от 12 мая 2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (утратил силу) и Указ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». Составной частью международного информационного обмена выступает межгосударственный обмен информацией, который служит созданию отдельных секторов информационного пространства. Межгосударственный обмен информацией осуществляется главным образом в рамках двух- или многосторонних соглашений Российской Федерации со многими государствами, в том числе странами СНГ и характеризуется тематической направленностью информации, подлежащей обмену.

---

[82] См.: Федеральный закон от 04.07.1996 г. № 85-ФЗ «Об участии в международном информационном обмене». URL: http://kremlin.ru/acts/bank/9688 (дата обращения: 11.08.2018).

Международно-правовые основы сотрудничества в информационной сфере. Российская Федерация принимает активное участие в процессе международного информационного обмена. Это реализуется, в частности, в заключении и ратификации комплекса международных соглашений, регулирующих отношения в области информационных технологий. «При этом можно выделить следующие четыре основные совокупности международных правовых актов (договоров, соглашений), определяющих основные направления международного сотрудничества в инфосфере:

1) соглашения, регулирующие общие вопросы в области информации: Конвенция о сотрудничестве в области культуры, образования, науки и информации в Черноморском регионе (Стамбул, 6 марта 1993 г.) (действует на территории РФ в соответствии с Федеральным законом от 25 ноября 1996 г. № 134-ФЗ «О ратификации Конвенции о сотрудничестве в области культуры, образования, науки и информации в Черноморском регионе»); Европейская конвенция об информации относительно иностранного законодательства (ETS № 062) (Лондон, 7 июня 1968 г.); Соглашение об информационном обеспечении выполнения многосторонних соглашений (Москва, 24 сентября 1993 г.) и др.;

2) соглашения о сотрудничестве в области правовой информации и обмена официальными изданиями: Конвенция о международном обмене изданиями (Париж, 5 декабря 1958 г.) (данная Конвенция ратифицирована Указом Президиума Верховного Совета СССР от 11 сентября 1962 г. № 461-VI); Конвенция об обмене официальными изданиями и правительственными документами между государствами (Париж, 5 декабря 1958 г.) (ратифицирована вышеупомянутым Указом Президиума Верховного Совета СССР); Соглашение между Правительством РФ и Правительством Республики Узбекистан об обмене правовой информацией (Москва, 6 мая 1998 г.) и др.;

3) соглашения о сотрудничестве в области защиты информации, содержащей сведения, составляющие государственную тайну или секретные материалы: Соглашение между Правительством РФ и Правительством ФРГ о взаимном обеспечении сохранности секретных материалов (Москва, 2 декабря 1999 г.); Соглашение

между Правительством РФ и Правительством Республики Беларусь о сотрудничестве в области защиты информации (Москва, 9 июля 1997 г.) и др.

4) соглашения, содержащие положения о создании совместных информационных систем и единых информационных банков, а также об обмене оперативной, статистической, научно-методической и иной информацией: Соглашение об общем аграрном рынке государств — участников СНГ (Москва, 6 марта 1998 г.); Соглашение о формировании единого экономического пространства (Ялта, 19 сентября 2003 г.); Соглашение между Правительством РФ и Правительством Соединенного Королевства Великобритании и Северной Ирландии о сотрудничестве в области борьбы с пре-ступностью (Москва, 6 октября 1997 г.); Соглашение по торговым аспектам прав интеллектуальной собственности (Марракеш, 15 апреля 1994 г.) и многие другие»[83].

Содержание международных соглашений по взаимодействию в инфосфере указывает на то, что в настоящее время взаимодействие такого рода между субъектами мировой политики связано не только с прямым обменом информацией, но затрагивает также и вопросы применения этой информации в различных областях — таких как наука, техника, образование, СМИ, элитарная и массовая культура, авторское и таможенное право, вопросы международной торговли, взаимодействие в военной сфере.

Россия и страны ЕС фактически стоят перед необходимостью активного участия в совместной разработке и принятии международных соглашений, направленных на достижение следующих целей:

1. Создание условий для равноправного и безопасного информационного обмена на основе общепризнанных норм и принципов международного права, устанавливающих, в частности, ответственность за информационно-компьютерные преступления, злоумышленное проникновение в национальные и корпоративные информационные системы и сети, электронное хулиганство, ха-

[83] *Ловцов Д. А.* Системология правового регулирования информационных отношений… С. 85–86.

керство, нарушение прав и законных интересов граждан в процессе информационного обмена.

2. Разработка коллективных мер организационно-правового характера по предотвращению использования ГТС «Интернет» и ИКТ в террористических, диверсионных и других преступных целях, защиты информационных прав граждан и национальных интересов государств, а также разработку международно-правовой процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия.

3. Развитие системы международного взаимодействия и координации деятельности правоохранительных органов по предотвращению и пресечению правонарушений в мировом информационном пространстве.

4. Гармонизация национальных законодательств об электронном документообороте, электронной торговле, электронной (электронно-цифровой подписи) на базе единых принципов и подходов.

5. Укрепление сотрудничества в сфере информационно-правового образования и формирования информационно-правовой культуры граждан стран-партнеров, информационно-правовой подготовки высококвалифицированных информационных деятелей наступающего нового глобального информационного общества, способных активно противостоять растущей информационно-компьютерной преступности.

Глобальный характер процессов формирования информационного общества, количественное и качественное развитие коммуникационной инфосферы, в том числе трансграничной, появление все новых областей применения вычислительной техники с претензий на качественное преобразование всех форм социальной и производственной деятельности человечества в целом ведут к осознанию необходимости развития институтов глобального информационного обмена и системы международно признанных правовых норм, регулирующих современные международные и межгосударственные правоотношения, так или иначе затрагивающие информационную сферу.

Соответственно, развитие международного законодательства, обеспечивающего правовые основы глобального информационного обмена и гарантирующего защиту законных прав и интересов граж-

дан, организаций и государств в условиях глобальной инфосферы оказывается необходимым и последовательно реализуемым мировым сообществом элементом программы построения устойчивого и безопасного мира, зафиксированной, например, в Концепции устойчивого (жизнеспособного) развития (sustainable development) человечества, провозглашенной Конференцией ООН «Окружающая среда и развитие» (3–4 июня 1992 г., Рио-де-Жанейро) в программном документе «Повестка дня на XXI век», в «целях тысячелетия», принятых Саммитом ООН по глобальному развитию до 2030 г. (25–27 сентября 2015 г., Нью Йорк)[84], в Окинавской хартии глобального информационного общества и других аналогичных по установкам документах.

[84] См., напр.: *Перелет Р. А.* Переход к эре устойчивого развития? URL: http://www.rus-stat.ru/stat/6902003-1.pdf#page=4 (дата обращения: 11.08.2018) ; *Миннекаева Д. Р.* «Повестка дня на XXI век» — путь к устойчивому развитию. Теоретические основы перспективной программы Организации Объединенных Наций. URL: http://old.tisbi.org/science/vestnik/2003/issue4/U3.html (дата обращения: 11.08.2018) и др.

Глава 3
СТРАТЕГИЯ И ТАКТИКА КИБЕРГЕДДОНА

В популярном в 90-е гг. фантастическом сериале «Вавилон-5» один из персонажей, сознание которого по сюжету воссоздано после его смерти с помощью компьютерных технологий, объясняет своему создателю: «Я не существую. Я всего лишь массив данных в компьютере. Однако, с точки зрения компьютера, команды, которые отдаю я, ничем не отличаются от ваших — это такие же цепочки единиц и нолей».

В последние десятилетия инфосфера 2.0 становится пространством активного взаимодействия между людьми, группами и сообществами людей, предприятиями, государственными органами, государствами и группами государств — в дву- и многосторонних сочетаниях произвольной конфигурации. При этом фактически в информационном пространстве не может существовать иерархия субъектов взаимодействия, так что в этом смысле современная цивилизация уже близка к ситуации, описанной в сериале.

Интернет задумывался как среда хранения и обмена информацией. В 2000-е гг. он превращается в среду создания информации. Но и это только первый шаг, поскольку проникновение информационных технологий практически во все сферы современной жизни если и не стирает, то размывает грань между информационным

и материальным взаимодействием: концепции «умного дома» и «интернета вещей», первые шаги роботизированного автотранспорта и военные беспилотники различного назначения в данном случае — частные примеры, которые продолжают множиться ежедневно. Однако до тех пор, пока мы не можем говорить всерьез об искусственном интеллекте, инициаторами взаимодействия в конечном счете остаются люди. Соответственно, люди приносят в инфосферу все формы взаимодействия, свойственные им в материальном мире, включая правонарушения, преступления, агрессию, войну.

Формы подобного взаимодействия в инфосфере многочисленны и не всегда поддаются однозначной оценке с точки зрения, допустим, национального или международного права, равно как и с точки зрения здравого смысла. Тем не менее с некоторым приближением акты направленного агрессивного взаимодействия в информационном пространстве можно разделить на действия, направленные на причинение контрагентам прямого, материально выраженного ущерба (в этом случае мы будем говорить о киберпреступности и кибервойнах), и на действия, нацеленные на изменение сознания контрагентов выгодным для себя способом (в этом случае мы будем говорить о пропаганде, информационных преступлениях и, наконец, информационных войнах).

«Информационные войны — это контентные войны, имеющие своей целью изменение массового, группового и индивидуального сознания, навязывание своей воли противнику и перепрограммирование его поведения. В процессе информационных войн идет борьба за умы, ценности, установки, поведенческие паттерны и т. п.»[1]. Подобные войны велись на всех этапах существования человечества (см. гл. 4: введение); появление Интернета просто придало этим войнам невиданные ранее масштаб, интенсивность и (предположительно) эффективность. Объект воздействия информационной атаки может быть как отдельной личностью или группой лиц, занимающих ключевое положение в той или иной стратегической ситуации, так и целый народ или население целой страны; в качестве

[1] *Овчинский В., Ларина Е.* Кибервойны XXI века: О чем умолчал Эдвард Сноуден. М., 2014. С. 17.

оружия могут быть использованы любые информационные объекты, расчитанные на восприятие сознанием объекта воздействия и изменение его поведения в желаемом направлении — в формате текста, изображения, аудио- или видеоряда, любой последовательности сигналов.

«Что же касается кибервойн, то это целенаправленное деструктивное воздействие информационных потоков в виде программных кодов на материальные объекты и их системы, их разрушение, нарушение функционирования или перехват управления ими»[2].

Ричард А. Кларк, американский политик и публицист, в своей книге «Кибервойна» (2010) определяет кибервойну как «сознательное проникновение одного национального государства в компьютеры или сети другого национального государства с целью нанесения ущерба или разрушения»[3]. Генеральный Секретарь ITU (International Telecommunication Union — Международный союз электросвязи) Хамаду И. Тур в докладе «В поисках кибермира», опубликованном в 2012 г., писал: «Понятие кибервойны предполагает угрозы не только для собственно военных систем и устройств, но также и для критически важной гражданской инфраструктуры, например, энергетических сетей, находящихся под управлением систем автоматизированного диспетчерского управления и мониторинга семейства SCADA, которые обемпечивают их устойчивое и безопасное функционирование»[4].

«По де-факто сложившемуся, но юридически не закрепленному мнению подавляющего большинства военных и специалистов по информационной безопасности (вне зависимости от их страновой принадлежности), под кибервойнами понимаются целенаправлен-

---

[2] *Овчинский В., Ларина Е.* Кибервойны XXI века… С. 18.

[3] *Clarke R.A., Knake R. K.* Cyberwar. The Next Threat to National Security and What to Do About It. N.Y., 2010. P. 28.

[4] *Тур Х. И.* (Hamadoun I. Tour). В поисках кибермира / Постоянная группа по мониторингу информационной безопасности Всемирной федерации ученых. Январь 2011 года. Официальное уведомление. URL: http://nauka.x-pdf.ru/17bezopasnost/507676-1-v-poiskah-kibermira-hamadun-ture-hamadoun-tour-generalniy-sekretar-mezhdunarodnogo-soyuza-elektrosvyazi-postoyannaya.php (дата обращения: 25.08.2018).

ные действия по причинению ущерба, перехвату управления или разрушению критически важных для функционирования общества и государства сетей и объектов, производственной, социальной, военной и финансовой инфраструктуры, а также роботизированных и высокоавтоматизированных производственных, технологических линий. Средством боевого воздействия в кибервойнах является программный код, нарушающий работу, выводящий из строя, либо обеспечивающий перехват управления различного рода материальными объектами и сетями, оснащенными электронными системами управления.

Информационные и кибервойны представляют собой две разновидности войн, ведущихся в сетевом электронном пространстве, которое охватывает не только Интернет, но и закрытые государственные, военные, корпоративные и частные сети. Для каждого из этих двух типов войн свойственны свои инструментарии, методы, стратегии и тактики ведения, закономерности эскалации, возможности предупреждения и т.п»[5].

Следует иметь в виду, что данное разделение носит более методологический, нежели фактический характер: зачастую акты кибер- и информационной агрессии неразрывно связаны между собой или даже невозможны друг без друга. К примеру, взлом электронной почты государственного деятеля является определенно киберпреступлением (если его целью является, допустим, шантаж с целью получения личной выгоды), но может считаться и актом кибервойны (если целью является передача враждебному государству секретных сведений или оказание на адресанта политического давления); публикация полученных этим способом данных (допустим, свидетельствующих о противозаконной деятельности высокопоставленных лиц, что подрывает доверие к государственным органам), а также намеренное обнародование самого факта взлома (что указывает на низкую защищенность государственной информационной системы, то есть неэффективную работу спецслужб и, соответственно, провоцирует панические или протестные настроения избирателей) является целенаправленным

[5] *Овчинский В., Ларина Е.* Указ. соч. С. 18–19.

воздействием на сознание, а значит, должно быть оценено как акт войны информационной. С другой стороны, распространение и тиражирование подобной информации может быть осуществлено с помощью фейковых аккаунтов в соцсетях, спам-рассылок и накруток в поисковых системах, что опять-таки относится к сфере киберпреступлений либо кибервойны. Существуют и пограничные случаи, которые связаны со сферой кибер- или информационной безопасности, хотя формально и не касаются вопросов информационной войны или киберпреступности. К примеру, анализ рассеянных данных субъекта (например, статистики его переходов по гиперссылкам, взаимодействия с платежными, социальными, коммерческими, игровыми и другими службами в Интернете, анализ публикаций субъекта в социальных сетях, позволяющий отследить его предпочтения или график перемещений и т. п.), не будучи противозаконным сам по себе, может предоставить злоумышленникам информацию, пригодную для использования в преступных целях. Соответственно, эта потенциальная возможность предъявляет дополнительные требования по защите персональных данных субъекта в инфосфере.

Следует, однако, учитывать, что если конкретные, материально выраженные последствия киберпреступления или военных действий в киберпространстве, как правило, возможно более или менее однозначно идентифицировать и описать (взлом почты или банковского аккаунта, перехват управления устройствами, спровоцированный извне сбой систем управления электрическими сетями, вирусная атака, уничтожившая базу данных или вызвавшая технический сбой на оборонном предприятии, и т. п. либо имели место, либо не имели места вне зависимости от того, были ли они обнаружены противодействующей стороной), то воздействие на сознание носит более тонкий и, соответственно, зачастую недоказуемый характер, а последствия такого воздействия могут иметь как непосредственно просчитываемое (самоубийства участников суицидальных интернет-сообществ), так и отложенное опосредованное (политическая пропаганда, меняющая поведение субъекта на системном уровне) характер. Собственно, этот факт заставляет нас анализировать

кибер- и информационную безопасность по отдельности и отвести этим темам разные разделы настоящего исследования.

Приведенное выше разведение не является общепринятым в медийном и политическом дискурсе. Неспециалисты часто прибегают к расширительному толкованию термина: фактически под кибервойнами понимается любое противоборство в кибер- или интернет-пространстве. Зачастую кибервойнами называют ведущиеся посредством электронных СМИ информационные кампании высокой сложности, ориентированные на изменение мнений, ценностных установок или поведения референтной группы, а также репутационные войны между государствами и «войны брендов» между крупными корпорациями, то есть как раз то, что мы определяем как информационные войны. Неопределенность в применении и понимании термина кибервойны связана в значительной степени с историей развития информационных технологий вообще и Интернета в частности. Сначала в профессиональную аудиторию был внедрен термин «информационная война», предложенный компанией RAND в 1990 г. Затем специалист RAND Мартин Либицки опубликовал книгу «Что такое информационная война»[6]. Либицки выделяет семь способов ведения информационной войны: командно-управленческий, разведывательный, психологический, хакерство, экономический, электронный, киберборьба; таким образом, в его версии термин включает в себя и техническое, и контентное противоборство в киберпространстве, а также ряд несвязанных напрямую с инфосферой форм межгосударственных конфликтов. При этом основное внимание в работе уделяется направленному психологическому воздействию и так называемым специальным информационным операциям, в первую очередь дезинформации.

Развитие возможностей информационных технологий привело к осознанию необходимости рассматривать кибервойны как самостоятельную форму агрессивного взаимодействия. По-видимому, приоритет в этом принадлежит американским военным аналитикам Дж. Аркуилла и Д. Ронфилду, опубликовавшим в журнале Compar-

[6] *Libicki M. C.* What Is Information Warfare? Washington, D.C., 1995. 104 p.

ative Strategy статью «Cyberwar is Coming!»[7]. В период между 2007 и 2010 гг. разведение кибервойн и информационных (контентных) войн можо считать общепринятым стандартом как для военных и сотрудников спецслужб, так и для профильных специалистов по компьютерной и информационной безопасности — в первую очередь, в странах, вышедших на позиции признанных мировых лидеров в кибервоенной сфере, то есть в США, КНР, Великобритании, Израиле. В то же время в России некоторые аналитики продолжают отождествлять информационные войны и кибервойны, рассматривая их прежде всего в аспекте воздействия информационных потоков на коллективную психику и сознание человека. В результате потенциальные угрозы были недооценены, и Россия значительно позже других крупных игроков приступила к активным и осознанным действиям в кибервоенной сфере.

§ 1. Киберпреступность и кибербезопасность

«Киберпространство в строгом смысле этого слова представляет собой ту часть цифровой среды, где происходит управление различного рода объектами физического мира, посредством передачи программ в виде сигналов по Интернету, другим сетям и телекоммуникационным каналам»[8]. При этом сам факт существования информационных сетей общего доступа делает принципиально возможным существование несанкционированных управляющих сигналов, порождая феномен киберпреступности. Это явление в последние десятилетия приняло интернациональный характер, зависящий от уровня глобализации информации и приводящий к серьезным негативным последствиям в экономике различных стран. Распространенность и дешевизна средств доступа к информационным ресурсам, лавинообразно нарастающая с ростом рынка

[7] См.: *Arquilla Jh., Ronfeldt D.* Cyberwar is Coming! // Comparative Strategy. 1993. Vol. 12, № 2. URL: https://www.rand.org/pubs/reprints/RP223.html (дата обращения: 25.08.2018).

[8] *Овчинский В., Ларина Е.* Указ. соч. С. 3.

сравнительно дешевых персональных вычислительных средств, с ростом мощности мобильных устройств связи и повышением охвата и качества работы коммуникационных сетей, «демократизирует» киберпреступность, поскольку совершение преступления в инфосфере зачастую требует от злоумышленника только наличия минимальной технической подготовки и общераспространенного доступа к минимальной инфраструктуре. Таким образом, агрессия в киберпространстве общедоступна, причем ее результаты в наибольшей степени угрожают технически и экономически развитым странам и экономикам.

Киберугрозы приобретают глобальный характер. В традиционном докладе «Глобальные угрозы — 2018» эксперты Международного экономического форума называют хакеров третьей по значению угрозой цивилизации — сразу после стихийных бедствий и глобального потепления[9]. За пять лет, начиная с 2012 г., количество взломов компьютерных систем крупнейших мировых компаний увеличилось в два раза — с 68 до 130. Несмотря на то, что большинство попыток хакеров пока безуспешны, вероятность порабощения экономических систем киберпреступниками становится все реальнее. В прошлом году количество и масштаб цифровых атак (равно как и масштаб освещения этих атак в прессе) становится беспрецедентным: хакеры взламывали системы больниц и школ, останавливали работу автомобильных концернов, публиковали сценарии популярных сериалов и вымогали огромные деньги у пользователей. В мае 2017-го программное обеспечение, названное WannaCry, заразило более полумиллиона компьютеров по всему миру. По оценкам экспертов «Лаборатории Касперского», в первый день заражения большинство атак пришлось на Россию: их пытались отражать мобильные операторы, сети МВД, РЖД и Следственного комитета. Спустя несколько недель на европейские и российские компании пошел войной усовершенствованный вирус Petya годовой давности (обновление было названо NotPetya): тогда пострадали банки, энергетические компании и аэропорты. Еще через несколько

[9] См., напр.: URL: https://www.bbc.com/russian/features-42747983 (дата обращения: 25.08.2018).

месяцев отечественные концерны поразил шифровальщик Bad Rabbit. Кража данных примерно 150 миллионов человек из компании Equifax была менее новаторской, чем другие атаки, но тем не менее значительной — отчасти потому, что она показала, сколько персональных данных может храниться у одной компании, в то время как общественность вообще не понимает, как они к ней попали. Повсеместное использование хакерами персональных устройств сторонних пользователей для майнинга криптовалют или следящие функции многочисленных устройств с голосовым управлением, от смартфонов до стиральных машин, которые используются разработчиками как минимум для таргетирования рекламных услуг, выглядят на этом фоне уже обыденностью.

Добавим сюда многочисленные скандальные разоблачения глобального масштаба, материалы которых были получены хакерскими методами — от похищения, распространения и публичной огласки документов «Панамского досье» компании Mossack Fonseca, занимающейся регистрацией и сопровождением офшоров, до действий предположительно пророссийской группы Fancy Bear, которую обвиняют во взломах информационных систем НАТО, Белого дома, Демократической партии США, правительственных информационных систем Франции и ФРГ, МОК и WADA. В свою очередь, WADA использует в расследовании «российской государственной допинговой программы» базу данных РусАДА, полученную при неясных обстоятельствах — вероятно, также в результате кибератаки либо кражи информации кем-либо из сотрудников агентства[10]. Масштаб этих событий и особенно градус освещения в прессе таков, что грань между киберпреступлениями, кибервойной и информационной войной совершенно размывается. В западной прессе постоянно звучат обвинения в кибератаках, якобы инспирированных российскими и/или китайскими правительственными органами или курируемыми спецслужбами хакерскими группами; однако известны и обратные примеры. Так, опубликованный WikiLeaks доклад Vault8 обвиняет ЦРУ в распространении под

[10] См., напр.: URL: https://www.sport-express.ru/doping/reviews/vada-pohvastalos-novym-kompromatom-na-rossiyu-1333611/ (дата обращения: 25.08.2018).

видом программ «Лаборатории Касперского» вредоносных кодов, использующих уязвимости «нулевого уровня» для получения доступа к персональной информации пользователя и контроля за его устройствами. Факт распространения фальшивых сертификатов подтвердил в своем «Твиттере» сам Евгений Касперский[11]. При этом встречные обвинения в распространении бэкдоров под видом антивирусных программ поступают от правительств США и Великобритании уже в адрес самой «Лаборатории Касперского»[12]. Стоит обратить внимание, что если факт подобных киберпреступлений на государственном уровне в ряде случаев может быть оспорен, то их техническая возможность, кажется, уже ни у кого не вызывает сомнений. Более того, боязнь кибератак при активной поддержке СМИ и развлекательной кинопродукции («Пароль „Рыба-Меч“» и т. п. фильмы, эксплуатирующие образ всемогущих и неуловимых хакеров как суперпреступников нового поколения) явно грозит перерастанием в массовую истерию.

Кража данных банковских карт или даже перехват управления электрическими сетями с целью их дистанционного отключения — угрозы по крайней мере предсказуемые и в этом смысле потенциально поддающиеся контролю. Проблема заключается в том, что количество сфер человеческой жизни, которым киберпреступники могут угрожать напрямую, растет по экспоненте, и предусмотреть защиту во всех возможных случаях не представляется возможным. Так, быстрыми темпами развивается «интернет вещей» — концепция, предполагающая создание вычислительной сети физических объектов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. Эта концепция предполагает качественно новый уровень автоматизации бытовых и производственных процессов («умный дом», «умный город»

---

[11] См., напр.: URL: https://meduza.io/news/2017/11/10/wikileaks-ts-ru-maskirovalo-svoi-virusy-pod-produktsiyu-laboratorii-kasperskogo (дата обращения: 25.08.2018).

[12] См., напр.: URL: https://www.1tv.ru/news/2017-12-02/337189-spetssluzhby_velikobritaniya_zapretili_gosuchrezhdeniyam_ispolzovat_antivirus_laboratorii_kasperskogo (дата обращения: 25.08.2018) ; URL: http://www.interfax.ru/russia/587733 (дата обращения: 25.08.2018).

и т. п.). В результате уже в настоящее время большинство IP-адресов принадлежат не пользовательским и корпоративным устройствам или традиционным интернет-ресурсам, а промышленным, инфраструктурным объектам, а также системам управления вещами и сетями, буквально окружающими современного горожанина. Согласно данным компании Cisco, уже в настоящее время на «интернет вещей» приходится 10 млрд IP-адресов, а в 2020 г. число таких адресов возрастет не менее чем до 50 млрд[13]. По оценкам ведущей аналитической компании Neilsen, уже сегодня «Интернет вещей» берет на себя более 70 % трафика[14].

При этом всеобщая интернетизация вещной среды, окружающей человека как на производстве, так и в быту, крайне обостряет проблему информационной безопасности, поскольку многократно увеличивает количество взаимодействующих сетей. В ситуации, когда хакерским атакам практически ежемесячно подвергаются государственные сервисы и сайты крупных корпораций, невозможно ожидать обеспечения безопасности на уровне каждого объекта, интегрированного в «интернет вещей». Согласно данным мониторинговых исследований компании Symantec, потенциальную опасность представляет не только контроль злоумышленника над подобным устройством, но и возможность их массового использования для организации DDoS-атак. «Этому способствует сравнительно низкий уровень защиты устройств IoT, обусловленный в том числе их скромными вычислительными возможностями и ограничениями ОС, а также слабым контролем в процессе развертывания и эксплуатации (во многих случаях работает принцип „включил и забыл“, остаются даже пароли, заданные производителем по умолчанию). В результате хакеры получают контроль над оборудованием локальных сетей, модемами, сетевыми хранилищами, системами видеонаблюдения и даже промышленными управляющими системами. Подконтрольные злоумышленникам устройства затем используются

[13] См.: Cisco Visual Networking Index ™ (VNI) Complete Forecast for 2016 to 2021). URL: https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html?dtid=osscdc000283 (дата обращения: 25.08.2018).

[14] См.: *Овчинский В., Ларина Е.* Указ. соч.

в атаках DDoS на более важные цели, в качестве которых обычно выступают компьютеры крупных компаний»[15]. Особое внимание специалистов по кибербезопасности обращают на себя мобильные, а в последние годы и стационарные (например, телевизоры и телеприставки) устройства на базе платформы Android, которая непрерывно развивается (что ведет к несогласованности версий и повышении вероятности ошибок) и при этом не обладает серьезным потенциалом по защите от вредоносного воздействия. Уже статистика 2012 г. показывает, что вредоносные программы и коды, рассчитанные на незаконное управление Android-устройствами, составили 99 % от всех подобных программ, обнаруженных в информационном пространстве, в последующие годы ситуация продолжила ухудшаться[16]. Напомним, что речь зачастую идет об устройствах, которые в рамках набирающей популярность политики интеграции функций становятся платежными устройствами, позволяют получить доступ к банковским счетам и персональным данным клиентов и т. п.

Следующим шагом на пути к тотальной интернетизации становится «Интернет тел» (англ. Internet of Bodies) — экосистема умных медицинских приборов (имплантов и носимых устройств лечебного и/или диагностического назначения), фитнес-трекеров, а в перспективе также систем прямого взаимодействия компьютер-человек и иных носимых и имплантированых устройств, расширяющих возможности субъекта. В качестве первого шага в массовом распространении подобных «гуманизированных» интерфейсов можно рассматривать очки Google Glass. По оценкам экспертов, в течение ближайших двух-трех лет успехи нанотехнологий позволят создать массовые продукты на основе контактных линз, имплантированных контрольных чипов для людей с хроническими заболеваниями

---

[15] Symantec Research Finds IoT Devices Increasingly Used to Carry out DDoS Attacks. URL: http://investor.symantec.com/About/Investors/press-releases/press-release-details/2016/Symantec-Research-Finds-IoT-Devices-Increasingly-Used-to-Carry-out-DDoS-Attacks/default.aspx?utm_source=ixbtcom (дата обращения: 25.08.2018).

[16] См.: *Згоба А. И., Маркелов Д. В., Смирнов П. И.* Кибербезопасность: Угрозы, вызовы, решения // Вопр. кибербезопасности. 2014. № 5 (8). С. 30–38.

и т. п. Только на территории США ежегодно активируются не менее 10 млн медицинских приборов различного назначения (в том числе носимых и имплантированных), дистанционно управляемых через Интернет. Как правило, такие системы имеют единые пункты контроля в компаниях-изготовителях. Соответственно, появляется потенциальная возможность не только перехвата управления отдельным устройством, но и централизованной атаки на целый сектор устройств, которая позволила бы кибертеррористам вызвать массовые жертвы среди населения. Во всяком случае, к примеру, в США, начиная с 2008 г., серьезно прорабатывается тема угрозы дистанционного взлома кардиостимуляторов[17].

Информационные технологии с коммуницированием как по закрытым, так и по общедоступным сетям де-факто стали обязательным компонентом таких решающих для мировой экономики направлений, как робототехника, 3D-печать, биотехнологии. Потенциальное удешевление и повсеместное внедрение этих технологий должно превратить их в основу нового промышленного уклада[18], однако это требует всеобъемлющего распространения коммуникационных технологий и, соответственно, открывает все новые области для действий киберзлоумышленников. Идеология «тонкого клиента», облачные системы вычисления и использование ботнетов позволяет подготовленному преступнику или кибертеррористу, имея на руках лишь маломощное устройство минимальной стоимости с разовым анонимным выходом в общественную сеть, атаковать любой из этих сегментов с тем большими последствиями, чем более технологически развитым является атакуемая корпорация или государственная структура. Важным моментом риска становится в данном случае и человеческий фактор: даже закрытые сети становятся уязвимы в ситуации, когда пользователь работает с ними и с Интернетом через одно и то же устройство.

2017-й мировая пресса уже окрестила «Годом кибермагеддона». Вредоносное обеспечение постоянно совершенствуется, и порой

---

[17] См., напр.: URL: https://geektimes.ru/company/medgadgets/blog/265068/ (дата обращения: 25.08.2018).

[18] См., напр.: *Шваб К.* Четвертая промышленная революция. М., 2016. 138 с.

даже самые мощные системы безопасности не способны его отследить. Авторы доклада «Глобальные угрозы — 2018» вообще считают, что единственным способом замедлить темпы распространения трансграничных кибератак может стать дефрагментация или распад Интернета. Правительства разных стран рано или поздно отгородятся от глобальной сети и создадут свои изолированные мини-копии. Однако распад международной паутины на множество частей может спровоцировать остановку развития Интернета или вовсе уничтожит его. Во всяком случае, известно, что российские и китайские государственные службы всерьез рассматривают подобную возможность на случай политических осложнений[19]. С другой стороны, в качестве возможного ответа рассматривается децентрализация данных Интернета, которая должна минимизировать последствия кибератак. Британский ученый Тим Бернес-Ли, создатель Всемирной паутины, считает нынешний Интернет извращенной версией первоначального замысла, согласно которому любой пользователь мог быть активным участником системы, иметь собственный домен или сервер. Изобретатель предлагает вернуться к идее Интернета как децентрализованной системы: если каждый будет хранить свою личную информацию, человечество приблизится к созданию «идеального» Интернета[20]. Наконец, в качестве своеобразного противоядия рассматривается и доктрина абсолютной открытости персональных данных и отказа от права на приватность, провозглашенная, например, персонажами романа-антиутопии Дэйва Эггерса «Сфера».

Киберпреступность и кибератаки как потенциальная, а затем и реальная угроза, всерьез анализировались с первых шагов становления информационного общества. Соответственно, накоплен существенный пул контрмер как в юридической, так и в технической сфере. Уже в середине 90-х гг. прошлого века группа экспертов Организации экономического сотрудничества и развития (ОЭСР)

---

[19] См., напр.: URL: https://vz.ru/society/2016/12/29/744236.html (дата обращения: 25.08.2018) ; URL: https://www.bbc.com/russian/features-36741188 (дата обращения: 25.08.2018).

[20] См.: URL: https://news.rambler.ru/internet/38998477-internetu-grozit-unichtozhenie/ (дата обращения: 25.08.2018).

провела анализ законодательства и правоохранительной политики стран — членов ОЭСР с целью борьбы с компьютерными преступлениями, под которыми понималось «всякое незаконное, неэтичное и несанкционированное поведение, касающееся автоматизированных процессов и трансмиссии данных»[21]. Эксперты констатировали, что существует неясность относительно того, какой государственной политики в сфере уголовной ответственности за нарушение права на компьютерную собственность следует придерживаться: или «поддерживать развитие новой растущей компьютерной индустрии, или стремиться к охране и защите новой экономической реальности — информации»[22]. Также не были определены возможные экономические и правовые последствия неправомерного пользования средствами ЭВТ, поскольку границы «что допускается, что разрешено и что запрещено» сильно размыты.

Одним из главных факторов, мешающих разработке правоохранительных мер в сфере информационно-компьютерной преступности, является то, что преступное использование компьютера зачастую не оставляет материальных следов, это использование может быть подтверждено только с помощью экспертов соответствующего профиля, причем экспертная оценка не всегда может дать безусловно достоверные результаты. С другой стороны (особенно в случаях, когда мы имеем дело с кибертерроризмом или действиями проправительственных хакерских группировок), действия информаторов и экспертов сами находятся на грани или за гранью предусмотренных законодательством[23] и практически не отличимы от действий самих киберпреступников. Закон же традиционно строится на наличии внешних материальных свидетельств преступления.

---

[21] Здесь и далее цит. по: *Ловцов Д. А.* Системология правового регулирования информационных отношений в инфосфере : монография. М., 2016. С. 113.

[22] *Ловцов Д. А.* Информационное право : учеб. пособие. URL: http://sci-book.com/pravo-informatsionnoe/informatsionnoe-pravo-ucheb-posobie-rap2011.html (дата обращения: 25.08.2018).

[23] См., напр., анализ системы кибербезопасности США в журналистском расследовании: *Харриса Ш.* Кибервойн@: пятый театр военных действий. М., 2016. 392 с.

«Парадоксальная особенность компьютерных преступлений состоит и в том, что трудно найти другой вид преступления, после совершения которого в ряде случаев его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще „компьютерного взлома", мало что утаивая от представителей правоохранительных органов. Психологически этот парадокс вполне объясним. Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб. Во-вторых, преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт»[24].

В правоведении ведется полемика о том, какие действия следует относить к разряду компьютерных преступлений. Сложность решения вопроса заключается также и в том, что диапазон противоправных действий, совершаемых с использованием средств ЭВТ, чрезвычайно широк и в ряде случаев требует профессиональной подготовки высокого уровня. Создание в США и появление на рынке компактных и сравнительно недорогих персональных компьютеров дало возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контроле доступа к информации, об обеспечении ее качества (конфиденциальности, сохранности, целостности и др.).

Особенно остро проблема несанкционированного доступа (НСД) к компьютерной информации дала о себе знать в странах с развитой информационной инфраструктурой. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе и уголовно-правовые средства защиты. Например, в Уголовном кодексе Франции система преступлений против собственности пополнилась в 1992 г. специальной главой «О посягательствах на системы автоматизированной обработки данных». В ней предусмотрена ответственность за не-

[24] *Ловцов Д. А.* Системология правового регулирования… С. 119.

законный доступ ко всей или части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы системы или ввод в нее обманным способом информации, уничтожение или изменение базы данных. Одним из первых компьютерных преступлений на территории бывшего СССР стало автоматизированное хищение 78 584 рублей, совершенное в Вильнюсе в 1979 г.

Наиболее распространенными являются экономические компьютерные преступления. Они совершаются по корыстным мотивам и включают компьютерное мошенничество, кражу программ («компьютерное пиратство»), кражу услуг и машинного времени, экономический шпионаж и др.

Компьютерные преступления против государственных и общественных интересов включают преступления, направленные против государственной и общественной безопасности, угрожающие обороноспособности государства, а также злоупотребления с АИС электронного голосования, взаимодействия с органами власти и др.

Классификация компьютерных преступлений возможна по различным признакам. Очевидным является следующее разграничение:

1) преступления, в которых основной целью является причинение вреда или получение незаконной прибыли непосредственно в инфосфере (например, хищение или искажение информации);

2) преступления, использующие действия в инфосфере как инструмент для обеспечения незаконной активности в иных областях деятельности (например, слежение за объектом посредством компьютерных сетей).

Однако этого, базового, разграничения определенно недостаточно.

Развернутая классификация компьютерных преступлений была разработана в начале 90-х гг. для Кодификатора международной уголовной полиции генерального секретариата Интерпола (код Q). Однако она предназначена для автоматических поисковых систем, поэтому носит сугубо прикладной характер и не является основанием для правоприменения.

В. А. Мещеряков в 1999 г. предложил следующую классификацию преступлений в информационной сфере:

«1. **Неправомерное завладение информацией или нарушение исключительного права ее использования.**

1.1. Неправомерное завладение информацией как совокупностью сведений, документов (нарушение исключительного права владения).

1.2. Неправомерное завладение информацией как товаром.

1.3. Неправомерное завладение информацией как идеей (алгоритмом, методом решения задачи).

2. **Неправомерная модификация информации.**

2.1. Неправомерная модификация информации как товара с целью воспользоваться ее полезными свойствами (снятие защиты).

2.2. Неправомерная модификация информации как идеи, алгоритма и выдача за свою (подправка алгоритма).

2.3. Неправомерная модификация информации как совокупности фактов, сведений.

3. Разрушение информации.

3.1. Разрушение информации как товара.

3.2. Уничтожение информации.

4. Действие или бездействие по созданию (генерации) информации с заданными свойствами.

4.1. Распространение по телекоммуникационным каналам информационно-вычислительных сетей информации, наносящей ущерб государству, обществу и личности.

4.2. Разработка и распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ.

4.3. Преступная халатность при разработке (эксплуатации) программного обеспечения, алгоритма в нарушение установленных технических норм и правил.

5. Действия, направленные на создание препятствий пользования информацией законным пользователям.

5.1. Неправомерное использование ресурсов автоматизированных систем (памяти, машинного времени и т. п.).

5.2. Информационное «подавление» узлов телекоммуникационных систем (создание потока ложных вызовов)»[25].

---

[25] Цит по: *Погонышева Д.А.* Безопасность информационных систем : учеб. пособие. URL: https://it.wikireading.ru/4299 (дата обращения: 25.08.2018).

Определенным этапом для российского законодательства стало принятие в 1992 г. Закона РФ от 23 сентября 1992 г. № 3523-I «О правовой охране программ для электронно-вычислительных машин и баз данных» (ныне утратил силу), содержавшего положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таковых влечет уголовную ответственность. В 2006 г. был принят Гражданский кодекс РФ (часть четвертая), который содержит ряд норм, связанных с охраной компьютерной информации; в 1995 г. — Федеральный закон «Об информации, информатизации и защите информации».

Результатом проработки юридическим сообществом проблемы правового регулирования сферы защиты информационных сетей и объектов стало включение в УК РФ от 13 июня 1996 г. группы статей, предусматривающих основания уголовной ответственности за нарушения в сфере компьютерной информации. В действующей редакции УК РФ компьютерным преступлениям посвящена гл. 28 УК РФ. Под компьютерными преступлениями здесь понимаются те предусмотренные уголовным законом общественно опасные деяния, в которых либо компьютерная информация является объектом преступного посягательства, либо уголовно наказуемое деяние осуществляется с помощью компьютерной техники. К такого рода дейниям относятся:

«1. Неправомерный доступ к охраняемой законом компьютерной информации (сведениям в форме электрических сигналов), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

2. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телеком-

муникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (свыше 1 млн рублей)»[26].

Ст. 274.1 оговаривает специфику наказаний за аналогичные действия, повлиявшие на критическую значимую информационную инфраструктуру Российской Федерации.

В качестве предмета или орудия совершения преступления может выступать компьютерная информация, компьютер, компьютерная система или информационно-телекоммуникационная сеть. Преступления, имеющие своим предметом только лишь аппаратно-технические средства вычислительных машин (хищение, уничтожение), подпадают под другой тип уголовных правонарушений, закрепленных в гл. 21 УК РФ — «Преступления против собственности». Глава 28 УК РФ имеет своей целью охрану именно информационных отношений в инфосфере и только в силу этого защиту и аппаратно-технических средств, которые являются материальными носителями информационных ресурсов.

Компьютерная информация сама по себе может являться средством преступного посягательства. В этом случае отношения по охране компьютерной информации страдают неизбежно, то есть она сама становится предметом общественно опасного деяния. Следует учитывать, что невозможно противоправно воспользоваться информацией, хранящейся в компьютере, не нарушив при этом ее защиты, то есть не совершив одного из действий, предусмотренных в Федеральном законе «Об информации, информационных технологиях и защите информации». Поэтому даже при совершении, например, такого преступления, как электронное хищение денег, ответственность должна наступать по правилам идеальной совокупности преступлений.

Характеризуя объективную сторону рассматриваемых составов преступления, следует заметить, что большинство из них конструктивно сформулированы как материальные, поэтому предполагают

---

[26] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 12.11.2018). URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 25.08.2018).

не только совершение общественно опасного деяния, но и наступление общественно опасных последствий либо создание угрозы их наступления, а также установление причинной связи между этими двумя признаками. Почти все составы гл. 28 УК РФ относятся к преступлениям небольшой и средней тяжести, и только два — к тяжким преступлениям.

Типичными преступными целями совершения компьютерных преступлений согласно УК РФ являются шпионаж (экономический, политический и др.), саботаж (несанкционированная эксплуатация АИС), подделка документов (получение фальшивых дипломов, фиктивное продвижение по службе и др.); хищение компьютерной информации, денег (подделка счетов и платежных ведомостей; фальсификация платежных документов, вторичное получение уже произведенных выплат, перечисление денег на подставные счета и др.), вещей (совершение покупок с фиктивной оплатой, добывание запасных частей и редких материалов); внесение изменений в компьютерную информацию, приписка сверхурочных часов работы, кража машинного времени и др. В качестве типичных киберугроз можно обозначить:

— незаконный сбор информации о пользователях киберустройств (обычно с целью последующего противоправного использования);

— распространение вредоносных программ и кодов, ориентированных на причинение вреда материальным объектам киберпространства, похищение персональных данных пользователя, перехват управления компьютерной техникой;

— массовая рассылка сообщений рекламного или псевдоинформационного характера, обычно приобретающая назойливый характер и в ряде случаев критически засоряющая коммуникационные каналы (так называемый спам

— использование различных форм интернет-коммуникации с целью заставить пользователя раскрыть свои персональные данные, пароли, коды подтверждения электронных платежных систем, а также открыть доступ на свои устройства вредоносным программам (так называемый фишинг);

— организация массовых запросов на сетевые ресурсы жертвы с целью вызвать перегрузку ресурса (распределенная атака типа «отказ в доступе», обычно с использованием дистанционно контролируемой бот-сети);

— похищение предоставляемых через интернет услуг, платежей и т. п.;

— похищение или повреждение информации пользователя, в том числе интеллектуальной собственности;

— компьютерный взлом систем защиты информации, в частности, систем защиты программного обеспечения (так называемый крекинг).

Защита компьютерной информации также требует законодательного обеспечения, которое представляет собой взаимосвязанный комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов правоотношений, субъектов и объектов защиты, методы, средства и формы защиты и их правовой статус. К основным правовым способам и средствам защиты информации в компьютерных системах наряду с УК РФ (гл. 28, ст. 272, 273, 274) относятся:

— Конституция РФ. Она определяет основные права и обязанности человека, общества и государства в отношении информации и соответствующих тайн, а именно право на неприкосновенность частной жизни, защиту чести и доброго имени, тайну переписки, телефонных и иных сообщений, поиск, получение, создание и распространение информации любым законным способом, наконец, право на благоприятную среду, в которой по новейшим концепциям государственного строительства (например, согласно Доктрине информационной безопасности РФ) безусловно включается также и информационная среда;

— Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», регулирующий «отношения, возникающие при: 1) осуществлении права на поиск, получение, передачу, производство и распространение информации; 2) применении информационных технологий;

3) обеспечении защиты информации»[27]. Закон определяет ряд ключевых понятий, необходимых для установления правовых отношений в инфосфере: «информация», «информационные технологии», «информационная система», «электронное сообщение»; «информационно-телекоммуникационная сеть»; «оператор информационной системы»; «обладатель информации», «доступ к информации», «предоставление информации», «распространение информации», «документированная информация», «конфиденциальность информации» и др.[28];

— Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Закон оговаривает меры по обеспечению безопасности персональных данных при их обработке, устанавливая, в частности, обязанность оператора принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения и др. «Контроль и надзор за выполнением требований по обеспечению безопасности обрабатываемых персональных данных, устанавливаемых Правительством РФ, возлагается (без права ознакомления с данными) на федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности и в области противодействия техническим разведкам и технической защиты информации»[29].

Развитие сферы киберпреступности требует от субъектов инфосферы задумываться о создании комплексных мер кибербезопасности. Под кибербезопасностью понимается набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности,

---

[27] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.08.2018).

[28] Там же.

[29] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.08.2018).

подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. «Кибербезопасность — раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов, с целью выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности»[30]. Кибербезопасность предполагает превышение параметров защиты кибертехники, информационных ресурсов и пользователей инфосферы над совокупностью актуальных угроз киберсреды. Методы индивидуальной, корпоративной и государственной кибербезопасности реализуются на нескольких уровнях:

— инфраструктурный уровень, предусматривающий защиту материальной составляющей киберсферы от внешнего воздействия, включая разработку защищенных устройств, средств автономного питания и защиты данных от воздействия стихийных сил, а также средств радиоэлектронной борьбы. Сюда же следует отнести разработку систем дублирования и распределенного хранения данных, затрудняющего их похищение и/или повреждение. В ситуациях высокого приоритета этот уровень требует создания независимых информационных сетей и ресурсов, не предусматривающих прямого или дистанционного доступа сторонних лиц в какой бы то ни было форме;

— уровень программного обеспечения, предусматривающий разработку брандмауэров и антивирусов, сбор данных о вредоносных программах и кодах, сбор данных об уязвимостях программных кодов и их своевременное устранение, разработку систем безопасного доступа для дорогостоящих программ;

— пользовательский уровень, предполагающий просветительскую работу и обучение субъектов киберпространства правилам

---

[30] *Алпеев А. С.* Критически важные объекты: терминология безопасности // Вопр. кибербезопасности. 2016. № 4 (17). С. 39–42.

и нормам безопасного поведения в киберсфере, что снижает эффективность большинства актуальных угроз;

— нормативный уровень, предполагающий наработку для субъектов киберпространства алгоритмов правового поведения, обеспечивающих максимальный уровень безопасности.

Обеспечение безопасности компьютеров, будь то серверов, настольных компьютеров, ноутбуков или смартфонов, является целью работы самых различных групп внутри ИТ- и интернет-сообществ. Тем не менее даже нахождение технологического решения для проблемы кибербезопасности не означает, что сама проблема исчезает — просто появляется возможность ее решения. Например, комплексное шифрование с использованием алгоритмов SSL/TLS является широко известной технологией, которую можно использовать для устранения многих киберугроз. Однако оно не было принято повсеместно. Частично это обусловлено историческими причинами и организационной инертностью, а также неграмотностью или плохой информированностью. Наличие хорошо известных решений хорошо известных проблем имеет небольшую ценность, если эти решения не используются.

§ 2. Кибервойны

Термин «кибервойны» прочно вошел не только в лексикон военных и специалистов по информационной безопасности, но и политиков, представителей экспертного сообщества, журналистов. Кроме того, кибервойны активно обсуждаются заинтересованными неспециалистами, прежде всего в социальных сетях и на других площадках онлайн-коммуникации. Это неизбежно придает термину оттенок несерьезности, роднит с многочисленными «теориями заговора», что вряд ли оправдано на практике.

Кибервойны тесно связаны с кибершпионажем, киберпреступностью и кибертерроризмом, так же, как и преступность, терроризм и шпионаж в материальном мире связаны с «традиционной» войной и друг с другом. Все эти виды агрессивного взаимодействия используют в киберпространстве сопоставимые технологии и про-

граммные средства, и говорить о разнице между ними, вероятно, будет возможно только в случае начала неограниченной по целям и средствам и тотальной по масштабам кибервойны.

Оговорим используемую терминологию. Здесь и далее под **кибервойнами** понимается целенаправленные действия одной стороны по причинению ущерба, перехвату управления или разрушению критически важных для функционирования общества и государства (а также в некоторых случаях системообразующих частных корпораций) информационных сетей и объектов производственной, социальной, военной и финансовой инфраструктуры, роботизированных и высокоавтоматизированных производственных, технологических линий другой стороны, проводимые посредством использования специализированных программ, кодов и — реже — технических устройств[31].

По целям и задачам агрессивные действия в киберпространстве разделяют на кибершпионаж и кибератаки. При этом в тех случаях, когда за кибератаками стоят не государственные или аффилированные с ними частные службы, а внесистемные агрессивные сообщества экстремистского толка, принято говорить об актах **кибертерроризма** (термин был предложен еще в 1980-х гг. для описания перспектив перехода террористической активности в формирующуюся инфосферу, при этом до настоящего времени термин применяется непоследовательно и однозначно не определен)[32].

Под **кибершпионажем** понимается несанкционированное получение информации с целью получения личного, экономического, политического или военного превосходства, осуществляемый с использованием обхода (взлома) систем компьютерной безопасности, с применением вредоносного программного обеспечения, включая «троянских коней» и шпионских программ. Кибершпионаж может осуществляться как дистанционно, с помощью Интернета, так и путем проникновения в компьютеры и компьютерные

---

[31] См.: *Киселёв В., Костенко А.* Кибервойна как основа гибридной операции // Армейский сборник. 2015. Т. 257, № 11. Ноябрь. С. 3–6.

[32] См.: *Collin B.* The Future of Cyberterrorism // Crime & Justice International Journal. 1997. Vol. 13. Вып. 2.

сети предприятий обычными шпионами («кротами»). В последние годы под кибершпионажем понимают также анализ спецслужбами поведения пользователей социальных сетей, таких как Facebook и Twitter, с целью выявления экстремистской, террористической или антиправительственной деятельности. Как и традиционная разведдеятельность, кибершпионаж обычно незаконен в стране-жертве и поддерживается властями атакующей стороны, при этом одна и та же страна, достаточно значимая в военно-политическом и/или экономическом отношении, обычно является и субъектом, и объектом кибершпионской активности.

Под **кибератаками** подразумевают прямое или косвенное спланированное воздействие средствами программных кодов на информационные, компьютерные или инфраструктурные ресурсы жертвы с целью причинения ущерба. Доклад Национальной академии наук и Национального совета по научным исследованиям США «Технологии, политика, законодательство и моральные принципы в отношении приобретения и использования США возможностей кибератак» 2009 г. определяет кибератаки как «…преднамеренные действия для изменения, разрушения, искажения, нарушения или уничтожения компьютерных систем или сетей и информации и/или программ, размещенных (резидентных) или передающихся в этих системах или сетях»[33]. Специалисты выделяют следующие виды кибератак:

Вандализм — использование каналов информационного управления (обычно Интернета) для порчи интернет-страниц, замены содержания оскорбительными или пропагандистскими картинками (при отсутствии цели добиться прямой экономической выгоды, например, посредством шантажа владельца сайта).

Сбор информации — взлом частных страниц или серверов для сбора секретной информации и/или ее замены на фальшивую в интересах другого государства, конкурирующей компании и т. д.

---

[33] Technology, Policy, Law, and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities / eds. W. A. Owens, K. W. Dam, H. S. Lin // National Research Council: Computer Science and Telecommunications Board. 2009. URL: http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf (дата обращения: 25.08.2018).

DDoS-атаки, или атаки типа «отказ в обслуживании» — организация множественных одновременных запросов с подконтрольных атакующему компьютеров на сервера, сетевые ресурсы или маршрутизаторы атакуемого для создания перегрузки каналов связи и/или вычислительных мощностей и в результате нарушения функционирования сайтов или компьютерных систем.

Вмешательства в работу оборудования — атаки на компьютеры, которые занимаются контролем над работой гражданского или военного оборудования, что приводит к его отключению или поломке.

Атаки на пункты инфраструктуры — атаки на компьютеры, обеспечивающие жизнедеятельность городов, их инфраструктуры, такие как телефонные системы, системы водоснабжения, электроэнергии, пожарной охраны, транспорта.

Средства проведения кибератак обычно называют кибероружием. Под **кибероружием** понимается программное обеспечение или (реже) специализированное оборудование, предназначенные для нанесения ущерба в киберпространстве. При этом следует иметь в виду, что не любая вредоносная программа (например, вирус или троян) должна считаться кибероружием. Ключевым здесь следует считать избирательность действия кибероружия, предсказуемость результатов его применения, возможность управляемого распространения в Сети.

Отечественные исследователи выделяют следующие типы кибероружия.

Элемент маркированного списка, то есть автоматически активируемый элемент программного кода. Обладает высокой избирательностью и предсказуемостью воздействия, обычно не требует для активации прямой команды от разработчика кода, применяется для нарушения нормального функционирования систем.

Адаптивная система с внешним управлением — вредоносный код, который внедряется в информационную систему извне (например, посредством фишинговых рассылок) и позволяет нарушить функционирование критической инфраструктуры противника по команде оператора.

Автономная адаптивная система — экспертная система, опирающаяся на базу знаний об объекте воздействия, накопленную разведывательными службами классическими методами.

Автономная самообучающаяся система — абстрактная система искусственного интеллекта, способная проникнуть в систему произвольным путем.

Кроме того, в ряде случаев к кибероружию относят так называемые **бэкдоры** — дефекты алгоритма, позволяющие получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом. Специфика бэкдора в том, что он не внедряется в систему сторонним злоумышленником, а намеренно встраивается в него самим разработчиком (например, по требованию спецслужб) либо является результатом ошибки программистов, но намеренно скрывается по обнаружении для последующего использования в кибервоенных целях.

Получили широкую известность следующие системы кибероружия:

— Stunxet — вирусная программа, нацеленная на компьютеры на базе операционной системы Microsoft Windows. Stuxnet был обнаружен в июне 2010 г.;

— Duqu — набор компьютерных вредоносных программ, обнаруженных 1 сентября 2011 г., которые, как полагают, связаны с червем Stunxet;

— Flame — также известный как Flamer — модульное компьютерное вредоносное ПО, обнаруженное в 2012 г., которое атакует компьютеры, работающие под управлением операционной системы Microsoft Windows. Программа используется для целенаправленного кибер-шпионажа в ближневосточных странах;

— Mirai — вредоносное ПО, которое превращает сетевые устройства под управлением Linux в удаленные контролируемые боты, которые могут использоваться как часть ботнета при крупномасштабных сетевых атаках.

Следует обратить внимание, что сходные результаты в условиях технологической войны могут быть достигнуты и кибернетическими и иными средствами, что требует повышенной внимательности к применяемой терминологии в каждом отдельном случае. К примеру, перехват управления вражеским беспилотным летательным аппаратом (даже если он осуществлялся с применением средств радиоэлектронного подавления) следует считать скорее актом ки-

бервойны. Однако если аппарат просто потерял управление или был уничтожен в результате удара установки РЭБ, то перехвата управления не происходило и о кибервойне речи не идет.

История и хронология реальных кибервойн остается предметом идеологизированных дискуссий. Электронный журнал «Вестник НАТО» опубликовал интерактивный ресурс «История кибератак: хроника событий», где первой доказанной кибервоенной операцией называется атака в апреле 2007 г. на эстонские государственные сайты и сети со стороны неизвестных иностранных злоумышленников, вероятно, аффилированных с российскими государственными структурами. В качестве следующего эпизода рассматривается взлом сетевых ресурсов правительства Грузии в августе 2008 г., который не нанес прямого ущерба. Однако оказал давление на правительство страны в разгар военного конфликта с РФ[34]. В свою очередь, отечественные эксперты обычно называют первым установленным случаем использования кибероружия в ходе «традиционных» военных действий применение программ, блокирующих работу сирийских ПВО и радиоэлектронной разведки во время проведения спецслужбами США и Израиля операции «Оливы» в 2008 г.

Параллельно кибервойны и кибероружие обретали официальный статус. В этот период формируются Агентство сетевой и информационной безопасности Европейского союза (2005), Кибернетическое командование США (2010), Войска информационных операций (Россия, 2014 г.).

«Масштабное применение кибероружия по данным „Лаборатории Касперского“ впервые имело место в Иране в 2010 г. В отличие от обычных вредоносных программ, работающих в популярных операционных системах, примененный против Ирана вирус Stuxnet был специально создан для проникновения в автоматизированные системы, регулирующие и управляющие определенным типом оборудования, связанным с конкретными технологическими цепочками

[34] См.: Киберпространство: хорошее, плохое и свободное от вирусов: История кибератак: хроника событий (интерактивная хроника) // Вестн. НАТО. URL: https://www.nato.int/docu/review/2013/Cyber/timeline/RU/index.htm (дата обращения: 25.08.2018).

в атомной промышленности. Первоначально никто не брал на себя ответственность за создание и использование этого вируса, однако не так давно американские официальные лица подтвердили, что он был создан в системе АНБ с участием израильских компаний для противодействия иранской атомной программе. Еще более сложная, многокомпонентная боевая программа была применена американцами и израильтянами против нефтяных терминалов и нефтеперерабатывающих заводов все того же Ирана. Кроме того, были зафиксированы случаи использования компьютерных вирусов для вывода из строя систем SCADA крупнейшей саудовской нефтяной и катарской газовой компаний. Примером ответного кибердара можно считать перехват системы управления новейшим американским беспилотником и его принудительная посадка на территории Ирана»[35] (4 декабря 2011 г.).

За последнее десятилетие кибероружие существенно эволюционировало от уровня узкоспециальных кодов типа Stuxnet до сложных адаптивных систем перехвата управления, подобных Flame и Jaiss. При этом разработкой кибероружия занимаются не только государственные органы, но и многочисленные частные компании, а также неофициальные группы специалистов-хакеров, зачастую работающих при государственной поддержке или на подряде у спецслужб. Этот подход вписывается в традиционное для США привлечение частных компаний к выполнению заказов военных и разведывательных структур. Согласно данным, опубликованным Э. Сноуденом, в АНБ до 70 % не только исследовательских, но и текущих оперативных работ выполняется частными подрядчиками. АНБ, по свидетельству Харриса, занимается массовой скупкой бэкдоров у частных корпораций, специализирующихся на поиске системных уязвимостей. Аналогичным образом действуют спецслужбы Великобритании, Израиля, Китая и др. Так, в августе 2018 г. Министерства внутренней безопасности, общественной безопасности и дел иммиграции Австралии, Великобритании, Канады, Новой Зеландии, и США выпустили совместный меморандум, в котором

[35] *Овчинский В., Ларина Е.* Указ. соч. С. 21.

призывают IT-компании обеспечить бэкдоры для получения доступа к зашифрованным данным своих пользователей[36].

Имеющийся опыт кибервойн, кибершпионажа и крупномасштабной киберпреступности занимает незначительный по историческим меркам период, однако уже сейчас дает достаточно материалов для выделения основных черт кибервойн, принципиально отличающих их от всех других типов военных действий.

Прежде всего особенностью следует назвать анонимность кибервойн, возникающую как следствие трудностей в доказуемом определении киберагрессора. Эти трудности неизбежны, поскольку кибервойна не предполагает прямого взаимодейсвия субъекта и объекта атаки, но происходит удаленно посредством компьютерных сетей, как правило, через многоуровневый анонимизированный доступ. Помимо этого, всеми сторонами войны в киберсфере разрабатываются и совершенствуются специализированные программные комплексы-помехопостановщики, затрудняющие отслеживание хакерской активности. В результате, например, кибершпионская сеть Red October смогла с 2007 по 2012 г. практически беспрепятственно действовать против дипломатических ведомств, государственных структур и научно-исследовательских организаций разных стран мира, и только после этого была обнаружена экспертами «Лаборатории Касперского»; при этом ни полноценно блокировать обнаруженную систему, ни идентифицировать автора и заказчиков не удалось[37]. Поскольку единственным существенным отличием между кибервоенной и шпионской программами является итоговый функционал (перехват управления автоматическим устройством осуществляется в обоих случаях, но шпионская программа скачивает данные определенного типа, в то время как боевой софт наносит ущерб данным, устройствам или технологическим цепоч-

---

[36] См., напр., *Шмыров В.* Силовики США и Великобритании потребовали у ИТ-компаний дать им бэкдоры для слежки за пользователями. URL: http://safe.cnews.ru/news/top/2018-09-04_sshavelikobritaniya_i_drugie_strany_trebuyut_ot (дата обращения: 25.08.2018).

[37] См. детальное описание ситуации на сайте «Лаборатории Касперского». URL: https://securelist.ru/the-red-october-campaign-an-advanced-cyber-espionage-

кам), степень анонимности кибервойн должна быть сопоставима с анонимностью кибершпионажа.

Еще одной спецификой кибервойн является их потенциальная бесследность, которая приводит к неочевидности самого факта ведения кибервоенных действий. Любая существующая система традиционного вооружения имеет опознаваемые признаки применения, которые позволяют более или менее однозначно идентифицировать начало агрессии и реагировать соответственно. С первых дней разработки различного рода хакерского софта одной из главных задач было обеспечение неоопознаваемости последствий его использования. Следует ожидать, что и действия боевого кибероружия будут имитировать обычные сбои в работе информационных систем на программном или инфраструктурном уровне, последствия ошибочных действий персонала или результаты неспециализированных действий злоумышленников, не связанных с государственными структурами. Эпизоды, ставшие достоянием общественности — к примеру, описанная выше ситуация с применением червя Stuxnet — демонстрируют, что задачи этого рода не только принципиально разрешимы, но и разрешаются на практике. С учетом анонимности атакующего, в большинстве случаев агрессор может надеяться, что акт кибернападения вообще не будет однозначно идентифицирован и у государства-жертвы не будет оснований для нанесения ответного удара традиционными средствами.

Отсюда следует еще одна особенность кибервойн, важная для понимания юридических аспектов кибервоенных действий: проблематичность или невозможность для обозначения хронологических рамок, определения начала и конца кибервойны. «Все привычные человечеству виды войн начинались с хорошо фиксируемых материальных действий и, соответственно, имели четкую временную привязку. Многокомпонентные программы или минималистичные фрагменты базового кода, основное оружие кибервойн, могут проникать в сети и управляющие системы разнообразных военных и гражданских объектов и инфраструктур заблаговременно. В этом

---

network-targeting-diplomatic-and-government-agencies/3632/ (дата обращения: 25.08.2018).

случае фактическим началом войны будет проникновение этих программ в сети, а фиксируемым моментом начала боевых действий станет активация указанных программ в целях разрушения либо перехвата управления над инфицированными сетями и объектами»[38].

Особенностью кибервоенных действий следует назвать также отсутствие локальной привязки: здесь нельзя говорить о «фронте» и «тыле» в традиционном смысле слова, а любой гражданский объект или элемент инфраструктуры может оказаться как объектом кибератаки, так и инструментом, используемым злоумышленником для удара по стратегически более значимой цели. С другой стороны, системы распределенного хранения данных и участие субъектов коммуникации в глобальных информационных ресурсах, таких как социальные сети, придает в ряде случаев кибервоенным действиям глобальный характер вне зависимости от масштаба конкретной акции.

Важным аспектом кибервойн является также отсутствие каких бы то ни было инструментов оценки и противодействия им со стороны международного права. На данный момент ни один факт ведения войны в киберпространстве официально не признан, а существующие (реальные или мнимые) столкновения описываются (не обязательно корректно) в рамках национальных законодательств и национальных доктрин безопасности. В результате возникает неизбежное столкновение интересов. Кроме того, поскольку кибератаки или кибершпионаж рассматриваются как уголовные преступления, то ни одно из государств, претендующих на легитимность собственных действий в международном правовом поле, не признается в актах кибервойны официально. Соответственно, кибервойны как бы не ведутся, и материал для переговоров, оговаривающих нормы военной этики и военного этикета, отсутствует. Кроме того, официальное признание наличия боевых действий в киберпространстве и попытка ввести их в правовое поле потребовали бы частичного раскрытия методов киберборьбы, которые на данный момент все стороны рассматривают как секретные.

Непроработанность правовых норм в киберконфликтах рассматривается аналитиками как источник дополнительной опасности,

[38] *Овчинский В., Ларина Е.* Указ. соч. С. 23.

поскольку превращает любое столкновение в войну без правил и провоцирует обе стороны на агрессивные действия с использованием любых наличных средств кибернападения и активной обороны. Существующие международные соглашения в военной сфере во многом призваны не только уменьшить потенциальную опасность конфликтов, но и предотвратить возможные недоразумения либо остановить потенциально опасные действия противника, допустим, методом «демонстрации флага». Однако в киберсфере подобных согласованных «маркеров» на данный момент не существует, к тому же в конфликте зачастую участвуют стороны, не признающие действенности подобных соглашений (кибертеррористы неправительственных организаций экстремистского толка). Наконец, если в традиционной войне существует фактор психологического сдерживания в лице доктрины гарантированного взаимного уничтожения, то масштаб разрушительного воздействия кибероружия для подавляющего большинства населения на данный момент остается теорией, а боестолкновения в киберпространстве зачастую рассматриваются как род интеллектуальной игры, не имеющей материальных последствий для участников. В результате теоретически даже подозрение о возможности киберагрессии может спровоцировать эскалацию взаимной кибервоенной активности, которая потенциально способна перерасти в полномасштабный военный конфликт с применением традиционных средств поражения.

В совокупности специфические черты кибервойн заставляют говорить об их уникальном характере в сравнении с войнами традиционного типа. «Теперь военные называют киберпространство „пятым театром“ боевых действий и считают достижение превосходства на этом театре необходимым для выполнения миссии, точно так же, как и на четырех других — суше, море, воздушном и космическом пространстве»[39]. При этом с юридической точки зрения кибервойны на данный момент едва ли не опаснее традиционных, поскольку их легче развязать, труднее обнаружить и еще труднее остановить.

Отдельно следует оговорить ряд социокультурных, политико-экономических и психологических проблем, связанных со спе-

[39] *Харрис Ш.* Указ. соч. С. 24.

цификой кибероружия. Единственное, с чем, по-видимому, имеет смысл сравнивать последствия применения кибероружия на данный момент — это различные виды ОМП. Сравним ситуацию с контролем над боевым программным обеспечением и над производством и распространением ядерных технологий. Опасные инциденты, связанные с попытками террористических группировок завладеть расщепляющимися материалами или технологиями производства атомного оружия, зафиксированы уже в 60-е гг., а к моменту подписания Конвенции МАГАТЭ о физической защите ядерных материалов (март 1980 г.) произошло более 150 подобных эпизодов[40]. Тем не менее эти и более поздние попытки были успешно пресечены, поскольку спецслужбы научились контролировать трафик радиоактивных материалов, отслеживать деятельность производителей соответствующего оборудования и выявлять логистику практически в режиме реального времени. Производство традиционного ОМП достаточно дорого, требует развитой материально-технической базы, наличия средств доставки, требует значительного количества участников боевой операции и сложной координации их действий. Соответственно, о производстве или приобретении террористами ядерного оружия на данный момент речи не идет, а все попытки применения в террористических целях химического или бактериологического оружия по своим последствиям на данный момент перекрываются одной террористической атакой 11 сентября 2001 г. в США, в которой как раз ОМП не применялось.

Прямо противоположная ситуация складывается с контролем за производством боевого софта. Главное, что требуется для его изготовления, — это высококвалифицированные программисты и аппаратная часть, которая может быть собрана своими силами из комплектующих, массово продаваемых на открытом рынке. В результате отследить работу подобного производства предельно

[40] См., напр., URL: http://catu.su/arhiv-materialov/162-2011-11–21–18-38-56, http://nvo.ng.ru/concepts/2004-10-08/4_terrorism.html, http://old.nasledie.ru/terror/25_3/article.php?art=33 ; Россия в формировании международной системы профилактики распространения оружия массового поражения / ред. А. Д. Богатуров. М., 2008. 208 с.

сложно, тем более что оно не требует финансовых вложений запредельного уровня и доступно не только государствам и крупным корпорациям, но и сравнительно небольшим политически активным группам. Кибервойны ведутся анонимно, их центры управления рассредоточены, но главное — для проведения кибератак используются в первую очередь коммуникации и элементы инфраструктуры, которые строятся жертвой атаки за собственные средства и для обеспечения собственных целей. Таким образом, кибероружие становится едва ли наиболее «демократичным» видом ОМП.

Дополнительным фактором дестабилизации обстановки в киберсфере является высокий темп технологического развития, практически не поддающийся осмысленному контролю. Потенциальные последствия применения кибероружия становятся все более разрушительными, а возможность его использования — все более доступной. Произвести или приобрести высокоуровневое кибероружие могут сегодня не только достаточно ограниченные в ресурсах государства, но и отдельные группы, сети и т. п. К примеру, использование уязвимостей в оборудовании, операционных системах и пользовательских программах, предположительно, в первую очередь обнаруживается и/или покупается спецслужбами, финансируемыми крупными государствами. Таким же образом структурами кибербезопасности аккумулируются программы и коды, позволяющие взламывать защитные системы. Проблема в том, что речь в любом случае идет об информации. Программа может быть легально или нелегально скопирована, код украден или воспроизведен, уязвимость обнаружена несколькими независимыми экспертами. При этом, в отличие от традиционного вооружения, кибероружие не требует затрат на репликацию, что критически удешевляет его применение; оно также требует минимальных инфраструктурных затрат для хранения и применения; наконец, его природа, построенная на анонимности, внезапности и распределенном присутствии в пространстве Интернета, сокращает инфраструктурные затраты агрессора.

С другой стороны, рост числа потенциально уязвимых устройств, сетей и информационных объектов требует экспоненциального роста средств и ресурсов, расходуемых на киберзащиту. К примеру,

достижение приемлемого уровня кибербезопасности всех военных, правительственных и критически важных корпоративных и общесоциальных компьютерных систем и объектов в США требует вложений, сопоставимых с текущим уровнем военного бюджета. Ситуация усугубляется в результате возникновения так называемой «ловушки сложности», неизбежной при ускоренном техническом прогрессе. В технологическом обществе не только растет зависимость от программных и инфраструктурных киберобъектов, но и накапливается уровень неопределенности, порождаемый неустраненными и/или неустранимыми ошибками, заложенными на непредсказуемом уровне структуры. Соответственно, рост совокупного объема применения цифровых технологий, внедрение их в новых сферах, усложнение инфраструктуры неизбежно ведут к понижению уровня совокупной надежности информационных систем. В результате даже незначительный технический сбой на одном из узлов инфраструктуры потенциально способен инициировать распространяющийся в сети каскад вторичных сбоев и отказов, парализующий целые сектора инфосферы. Для политических систем эта ситуация была описана А. Даллесом как «эффект домино».

Если прибавить к этому возможность непредсказуемого агрессивного воздействия на систему (не обязательно кибернетического по своей природе), то мы опять-таки увидим, что высокотехнологическое общество, не выработавшие (ввиду ограниченности времени на адаптацию к новым реалиям) механизмы устойчивой защиты, опять-таки оказывается более уязвимым[41]. При этом новейшая история уже знает эпизоды, в которых возникновение техногенных катастроф приписывается кибератакам враждебных государств. В большинстве случаев специалисты оценивают подобные версии как очередную «теорию заговора». К примеру, вызванные ураганными ветрами массовые отключения электросетей на Восточном побережье США в 2011 г. в ряде СМИ были названы результатом атаки китайских хакеров. Однако в 2015 г. компания Lloyds и Кембриджский университет провели исследование, пока-

[41] См., напр., описанную по приведенной ссылке ситуацию с неспособностью системы ПРО США отразить ракетную атаку, возникшей в результате не-

завшее, что такая атака принципиально возможна и может нанести экономике США ущерб порядка 1 трлн долларов[42]. В результате эмоциональное напряжение вокруг темы кибератак возрастает, что повышает (за счет человеческого фактора) опасность ложной интерпретации тех или иных катастрофических событий как последствий кибератаки на официальном уровне и, соответственно, повышает угрозу ответного удара как минимум средствами кибероружия. Если учесть, что, несмотря на все усилия по контролю за потенциальным применением традиционного ОМП, история холодной войны знает несколько эпизодов, когда несуществующая угроза интерпретировалась как реальная (с готовностью пустить в ход ответные меры), то следует признать возможность эскалации несуществующего конфликта в киберсфере и начала тотальной кибервойны на основании ошибочной оценки ситуации вполне вероятным сценарием.

Наконец, удаленный, распределенный, анонимный и виртуализованный характер кибератаки дает агрессору ощущение дешевого могущества и безнаказанности, провоцируя на удар там, где в другой ситуации он оценил бы сопутствующий риск как неприемлемый. При этом государства, принимающие участие в нескольких военных и/или политических конфликтах (причем ввиду высокой инерционности социума не обязательно одновременно), могут оказаться под ударом в непредсказуемый момент и стать жертвой неизвестного противника. Работает принцип кумулятивности рисков, тем более что доступность и поддержанная информационным полем опасность кибероружия в последние десятилетия может актуализировать даже давно забытые конфликты.

Стоит, однако, отметить, что на практике киберугроза государственного масштаба со стороны международных террористических организаций или террористов-одиночек пока что остается

предсказуемой неработоспособности цифровой системы анализа данных. URL: https://warhead.su/2018/01/21/ne-propatchili-kak-odin-malenkiy-bag-ugrobil-28-amerikantsev (дата обращения: 25.08.2018).

[42] См. URL: https://threatpost.ru/kiberataka-na-elektroset-ssha-mozhet-stoit-strane-1-trln/9701/ (дата обращения: 25.08.2018).

материалом для сетевых дискуссий и голливудских блокбастеров. Исключения могут касаться шпионажа, DDoS-атак, а также актов кибервандализма или информационного хулиганства вроде ложных сообщений о минировании с помощью интернет-телефонии[43] — действия, способные доставить государству определенные неприятности, но на данный момент по результатам малозначительные и в большинстве случаев не вызывающие неустранимых тяжких последствий. В реальности основными субъектами столкновений в киберпространстве, по-видимому, остаются игроки уровня государств или крупнейших частных корпораций, способные собрать и финансировать квалифицированную команду специалистов и обеспечить ей физическую безопасность от ответного удара традиционными средствами. Среди таких игроков, как правило, называют США, КНР, Британию, Россию, Германию, Израиль, Северную и Южную Корею. Эти государства в последние несколько лет объявили о создании в структуре собственных ВС и/или спецслужб специализированных кибервоенных подразделений.

США

Изначально США обладают исключительными преимуществами в кибервоенной сфере, что определяется как финансовыми возможностями государства, так и особой ролью американских компаний в формировании современной техно- и инфосферы. До настоящего момента не оспаривается доминирование американских компаний (таких, как CISCO, Intel, AMD, Microsoft, Apple, Google, AOL, EBay и др.) в различных сферах IT-рынка, от создания технической инфраструктуры и стандартов до пользовательских программ и устройств, кроме, возможно, рынка мобильных цифровых технологий. В свою очередь, это дает американским службам, работающим в сфере кибервоенных действий и кибербезопасности, режим наибольшего благоприятствования в киберпространстве. При этом все остальные игроки инфосферы в большей или меньшей степени оказываются в зависимости от американских технологий

[43] См., напр., https://ria.ru/trend/mass-calls-mining-buildings-russia-13092017/ (дата обращения: 25.08.2018)

и спроектированных в США программ и техники. Собственно Интернет в его нынешнем виде стартовал в США как научно-оборонный проект. Хотя управление Интернетом с 1995 г. полностью передано в ведение общественных организаций и во многом децентрализовано, это не мешает появлению конспирологических версий, согласно которому вся Всемирная паутина по-прежнему контролируется ЦРУ, АНБ или иными силовыми структурами американского правительства[44].

США не только были в числе пионеров военного применения компьютерной техники, но и одними из первых осознали возможности непосредственного военного вмешательства в киберсферу. Одно из первых применений спецслужбами США аналога кибероружия против СССР, по свидетельству Томаса Рида, бывшего командующего ВВС США, произошло еще в разгар холодной войны в июне 1982 г. Он рассказывает, как космический аппарат раннего предупреждения США обнаружил огромный взрыв в Западной Сибири. Это был, как оказалось, взрыв на советском газопроводе. Причиной стала активация вредоносной программной закладки в компьютерной системе управления газокомпрессорными станциями, которую советская разведка через ряд подставных фирм третьих стран закупила у канадской фирмы. Центральное разведывательное управление США (ЦРУ), контролируя проведение данной сделки, с помощью соответствующих специалистов провело модификацию программного обеспечения таким образом, чтобы после определенного длительного периода времени его работа привела к резкому увеличению скорости газового компрессора и повышению давления, выходящего далеко за пределы допустимого для сварных швов в местах сочленения труб газопровода с одновременным отключением датчиков контроля давления. В результате, по заявлению Т. Рида, произошли наиболее крупные неядерный взрыв и пожар, когда-либо до этого наблюдавшиеся с космической орбиты[45]. Факт подобной катастрофы никогда не подтверждался отечественными специали-

---

[44] См., напр., *Овчинский В., Ларина Е.* Указ. соч.

[45] *Reed T. C.* At the Abyss: An Insider's History of the Cold War. Novato, Calif. 2004. 384 p. См. анализ ситуации: *Захматов В. Д., Глушкова В. В., Кряжич О. А.*

стами профильных организаций, а возможность ее организации ставится под сомнение независимыми экспертами (прежде всего потому, что большинство газопроводов и в СССР, и в США на тот момент управлялись в ручном режиме и не предполагали использования автоматизированных, тем более компьютеризированных, систем управления), однако даже если эта история не соответствует действительности, ее появление свидетельствует как минимум о том, что американские спецслужбы уже в 80-е гг. (или ранее) прорабатывали подобные сценарии использования кибероружия в секретных операциях.

В 2000 г. Джон Серабьян, редактор издания «Информационные операции» Центрального разведывательного управления США, в своей речи на заседании объединенного комитета конгресса по экономике, посвященном киберугрозам, заявил, что ЦРУ «…отмечает появление с возрастающей частотой у многих зарубежных государств доктрин и программ развития форм и способов веления специальных наступательных операций в киберпространстве». По ходу выступления он подчеркнул, что государства, разрабатывающие киберпрограммы, «признали особую значимость атак на компьютерные системы противника как военного, так и общегражданского назначения»[46].

Первым шагом в направлении разработки стратегии кибервойны стало подписание летом 2002 г. президентом Дж. Бушем директивы по национальной безопасности NSPD16, в которой он потребовал разработки национальной политики и порядка действий при использовании киберпространства как сферы противоборства. В директиве отмечалась необходимость «подготовки правительством руководства национального уровня по политике США в сфере проведения кибератак в отношении своих противников»[47].

Взрыв, которого… не было! URL: http://ogas.kiev.ua/perspective/vzryv-kotorogo-ne-bylo-581 (дата обращения: 25.08.2018).

[46] Цит. по: *Паршин С. А., Горбачев Ю. К., Кожанов Ю. А.* Кибервойны — реальная угроза национальной безопасности? М., 2011. С. 31.

[47] National Security Presidential Directive 16: [To Develop Guidelines for Offensive Cyber-Warfare]. 20 July 2002 // G. Bradley Bush Orders Guidelines for Cyber-Warfare. Wash. Post. Feb. 7, 2003, at A01. URL: https://web.stanford.edu/class/

А уже 14 февраля 2003 г. Дж. Буш подписал «Национальную стратегию по защите киберпространства», которая фактически явилась первой инициативой, определившей необходимость координации и сосредоточения усилий всех учреждений США по обеспечению защиты киберпространства на федеральном, военном и местном уровнях. В документе кибербезопасность национальной информационно-коммуникационной инфраструктуры была отнесена к сфере ответственности министерства внутренней безопасности. В нем, наряду с рядом других инициатив, органам государственного управления предписывалось «усилить координацию в реагировании на кибератаки в рамках национального разведывательного сообщества и органов обеспечения внутренней безопасности». Этот документ особо подчеркнул, что США оставляют за собой право реагировать «соответствующим образом», если страна подвергнется компьютерной атаке, и эта реакция может повлечь применение Соединенными Штатами кибероружия.

Как следствие, чуть позже в том же году Министерство обороны опубликовало документ под назнанием «Дорожная карта информационных операций» (Information Operations Roadmap). В нем министр обороны, в частности, отметил, что «дорожная карта олицетворяет собой очередной пример приверженности министерства к трансформации наших военных возможностей с целью соответствия перспективным угрозам и использованию новых возможностей, предоставляемых инновациями и быстро развивающимися информационными технологиями»[48]. В этой публикации подчеркивается, что сети являются оперативными центрами тяжести, и МО должно быть подготовлено к «борьбе с сетями» как основными элементами системы управления.

Директива Министерства обороны США D-3600.1 от 14 августа 2006 г. впервые четко определила основные задачи и функции

---

msande91si/www-spr04/readings/week5/bush_guidelines.html (дата обращения: 25.08.2018).

[48] См.: Information Operations: Doctrine, Tactics, Techniques, and Procedures. URL: http://www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.pdf (дата обращения: 25.08.2018).

информационных операций, в целом означающие комплексное применение сил и средств: радиоэлектронной войны, операций в компьютерных сетях, психологических операций, военной дезинформации и оперативной безопасности. Данная директива также сформулировала политику МО США в области проведения информационных операций — «они должны применяться в целях обеспечения завоевания всестороннего и всеобъемлющего превосходства (full spectrum dominance) за счет реализации превосходства в перспективных технологиях, поддержания стратегического доминирования США в информационных технологиях и извлечения выгоды от близкого к реальному времени глобального распространения информации для воздействии на систему управления противника и его цикл подготовки и принятия решений, все, что должно обеспечить завоевание и удержание Соединенными Штатами информационного превосходства»[49]. Кроме того, как требует директива, информационные операции «…должны разрабатываться таким образом, чтобы они могли проводиться согласованно с применением различных основных, обеспечивающих, поддерживающих и разведывательных сил с целью формирования и полной реализации боевого потенциала ВС»[50].

К силам информационных операций (ИО) в уставе JP 3–13 2006 г. отнесены:

— силы, составляющие ядро ИО: радиоэлектронная война (EW), психологические операции (PSYOP), военная дезинформация (MILDEC), оперативная безопасность (OPSEC) и операции в компьютерных сетях (CNO). Из этих сил три — PSYOP, OPSEC и MILDEC — играют главную роль в операциях ВС многих государств. Интегрированные боевые возможности основных сил, объединенных с боевыми возможностями сил обеспечения ИО

[49] The National Strategy to Secure Cyberspace. February 2003. URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (дата обращения: 25.08.2018).

[50] Цит. по: *Корсаков Г. Б.* Роль информационного оружия в военно-политической стратегии США // США и Канада: экономика, политика, культура. 2012. URL: http://naukarus.com/rol-informatsionnogo-oruzhiya-v-voenno-politicheskoy-strategii-ssha (дата обращения: 25.08.2018).

и сил, связанных с проведением ИО, должны обеспечить ВС США возможность значительного влияния на противника и успешных действий в складывающейся информационной и оперативной обстановке;

— силы и мероприятия обеспечения ИО: «информационная устойчивость» (Information Assurance — IA), «физическая безопасность» (Physical Security — PhS), «физическое (огневое) воздействие» (Physical Attack — PhA), контрразведка (Counterintelligence — Cl); «сбор и использование данных от подвижных и неподвижных систем и средств видовой разведки объединенных сил (ОС) США в районе боевых действий» (Combat Camera — COMCAM). Силы и мероприятия, обеспечивающие ИО, непосредственно или косвенно влияют на характер и содержание информационной обстановки и способствуют повышению эффективности ИО. Они должны быть тесно увязаны, интегрированы и скоординированы с применением сил, составляющих ядро ИО. Эти силы и мероприятия могут быть также использованы в интересах достижения других более широких целей для обеспечения боевых действий ВС США;

— силы и мероприятия, связанные с проведением ИО: «Связь с общественностью (Public Affairs — PA), „Гражданско-военные операции“ (Civil-Military Operations — CMO), „Поддержка органами МО публичной дипломатии» (Defense Support to Public Diplomacy — DSPD). Основная цель их применения не должна быть поглощена только целью ИО. По этой причине органы PA, CMO и DSPD обязаны выполнять свои задачи в тесном сотрудничестве и при тщательной координации совместных действий со штабными органами планирования ИО в военной операции.

23 июня 2009 г. министр обороны США Р. Гейтс приказал командующему Стратегического командования США К. Чилтону создать Кибернетическое командование — USCYBERCOM. В мае 2009 г. командующий Кибернетическим командованием генерал К. Александер изложил свои взгляды в докладе для подкомитета по вооруженным силам Палаты представителей Конгресса, в котором отметил, что США необходимо реорганизовать свои наступательные и оборонительные кибероперации, для чего потребуется больше ресурсов и профессиональной подготовки. Питер Вуд, исполнитель-

ный директор First Base Technologies LLP и эксперт в кибервойнах, заявил, что США полностью вправе защитить себя: «Мое личное мнение таково, что единственный способ противостоять как криминальной, так и шпионской онлайновой деятельности — быть проактивным. Если США примет формальный подход к этому — это хорошо. Китайцы рассматриваются как источник многих атак на западные технологические инфраструктуры, в частности, недавнюю атаку на сети электропередач в США. Если это будет признано организованным нападением, я хотел бы обнаружить и ликвидировать источник этих атак. Единственная проблема в том, что Интернет, по самой своей природе, не имеет границ, и если США надевают на себя мантию „глобального полицейского", это не дает возможности заходить на нужную глубину»[51].

Киберкомандование США начало функционировать 21 мая 2010 г., и достигло полной оперативной готовности 31 октября 2010 г. Киберкомандование объединило под своим началом несколько ранее существовавших организаций, в частности Соединение глобальных сетевых операций (JTF-GNO) и Объединенное командование сетевой войны (JFCC-NW). Агентство военных информационных систем — подразделение JTF-GNO — было переведено в штаб-квартиру Киберкомандования в Форт-Миде. Министр обороны США Эштон Картер 6 апреля 2016 г. дал «первое задание военного времени» киберкомандованию Пентагона атаковать Исламское государство (ИГ)[52] с целью не позволить командованию ИГ планировать и руководить операциями, а также нарушить финансирование структур ИГ, в определенном смысле это можно считать первым официально объявленным актом кибервойны. Наконец, 2 августа 2017 г. президент США Дональд Трамп своим указом присвоил Киберкомандованию статус единого боевого командования, что означает его формальную независимость от других родов войск, высокую самостоятельность действий и прямое подчинение Единому стратегическому командованию США.

---

[51] См.: URL: http://news.bbc.co.uk/2/hi/technology/8033440.stm (дата обращения: 25.08.2018).

[52] Запрещена в России.

В 2011 г. Министерством обороны США была принята Стратегия операций в киберпространстве (The 2011 U. S. Department of Defense Strategy for Operating in Cyberspace), содержащая оценку проблем и возможностей, возникающих в связи с ростом значения информационных технологий для военных, разведывательных операций и бизнеса. Полный текст документа объемом в 40 страниц засекречен, в июле 2011 г. был опубликован для широкого доступа его 19-страничный релиз, где описан стратегический контекст и пять «Стратегических инициатив», описывающих миссию Пентагона в киберпространстве. К числу этих миссий относятся:

«1) использовать киберпространство в качестве оперативного пространства, организовать его оснащение и тренировки персонала так, чтобы министерство обороны могло в полной мере воспользоваться потенциалом киберпространства;

2) применять новые концепции защиты для защиты компьютерных сетей и систем министерства обороны;

3) партнерство с другими американскими правительственными ведомствами и учреждениями и частным сектором в интересах общенациональной стратегии кибербезопасности;

4) выстроить надежные отношения с союзниками США и другими международными партнерами в целях усиления общей кибербезопасности»;

5) увеличить изобретательность нации благодаря высокому профессионализму кадров и быстрым технологическим инновациям»[53].

По оценке Ли Шушэня, научного сотрудника Академии военных наук КНР, доктрина является «принципиальной попыткой США сохранить свое беспрецедентное глобальное военное превосходство». Ли отметил, что стратегия «явно направлена на суверенные государства в качестве объектов кибератак». Согласно оценке президента Пекинского университета почты и телекоммуникаций Фан Бинсиня, США «делают акцент на наступательную, а не оборонительную сторону кибервойны», и, следовательно, могут «достигать своих

[53] Department of Defense Strategy for operating in Cyberspace: July 2011. URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (дата обращения: 25.08.2018).

политических и военных цели, в том числе осуществлять вмешательство во внутренние дела других стран и военное вторжение, путем использования технологических возможностей Интернета»[54]. Новостной ресурс CRN News.com привел мнения ряда американских экспертов в области кибербезопасности, которые считают, что опубликованная стратегия «слишком расплывчата, ресурсно не обеспечена и, по-видимому, не будет гарантировать немедленного будущего всплеска»[55]. Кроме того, эксперты по безопасности расценивают планы Пентагона по привлечению ИТ-специалистов из частного сектора как фактор риска для общенационального технологического развития.

В марте 2013 г. глава АНБ и Киберкомандования США генерал Кейт Александер, отвечая на вопросы в Конгрессе, провозглашал, что американская «доктрина кибернаступления требует глубокого, постоянного и повсеместного присутствия в сетях противников, чтобы в нужный момент добиться максимального эффекта <…> Непревзойденный эффект по поражению систем противника будет достигнут за счет американского технологического и эксплуатационного превосходства» в сфере информационных технологий. Выступление Александера завершалось утверждением: «Мы уверены, что наша кибероборона является лучшей в мире»[56]. В конце апреля того же года американская пресса сообщила, что в январе 2013 г. хакеры сумели получить доступ к Национальному реестру плотин — закрытой базе данных, которую ведет Инженерный корпус армии США. Эта база данных содержит информацию о 79 000 плотинах на территории Америки. В ней указываются слабые места плотин,

---

[54] US cyber strategy dangerous: Chinese experts / ChinaDaily — USA. 2011–06–02. URL: http://usa.chinadaily.com.cn/china/2011-06/02/content_12632609.htm (дата обращения: 25.08.2018).

[55] *Hoffman S.* Partners Wary Of DoD Cyber Security Plan. URL: https://www.crn.com/news/security/231002371/partners-wary-of-dod-cyber-security-plan.htm (дата обращения: 25.08.2018).

[56] Statement of general Keith B. Alexander commander United States Cyber Command before the Senate Committee on armed services 12 march 2013. URL: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-091.pdf (дата обращения: 25.08.2018).

оценка количества погибших в случае прорыва и прочие важные данные[57]. При этом проникновение на сервер с информацией произошло в январе, а было обнаружено только в конце апреля. В том же году хакеры получили доступ к суперкомпьютеру в Национальной лаборатории имени Лоуренса в Беркли, на тот момент одному из самых мощных в мире; при этом, поскольку суперкомпьютеры АНБ и Министерства энергетики увязаны в единую общеамериканскую сеть, «глубина проникновения» расширяется еще больше. Действия взломщика, которым оказался Э. Миллер, не были замечены службами безопасности — факт взлома был установлен, когда хакер начал продавать аренду на доступ к суперкомпьютеру, причем только по показаниям другого хакера, который заключил сделку со следствием. В ноябре 2013 г. на слушаниях в Конгрессе США Майкл Роджерс, глава Комитета по разведке, оценил общие потери от китайского экономического кибершпионажа, связанные с хищением интеллектуальной собственности, в сумму порядка 150 млрд долларов, при этом подтвердив, что китайским кибершпионам удалось похитить научно-техническую документацию по ряду особо секретных военно-технологических разработок[58]. Таким образом, несмотря на высокий уровень военно-организационной проработки, финансового и технологического обеспечения кибервойн, говорить о безусловном доминировании США в киберпространстве не приходится.

После корректировки матрицы угроз по ведению операций в киберпространстве, на основании которой производилась оценка кибервозможностей свыше 175 стран и организаций, фирмой Technology for Solutionary был составлен перечень десяти наиболее угрозообразующих из них:

1. Китай.
2. Коммерческая сеть РФ RBN (Russian Business Network).
3. Иран.
4. Сети связи России, имеющие непосредственное подключение к сетям Франции.

---

[57] См., напр., информацию на сайте SecurityLab. URL: https://www.securitylab.ru/news/440120.php.

[58] См.: *Овчинский В., Ларина Е.* Указ. соч.

5. Экстремистские/террористические группы.
6. Израиль.
7. КНДР.
8. Япония.
9. Турция.
10. Пакистан[59].

Одним из уникальных характеристик кибероружия является его способность к применению из любой точки мира. Компьютеры, физически находящиеся в других странах, могут быть скомпрометированы и использованы как платформы для инициализации кибератаки. Поэтому экспертно-технические возможности по расследованию должны быть сформированы таким образом, чтобы можно было не просто отслеживать эту атаку до точки ее возникновения, но и выявлять заинтересованную сторону, стоящую за данной атакой.

В этой связи большие надежды возлагаются на недавно появившуюся концепцию цифровой ДНК (digital DNA), которая должна помочь в формировании таких критических возможностей. Большинство кибератак не попадают под доказательную юридическую базу, которая могла бы быть использована для оценки намерений и возможностей атакующего и обеспечить вскрытие конкретных организаций или иных структур, стоящих за атакой. Поэтому с целью формирования цифровой ДНК в отношении всех ранее имевших место атак должны быть собраны существенные улики о технике, характеристиках кибероружия и методиках действий, использованных в этих кибератаках.

Данные улики должны быть отработаны и внедрены в практику ведения разведки в киберпространстве. Глубокий анализ этих улик позволит описать «цифровую ДНК», что может помочь в определении источника вредоносного кода. Основа для проведения юридического киберрасследования представлена идентификатором ASDF.

---

[59] См., напр.: *Давыдов В. Н.* Глобальные угрозы информационного общества // Противодействие терроризму: Проблемы XXI века : информ.-аналит. и науч.-практ. журнал, 2012. URL: https://stategovernor.admhmao.ru/upload/iblock/47e/counter_terrorism_2012_3.pdf (дата обращения: 25.08.2018).

Идентификатор ASDF состоит из четырех наборов характеристик «цифровой ДНК», необходимых для установления критических характеристик вредоносного кода, использованного для атаки:

A = attributes (свойства), abilities (способности), architecture (архитектура), assembly (сборка), adaptation (адаптивность);

S = style (стиль), signatures (сигнатуры), syntax (синтаксис), structure (структура), source (источник), specifications (технические характеристики), scope (предназначение);

D = demographics (демографические данные), delivery (доставка), development (разработка), discipline (дисциплинированность), data (данные), design (модель);

F = functions (функции), features (характерные черты), faults (недостатки), formidability (уровень угрозы), fields (сферы применения), form (тип), factors (факторы).

Именно определяющая информация, содержащаяся в «цифровой ДНК», должна стать основой для начала политической акции и даже непосредственного военного реагирования. Улики в виде цифровой ДНК должны формировать юридическую доказательную базу такого уровня достоверности, чтобы не оставалось никаких сомнений в источнике происхождения киберугрозы. На сегодняшний день в США примерно 7 000 сотрудников заняты в сфере борьбы с киберпреступностью, исследовании и анализе кибератак и контрразведке. Следует иметь в виду, что данное понимание термина «цифровая ДНК» не является общепринятым и может встретиться в иных значениях.

Утверждение о том, что силовые структуры США в настоящее время разворачивают системы разведовательных и наступательных кибервооружений в информационных сетях по всему миру (что фактически является первой фазой необъявленной кибервойны), основано на анализе обнаруженных службами кибербезопасности системных угроз. Так, в 2013 г. компания «Лаборатория Касперского» проанализировала функционал кибервоенной платформы Flame. По словам эксперта компании Александра Гостева, «Flame — это троянская программа, бекдор, имеющая также черты, свойственные червям и позволяющие ей распространяться по локальной сети и через съемные носители при получении соответствующего приказа

от ее хозяина. По размеру Flame почти в 20 раз больше атаковавшего атомный проект Ирана червя Stuxnet и включает в себя много различных функций для проведения атак и кибершпионажа. <…> Flame — это большой набор инструментов, состоящий более чем из 20 модулей. Назначение большинства связано с тестированием уязвимостей, обеспечением проникновения и его маскировкой, поддержанием долговременного доступа в закрытую сеть через уязвимости, снятием разнообразных типов информации и кражей файлов из сети или аппаратного средства и, наконец, с разрушением и/или перехватом управления физическими объектами и сетями. По наблюдениям экспертов в сфере кибербезопасности, хозяева Flame искусственно поддерживают количество зараженных систем на некоем постоянном уровне. Это можно сравнить с последовательной обработкой полей: они заражают несколько десятков узлов, затем проводят анализ данных, взятых на компьютерах жертв, деинсталируют Flame из систем, которые им неинтересны, и оставляют в наиболее важных, после чего начинают новую серию заражений»[60].

Благодаря опубликованному в газете Washington Post от 30.08.2013 г. материалу, основывающемуся на разоблачениях Э. Сноудена, достоянием общественности стали сведения о разработке американскими спецслужбами программы GENIE, позволяющей сотрудникам киберразведовательных структур США проникать в зарубежные информационные сети и ставить их под негласный контроль. В бюджетных документах указано, что 652 млн долларов было потрачено на разработку и использование «секретных имплантатов» (сложных многофункциональных вредоносных программ), при помощи которых ежегодно инфицируются десятки тысяч компьютеров, серверов, маршрутизаторов и т. п. по всему миру. По результатам реализации программы на конец 2013 г. было заражено как минимум 85 тыс. устройств по всему миру. При этом невозможность тотального контроля определяется исключительно необходимостью использовать человека-оператора для получения удаленного контроля

[60] *Гостев А.* Flame: что известно на данный момент // Информационная безопасность. Блог компании «Лаборатория Касперского». URL: https://habr.com/company/kaspersky/blog/144967/ (дата обращения: 25.08.2018).

над зараженным компьютером: в результате по состоянию на 2011 г. 1 870 сотрудников проекта GENIE могли полноценно использовать порядка 10 % из 68 975 инфицированных машин. В 2013 г. планировался вывод на расчетную мощность автоматизированной системы под кодовым названием TURBINE, которая должна одновременно управлять миллионами имплантатов, что должно было гарантировать возможности сбора разведывательной информации и осуществления активных атак вплоть до разрушения и/или перехвата управления над материальными объектами и сетями по всему миру. Эти свидетельства подтверждаются данными хакерской группы Shadow Brokers, указывающими на реализацию структурами АНБ комплексной кибервоенной системы BADDECISION, объединяющей предыдущие разработки в этом направлении[61].

Опубликованные в рамках пакета документов из досье Э. Сноудена бюджетные документы ЦРУ продемонстрировали активную вовлеченность этой организации в наступательные кибероперации. Согласно своему уставу, ЦРУ является единственным органом, уполномоченным законно осуществлять и контролировать тайные операции по указанию президента США, вербовать агентов, привлекать для тайного сотрудничества сторонние организации. Одновременно поступает информация о систематических закупках эксплойтов и бекдоров, которые АНБ проводит на так называемом «сером» рынке хакерского софта. Таким образом, уже сейчас американские спецслужбы способны проводить против любого объекта в мире «частные» кибервоенные действия, формально не связанные с правительством США, используя при этом профинансированные из американского бюджета, но опять-таки формально не связанные с какими-либо действиями или разработками официальных структур системы кибервооружений. Фактически это означает, что кибервоенная активность США абсолютно бесконтрольна и по факту безответственна. Более того, для проведения кибератак могут использоваться уязвимости, обнаруженные государственными

[61] См., напр., Документы Сноудена подтверждают достоверность данных Shadow Brokers // Блог компании ESET NOD32. 20 августа 2016. URL: https://habr.com/company/eset/blog/308150/ (дата обращения: 25.08.2018).

и частными компаниями в рамках вполне легальной деятельности по обеспечению информационной безопасности, но не устраненные по прямому указанию американских спецслужб[62].

«Совокупность фактов и сведений позволяет ряду аналитиков утверждать, что кибервойна США против остального мира, и в первую очередь Китая, России и Ирана, уже началась. Пока она находится на первой стадии эскалации, а именно в фазе тотального шпионажа, обнаружения множественных уязвимостей и внедрения в них программ-имплантатов многоцелевого применения. Причем в любой момент начальная фаза неопознанной войны может по сигналу оператора быть переведена в фазу разрушительных в прямом физическом смысле этого слова военных действий. Поскольку кибервоенная доктрина США изначально сформулирована как наступательная и предполагает активные меры по обеспечению и сохранению доминирования США в военной, технической, политической и экономической сферах, эти выводы следует оценивать как вполне вероятные»[63]. При этом стоит отметить, что важным аспектом кибервойн американские военные специалисты полагают их нелетальный характер, а основной целью «информационных операций» провозглашают победу с минимальными издержками как для своей стороны, так и для мирного населения страны-противника: «целью любой военной операции (боевых действий) должно стать не физическое уничтожение противника, разрушение его военной инфраструктуры, уничтожение военной техники и личного состава, а принуждение его сложить оружие и прекратить сопротивление»[64].

КНР

Если США изначально — центр научных и технических разработок в сфере кибертехнологий, то КНР в большинстве высокотехнологических отраслей — центр массового производства, в том числе продукции под американскими брендами. При этом на дан-

---

[62] См., напр., *Харрис Ш.* Кибервойн@: пятый театр военных действий.

[63] *Овчинский В., Ларина Е.* Указ. соч. С. 40–41.

[64] *Давыдов Д.* Развитие кибервойск США до 2020 г. URL: https://tinyurl.com/y8g8q47e (дата обращения: 25.08.2018)

ный момент Китай не только более или менее успешно копирует чужие технологии, в том числе с использованием технологического шпионажа. Уже сейчас именно Китай является одним из ключевых центров в ряде передовых разработок, например, в вопросах беспроводной стационарной и мобильной связи четвертого и пятого поколений — технологий, напрямую связанных с перспективами тотальной информатизации общества. По ряду ключевых технологических показателей (например, количество и мощность суперкомпьютеров, применяемых в военной, научной и экономической сфере) КНР борется с США за первое место (в рейтинге топ-500 на ноябрь 2018 г. этим странам принадлежит, соответственно, 227-я и 109-я позиция при постоянном наращивании Китаем количественного превосходства, с сохранением конкуренции за звание текущего лидера мощности) и многократно обходит Россию (4 позиции в том же рейтинге, 79-е место у наиболее производительного из российских компьютеров «Ломоносов-2»)[65].

По оценкам экспертов в сфере информационной безопасности и кибервойн, именно в составе Народно-освободительной армии Китая (НОАК) на сегодняшний день сформированы лучшие в мире кибервойска. Китай, проигрывая США в сфере традиционных и ядерных вооружений, сделал ставку на «асимметричное сдерживание», в частности вкладывая значительные средства в развитие кибервойск. В качестве концептуальной идеи формирования перспективного облика вооруженных сил и обеспечения национальной безопасности в КНР принята концепция интегрированной электронно-сетевой войны (INEW — Integrated Network-Electronic Warfare)[66]. Эта концепция стала отражением идеи использования «исторического шанса» для Китая, то есть идеи, приведшей к созданию «теории перешагивания» (*куаюэ лунь*), обосновывающей возможность для НОАК перешагнуть в эпоху войн нового поколения, сконцентриро-

[65] См.: Top500: The list: November 2018. URL: https://www.top500.org/lists/2018/11/ (дата обращения: 18.11.2018).

[66] См. напр.: *Deepak Sharma.* Integrated Network Electronic Warfare: China's New Concept of Information Warfare. URL: https://idsa.in/system/files/jds_4_2_dsharma.pdf (дата обращения: 25.08.2018).

вавшись на создании и принятии на вооружение передовых образцов оружия и военной техники, в первую очередь созданных с использованием современных информационных технологий. В итоге КНР удалось создать на сегодняшний день наиболее эшелонированную и мощную кибероборону страны, одновременно развивая наступательные кибервооружения. В этой связи в большинстве публикаций военной науки Китая уделяется самое пристальное внимание развитию национальной концепции информационной войны, определению ее основного содержания, целей и задач, форм и способов ее ведения, используемых сил, средств и ресурсов, а также разработке планов создания формирований видов вооруженных сил, способных вести эффективные боевые действия в новых условиях, поскольку информационная война рассматривается китайскими военными аналитиками как исключительная возможность для существенного повышения боевого потенциала НОАК на основе современных информационных технологий.

Становление китайских средств кибербезопасности осуществляется в соответствии с Национальной стратегией инновационного развития, принятой Госсоветом КНФ как «Основы государственного плана среднесрочного и долгосрочного развития науки и техники на 2006–2020 гг.» и включающей вопросы использования цифровых и компьютерных технологий для обеспечения национальной безопасности. Их становлению и развитию был посвящен, например, специальный доклад ASPI (Australian Strategic Policy Institute, Австралийский институт стратегической политики) «Enter the Cyber Dragon» (июнь 2013 г.)[67].

Силы кибероперациий КНР подчинены 3-му и 4-му управлениям Генштаба НОАК, ответственным, соответственно, за безпасность систем связи и за РЭБ и ведение кибервойны. Среди подчиненных им кибервоенных структур чаще всего называется «Подразделение 61398» (кит. 61398 部队), или «2-е бюро» — подразделение На-

[67] См.: *Feakin T.* Special Report — Enter the Cyber Dragon: Understanding Chinese intelligence agencies' cyber capabilities. URL: https://www.aspi.org.au/report/special-report-enter-cyber-dragon-understanding-chinese-intelligence-agencies-cyber (дата обращения: 25.08.2018).

родно-освободительной армии Китая, базирующееся в Шанхае и отвечающее за проведение военных операций в области компьютерных сетей против США и Канады, а также «Подразделение 61046», или «8-е бюро», работающее на европейском направлении. В докладе, опубликованном 18 февраля 2013 г., компания Mandiant, оказывающая услуги в сфере компьютерной безопасности, обвинила это подразделение в ведении с 2006 г. масштабного кибершпионажа, прежде всего против компаний и организаций англоязычных стран[68]. В мае 2014 г. Федеральное Большое жюри США предъявило пяти офицерам Подразделения 61398 обвинения в краже конфиденциальной деловой информации у американских компаний и заражении их компьютерных сетей вредоносными программами[69].

Киберподразделения НОАК тесно взаимодействуют с негосударственными структурами, например, с так называемым «Альянсом красных хакеров» (Red Hacker Alliance). «RHA является своего рода неформальной, но управляемой государством сетью хакеров, включающую десятки тысяч хакеров из Китая и других стран, в основном из китайской диаспоры по всему миру»[70].

Параллельно с активными действиями киберразведки китайские кибервоенные структуры осваивают более сложные приемы кибервойны, например использование сложных платформ типа многофункциональных троянов. В частности, такие технологии использовались в сентябре 2010 г. в атаке на австралийские правительственные сети, в январе 2012 г. применялись против европейского военного авиакосмического агентства и серверов компании ASC. Предполагалась причастность RHA к размещению системы бекдоров в сетях компании RSA — производителе электронных ключей безопасности в марте 2011 г. и в сетях индийских правительствен-

---

[68] Forrester: FireEye Named the Leader in External Threat Intelligence Services. URL: https://www.fireeye.com/current-threats/threat-intelligence-reports.html (дата обращения: 25.08.2018).

[69] См.: *Finkle J., Menn J., Viswanatha A.* U.S. accuses China of cyber spying on American companies // Reuters: November 21, 2014. URL: https://www.reuters.com/article/us-cybercrime-usa-china/u-s-accuses-china-of-cyber-spying-on-american-companies-idUSKCN0J42M520141120 (дата обращения: 25.08.2018).

[70] *Овчинский В., Ларина Е.* Указ. соч. С. 42.

ных аэрокосмических предприятий в сентябре 2012 г.[71] В результате, предположительно, китайским хакерам удалось проникнуть в корпоративные сети Lockheed Martin, Northrop Groumman и IBM и получить стратегически важную научно-техническую и технологическую документацию, касающуюся военных разработок[72].

Документы, ставшие доступными широкой общественности после утечки дипломатических источников США 2010 года, содержат опасения американских специалистов, что Китай использует доступ к исходному коду программных продуктов компании Microsoft и организует «утечку мозгов из частного сектора» в целях повышения военного потенциала страны[73].

Джейсон Фриц в статье 2008 г. утверждает, что китайское правительство с 1995 по 2008 г. было замешано в ряде громких скандалов, связанных со шпионажем и использованием в целях шпионажа «децентрализованной сети студентов, бизнесменов, ученых, дипломатов и инженеров из китайской диаспоры»[74]. Перебежчик из китайских спецслужб, сдавшийся властям Бельгии, заявил, что промышленный шпионаж в странах Европы ведут сотни агентов КНР, а бывший китайский дипломат Чэнь Юнлинь сказал, что в Австралии китайских агентов порядка тысячи. В 2007 г. высокопоставленный российский чиновник был приговорен к 11 годам заключения за передачу Китаю информации о ракетно-космической технике. Шпионаж Китая в США преследует такие цели, как «программы аэрокосмической промышленности, дизайн космического челнока, высокопроизводительные компьютеры, конструкции ядерного оружия и крылатых ракет, полупроводниковые приборы и интегральные схемы, а также детали продажи США оружия Тайваню»[75].

---

[71] См., напр.: URL: http://itsec.ru/newstext.php?news_id=79265, http://itsec.ru/newstext.php?news_id=77720.

[72] См., напр.: URL: http://itsec.ru/newstext.php?news_id=77944.

[73] US embassy cables: China uses access to Microsoft source code to help plot cyber warfare, US fears // The Guardian. 04.12.2010.

[74] *Fritz J.* How China will use cyber warfare to leapfrog inmilitary competitiveness // Culture Mandala. The Bulletin of the Centre for East-West Cultural and Economic Studies. Vol. 8, № 1. P. 28–80.

[75] Ibid.

Китайское правительство отрицает свою причастность к кибершпионажу и акциям кибервойн, заявляя, что Китай является не агрессором, а скорее жертвой растущего числа кибератак; в то же время эксперты по компьютерной безопасности возлагают на Китай ответственность за ряд кибератак на ряд государственных учреждений и предприятий в Соединенных Штатах, Индии, России, Канаде и Франции[76].

По оценке Д. Фрица, Китай расширил возможности ведения кибервойн путем приобретения иностранной военной техники, включая «системы космического мониторинга и сбора разведданых, противоспутниковое оружие, антирадары, инфракрасные приманки и генераторы ложных целей»[77], а также наращивает информатизацию своих вооруженных сил путем подготовки «бойцов кибервойск», совершенствования военных информационных сетей, создания виртуальных лабораторий, электронных библиотек и электронных комплексов. Благодаря этому руководство КНР рассчитывает подготовить силы для участия в различного рода военных действий, включая кибервойны.

В новой военной доктрине Китая упоминаются хакерские подразделения и кибероперации. Это первое официальное признание властями факта существования таких отрядов. Упомянуто три типа подразделений:

— специализированные военные силы для сетевой борьбы: призваны вести оборонительные и наступательные операции;

— группы специалистов из гражданских организаций, уполномоченные военным руководством вести сетевые операции. Среди «гражданских организаций» — Министерство государственной безопасности и Министерство общественной безопасности;

---

[76] См.: China to make mastering cyber warfare A priority. Washington, D.C., United States, Washington, D.C.: National Public Radio, 2011 ; см. также свидетельство эксперта «Лаборатории Касперского» А. Гостева об активизации действий китайских кибершпионов на российском направлении (*Холявко А.* «Лаборатория Касперского» назвала мишени китайских хакеров в России // Ведомости. 06 декабря 2017 г.).

[77] Ibid.

— «внешние субъекты», которые могут быть организованы и мобилизованы для сетевых операций[78].

Примером (предположительно) разработанного специалистами НОАК и/или аффилированных с ней гражданских структур КНР может послужить обнаруженный в 2004 г. сотрудниками компании Symantec вирус Myfip. Вирус, как правило, хорошо маскируется, и при его активации в заданный момент времени на недостаточно защищенной компьютерной сети может полностью разрушить файловую систему компьютеров. В ходе одной из таких атак с применением данного вируса специалистам группы экстренного реагирования на чрезвычайные ситуации в компьютерных сетях CERT (Computer Emergency Response Team) в составе центра защиты информационных систем ОСК ВС США удалось установить, что похищенная в ее ходе информация была передана в г. Нанкин в Китае. Этот вид атак способен полностью скомпрометировать всю информационно-коммуникационную систему и обеспечить хищение любого из следующих типов файлов:

.pdf — Adobe Portable Document Format;
.doc — Microsoft Word Document;
.dwg — AutoCAD drawing;
.sch — CirCAD schematic;
.pcb — CirCAD circuit board layout;
dwt — AutoCAD template;
dwf — AutoCAD drawing;
max — ORCAD layout;
.mdb — Microsoft database.

Любая сеть, инфицированная вирусом Myfip, может быть организационно разрушена с потерей документов, планов, связей и баз данных. При этом вся важная информация с указанными типами расширений файлов может быть похищена, а данные на пораженных машинах стерты или дезорганизованы, в результате чего источник атаки установить не удастся.

---

[78] См.: URL: https://xakep.ru/2015/03/19/china-cyberwar/ (дата обращения: 25.08.2018).

За последнее десятилетие обвинения в использовании средств кибервойны Китаю предъявляли США, Канада, Индия, Австралия и Тайвань. Следует отметить, что Правительство КНР отрицает проведение кибероперaций против других стран и, в свою очередь, обвиняет Соединенные Штаты в организации кибервойны против Китая, которую отрицает руководство США. При этом КНР постоянно и целенаправленно прилагает существенные усилия для организации контроля киберпространства внутри страны, что существенно понижает эффективность возможных ответных действий противника в киберсфере. Причем речь идет не только об информационной изоляции китайского сегмента Интернета. Так, за право сохранить доступ к китайскому рынку корпорация Microsoft, отказывающаяся показать свои секретные операционные коды даже своим крупнейшим деловым клиентам в США, передала копию этих кодов китайскому правительству. В результате китайские специалисты модифицировали версию и (легально!) продают внутри страны версию Windows со своими собственными шифровальными кодами. В КНР также разработали собственную операционную систему Kylin, ставшую платформой для программных приложений Народно-освободительной армии Китая.

В сфере обеспечения внутренней безопасности КНР ориентируется на систему жесткого регулирования активности интернет-пользователей. Так, начиная с 1998 г., в стране разрабатывалась программа фильтрации интернет-контента «Золотой щит» (англ. The Golden Shield Project, кит. 金盾工程, jīndùn gōngchéng, неофициальное название — «Великий китайский файрвол»), официально внедренная в 2003 г. Проект ограничивает доступ к ряду иностранных сайтов с территории КНР. Например, страницы, содержащие критическое освещение внутренней политики КНР, освещающие проблемы тибетского и уйгурского сепаратизма, террористическую пропаганду и социально опасный контент, а также ряд религиозных и философских доктрин, в том числе экстремистского толка. Веб-сайты, базирующиеся на территории Китая, не могут ссылаться и публиковать новости, взятые из зарубежных новостных сайтов или СМИ, без специального одобрения. Веб-страницы фильтруются по ключевым словам, связанным с государственной безопасностью,

а также по черному списку адресов сайтов. По свидетельствам очевидцев, тотальность информационного контроля в КНР приводит к столь же тотальному распространению технологий обхода этого контроля, в том числе на аппаратном уровне[79].

27 декабря 2016 г. Китай опубликовал национальную Стратегию по обеспечению безопасности в Интернете. Согласно документу, власти Китая будут добиваться безопасного, открытого, узаконенного киберпространства, которое также должно быть мирным. Кроме этого, правительство КНР будет решительно защищать суверенитет и нацбезопасность страны в киберпространстве, защищать основную информационную инфраструктуру страны, бороться с проявлениями кибертерроризма и преступлениями в Интернете. Отмечается, что будет улучшен механизм управления киберпространством, будет развиваться сотрудничество Китая с другими странами в этой области[80].

1 июня 2017 г. вступил в силу Закон о кибербезопасности КНР, ставящий целью обеспечение «сетевой безопасности, защиты суверенитета киберпространства и национальной безопасности, отстаивания социальных и общественных интересов, защиты законных прав и интересов граждан, юридических лиц и других организаций в целях содействия здоровому развитию информатизации экономики и общества»[81]. Согласно данному закону, государство берет на себя функции центрального регулятора киберрынка и разработчика стандартов взаимодействия сетевых операторов и пользователей. При этом любые формы оказания сетевых услуг предполагают регистрацию с предъявлением удостоверения личности. При этом большое внимание уделяется защите персональных данных пользователя. Вообще предполагается высокий уровень контроля за сетевой активностью пользователей при центральной роли государственных структур и прописанной ответственности отдельных

---

[79] См., напр.: URL: http://jj-tours.ru/articles/china-add/china-internet-block-outflank.html и др. (дата обращения: 25.08.2018).

[80] См.: *Булатов И.* Китай опубликовал стратегию по кибербезопасности. URL: https://ria.ru/world/20161227/1484679179.html (дата обращения: 25.08.2018).

[81] URL: http://tass.ru/mezhdunarodnaya-panorama/4290068 (дата обращения: 25.08.2018).

операторов и провайдеров. «Государство обеспечивает систему мониторинга кибербезопасности, раннего предупреждения и оповещения. Ведомства должны координировать работу правительственных учреждений с целью укрепления интернет-безопасности, сбора информации и анализа, а также уведомлений в соответствии с постановлениями»[82]. Китайские специалисты высоко оценивают данный закон как основу для организованных действий государства и общества, при этом зарубежные эксперты и представители корпораций утверждают, что прописанные в законе избыточные меры контроля могут привести к выходу с китайского рынка ряда крупных высокотехнологических компаний.

Российская Федерация

«Русские хакеры» как основополагающая угроза современному западному миру — новость, систематически озвучиваемая в последние два года, начиная с предвыборной компании в США 2016 г.[83] Предполагается, соответственно, что финансируемые российскими спецслужбами группировки (обычно указывают, например, на хакерские группы Fancy Bear и Cosy Bear[84]) способны преодолевать любую киберзащиту, более или менее успешно похищать засекреченную информацию, напрямую воздействовать на ход процесса голосования и, наконец, активно влиять на сознание западных избирателей. В реальности на фоне упомянутых выше сведений о возможностях американских кибервоенных структур картина выглядит фантасмагорично и в основном является скорее частью информационной войны против РФ, чем фиксацией реального положения дел в киберпространстве. В 2017 г., оценивая кибервоенный потенциал РФ, специалисты по кибербезопасности компании Zecurion Analytics поставили его на 5-е место в мире после США,

---

[82] URL: http://tass.ru/mezhdunarodnaya-panorama/4290068 (дата обращения: 25.08.2018).

[83] См., напр., URL: https://tinyurl.com/y8ebr34g (дата обращения: 25.08.2018).

[84] См., напр.: *Lipton E., Sanger D.E., Shane S.* The Perfect Weapon: How Russian Cyberpower Invaded the U.S. // The New York Times: Dec. 13, 2016. URL: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html (дата обращения: 25.08.2018).

КНР, Британии и КНДР, хотя корректность их оценки ставилась под сомнение[85].

В реальности, несмотря на заметное присутствие компаний и специалистов из РФ на мировом информационном рынке (в том числе и в сфере компьютерной безопасности, например «Лаборатория Касперского»), отставание России в компьютерных технологиях остается значительным. Прежде всего это касается инфраструктуры и компьютерных мощностей. Основной объем используемой техники, в том числе применяемой в правительственных учреждениях, построен на основе импортных микрочипов (или напрямую закуплен у иностранных производителей) и использует отработанные для такого рода техники пользовательские операционные системы зарубежного производства. Исключением являются рабочие станции и серверы на базе процессоров «Эльбрус». Новейшие из них («Эльбрус-4С» и «Эльбрус-8С») по своим возможностям сопоставимы с разработками компании Intel. Они комплектуются отечественной операционной системой ОС «Эльбрус», разработанной на базе Linux. На данный момент они проигрывают американским разработкам не столько по мощности, сколько по соотношению цена/качество, поэтому практически не представлены на пользовательском рынке и преимущественно закупаются правительственными и оборонными структурами в тех случаях, когда это оправдано соображениями безопасности. Однако производство «Эльбрусов» до настоящего времени не вполне локализовано[86]. Тем не менее на данный момент единственный крупный скандал, связанный с утечкой данных из околоправительственных структур РФ, — история с электронным «Досье РусАДА», которое, по некоторым свидетельствам, было якобы похищено и передано комиссии WADA именно в результате хакерской атаки. Атаки DDoS-ботов и вирусов-кодировщиков на правительственные, корпоративные и банковские ресурсы РФ летом 2017 г. не затрагивали защищенных сетей и, по-видимому,

---

[85] См., напр.: *Коломыченко М.* В интернет ввели кибервойска: Аналитики оценили количество хакеров на госслужбе // Коммерсантъ. 10 января 2017.

[86] См. подробнее: URL: http://youinf.ru/kakaya-proizvoditelnost-u-elbrus-8s/ (дата обращения: 25.08.2018).

не привели к критическим сбоям в функционировании структур Минобороны или утере государственных секретов. Учитывая уровень предполагаемой нагрузки на оборонную и научную киберсферу России, а также череду хакерских скандалов в структурах АНБ, Пентагона, партийных и правительственных органах США, такое «отсутствие результатов» выглядит достаточно неплохо.

Таким образом, сфера кибероборонны в России выглядит сравнительно (не безусловно) обеспеченной. В то же время картина в сфере российского потенциала кибернападения на данный момент непрозрачна и неочевидна. Только в 2013 г. министр обороны РФ С. К. Шойгу официально объявил о формировании в составе ВС России Войск информационных операций. Их задачами являются централизованное проведение операций кибервойны, управление и защита военных компьютерных сетей России, защита российских военных систем управления и связи от кибертерроризма и надежное закрытие проходящей в них информации от вероятного противника[87]. 14 января 2014 г. С. К. Шойгу подписал приказ о создании в составе Генерального штаба ВС России кибернетического командования, основная задача которого заключается в защите от несанкционированного вмешательства в электронные системы управления России. Таким образом, информационные войска РФ обрели официальный статус относительно недавно, так что еще в январе 2017 г. экс-руководитель комитета верхней палаты парламента по вопросам обороны Виктор Озеров заявлял, что таких войск в структуре армии страны попросту нет.

При этом «русскую киберугрозу» в целом принято оценивать как достаточно серьезную и требующую серьезного организованного противодействия. Для этой цели, например, в Евросоюзе запущен специальный отдел EastStratCom Task Force. В Латвии в 2015 г. открылся Центр стратегических коммуникаций НАТО — спецподразделение для информационной борьбы с Россией. Годом позже Совбез Украины призвал к созданию мощной информационной армии для противостояния Москве.

---

[87] См.: URL: https://rg.ru/2017/02/22/shojgu-obiavil-o-sozdanii-vojsk-informacionnyh-operacij.html (дата обращения: 25.08.2018).

Мэтью Берроуз, бывший аналитик ЦРУ и эксперт The Atlantic Council, заявил, что Россия достаточно конкурентоспособна в плане возможностей в сфере кибервойны. Российское государство в информационной борьбе однозначно сильнее Китая, признал специалист и добавил, что Москва проводит свои операции на высоком уровне[88]. Потенциал России прокомментировал и командующий Центром кибероборонь армии Китая генерал У Цзинтян. Он сказал, что особенность россиян заключается в их непредсказуемости и серьезных способностях. Именно этим поясняется разработка и реализация программы по привлечению российских хакеров американцами к выполнению своих задач. Кибервзломщики из России — вне конкуренции, заверил китайский военный[89].

Агентство Zecurion Analytics на основании информации о военных бюджетах стран мира, стратегий безопасности в кибернетической сфере, справочных данных подсчитало численность войск информационных операций в разных государствах, а также предположительные объемы их финансирования на 2017 г. (табл. 1). Бюджет российского подразделения численностью в тысячу человек составил $300 млн в год[90].

Таким образом, на общемировом фоне «количественные» показатели российских кибервойск выглядят достаточно скромно, однако они завоевали себе серьезную репутацию в киберсфере. Следует предположить, что российское киберкомандование нашло способы более рационально применить имеющиеся в его распоряжении сравнительно ограниченные ресурсы.

Основой активных действий правительственных органов и структур РФ в киберпространстве являются национальная Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента РФ от 5 декабря 2016 г., а также Федеральный

---

[88] URL: https://pronedra.ru/weapon/2017/02/23/vojska-informacionnyh-operacij/ (дата обращения: 25.08.2018).

[89] Там же.

[90] См.: Кибервойны 2017: Баланс сил в мире. URL: http://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf (дата обращения: 25.08.2018) ; Россию включили в пятерку стран с самыми развитыми кибервойсками. URL: https://habr.com/post/357236/ (дата обращения: 25.08.2018).

закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ; Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ и, наконец, Военная доктрина Российской Федерации, утвержденная в текущей редакции указом Президента РФ от 25 декабря 2014 г. Военная доктрина объявляет «воздействие на противника на всю глубину его территории одновременно в глобальном информационном пространстве, в воздушно-космическом пространстве, на суше и море» одной из характерных черт современных информационных конфликтов, и предполагает в качестве одного из направлений военного строительства «развитие сил и средств информационного противоборства»[91].

Таблица 1

Численность и финансирование войск информационных операций в мире

Страна	Численность и финансирование информационных операций
Китай	20 тыс. человек / $1,5 млрд в год
США	9 тыс. человек / $7 млрд в год
КНДР	4 тыс. человек / $200 млн в год
Великобритания	2 тыс. человек / $450 млн в год
Россия	1 тыс. человек / $300 млн в год
ФРГ	1 тыс. человек / $250 млн в год
Израиль	1 тыс. человек / $150 млн в год
Франция	800 человек / $220 млн в год
Южная Корея	700 человек / $400 млн в год

Кибервойны: перспективы

История развития вооружений показывает, что изобретение новых средств нападения, особенно основанных на принципиально новых технических или тактических решениях, обычно зна-

[91] Военная доктрина Российской Федерации // Рос. газета. № 6570 (298). 30 декабря 2014 г.

чительно опережает разработку и внедрение адекватных средств защиты. Тем не менее рано или поздно такие средства появляются и получают всеобщее распространение, нивелируя стратегический эффект нового оружия. На данный момент единственным исключением оказалось ядерное оружие, доставляемое с помощью баллистических и крылатых ракет. Что касается кибероружия, пока трудно прогнозировать развитие кибероборонительных систем и новейших средств кибернападения. Вероятнее всего, ключевыми моментами могли бы стать развитие технологий искусственного интеллекта и/или технологий глубокой интеграции человеческого и компьютерного сознания. В первом случае речь может идти о локализованном в суперкомпьютере или распределенном в Сети интеллекте-эксперте, который мог бы анализировать громадные потоки данных в реальном времени, выделяя среди них те, которые могут представлять потенциальную угрозу для защищаемых информационных структур и в случае обнаружения угрозы реагировать на них самостоятельно по заданному алгоритму либо запрашивать санкции у «человеческого» командования на проведение ударных кибероперaций. Для этого киберинтеллект может самостоятельно накапливать информацию об уязвимостях потенциально враждебных информационных ресурсов и средства оптимального воздействия на них с целью перехвата управления. В этом случае, однако, подобная интеллектуальная система фактически получает абсолютные полномочия (которые трудно обойти человеческим контролем ввиду того, что подобный искусственный разум мог бы контролировать также и информацию, транслируемую эксперту-человеку, провоцируя на требуемую интерпретацию). Дальнейший сценарий близко соответствует сюжетам, отработанным в фантастических франшизах «Терминатор» и «Матрица». Второй вариант предполагает, что компьютерные ресурсы, в том числе искусственный интеллект, выполняют исключительно служебную роль, в то время как человек остается субъектом информационной активности и при этом получает возможность обрабатывать непредставимые для нынешнего состояния технологий объемы информации. Однако в данном случае (помимо дискутируемой технической возможности подобного взаимодействия человек-компьютер и способности чело-

веческого разума выдержать работу в подобном режиме) вопросы вызывает сохранение подобным субъектом человеческой природы (не говоря уже о том, что сам подобный кибернетизированный субъект может оказаться прямым объектом кибератаки). В любом случае, на данный момент подобные перспективы фантастичны, хотя использование искусственного интеллекта (в современном понимании, как сложных и более-менее эффективных, обучаемых и самообучающихся, но не самостоятельных, не способных в собственном смысле к целеполаганию и, следовательно, к самоосознанию компьютерных экспертных систем) в кибервойнах, по-видимому, уже становится реальностью.

Глава 4
ИНФОРМАЦИОННЫЕ ВОЙНЫ: ЭПИСТЕМОЛОГИИ АПОКАЛИПСИСА

Информация как средство агрессивного взаимодействия является важной составляющей многих исторических эпизодов и отрефлектирована в древнейших памятниках культуры. Миф о троянском коне — это миф об использовании дезинформации, надежд, ожиданий, верований и суеверий противника для получения военного преимущества. Народы всей Земли использовали устрашающую окраску, воинственные кличи, перебранку перед началом сражения для поднятия боевого духа своей армии и подрыва уверенности в своих силах у вражеской. Китайская история и мифология содержит множество легенд о мудрых военачальниках и правителях, побеждавших врагов без боя, например, благоустраивая жизнь подданных и распространяя об этом слухи среди мятежников. Психологическое преимущество использовалось и как способ контроля над действиями противника во время войны; так, Сунь-Цзы рекомендует: «Вызвав гнев [в полководце противника], приведи его в состояние расстройства»[1]. Абд ар-Рахман ибн Абд ал-Хакам описывает хитрость полководца Тарика ибн Зияда, обманом заста-

[1] *Сунь-Цзы* Искусство войны. URL: http://militera.lib.ru/science/sun-tszy/01.html.

вившего пленников поверить, что арабские воины — безжалостные убийцы и людоеды; это вселило в сердца врагов ужас и лишило их воли к сопротивлению. При этом реальная жестокость, демонстративно проявляемая воюющими сторонами, служила той же цели. Одновременно стратеги, правители и философы не устают повторять тезисы о важности внутреннего единства воюющей стороны. В трактате У-Цзы: «Если государь, знающий Путь, хочет направить свой народ на войну, он прежде всего достигает согласия и только потом берется за большое предприятие»[2]. Древнегреческая легенда гласит, что спартанцы, угнетаемые поражениями во Второй Мессенской войне, обратились по внушению оракула к Афинам с просьбой дать им полководца. Афиняне в насмешку послали им хромого школьного учителя Тиртея. Однако Тиртей сумел воспламенить сердца спартанцев своими песнями, вдохнул в них несокрушимую отвагу и тем доставил им торжество над врагами. Отсутствие же подобного единства ведет государство к катастрофе. Пушкин, описывая в драме «Борис Годунов» поход сил Лжедмитрия на Русь, дает одному из его полководцев следующую реплику: «Но знаешь ли, чем сильны мы, Басманов? / Не войском, нет, не польскою помогой, / А мнением; да! мнением народным»[3]. Действительно, в конечном счете Московское царство, обладающее военным преимуществом, но сокрушенное внутренней рознью, не смогло противостоять самозванцу. Если прибавить к этому разведку и контрразведку, которые также неотделимы от сферы информационных войн, то придется сделать вывод, что информационная война — неотъемлемая часть войны «традиционной». Более того, возникает впечатление, что это вообще едва ли не нормальное состояние в любых межнациональных контактах, по крайней мере, там, где взаимопроникновение и взаимная ассимиляция не является осознанным и добровольным выбором обеих сторон; соответственно, «…каждый человек, военный или

---

[2] *У-Цзы* Трактат о военном искусстве. URL: http://www.vostlit.info/Texts/Dokumenty/China/I/U-tsy/text1.htm.

[3] *Пушкин А. С.* Борис Годунов / А. С. Пушкин. Драматические произведения. Проза. М., 1984. С. 68.

гражданский, участвует в информационной войне в той или иной ее форме»[4].

С другой стороны, в этом подходе явно доминирует не столько объективно наблюдаемая агрессия контрагента коммуникации, сколько собственная агрессия субъекта на присутствие в информационном поле Другого как альтернативного центра коммуникативной активности, по умолчанию оцениваемого в черно-белой, бинарной шкале. Любое взаимодействие с Другим в этой системе сводится либо к подчинению себя Другому, либо к подчинению Другого себе, а это, в свою очередь, заставляет нас вообще свести любую коммуникацию (в том числе на межличностном уровне) к формату «войны всех против всех». В этом случае мы должны (по аналогии с концепцией истории Карлейля) говорить о «героическом» подходе к взаимодействию в инфосфере, поскольку определяющим моментом здесь полагается процесс взаимодействия (и неизбежного столкновения) более или менее осознаваемых воль и интересов политических субъектов (по преимуществу — лидеров государств и/или экономических и политических элит, противопоставляемых управляемому тем или иным способом населению). Все принятые решения и все совершенные действия имеют осознаваемую политическими субъектами цель, которая в ретроспекции может быть реконструирована в соответствии с принципом «кому выгодно», а политика является одновременно способом самоосознания и сферой самореализации этих субъектов. Все формы конфронтации, в том числе информационной, являются не целью, но неизбежным следствием базовой для любого социально-экономического процесса нехватки ресурсов и стремления к сохранению и преумножению «своего», в том числе в ущерб Другому. Очевидно, что с выходом политического и исторического процесса на глобальный уровень и окончательным поглощением «фронтира» признанными полити-

[4] По словам В. Маркоменко, зам. генерального директора Федерального агентства правительственной связи и информации (ФАПСИ) при президенте РФ. Цит. по: *Почепцов Г. Г.* Информационные войны: Основы военно-коммуникативных исследований. URL: http://www.ligis.ru/librari_2/049/02.html (дата обращения: 25.08.2018).

ческими субъектами осознание ограниченности перспектив собственного развития существованием и информационной активностью «Другого», и, как следствие, уровень конфронтационности в любых коммуникациях в рамках героической модели должны нарастать. Высшей, стратегической ценностью при таком подходе становится ретроспективность, «преемственность» и «безопасность», сохранение устоявшейся культурной парадигмы, а «Другой» однозначно маркируется как «угроза», что требует либо встречной активности, то есть агрессии и экспансии (при естественной обратной реакции, а значит нарастании эскалации, и, с высокой вероятностью, перехода от собственно информационной войны к ее «горячей» стадии), либо самоизоляции («Железный занавес» в СССР, концепция «суверенного интернета» в современной России, информационная изоляция населения Северной Кореи, «Великий китайский файервол» и т. п. Сюда же следует отнести самозамыкание Японии эпохи сёгуната Токугава как хороший пример законченного и удачного опыта самоизоляции с ожидаемо тяжелыми политико-экономическими и социокультурными последствиями). Таким образом, при описании данной модели взаимодействия субъектов в инфосфере термин «героическая» следует дополнить до «***героико-параноидальная***».

Попытками выйти за пределы конфронтационного модуса, неизбежного в рамках героико-параноидальной модели, в общественном сознании XX–XXI вв. становятся концепты толерантности, мультикультурализма, взаимодополнения культур, разделения ценностей и интересов, открытого общества, наконец, как крайняя точка, обратная модусу тотальной информационной войны, — идея неизбежного размывания национальных общностей как логического следствия развития информационного общества (а также постмодернистская концепция размывания границ личности). Методологически в основе данной концепции лежит проспективный подход к историческому процессу, который можно также назвать «фаталистическим» или «неомарксистским»: предполагается, что человечество с неизбежностью (в силу экономической целесообразности) движется к некоей новой и более совершенной, «комфортной» стадии (постиндустриальное общество, трансгуманизм, сингулярность), которое заменит предыдущую формацию в силу большей

экономической эффективности, в результате чего и прежние формы самоидентификации субъекта неизбежно будут вытеснены новыми. Конфликты в инфосфере в таком случае теряют функцию подлинного противостояния цивилизаций, культур, укладов и традиций и превращаются в хаотичское, псевдосознательное столкновение отмирающих архаических и формирующихся перспективных дискурсов в поисках необходимого баланса (подобно религиозным войнам периода становления индустриального общества в Европе). В свою очередь, в качестве идеала рассматривается коммуникация как равноправное взаимодействие, взаимодополнение и взаимопроникновение в процессе социокультурного сотворчества («коммуникативное действие» Хабермаса). Субъекты всех уровней сложности взаимодействуют в инфосфере на равных. Конфликтогеничная бинарная логика «своего и чужого» заменяется концепцией «пастишности», многокомпонентной системы координат, в которой необходимый подход актуализируется ситуационно. Соответственно, любое сообщество — этническое, государственное, религиозное — существует только «здесь и сейчас», неизбежно трансформируясь в следующий момент исторического времени и трансформируя по мере необходимости собственную историю и культуру. Культурные категории являются не константами, но конструктами, а субъект — временной и трансформируемой (сознательно и бессознательно, извне и изнутри) под воздействием гуманитарных технологий совокупностью конструктов, саморепрезентирующейся в информационном пространстве через месседжи. В результате, однако, история теряет логическую связность, перестает быть уроком и сферой смыслов, превращаясь в неизбежное и малоуправляемое следствие экономической необходимости на уровне онтологии и чередой манифестов-месседжей на уровне инфосферы; моральная составляющая субъекта актуализируется в момент выбора, но фактом выбора в общественно значимом действии снимается задним числом как неактуальная («Невыносимая легкость бытия» М. Кундеры), любая форма коммуникации растворяется в необязательности. В результате субъект инфосферы теряет критерии оценки реальности, способность и стимул к подлинному развитию, он нестабилен и гедонистичен. Характеристики этого «идеального субъекта» четко

укладываются в клиническую картину диссоциативной психопатии; соответственно, данный подход к описанию инфосферы можно описать как «***диссоциативно-психопатический***».

Наряду с ретроспективным и проспективным, мы можем выделить еще один актуальный подход к описанию инфосферы вообще и информационной агрессии в частности. Этот подход, парадоксальным образом соединивший стоическое само-стояние элитарной концепции личности, свойственное в равной степени восточным и западным философским школам, и практические наработки военных стратегов и профессиональных управленцев, кладет в основу описания инфосферы принцип неопределенности. Коммуникативная среда, как и любая другая, воспринимается одновременно как ресурс и вызов, пространство возможностей и угроз, требующее для сохранения устойчивости любой системы креативности, адаптивности и системного анализа входящей информации. Теория неопределенности вновь выдвигает на первый план личность, героя, однако героя иного склада, чем структурно интегрированный «сакральный правитель» героической модели. В ситуации, когда количество факторов неисчислимо, когда ключевой параметр может быть определен ошибочно и когда катастрофа может быть отложена, но не исключена, а сверхзадача — не избежать волны цунами, а взобраться на ее гребень, героем становится харизматический лидер, авантюрист, искатель приключений. Н. Талеб прямо указывает в качестве прототипа фигуры пиратов, конкистадоров, авантюристов; речь, соответственно, идет об «***авантюрном***» подходе, предполагающем конфликты в инфосфере необходимой и неизбежной, но не исключительной составляющей информационного обмена.

На первый взгляд, авантюрный подход, не фиксируя внимание на предзаданных принципах и идеологемах, должен позволить наиболее адекватно описывать реалии инфосферы. Однако тенденция рассматривать субъекты коммуникации, то есть личности и группы личностей, как амортизируемый ресурс, то есть нацеленность на (рационально организованную) эксплуатацию и в конечном счете истощение возможностей человека как *средства* выживания над-человеческой структуры, более того, тенденция рассматривать субъект как средство для самого (неактуализируемого и неакту-

ального в инфосфере) субъекта придает данной эпистемологии мрачноватые черты неоварварства. Именно в рамках этого подхода внедряется в массовое сознание концепт «зоны комфорта», описываемый как заведомо неприемлемое состояние субъекта, то есть *нормальным* состоянием субъекта считается погружение в дискомфорт, в непрерывный стресс, что как раз ведет его к астеническому состоянию, к неврозу как следствию высокого уровня амортизации ресурса. Соответственно, данный подход к описанию инфосферы будет далее обозначен нами как «***невротический***».

Подчеркнем: анализ трех наиболее распространенных моделей описания инфосферы привел нас к выбору определений, позаимствованных из психопатологической терминологии. В данном случае они используется не в прямом значении, но как символический образ, с нашей точки зрения уместный для указания на существенные метасвойства рассматриваемых эпистемологических систем. Каждый из этих трех подходов а) целиком замкнут на себя, внутренне непротиворечив, при этом два из них объективную реальность воспринимают как вторичную и второстепенную по отношению к используемой концепции реальности, третий же отказывает субъекту коммуникации в праве на любые свойства, кроме инструментальных, то есть в конечном счете на самостоятельность, уничтожая онтологию личности; б) построен на ментальном неприятии других подходов и при этом непротиворечиво включает эти подходы в свою систему мирописания, обычно как угрозы того или иного рода; в) в конечном счете провоцирует разрыв эпистемологической системы и первичной реальности в сфере практической деятельности, что неизбежно ведет к расколу сознания и повышению общего уровня информационной, а зачастую и деятельностной агрессии. Речь не идет о принципиальной неверности этих систем. Речь идет о том, что во всех случаях это *неполные* образы мира, декларирующие свою *полноту* и практическую значимость на основании внутренней непротиворечивости. Проблема заключается в том, что во всех трех случаях перед нами модели, прогнозирующие надвигающийся цивилизационный кризис глобального уровня и претендующие на роль универсального рецепта преодоления указанного кризиса. Далее будут детально рассмотрены идеологические основы, исто-

рия и функционирование упомянутых моделей, детализированы их сильные и слабые стороны. В конечном счете это позволит нам оценить их «рецептурный» потенциал как в условиях ожидаемого кризиса, так и в качестве эпистемологической основы для построения посткризисного информационного пространства.

§ 1. Параноидально-героический поход. Геополитика и доктрина национальной безопасности

«Новая информационная парадигма геополитики означает, что в XXI в. судьба пространственных отношений между государствами будет определяться, в первую очередь, информационным превосходством в виртуальном пространстве. Тем самым вопрос о роли символического капитала культуры в информационном пространстве приобретает не абстрактно-теоретическое, а стратегическое геополитическое значение. Но социокультурные факторы активизируются только благодаря человеческой активности, поэтому в центре информационных технологий находится сам человек политический как творец и интерпретатор современной политической истории»[5].

Так же, как и «информационное общество» (см. гл. 1), информационную войну в любом случае придется признать реальностью как минимум на уровне социокультурного феномена. Термин «информационная война» в последнее время становится одним из наиболее популярных в устах политиков и политических журналистов. В частности, информационная война рассматривается как составляющая «гибридных войн», обычно рассматриваемых как войны «нового поколения». «Понятие „информационная война“ носит синтетический характер. Оно вобрало в себя в ходе исторической эволюции целый ряд явлений, обнаруживающихся в человеческом сообществе при взаимодействии масс, толп, народов, социальных групп. При этом оно в соответствии с целями воздействия

[5] *Василенко И. А.* Геополитика современного мира : учеб. пособие. URL: https://studfiles.net/preview/5248911/page:7/ (дата обращения: 25.08.2018)

на людей получало обозначение как пропаганда, контрпропаганда, спецпропаганда, психологическая война, техника дезинформации и т.п»[6]. Как упоминалось выше, строгого и общепринятого в среде специалистов определения данного термина не существует. К примеру, в комплексе документов Комитета начальников штабов США (в частности, в инструкции КНШ 3210.01 А «Концепция информационных операций объединенных группировок вооруженных сил» от 1996 г., Едином уставе КНШ № 3–13 «Доктрина совместных действий по проведению информационных операций», директивах, уставах и наставлениях штабов видов вооруженных сил 1998-го) находим следующую концепцию информационного противоборства: «Информационные операции являются более широким понятием, нежели борьба с системами управления, но не подменяют его. Задача БСУ как самостоятельного вида боевого обеспечения — борьба с системами управления и связи как с целевыми объектами, а цель проведения ИО — воздействие на информационные системы противника и циркулирующую в них информацию или уничтожение их. При организации информационных операции действия по БСУ централизованно интегрируются в них и становятся их неотъемлемыми элементами»[7]. Поскольку речь идет о воздействии «на циркулирующую информацию», речь идет не только о дезинформации, но и о том, что в американской традиции принято называть «психологическими операциями», то есть о целенаправленном воздействии на сознание как ключевых субъектов в военной или политической структуре противника, так и широких масс населения (пропаганда, контрпропаганда и т. п. — «информационные войны» в узком смысле слова, или же «контентные войны»). Сюда же включен и тот аспект взаимодействия, который описан нами выше как кибервойны. Следует отметить, что с чисто практической точки зрения комплексный подход вполне оправдан: для ведения ин-

[6] *Жирков В.* Предисловие // Н. Л. Волковский. История информационных войн : в 2-х ч. Ч. 1. СПб., 2003. С. 3.

[7] Цит. по: *Жуков В.* Взгляды военного руководства США на ведение информационной войны. URL: http://pentagonus.ru/publ/22-1-0-175 (дата обращения: 25.08.2018).

формационных войн в равной степени важны как контроль над распространяемым контентом, так и контроль над каналами его распространения.

Воздействие информации и коммуникационного процесса на человеческое сознание трудно переоценить. Софист Горгий (около 483 — около 375 до н. э.) писал: «Слово есть великий властелин, который, обладая весьма малым и совершенно незаметным телом, совершает чудеснейшие дела. Ибо оно может и страх изгнать, и печаль уничтожить, и радость вселить, и сострадание пробудить <…> А что сила убеждения, которая присуща слову, душу формирует как хочет, это должно узнать, во-первых, из учений метереологов, которые, противопоставляя мнение мнению, удаляя одно мнение и вселяя другое, достигли того, что невероятные и неизвестные вещи являются очам воображения. Во-вторых же <…> из словесных состязаний в народных собраниях, в которых [бывает что] одна речь, искусно составленная, но не соответствующая истине, [более всего] нравится народной массе и убеждает ее. В-третьих же, быстрота ума, с легкостью меняющая веру, в [то или иное] мнение»[8].

Разумеется, «воспламеняющее» действие слова, «мгновенно» изменяющее настроение массы, как правило, иллюзия. Гюстав ле Бон, впервые разрабатывавший психологию масс как научную дисциплину, писал: «Факторы, определяющие характер мнений и верований толпы, бывают двоякого рода: факторы непосредственные и факторы отдаленные.

Отдаленные факторы — это те, которые делают толпу доступной к восприятию известных убеждений и совершенно неспособной проникнуться некоторыми другими взглядами. Эти факторы подготавливают почву, на которой впоследствии внезапно развиваются какие-нибудь новые идеи, поражающие своей силой и результатами. Впрочем, внезапность появления этих идей только кажущаяся. Действительно, некоторые идеи зачастую возникают в толпе и приводятся в исполнение с быстротой молнии, но это так лишь

[8] *Горгий*. Похвала Елене. URL: http://simposium.ru/ru/node/13780 (дата обращения: 17.08.2018).

с первого взгляда, так как на самом деле этот взрыв всегда является результатом долгой предшествующей работы.

Непосредственные факторы, влияющие на толпу, действуют уже на подготовленную отдаленными факторами почву и без этого не вызвали бы никаких результатов; они порождают в толпе активную уверенность, то есть облекают в известную форму идею и развивают ее со всеми ее последствиями. Благодаря этим непосредственным факторам в толпе возникают решения, увлекающие ее; благодаря им разражается бунт, устраивается стачка, или же громадное большинство вдруг возносит какого-нибудь человека к власти или низвергает какое-нибудь правительство»[9]. Таким образом, даже в эпоху галопирующего развития средств массовой информации значение непосредственного информационного воздействия все-таки ограничивалось возможностью соотнесения информации (в том числе, например, пропагандистского лозунга) с объективной реальностью. Однако последние десятилетия привнесли в ситуацию ряд принципиальных новшеств:

Тотальность информационного поля. Практически для того, чтобы изолировать свое сознание от актуального политического дискурса, субъект должен физически изолироваться от общества и полностью обрубить коммуникационные каналы. Такое отшельничество технически реализуемо, но распространение коммуникационных технологий делает его все более проблематичным. С другой стороны, тотальное информационное поле осознается как всеобщее, общеизвестное и общественно значимое, таким образом превращаясь в недискутируемый аргумент для непосредственной политической реакции. Характерным примером может считаться информация о якобы имевшей место 4 апреля 2018 г. химической атаке, совершенной правительственными войсками Сирии. Эта информация была опубликована организацией «Белые каски», причем решение о нанесении авиаудара по сирийским военным объектам было принято командованием возглавляемой США Коалиции до получения каких-либо данных объективного контроля. Однако

[9] *Бон ле Г.* Психология народов и масс. URL: http://lib.ru/POLITOLOG/LEBON/psihologia.txt_with-big-pictures.html#25 (дата обращения: 25.08.2018).

информация тиражировалась западными и арабскими СМИ как безусловно достоверная и сформировала эмоциональный фон, при котором, видимо, «наказание кровавого тирана» соответствовало ожиданиям потребителей информации стало единственно возможным решением для Стратегического командования США и их союзников.

Глобализация контента. Субъект коммуникации получает в реальном времени доступ к неограниченному объему информации (как первичной — сообщения о новостях, так и более или менее отрефлектированной экспертами неконтролируемой степени квалифицированности). В этой же области лежит понятие «*эффекта CNN*», при котором информация становится одновременно доступной как президентам, так и простым зрителям (что дает, соответственно, основания гражданам требовать от политиков реакции на эту информацию). Полковник армии США К. Эллард утверждает: «В случае Сомали реально мотивировали международное сообщество к действию телевизионные образы маленьких детей с их животами, разбухшими от голода»[10]. При этом большая часть получаемой субъектом информации не связана с его непосредственным опытом, то есть ее достоверность не может быть непосредственно подтверждена или опровергнута. Соответственно, у контрагента, транслирующего информацию субъекту, появляется возможность искажения данных. В эпоху становления цифровой эпохи появляется сатирическая комедия Барри Левинсона «Плутовство»/«Хвост виляет собакой» («Wag the Dog»), в которой, чтобы отвлечь население США от сексуального скандала, в который перед выборами попал действующий президент, опытный пиарщик создает в информационном поле фиктивную войну в Албании. Нужные настроения поддерживаются размещенными в прессе смонтированными фотографиями «страдающих детей» и «оставшихся в плену американских солдат» и т. д. На попытку ЦРУ прояснить ситуацию (никакой войны на самом деле нет) он отвечает: «Называйте это „репетицией“ или

[10] *Allard K.* Co-operation, command and control // Co-operation, command and control in UN peace-keeping operations. A pilot study from the Swedish War College. Stockholm, 1996. P. 100.

„национальной безопасностью". Как угодно. Но если вы считаете, что войны нет, то тогда зачем вы нужны? Идите домой и играйте в гольф. Так что вам придется принять нашу войну, потому что, кроме нашей, нет никакой другой».

Глобализация интересов. Наличие глобальных коммуникаций, глобальной системы перемещений и глобальной экономики приводят к тому, что субъект ощущает себя вовлеченным в удаленные процессы, при этом, как показано, не имея возможности получить непосредственное представление об истинном положении вещей.

Фреймированность контента. Инфосфера предоставляет своим пользователям множество независимых (или псеводнезависимых) конкурирующих каналов и форм коммуникации, большинство из которых не контролируются (по крайней мере, напрямую) какими-либо правительственными структурами. При этом доступ к неконтролируемой информации в современной инфосфере многократно упростился, и хотя вопрос о мере воздействия альтернативных источников информации на массовое сознание дискуссионен, однако очевидно, что сама возможность тотального контроля над сферой сознания в настоящее время меньше, чем столетие назад — при многократном росте возможностей инструментария и технологий такого контроля. Пол Кеннеди констатирует: «Правительствам авторитарных государств становится все труднее держать свои народы в неведении. Чернобыль был быстро сфотографирован французским коммерческим спутником, а снимки быстро переданы на весь мир, включая и сам Советский Союз. Подавление китайским правительством выступления студентов на площади Тяньаньмэнь и шок, испытанный всем миром от этого события, сразу же потрясли и Китай благодаря радио, телевидению и телефаксу. Когда в конце 1989 г. рухнули коммунистические режимы в Восточной Европе, сообщения и видеосюжеты о падении одного из них стимулировали сходные процессы в соседних государствах»[11].

Мультимедийность контента. Современные СМИ, в том числе интернет-СМИ и блогосфера, многократно усиливают вовлеченность субъекта, воздействуя на каналы восприятия, недоступные

[11] *Кеннеди П.* Вступая в двадцать первый век. М., 1997. С. 71.

пропаганде предшествующих эпох (аудиальная, визуальная, графическая информация), что позволяет практически гарантированно нащупать приоритетный канал восприятия любого субъекта. Любительская видеосъемка с использованием общедоступных средств индивидуальной связи, спутниковая фотография, управляемые дроны, веб-камеры, трансляция в режиме реального времени создают эффект присутствия, заставляют субъекта воспринимать самого себя как очевидца событий. Одновременно возможность записи, воспроизведения и многократного повторения информации нивелирует фактор времени. При том что никаких гарантий подлинности увиденного и услышанного, а тем более гарантий корректности подачи информации в модерируемом неизвестным контрагентом канале субъект не получает.

Перефразируя ле Бона, можно утверждать, что современный обыватель находится в состоянии постоянного раздражения и постоянной готовности к трансформации идеи в непосредственное действие, в том числе социально значимое. Многочисленные «политические флешмобы», популярные, например, у российской оппозиции последних лет, показывают размывание границы между инфосферой и повседневной реальностью: протестное настроение становится именно настроением, протестное действие — мгновенно инициируемой и не нуждающейся в подготовке, игровой по своей природе акцией, а главным значением такого действия оказывается создание «информационного повода» для СМИ и очередной порции мультимедийного контента для внешнего или внутреннего «потребления». Однако уровень вовлеченности в информационное пространство становится настолько велик, что граница между флешмобом и государственным переворотом способна исчезнуть в любой момент. В апреле 2010 г. журнал Time опубликовал список 100 самых влиятельных людей 2010 г. Первое место в нем занимает Ваэль Гоним, египтянин, создавший в социальной сети Facebook страницу, где призывал соотечественников выходить на улицу с протестами. Таким образом, его можно считать одним из первых практиков «твиттер-революции». Лауреат Нобелевской премии и бывший директор МАГАТЭ Мохаммед эль-Барадеи в статье журнала Time отметил: «Ваэль быстро понял, что социальные медиа,

особенно Facebook, возникли как сильнейший коммуникативный инструмент для мобилизации людей вокруг новых идей. Это был призыв к мирной революции, который услышали и восприняли к действию 12 миллионов египтян, свергнувшие ненавистный режим Хосни Мубарака»[12].

При этом трансверсия информационной и материальной реальностей, особенно с учетом легкодоступных инструментов коррекции и преобразования цифровой мультимедийной информации (таких, как Adobe Photoshop), совмещает сферу практических интересов и игровое поведение. Субъект ощущает себя включившимся в гигантскую ролевую игру, при этом, как правило, не осознавая, что пытается вести свою партию в этой игре, располагая минимальным (или отрицательным) уровнем информированности, при прогнозируемом существовании в том же информационном пространстве более информированных и не менее активных игроков. В этом смысле оказывается вполне обоснованной озабоченность общественных и государственных структур по всему миру проблемой взаимодействия с коммуникативной сферой как средой прямого воздействия на реальность и, соответственно, отношение к информации именно как к инструменту воздействия, в экстремальных случаях — как к оружию. При этом субъекты политики в любом случае находятся в ситуации глобального экономического и политического взаимодействия, которые в наиболее известных формулировках описывают концепции «глобальной экономики» и «геополитики».

Под «**глобальной экономикой**» понимается установка на расширение и оптимизацию всех имеющихся экономических связей между государствами и людьми, ведущая к формированию мирового рынка товаров, капитала, материальных, производственных, трудовых и информационных ресурсов. К основным предпосылкам формирования глобальной экономики можно отнести:

— прорыв в развитии информационных технологий, приведший в конечном счете к созданию глобальных коммуникационных сетей;

— нарастающий локальный дефицит природных ресурсов;

---

[12] *ElBaradei M.* Wael Gonim // Time. 21.04.2011.

— революционный рост качества медицинского обслуживания и индустриализация сельского хозяйства, что приводит к различного рода демографическим проблемам — от демографического взрыва до старения населения в развитых странах;

— появление и распространение в мире оружия массового поражения;

— мощное техногенное давление на природу и ухудшение экологии;

— развитие транспортной инфраструктуры, что наряду с развитием инфосферы ведет к интернационализации капитала и производственных мощностей, а также нарастанию конкуренции — борьбы за рынки сбыта и ресурсы.

К проблемным областям глобальной экономики можно отнести спекулятивный характер биржевых операций, нарастающую на практике диспропорцию развития развитых и слабых экономик (что позволяет интерпретировать глобализацию как новую форму прямой и косвенной эксплуатации) и стремление к решению текущих локальных проблем исключительно за счет перемещения ресурсов. В результате, к примеру, экологические проблемы развитых экономик решаются за счет переноса издержек на экономику слабых регионов, то есть за счет «отодвигания» потенциальной катастрофы от собственных границ. Равным образом демографические проблемы развитых государств, ведущие, в частности, к сокращению трудовых ресурсов, решаются через импорт трудовых ресурсов, что разрушает собственное производство стран-экспортеров и одновременно формирует инокультурные анклавы на территориях стран-импортеров — источник столкновений на национальной и религиозной почве. В контексте рассматриваемого вопроса стоит обратить внимание на ситуацию всеобщей вовлеченности, при которой экономические интересы условного политического субъекта А в силу их глобальности и нарастающей конкуренции неизбежно сталкиваются с интересами условного субъекта В. Существуя в условиях глобализации, государство должно либо придерживаться протекционистской политики, защищая экономические интересы собственных граждан, либо, опираясь на концепцию глобального взаимодействия и взаимодополнения

экономик, выстраивать систему компромиссов, зафиксированную во взаимообязывающих международных соглашениях. Практика последних лет, однако, показывает, что работоспособность второго подхода не безусловна[13].

Изучение глобальных экономических связей — один из традиционных аспектов **геополитики**. Термин «геополитика» введен в научный обиход на рубеже XIX–XX вв. для обозначения дисциплины, изучающей формы и механизмы контроля за территорией. Историческим ядром геополитики выступает политическая география, ставящая во главу угла исследование прямых и обратных связей между свойствами территории и балансом (соперничеством или сотрудничеством) мировых сил. Александр Дугин проводит такое сравнение: «Марксизм и либерализм равно кладут в основу экономическую сторону человеческого существования <…> Но в отличие от „экономических идеологий", она [геополитика] основана на тезисе: „географический рельеф как судьба". География и территория выступают в геополитике в той же функции, как деньги и производственные отношения в марксизме и либерализме, к ним сводятся все основополагающие аспекты человеческого существования, они служат базовым методом интерпретации прошлого, они выступают как главные факторы человеческого бытия, организующие вокруг себя все остальные стороны существования»[14].

Помимо данного термина, употребляются также «геоэкономика», «мир-системный анализ» и «геофилософия» с не вполне эквивалентным значением и упором на различные аспекты национально-территориальных контактов (военно-стратегический, экономический, культурно-мировоззренческий). Так, Э. Люттвак в статье «От геополитики к геоэкономике: логика конфликта, грамматика торговли», опубликованной в журнале National Interest, противопоставляет геополитику с ее акцентом на использование военной мощи для достижения внешнеполитических целей и геоэкономику

---

[13] См., напр., URL: http://www.mk.ru/economics/2018/04/08/amerika-razvyazala-torgovuyu-voynu-so-vsem-mirom-pobediteley-ne-budet.html (дата обращения: 25.08.2018) и др. о протекционистской политике администрации Д. Трампа.

[14] *Дугин А. Г.* Основы геополитики. М., 1997. С. 12.

как политику, ориентированную на победу в экономическом состязании[15]. Фернан Бродель в фундаментальном труде «Материальная цивилизация, экономика и капитализм. XV–XVIII вв». использует термин «мир-экономика» для комплексного описания исторических процессов прошлого и настоящего, в которых материальная и духовная культура, политика, религия и военное дело оказываются тесно увязаны со множеством ландшафтных и климатических факторов как на региональном, так и на глобальном уровне[16]. С другой стороны, практически ориентированные геополитические концепции от описательно-культурологического уровня переходят к уровню нормативно-деятельностному и, соответственно, акцентируют упомянутый выше «героический» аспект политических процессов: у Дугина: «Геополитика — это мировоззрение власти, наука о власти и для власти. Только по мере приближения человека к социальной верхушке геополитика начинает обнаруживать для него свое значение, свой смысл и свою пользу, тогда как до этого она воспринимается как абстракция. Геополитика — дисциплина политических элит (как актуальных, так и альтернативных), и вся ее история убедительно доказывает, что ею занимались исключительно люди, активно участвующие в процессе управления странами и нациями, либо готовящиеся к этой роли (если речь шла об альтернативных, оппозиционных идеологических лагерях, отстраненных от власти в силу исторических условий) <…> Геополитика — это наука править»[17]. Описание геополитических процессов через столкновение воль и интересов принято называть «геополитическим прагматизмом», под которым понимается реализм во внешней политике, основывающийся на собственных эгоистических и прагматических интересах государства. Широко известно высказывание премьер-министра Великобритании Генри Пальмерстона (1784–1865) о том, что государство не может иметь ни постоянных друзей, ни постоянных

[15] См.: *Luttwak E.* From Geopolitics to Geo-Economics: Logic of Conflict: Grammar of Commerce // The National Interest. 1990. № 20. P. 12–34.

[16] См.: *Бродель Ф.* Материальная цивилизация, экономика и капитализм. XV–XVIII вв. URL: https://web.archive.org/web/20091123073344/http://www.i-u.ru/biblio/archive/brodel/ (дата обращения: 25.08.2018).

[17] *Дугин А. Г.* Указ. соч.

врагов, но одни лишь постоянные интересы. Принцип реальной политики (Realpolitik) исходит из представлений о неизбежности столкновения интересов государств в борьбе за ограниченные природные и другие ресурсы, контроль международных (транспортных, информационных) коммуникаций и т. п. Реалисты возлагают ответственность за международные отношения на великие державы. Геополитический прагматизм нашел отражение в устройстве Совета Безопасности ООН, где в качестве постоянных членов представлены великие державы, обладающие правом вето по резолюциям Совбеза. Крайним проявлением прагматизма является современная американская геополитика, возлагающая только на США ответственность за мировой порядок, что нашло отражение в доктрине «**превентивного интервенциализма**»[18]. Характерным для геополитического подхода является понимание глобальных процессов как игры (от англо-русской «Большой игры» на Востоке в XIX в. до «Великой шахматной доски» З. Бжезинского), причем в рамках реальной политики имеется в виду исключительно игра на выигрыш с географическим, экономическим и, как следствие, военно-политическим доминированием в качестве приза. При этом стратегии игры со временем радикально меняются. Изначально ключом к победе («гегемонии») признается господство над стратегически значимой территорией («теория хартленда», «атлантическая теория», идея Больших пространств в концепции евразийской школы. Например у Х. Маккиндера: «Тот, кто правит Восточной Европой, господствует над хартлендом; тот, кто правит хартлендом, господствует над Мировым островом; тот, кто правит Мировым островом, господствует над миром»[19]). (Как характерный пример анализа геополитической ситуации, построенного автором на столкновении двух территориально ориентированных концепций — «атлантической» (контроль над морскими торговыми путями) и евразийской «континентальной».) В новейшей геополитике становится популярной формула: «Кто владеет информационными и биологическими технологиями,

---

[18] По: *Дергачев В. А.* Геополитика : учебник для вузов. М., 2004. 526 с.

[19] *Маккиндер Х.* Демократические идеалы и реальность // Полис. Политические исследования. 2011. № 2. С. 134–144.

тот владеет миром» (перифраз афоризма Н. Родшильда «Кто владеет информацией, тот владеет миром»). Достоверная и своевременно полученная информация — ключ к принятию правильных стратегических решений. Одновременно информационное воздействие есть способ укрепления или трансформации геополитического, геоэкономического и геофилософского кода, что опять-таки возвращает нас к восприятию информации как оружия и напрямую требует преимущественного внимания к инфосфере в любой современной доктрине национальной безопасности. С другой стороны, соответствующая установка в системе принятия решений сама по себе является угрозой. Так, по мнению американских конфликтологов Рубинштейна и Крокера, геополитическая концепция Хантингтона, требующая защиты цивилизационных интересов Запада в неизбежном столкновении с конкурирующими цивилизациями, «представляет собой худший вариант самоосуществляющегося прогноза»[20], поскольку однозначно уводит элиты от перспективы разрешения международных конфликтов в сторону неизбежной конкуренции и противостояния.

Однако, в любом случае, как минимум феномен информационной войны необходимо признать актуальным. Инфосфера ощущает себя пространством многонаправленной агрессии, войны идей. Э. Тоффлер в «Метаморфозах власти» 1990 г. пишет: «Информационные войны бушуют в наших душах, ведь речь идет о том, как люди думают и принимают решения <…> и воображение при этом является столь же важным фактором, как и информация вообще»[21]. Г. Почепцов в статье «Информационные войны: тенденции и пути развития» говорит о культурно-историческом измерении информационных войн: «Войны могут выигрываться на поле боя, а проигрываться в сознании людей. Информационные войны сопровождают всю историю человечества. Сначала они были религиозными и идеологическими, причем для борьбы с носителями чужих взглядов

[20] Цит. по: *Василенко И. А.* Геополитика современного мира : учеб. пособие. URL: https://studfiles.net/preview/5248911/page:6/ (дата обращения: 25.08.2018).

[21] *Тоффлер Э.* Метаморфозы власти: знание, богатство и сила на пороге XXI века. М., 2003. С. 392–393.

применялись все виды репрессий»[22]. И. А. Василенко определяет информационную войну как планомерное информационное воздействие на всю инфокоммуникационную систему противника и нейтральных политических субъектов с целью формирования благоприятной глобальной информационной среды для проведения любых политических и геополитических операций, обеспечивающих максимальный контроль над пространством[23].

Исходной формой информационных войн считают внешнюю и внутреннюю пропаганду. Французский социолог Жак Эллюль предложил различать вертикальную и горизонтальную пропаганду[24]. Вертикальная — это классический вариант пропаганды, как мы все себе ее представляем, информационный поток сверху вниз с пассивным реагированием аудитории. Горизонтальная пропаганда реализуется в группе, а не идет сверху, в ситуации отсутствия формального коммуникативного лидера (что практически предвосхищает, допустим, формирование мнений в современных социальных сетях). Ж. Эллюль вводит также различия политической и социологической пропаганды. Под политической понимаются прямые коммуникативные акты, направленные на формирование определенного сознания и требуемых форм поведения. Это техники воздействия государства, партии, администрации. Социологическая же работает на объединение группы. Это стиль жизни и типы поведения, которые являются нормой в этом обществе. Социологическую пропаганду он считает более тяжелой для понимания, потому что она более незаметна. Если политическая пропаганда является распространением идеологии, то социологическая — ее проникновением благодаря существующим экономическим, политическим и социологическим факторам. В первом случае ее проводником являются СМИ, во втором — прямые культурные, экономические и политические контакты.

В своей книге «Война и антивойна» Э. Тоффлер приводит примеры того, что наиболее часто используется для воздействия на массы

---

[22] *Почепцов Г.* Информационные войны: тенденции и пути развития. URL: https://psyfactor.org/psyops/infowar7.htm (дата обращения: 25.08.2018).

[23] См.: *Василенко И. А.* Геополитика современного мира…

[24] См.: *Ellul J.* Propaganda. The formation of men's attitudes. N. Y., 1965. 352 p.

собственного или чужого населения в условиях текущего конфликта: обвинения в зверствах; гиперболизация ставок; демонизация и дегуманизация оппонента; поляризация; божественные санкции; мета-пропаганда, которая дискредитирует пропаганду другой стороны[25].

Ключевым недостатком пропаганды как метода следует назвать ее очевидность. Пропагандистское сообщение очевидно определяется как ангажированное, особенно если звучит в ситуации явного, особенно военного, конфликта. Кроме того, именно разница в мировосприятии, которая должна транслироваться в качестве рекомендуемой модели поведения, зачастую становится препятствием к усвоению предложенной интенции. «Решено было сместить смысловые акценты: убедить финнов в том, что Советский Союз не враг, а друг, который стремится установить добрососедские отношения с Финляндией. „Ваша родина получила независимость и самостоятельность в результате Великой Октябрьской революции и победы Советской власти в России. За эту независимость вместе с финским народом боролись русские большевики. Советское правительство никогда не покушалось на независимость Финляндии. Советский Союз желает мира и дружбы с финским народом. Так давайте же прекратим кровопролитие и протянем друг другу руки как труженики труженикам! Давайте прекратим кровопролитие и побратаемся друг с другом“, — говорилось в одной из листовок 1940 года… Надо сказать, что персонифицированное обращение наших агитаторов к финским „труженикам“ было малоэффективным. Европе вообще было чуждо контрастное классовое деление на рабочих и капиталистов, прописанное в советских учебниках. А потому попытка уговорить финских солдат сдать оружие, взывая к их пролетарской совести и сознательности, была, по меньшей мере, наивной»[26]. Тем не менее подобного рода просчеты фиксируются и в начальный период Великой Отечественной войны. При этом в любом случае листовки с призывами сдавать оружие и сохранить

[25] См.: *Toffler A., Toffler H.* War and anti-war. Survival at the dawn of the 21st century. London, 1993. 302 p.

[26] *Лянная Т. А.* На языке врага. URL: https://little-histories.org/2015/05/31/на-языке-врага/ (дата обращения: 25.08.2018).

свою жизнь в плену оказывали на немецких солдат куда большее воздействие уже в ситуации, когда проблема выживания становилась актуальной и безо всякой советской пропаганды, то есть после перелома в ходе войны; одновременно чем более угрожающим становилось в Германии реальное положение дел в тылу и на фронте, тем менее эффективно работала собственная пропаганда нацистов. Собственно, Эллюль полагает, что пропаганда тем эффективнее, чем незаметнее, и именно поэтому полагает «социальную пропаганду» наиболее действенной, хотя и наиболее сложной в организации[27].

Как следствие, можно назвать и второй ключевой недостаток пропаганды — ее по определению массовый характер. Классическая пропаганда ориентирована на массы (своего или чужого) населения или массы военнослужащих, что придает ей достаточно абстрактный, нецелевой характер: она малоэффективна в силу недостаточной таргетированности.

Ориентировочно в 1970–1980 гг. конфронтационное взаимодействие в информационном пространстве выходит на новый уровень. Дж. Стейн в 1995 г. публикует исследование «Информационная война», где подчеркивает, что целью такой войны является не столько текущее настроение (на которое воздействует пропаганда), сколько идеи и эпистемология. Относительно более конкретных целей он утверждает следующее: «Целью информационной войны является человеческий разум, особенно тот, который принимает ключевые решения войны и мира, а также тот, который принимает ключевые решения относительно того, где, когда и как применить потенциал и возможности, которые являются в их стратегических структурах»[28]. Р. Шафрански в том же году пишет: «Система целей информационной войны может включать каждый элемент эпистемологии противника». Ф. Бомар, изучая распространение и оценку информации в условиях военных действий, пишет в 1996 г.: «В парадигме войны знаний стратегическое преимущество зависит

---

[27] См.: *Ellul J.* Propaganda. The formation of men's attitudes.

[28] Здесь и далее цит. по: *Почепцов Г. Г.* Информационные войны: тенденции и пути развития. URL: https://psyfactor.org/psyops/infowar7.htm (дата обращения: 25.08.2018).

не от концентрации на фактах и числах, а от взаимно дополняющего ума тех, кто их интерпретирует. Национально распространенная возможность интерпретации весит больше, чем электронные информационные суперпути»[29]. Таким образом, целью информационной войны нового поколения становится целенаправленное изменение типовой реакции объекта воздействия на ситуацию через трансформацию его мировоззрения либо использование известных элементов мировоззрения противника для создания условий (прежде всего посредством дезинформации), обеспечивающих принятие заведомо ошибочных решений.

Классическим проявлением информационной войны нового поколения следует считать концепцию «мягкой силы». Дж. Най в книге «Bound to Lead: The Changing Nature of American Power» («Призвание к лидерству: меняющаяся природа американской силы», 1990) разделяет мощь государства на две составляющих: так «жесткую силу» (hard power) и «мягкую силу» (soft power). Под «жесткой силой» следует понимать мощь государства в собственном смысле, которая воплощена в его политическом, экономическом и военном потенциале и проецируется посредством соответствующих инструментов. «Мягкая сила» представляет совокупность ценностей, идеологем и культурного потенциала и проецируется посредством пропаганды, демонстрирующей превосходство того или иного мировосприятия в моральном, политическом или социально-экономическом плане[30]. Вот как он поясняет функционирование «мягкой силы» в книге «Мягкая сила. Средства достижения успеха в мировой политике» (2004): «Если Наполеон, распространявший идеи Французской революции, был вынужден полагаться на штыки, то ныне, в случае с Америкой, жители Мюнхена, равно как и москвичи, сами стремятся к результатам, достигаемым лидером прогресса <…> Когда ты можешь побудить других желать того же, чего хочешь сам, тебе дешевле обходятся кнуты и пряники, необходимые, чтобы двинуть людей

[29] *Почепцов Г. Г.* Информационные войны: тенденции и пути развития.

[30] См.: *Nye J.* Bound to lead: The changing nature of American power. New York, 1990. URL: http://www.kropfpolisci.com/exceptionalism.nye.pdf (дата обращения: 25.08.2018).

в нужном направлении. Соблазн всегда эффективнее принуждения, а такие ценности, как демократия, права человека и индивидуальные возможности, глубоко соблазнительны»[31].

Пропаганда собственного образа жизни сопровождается дискредитацией системы ценностей противника, что в результате включает механизмы ее незаметного саморазрушения. Информационная стратегия может быть представлена в виде следующего алгоритма:

— дискредитация всех основных атрибутов общественного устройства: вывод из строя системы управления;

— включение механизмов экономического саморазрушения: создание системы экономического управления через международные институты и финансовые программы «помощи»;

— перепрограммирование населения на новый образ жизни с помощью пропаганды новой системы ценностей: массированная пропаганда через СМИ;

— поддержка любых оппозиционных движений, подкуп элиты: раскол населения на враждующие группы, состояние хаоса и гражданской войны (см. теорию управляемого хаоса[32]);

— маскировка образа агрессора как бескорыстного «спасителя» страны от язв и пороков прежнего «тоталитарного» образа жизни[33].

Таким образом, важнейшим принципом ведения информационной войны является **стремление агрессора непрерывно расширять контролируемое информационное пространство**, действуя в обход сложившихся моральных норм и правил, сознательно нарушая все социальные ограничения и размывая нравственные установки. При этом СМИ концентрируют внимание на скандальных фактах, публикуют конфиденциальные сведения из личной жизни публичных политиков, ведут скандальные расследования, сознательно фальсифицируя информацию, смакуя пикантные подробности. Задача состоит в том, чтобы активизировать подкорковые механизмы чело-

---

[31] *Nye J. S.* Soft Power: The Means to Success in World Politics. N.Y., 2005. P. 8–9.

[32] *Манн С.* Теория хаоса и стратегическое мышление. URL: http://самарина.рф/new/TeoriXaos.html (дата обращения: 25.08.2018)

[33] По: *Василенко И.* Указ. соч.

века, включив механизм манипулирования чувствами и эмоциями людей — еще ле Бон отмечал, что эмоциональное воздействие при работе с массами, с толпой значительно эффективнее логического убеждения. Следует отметить, что известность подобных схем, в частности, их тиражирование СМИ и блогосферой, в свою очередь провоцирует аудиторию на повышенную конфликтность, поскольку ведет к ожиданию подобных действий от реального либо мнимого противника («самосбывающееся пророчество»); кроме того, картина «эпистемологической войны» сама оказывается удобным пропагандистским инструментом. Так в российской инфосфере (в том числе и в научном обороте) до сих пор в ходу так называемый «Меморандум Даллеса»[34], декларирующий перспективу разрушения СССР через подрыв нравственных и культурных устоев народа. В Европе в середине XX в. был в ходу прямой аналог «Меморандума», декларирующий уже подрывные намерения коммунистов по отношению к коллективному Западу — «Коммунистические правила революции»[35]. Подобные «документальные саморазоблачения», представляющие противника как источник эпистемологической угрозы и призванные актуализировать и канализировать агрессию толпы, использовались как инструменты пропаганды и в предшествующие эпохи (можно вспомнить, к примеру, «Протоколы сионских мудрецов» или фальшивое «Завещание Петра Великого»).

В качестве примера успешной военно-информационной компании Г. Почепцов рассматривает информационное сопровождение первой американо-иракской войны в Персидском заливе (1991–1992), где было два основных типа целевой аудитории: иракские солдаты и американское общественное мнение. «В случае иракских солдат активно использовались листовки (их было сброшено 29 миллионов) и радио, которое транслировало свидетельства сдавшихся солдат, перемежавшиеся молитвами из Корана и сообщениями о направленности бомбовых ударов на следующий день.

---

[34] URL: http://infosplanet.info/novoe-vremya/plan-dallesa/ (дата обращения: 25.08.2018).

[35] URL: http://infosplanet.info/xolodnaya-vojna/kommunisticheskie-pravila-revoljucii/ (дата обращения: 25.08.2018).

В результате 75 % сдавшихся подтвердили, что на них повлияли листовки и радио.

Что касается американского общественного мнения, то на него в сильной степени влияло телевидение: было установлено, что чем больше зритель смотрел ТВ, тем более уверенно он одобрял военные действия. Поддержка Дж. Буша превосходила 80 %. Во время военных действий наиболее эффективным средством воздействия на общественное мнение были ежедневные брифинги. Г. Джоветт и В. О'Доннелл увидели в процессе обработки общественного мнения в период подготовки войны в Персидском заливе три этапа <…> На первом, который пришелся на время после вторжения в Кувейт, когда была неопределенность со стороны вашингтонской администрации в связи с неясностью, что именно следует защищать: суверенность Кувейта, американские нефтяные интересы, границы Саудовской Аравии. Второй этап приходится на время после выступления Дж. Буша 1 ноября, в результате произошла резкая эскалация обвинений Саддама Хуссейна, где он был представлен в качестве более страшного врага, чем Адольф Гитлер. В этом контексте к 6 ноября Пентагон разместил в районе более 230 тыс. солдат. Третий этап был самым главным, в рамках него произошел перелом в общественном мнении, получивший название „фактора желтых бантов". Дж. Буш в этот период называл солдат „нашими парнями и девушками". Это была идея поддержки своих войск вне зависимости от поддержки/неподдержки войны в целом. Если в течение трех недель до 18 января неопределившиеся сообщения доминировали над поддержкой в соотношении 45 к 8, то в последующие шесть недель ситуация „желтых бантов" изменилась в соотношении 36 к 19»[36].

Контроль за информационным пространством очевидно требует контроля за каналами коммуникации и СМИ различного рода; соответственно, максимальной эффективности в данной ситуации добиваются глобальные медиахолдинги, такие, как America Online — Time Warner, Walt Disney Co, News Corporation и др. (см. гл. 2 § 2).

---

[36] *Почепцов Г. Г.* Информационные войны: Основы военно-коммуникативных исследований. URL: http://www.ligis.ru/librari_2/049/02.html (дата обращения: 25.08.2018).

При этом важно учесть, что распространяемый медиаконтент, даже с учетом глокализации, так или иначе включает в себя: вкусы, привычки, поведенческие шаблоны; потребительские нормы и товарные бренды; идеи, образы, идеологию и культуру.

Таким образом, глобальный медиаконтент становится инструментом глобальной рекламы и глобальной пропаганды, а глобальный медиарынок является классической сферой реализации концепции «мягкой силы» как инструмент адаптации локальных менталитетов к западной системе ценностей. Следовательно, речь идет о сознательном и целенаправленном использовании инфосферы как среды распространения эпистемологического оружия, причем единственным возможным оправданием этим действиям может служить тезис о цивилизационном превосходстве западных ценностей и западного образа жизни, о прозападной ориентации сознания как абсолютном благе, что уже само по себе предусматривает некритичное, тотальное принятие транслируемых ценностей. В силу тотального количественного, а зачастую и качественного, превосходства западных СМИ информационная победа Запада представляется неизбежной.

Однако это представление основано на идее субъекта, пассивно принимающего информационный поток, что, как правило, не соответствует действительности. Э. Фромм, комментируя информационный вал западных СМИ, говорил об эффекте информационного «перегрева», при котором личность инкапсулируется и превращается в «цифрового аутиста», погруженного в нарциссическую игру отражений в виртуальном мире и игнорирующего все формы социально-политической причастности[37]. Он же, однако, обозначает и траекторию выхода с кривой деградации: по его мнению, человеку как существу, взыскующему смысла, важно опереться на определенную систему нравственных координат — разделить добро и зло, чтобы противостоять внешним обстоятельствам. Когда человек четко идентифицирует себя с определенным обществом, видит себя частью какой-то группы или коллектива, он обрастает нравственными корнями, поскольку предлагаемая обществом систе-

[37] См.: *Фромм Э.* Анатомия человеческой деструктивности. М., 2007. С. 307.

ма культурно-нравственных ценностей становится для него опорой и помогает сохранить себя в агрессивной информационной среде.

Таким образом, сам факт очевидного наличия информационного давления требует мер противодействия и контроля за информационными каналами — если не для проявления встречной экспансии, то (в рамках концепции Realpolitik) для трезвой оценки как позитивной социокультурной составляющей транслируемой информации, выгод, которые могут последовать за принятием транслируемого кода, так и потенциальных или же активных угроз в этой сфере. Поскольку речь идет о культурном коде цивилизационного уровня, то задача, безусловно, входит в круг интересов государства, в число его обязательств по защите граждан страны и суверенитета. Существенно, что реакция западных политиков в ситуации явной или мнимой эпистемологической угрозы оказывается абсолютно симметричной[38]. То есть если степень воздействия информационной угрозы и может быть отнесена к области дискуссий, то игнорировать ее *в принципе* государство, претендующее на минимально самостоятельную позицию в геополитическом конгломерате интересов, попросту не имеет права и обязано принимать контрмеры.

«В тактике информационного противоборства можно выделить три наиболее часто использующихся приема ведения борьбы:

— размещение негативной информации с целью вызвать реагирование противника заранее в более выгодном для себя контексте („упреждающий удар“);

— размещение информации с целью определения реакции общественного мнения („пробный шар“);

— размещение информации с целью восстановления целостности своего информационного пространства („информационный контрудар“).

В более выигрышной позиции в информационной войне оказывается тот, кто нападает.

---

[38] См, напр., URL: https://www.novayagazeta.ru/news/2017/03/30/1302836 ; https://ria.ru/accents/20170712/1498353728.html ; http://zondnews.ru/news/SSHA-obvinili-Rossiyu-v-podryve-amerikanskikh-tsennostey/3732 (дата обращения: 25.08.2018) и др.

Тактика информационного воздействия строится на следующих закономерностях:

— эмоциональное сообщение сильнее рационального;

— фактическое сообщение сильнее интерпретирующего;

— сообщение о знакомом объекте сильнее, чем о незнакомом.

Информация может быть модифицирована в трех плоскостях:

— запрещена;

— распространена ограниченно;

— изменена.

Система управления информацией должна соответствовать четырем параметрам:

— целесообразности (исходим исключительно из целей и задач);

— нестандартности (индивидуальный подход к любой ситуации);

— оперативности;

— последовательности (четко прописанный и продуманный план действий)»[39].

Доктрина информационной безопасности гражданина Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646, оговаривает следующие понятия:

а) национальные интересы Российской Федерации в информационной сфере <…> — объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) угроза информационной безопасности Российской Федерации <…> — совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее — информационная безопасность) — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная

[39] Цит. по: *Моисеева О. А.* Россия в глобальном информационном пространстве : учеб.-метод. комплекс. М., 2013. С. 61–62.

целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) обеспечение информационной безопасности — осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления[40].

Характеризуя ситуацию в инфосфере, доктрина отмечает (выдержки):

<…> 12. Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации.

Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей <…>

19. Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств ис-

[40] См.: URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 25.08.2018).

пользовать технологическое превосходство для доминирования в информационном пространстве.

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети Интернет, не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими <…>

В качестве основных направлений обеспечения информационной безопасности доктрина называет (п. 23):

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами; <…>

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

Таким образом, фиксируя стремление к равноправному партнерству в информационной сфере, доктрина прописывает систему действий российского государства по сохранению геокультурного кода в условиях актуального информационного давления, определяя для этого организационно-правовые и управленческие нормы на ближайшую стратегическую перспективу.

Осознание инфосферы как сферы столкновения интенций и интересов субъектов геополитической игры делает особо актуальной проблему ***символического капитала***, которую можно определить как проблему «высокого престижа ценностей и принципов, на которых организовано пространство власти, что заставляет живу-

щий на этом пространстве народ и все окружающие его народы уважать сложившуюся систему геополитических сил. Современная политическая история знает два пути завоевания символического капитала в геополитике — через овладение символизмом культуры и через овладение символизмом идеологии»[41]. Под символизмом культуры здесь подразумевается творческое освоение путей духовного само-стояния, созидания духовной общности как осознанной реализации над-личностной задачи субъекта в истории с опорой на традицию и знанием перспектив, возможных развилок и цены выбора, следовательно, общность судьбы народа и власти. Символизм идеологии предполагает выработку форм адаптирующего сознания, комфортных прежде всего для власть имущих или на власть претендующих, но создающих видимость комфорта в силу навязываемого исторического и/или культурного выбора, что предоставляет субъекту сомнительное благо отказа от ответственности.

Здесь можно вспомнить продолжающиеся дискуссии об анонимности в инфосфере, где сторонники анонимности отстаивают оговоренное международными соглашениями право субъекта на приватность и опасаются деанонимизации как шага к цензуре и политическим репрессиям, в то время как их противники говорят как раз об ответственности, в том числе, допустим, ответственности распространителей экстремистского, порнографического и т. п. противозаконного контента. Не рассматривая специально юридическую сторону вопроса, авторы действительно не видят причин, по которым публичное высказывание в сети Интернет обязано создавать условия более безопасные, чем иные формы публичных действий и высказываний. Возьмем, к примеру, ситуацию политической борьбы. Если представитель оппозиции не боится участвовать в уличных акциях, оспаривая стратегию или тактику действующей власти и считая свои действия правильными, готов принимать их последствия, включая репрессии, то почему, допустим, Интернет должен сохранять статус «островка безопасности», гарантирующего безответственность за действия в инфосфере? Если учесть, что правоохранительные/репрессивные (в зависимости

[41] *Василенко И.* Указ. соч.

от оценки) органы в результате целенаправленных усилий обычно без труда пробивают завесу достаточно условной анонимности в инфосфере, то анонимность действительно мешает более самим пользователям Сети, чем условному репрессивному государству. Апелляция к проблеме кибербуллинга также не безупречна, поскольку в случае деанонимизации анонимность теряет не только преследуемый, но и преследователь. Хотя, в любом случае, вопрос сохраняет дискуссионный статус во всем мире[42].

Таким образом, если российское общество действительно претендует на причастность к культурным ценностям, принципиально отличным от символического кода западной цивилизации, то единственно правильным действием становится продвижение этих ценностей как во внешней, так и во внутренней информационной среде, поскольку (наряду с «социологической пропагандой» Эллюля) это нормальный способ их само-стояния, причем вполне адекватный и либеральной системе ценностей при условии сохранения свободной конкуренции идей. Проблема в том, что в условиях глобального доминирования одной точки зрения и контроля над основными коммуникативными каналами со стороны ее носителей, о «свободной конкуренции» речи идти не может. Соответственно, основной задачей становится создание и развитие каналов коммуникации, способных донести до субъектов российскую точку зрения на критически значимые ситуации и вызовы.

9 декабря 2013 г. президент России Владимир Путин подписал указ о ликвидации информационного агентства «РИА Новости» и создании на его базе международного информагентства «Россия сегодня» с государственным финансированием (государственное унитарное предприятие)[43]. Его генеральным директором был назначен Дмитрий Киселев. По его словам, агентство создано с целью «восстановления справедливого отношения к России как важной страны мира с добрыми намерениями»[44]. М. Симоньян, главный

[42] URL: https://tinyurl.com/y8yvdmcs (дата обращения: 25.08.2018).

[43] URL: http://россиясегодня.рф/ (дата обращения: 25.08.2018).

[44] URL: https://www.vesti.ru/doc.html?id=1165191 (дата обращения: 25.08.2018).

редактор медиагруппы, утверждает: «Акцент в работе будет сделан на увеличении доли эксклюзивной информации и формировании повестки дня, которая отличалась бы от принятой в большинстве СМИ. Зачастую журналисты из мейнстрим-медиа, особенно в Соединенных Штатах и Западной Европе, предпочитают не замечать те проблемы в своих странах, по которым они имеют обыкновение критиковать других, в том числе Россию. По многим мировым вопросам — взять хотя бы ситуацию вокруг Украины и Крыма, Сирии, Ирана, ситуацию в самих Соединенных Штатах — подавляющее большинство СМИ занимают одну и ту же позицию. Они — одинаковые. Мы — другие. При этом общественность за рубежом испытывает потребность в такой альтернативной точке зрения <…> Агентство будет рассказывать не только и не столько о России, сколько мировому сообществу о мировых событиях, но с российским взглядом. Россия — это ведущий мировой игрок, и ее голос должен быть слышен всегда. С нашей помощью все желающие за рубежом смогут получить информацию о позициях и интересах Москвы „из первых рук“, а не только в интерпретации зарубежных коллег, как это часто происходит»[45].

МИА «Россия сегодня» объединяет радиовещание, новостные ленты на русском, английском, испанском, арабском и китайском языках, информационные порталы на десятках языках, мультимедийные международные пресс-центры, производство и распространение фотоконтента и инфографики, информационные продукты в социальных сетях и производство контента для мобильных приложений. В России медиагруппа «Россия сегодня» развивает информационные ресурсы на русском языке: информационное агентство РИА «Новости», агентство экономической информации «ПРАЙМ», агентство спортивной информации «Р-Спорт», информационное агентство РИА «Недвижимость», рейтинговое агентство РИА «Рейтинг», портал переводных материалов зарубежных СМИ «ИноСМИ». За рубежом медиагруппа представлена международным новостным агентством и радио с мультимедийными информационными хабами Sputnik. Основной целевой аудиторией

[45] URL: http://jourdom.ru/news/47614 (дата обращения: 25.08.2018).

МИА, по мнению редакции, являются зарубежные СМИ, ведущие международные компании, политические партии, дипломатические миссии, государственные ведомства, некоммерческие организации, а также русскоязычные слушатели за рубежом.

Помимо новостных агентств, в продвижении российской повестки и аналитической работе в инфосфере участвуют ряд НКО и коммерческих организаций. Так, Минфин РФ выделяет в 2018 г. субсидии фонду Горчакова и РСМД, призванным, соответственно, осуществлять «поддержку публичной дипломатии, содействие участию российских неправительственных организаций в международном сотрудничестве, активное вовлечение институтов гражданского общества во внешнеполитический процесс» и «оказывать содействие в проведении международных внешнеполитических исследований, подготовке специалистов в области внешней политики и регионоведения, а также взаимодействии российских научных организаций с иностранными экспертно-аналитическими центрами по вопросам международных отношений»[46]. Субсидии из федерального бюджета также получают «Фонд поддержки и защиты прав соотечественников, проживающих за рубежом» и фонд «Русский мир». С 2011 г. также действует НКО Фонд развития и поддержки международного дискуссионного клуба «Валдай», которая управляет всеми проектами клуба. С 2014 г. клуб «Валдай» занимается «практически ориентированной работой по формированию глобальной повестки дня», говорится на его сайте. «Валдай» ежегодно собирает ведущих западных экспертов, интересующихся Россией, традиционно с участниками клуба проводит официальные встречи президент Владимир Путин[47].

На данный момент следует признать, что российские информационные проекты если и не являются безусловно успешными, то, во всяком случае, стали заметным явлением мирового медиарынка. Так, по данным ИНТЕРФАКС, на 2017 г. МИА «Россия сегодня»,

---

[46] URL: https://www.rbc.ru/economics/24/07/2017/59723c879a794741088d42d8 (дата обращения: 25.08.2018).

[47] См.: Валдай: Международный дискуссионный клуб. URL: http://ru.valdaiclub.com/ (дата обращения: 25.08.2018).

телеканал и социальные медиа Russia Today прочно занимают лидирующие позиции по цитируемости в российских СМИ[48]. Аудитория холдинга превысила 35 млн уникальных пользователей в месяц. Своего рода признанием заметности российской информационной политики можно считать, например, рассекреченный в апреле 2018 г. «Доклад по российским активным мероприятиям» Комитета по разведке палаты представителей конгресса США, где прямо указывается на Информагентство «Россия сегодня», радио Sputnik, телеканал RT и издание Russia Beyond the Headlines как часть «российского аппарата медиапропаганды», который применялся для «вмешательства в выборы». «Российское правительство использовало RT для продвижения своей кампании по негативному влиянию во время президентских выборов 2016 года в США», — говорится в отчете. В комитете утверждают, что у них есть «достаточные доказательства» того, что RT контролируется российскими властями (что достаточно странно, поскольку для такого утверждения не требуется глубокая аналитическая работа — достаточно просмотреть уставные документы компании), и «этот контроль позволил Кремлю использовать RT для продвижения своей кампании по вмешательству в выборы в 2016 году»[49]. Таким образом, если информационная война — реальность, то она далека от завершения, и даже в отдаленной перспективе ее результат не очевиден.

Комплексный анализ ***героического*** дискурса в инфосфере ожидаемо продемонстрировал его внутреннюю непротиворечивость. Этот подход компактно и последовательно описывает практически любые реалии глобального информационного пространства в его статике и динамике и может служить (и служит) основой для практических действий в сфере управления и законотворчества, характерных в том числе и для действующей власти РФ. В целом его

---

[48] См. http://www.unkniga.ru/vistavki-konferents/8106-mediatrendy-2017-v-prioritete-analitika.html (дата обращения: 25.08.2018).

[49] Цит. по: URL: https://russian.rt.com/world/news/507493-kongressa-ssha-rt-vmeshatelstvo, при этом на момент проверки (ноябрь 2018) референтный документ удален с сайта Конгресса.

концепты укладываются в канон рекомендаций *административной, или классической, школы управления*:

Объект: организация. *Цель*: доминирование с сохранением границы. *Ценности*: стабильность, безопасность. *Принципы*: централизация, регламентация, эффективность, инициатива, контроль, традиция. *Структура*: неизменная, прозрачная, пирамидально-иерархическая. *Личность*: функциональна, специализирована, неизменна. *Тип развития*: экстенсивный. *Практика*: героический подход, персонифицированный бог-хозяин, имеющий право на произвол, «культ личности» в различных формах. *Боги* (*творцы концептов*): Платон, Конфуций, Сунь Цзы, А. Смит, К. Е. Дюринг, А. Файоль, Ф. У. Тейлор, Г. Форд, М. Вебер. *Утопия*: Т. Мор «Утопия». *Антиутопия*: Е. Замятин «Мы».

Однако, даже если оставить за рамками описанные уже Вебером принципиальные недостатки административной школы, применение ее как эпистемологической основы действий в инфосфере приводит к ряду специфических и, видимо, критических проблем:

Богоизбранность. Установка на иерархию, на «знание своего места» требует безоговорочного авторитета власти, персонификации и несменяемости (см. феномен «личных структур» Александра, Чингиз-хана, Наполеона, Форда, Сталина, Кастро, «безальтернативности» Ельцина и в настоящее время Путина и Си Цзинпиня) — источник явного напряжения между декларируемой властью доктриной и реальностью, а также источник возможного кризиса (вплоть до катастрофического отказа системы) в ситуации, когда смена власти необходима по естественным причинам.

Тотальность. Изоморфность, прозрачность и несменяемость структуры заставляют использовать в качестве единственно допустимой эпистемологии ту, которая наиболее близка (или наиболее удобна) правящей элите, что де-факто размывает границу между «символизмом культуры» и «символизмом идеологии», заставляя минимально самостоятельного субъекта использовать в качестве единственно возможного цинический модус восприятия и объявить «чуждой» и «враждебной» любые отклонения — даже в бытовых мелочах, ввиду их неизбежной включенности в социокультурное поле. В случае найденного — реального или мнимого — совпадения

эпистемологий внутренних диссидентов и внешних контрагентов инфосферы автоматически формулируется вывод о заведомой ангажированности диссидента. Это и «русские деньги» как источник популярности ультраправых партий, евроскептиков и сепаратистских движений в Европе с одной стороны, и ярлыки типа «пятая колонна», «вашингтонский обком», «деньги Сороса» — с другой; отсюда же стремление в любой ситуации искать единственный источник, «центр силы», «выгодополучателя», что зачастую приводит к увлечению разнообразными «теориями заговора». Это заставляет власти тратить громадные ресурсы на контроль, при этом в многоукладном и поликультурном обществе (например, в РФ) задача представляется малореализуемой на практике. На уровне социума это ведет к нарастанию внутреннего напряжения, повышению уровня агрессии, в конечном счете — к доминированию цинического модуса в инфосфере и к разрушению национальной социокультурной общности: жесткая система неизбежно хрупка, и даже локальная демонстрация ее несостоятельности может обернуться тотальным крушением, как разрушилась социокультурная система Японии XIX в., столкнувшись с военно-дипломатическим давлением коммодора М. К. Перри и в конечном счете необходимостью заключить с мировыми державами неравноправные Ансэйские договоры.

Конфликтность. Героический подход нацелен на войну по определению, не считается с имеющимися ресурсами и игнорирует затраты.

Эгоцентризм, переходящий в самодовольство. Командно-административная эпистемология исходит из предположения о том, что действие, основанное на идеалах — привилегия и исключительное качество «своих», именно потому, что только «своя» эпистемология и собственные идеалы признаются актуальными. Сама возможность существования иной нравственной нормы, иных идеалов и иной искренности не допускается по определению или же описывается в терминах «империи зла», «Мордора» и т. п. Соответственно, предполагается, что оппоненты в информационном пространстве ***всегда*** только апеллируют к идеалам в пропагандистских целях, на деле прикрывая этим экономические интересы и претензию на полити-

ческое доминирование. Показательным примером служит система ***взаимных*** обвинений между западными и российскими политиками — в пренебрежении международным правом, интересами и жизнями гражданского населения в различных странах, правами человека и нравственными нормами. С другой стороны, обнаруженные формальные совпадения в той или иной области ведут к необоснованному выводу о совпадении ценностей и/или интересов (см. рассуждения о «стратегическом альянсе» России и Китая без сколь-нибудь серьезных подтверждений с китайской стороны, а также романтический образ «демократических» преобразований в ходе «арабской весны» в западной прессе). Какой-либо предметный диалог в таких условиях вообще возможен исключительно в циничном модусе Realpolitik, что не только препятствует взаимопониманию, но и искажает стратегическую перспективу, не позволяя корректно прогнозировать действия контрагентов коммуникации.

Непротиворечивость. Жесткая структура, тотально контролируемая и рассчитанная на максимальную эффективность, рано или поздно оказывается тормозом в развитии системы, поскольку развитие есть изменение, а структура изначально рассчитана на неизменность. Традиция провозглашается самостоятельной ценностью (а не отражением ценностных ориентиров), то есть должна быть сохранена даже ценой эффективности. Соответственно, жестко организованная структура может быть эффективна на короткой дистанции, но неизбежно проигрывает в исторической перспективе. Это мы видим по истории взлета и падения «Форда-Т» или истории упадка командной экономики и системы пропаганды СССР.

Замкнутость. Героический подход в инфосфере изначально ориентирован на сохранение границ. Такое сохранение возможно только при условии объявления информационной реальности самодостаточной («духовные скрепы», «культурный код», «единственно верное учение», «истинная вера» и т. п.), то есть при условии тенденции к игнорированию собственно ***информационной составляющей информационного поля***, которое в этом случае превращается исключительно в сферу враждебных или дружественных интенций. Соответственно, это установка в конечном счете исключает возможность принятия адекватных ситуации политических решений

ввиду отсутствия у элиты доступа к объективной картине реальности, подмененной идеологической доктриной (отсюда вторжение СССР в Афганистан, отсюда феномен «Крестового похода детей», отсюда же и вторжение войск Коалиции в Ирак).

Административный подход не терпит конкурентов и вытаптывает конкуренцию. Его конечная (не обязательно осознаваемая) цель, описанная Замятиным, одиночество регулируемого, машиноподобного совершенства в пустыне, где структура в конечном счете будет обречена на тепловую смерть. Даже если подобная «победа» в информационной войне подъемна экономически и возможна технически, вряд ли сами носители административного идеала действительно хотят его воплощения на практике. Но есть ли работоспособная альтернатива?

§ 2. Эволюционный, или диссоциативно-психопатический, подход. Неомарксистский фатализм: Homo Economicus в ожидании сингулярности

В последнее десятилетие инфосфера и связанные с ней события все чаще описываются как бой Давида с Голиафом. Дж. Ассандж и проект WikiLeaks, Э. Сноуден, хакеры группы Anonimus или владельцы и разработчики мессенджера Telegram по разным причинам вступают в схватку со всемогущими государственными структурами, корпорациями, спецслужбами и при всей ограниченности ресурсов, оказываются опасными, а временами и неодолимыми противниками. Недавняя история противоборства Telegram и Роскомнадзора — классический пример того, как могущественное, но неповоротливое надзорное ведомство под саркастические комментарии субъектов инфосферы пытается справиться с современным, технически продвинутым и организованным по распределенному принципу сервисом[50]. Даже попытки

[50] См.: URL: https://ura.news/articles/1036274596 (дата обращения: 25.08.2018) и др.

блокировать IP-адреса «по площадям» привели не к остановке работы мессенджера, а к многочисленным перебоям в работе не связанных с ним российских информационных сервисов, в том числе государственных. Об аналогичном эффекте см. в гл. 3 в параграфе о кибервойнах: при несопоставимом уровне финансирования, технического обеспечения и права доступа к бекдорам на административно-государственном уровне у военно-информационных подразделений в России и США, видимо, следует говорить о сопоставимой эффективности этих структур, и именно русские и китайские (а не американские) хакеры стали популярной страшилкой массмедиа. Тем убедительнее становится тезис о принципиальной непобедимости сетевых структур иерархическими: с сетью может конкурировать только сеть. Причем речь идет в строгом смысле не о непобедимости конкретного субъекта в инфосфере. Скорее, речь идет о том, что сетевые инструменты доступны, адаптивны и вариативны, что в силу несопоставимой разницы в накладных издержках делает тактику Голиафа принципиально проигрышной вне зависимости от профессионализма исполнителей, уровня используемой техники и вложенных средств. В условиях информационной революции архаически организованное количество начинает критически проигрывать качеству.

Централизованный подход к инфосфере опирается на доктрины исторического (то есть ретроспективного) единства, сохранения традиционных (патриотических, демократических, религиозных, национальных, гендерных, расовых и т. п.) ценностей, охраны эпистемологической границы. Он привязан к локальному восприятию, принципу единства территории, в то время как этот принцип уже сейчас изживает себя с развитием возобновляемой энергетики, не нуждающейся в будущем в транспортировке энергоресурсов, а зачастую и в масштабных электросетях, с развитием технологии трехмерной печати, подрывающей традиционную систему торговли и снимающей задачи контроля за торговыми путями, с открытостью информационного пространства, дезавуирующей саму возможность достижения культурной тотальности в каком бы то ни было регионе без принудительной изоляции этого региона от всемирной инфосферы, что неизбежно приведет к потере темпа обмена информацией,

технологическому упадку и экономической стагнации и одновременно снимающей с повестки дня вопрос о перемещении человеческих ресурсов ввиду возможности работы профессионалов в удаленном режиме[51]. Командно-административный подход, как и героический метод мышления, экономически затратны и поэтому неизбежно проигрывают более мобильным схемам в стратегической перспективе, а в ряде случаев — и в прямом тактическом столкновении.

События «Арабской весны» в Северной Африке и на Ближнем Востоке зачастую называют «революцией социальных сетей». Несмотря на то, что число реальных пользователей сетей «Фейсбук» и «Твиттер» на момент начала протестного движения в странах региона не превышала 20 %, для организации масштабных выступлений этого оказалось достаточно, что во многом было обусловлено как особенностями национального и панарабского информационного пространства, так и предпосылками экономического и социального характера. «Наиболее вероятным объяснением беспрецедентно успешной роли социальных сетей в тот период представляется их направленность на конкретную целевую аудиторию: молодых образованных пользователей Интернета, проявляющих интерес к внутриполитическим процессам и выражающих недовольство своим социальным статусом и уровнем дохода. Именно эта группа населения стояла у истоков протеста в Тунисе, Ливии и Египте, где экономический рост, улучшение качества здравоохранения и демографический взрыв в 1970–1980-х гг. привели к возникновению так называемого молодежного бугра — резкого увеличения численности населения в возрасте до 30–35 лет, что сопровождалось ростом безработицы среди квалифицированных специалистов, обусловленным преобладанием предложения над спросом на рынке труда. На этом фоне социальные сети стали наиболее эффективным средством воздействия на протестую аудиторию <…> Значительную роль в росте популярности социальных сетей как основного источника информации сыграли горизонтальные связи

[51] См., напр., доклад П. Щедровицкого. URL: https://www.znak.com/2017-12-12/petr_chedrovickiy_pochemu_rossiyskaya_ekonomika_i_obrazovanie_ne_uspevayut_za_ostalnym_mirom (дата обращения: 25.08.2018).

между пользователями, то есть сама природа сети, в которой все участники связаны между собой и способны свободно принимать и передавать информацию»[52]. При этом борьба правящих режимов с распространением в сетях антиправительственной информации, лозунгов, созданию организационных структур «сетевой» революции оказывались безуспешными в той степени, в которой режимы действовали в рамках командно-административной модели, то есть методом запретов и репрессий. По большому счету, это лишь способствовало формированию альтернативной информационной инфраструктуры, окончательно ускользавшей из-под правительственного контроля. Большего успеха власти достигли там, где ограничились мониторингом социальных сетей, а также информационной поддержкой собственной деятельности и политики, что было на том же горизонтальном уровне поддержано лояльной правящему режиму части населения. Характерным моментом было смещение политической активности от традиционных, опять-таки централизованных, структур типа оппозиционных партий, к стихийно возникающим сообществам, возглавляемым политически активными субъектами, но прежде всего действующим по принципу самоорганизации. Важным моментом стало преимущественное участие в событиях образованной молодежи и доминирование политических лозунгов и требований, несмотря на серьезные экономические проблемы, определяющим стали анализ стратегических проблем стратифицировавшихся режимов, тормозивших экономическое и политическое развитие собственных стран, и осознание актуальности личных и коллективных усилий в политическом процессе, принципа человеческого достоинства, а также владение информационными технологиями, что в меньшей степени доступно представителям социальных низов[53]. «Человечество пережило за не-

[52] *Орлов С.* Роль социальных сетей в организации протестных выступлений населения в ходе «арабской весны» (2014) — Зарубежное военное обозрение. 2014. № 12. С. 51–54 ; *Васильев М.* ИКТ как фактор «Арабской весны». URL: https://www.geopolitica.ru/article/informacionno-kommunikativnye-tehnologii-kak-faktor-arabskoy-vesny (дата обращения: 25.08.2018).

[53] См. напр., URL: http://studbooks.net/575895/politologiya/internet_faktor_protestnyh_dvizheniy (дата обращения: 25.08.2018).

сколько последних столетий существенную социально-культурную мутацию, заставляющую говорить о смерти „человека природы“ и рождении „человека культуры“. Человек обеспечивает свое существование не столько путем прямого потребления природных ресурсов, сколько путем их культурной переработки. Он все менее зависит от реальностей природы, и все более — от социальной и технологической ситуации культуры. Прежняя культурная ситуация, характеризующаяся балансом репродуктивных потребностей и культурно-продуктивной активности человечества, сменяется ситуацией, когда культурно-производительная деятельность далеко опережает репродуктивную потребность. В качестве „избытка“ создается новый мир, новая оболочка культуры, не имеющая аналогов в природе и истории. Соответственно, традиционные формы и механизмы жизни, которые тысячелетиями поддерживали „симбиоз“ и были ответственны за самосохранение человечества или перестают действовать, или даже становятся препятствием на пути самосохранения»[54].

Последний момент принципиально важен. Фактически речь идет о ситуации, когда центром социальной активности становятся субъекты, способные игнорировать низший, физиологический уровень иерархии потребностей, сделав ставку на высший по Маслоу — на самоактуализацию, причем именно инфосфера дает этим субъектам как инструмент самоактуализации, так и реализацию потребностей более низкого уровня, например, потребности в признании и уважении. Отметим, что страны Северной Африки и Ближнего Востока, подвергшиеся политическим трансформациям в ходе «Арабской весны», или страны Центральной Европы, Кавказа и Средней Азии с их «цветными революциями»[55] по ряду показателей, связанных с низшими уровнями иерархии — сытость, безопасность и т. д. — демонстрировали в среднем по региону вполне приемлемый или даже высокий уровень. Разумеется, активисты

---

[54] *Назачук А. В.* Этика глобализирующегося общества : учеб. пособие. URL: https://studfiles.net/preview/593669/ (дата обращения: 25.08.2018).

[55] См., напр., URL: http://elect-assist.ru/socialnye-seti-v-cvetnyx-revolyuciyax/ (дата обращения: 25.08.2018).

революций обещали своим последователям, что и по этим показателям жизнь общества улучшится, и также разумеется, что как минимум на первом этапе (а в случае Сирии, Ливии или Украины речь явно идет о более длительных сроках) на практике произошло обратное. Тем не менее значимо именно стремление отказаться от сиюминутных «экономических» интересов во имя ценностей более высокого порядка, и здесь показательным становится термин «революция достоинства» как попытка самоидентификации политически активных субъектов через над-физиологический уровень. Поскольку инфосфера становится не только сферой межсубъектной коммуникации, но и сферой производства, «человек культуры» приобретает безоговорочное и кумулятивно накапливающееся экономическое преимущество перед «человеком природы»; таким образом, в реальности можно говорить о «включении» физиологических потребностей в потребности более высокого уровня, с одной стороны, и об экономической составляющей культурных потребностей — с другой. Культура и образование как средство повышения экономической состоятельности субъекта сами необходимо монетизируются, а экономическая доминанта как инструмент описания субъекта, социума и дискурса выходит на первый план. При этом глобальный и инновационно-технологический характер современных экономических процессов диктует этому новому Homo Economicus ряд ценностных сдвигов, которые идут вразрез с традиционной системой ценностей, необходимо привязанной к локусу, сохранности этнокультурной группы, межпоколенческой преемственности в языковой, социальной, религиозной сфере, что обеспечивает сохранность устоявшихся производственных моделей. Экспоненциальное развитие технологий, гибкое индивидуализированное производство, не требующее специальных усилий субъекта система распределения и обслуживания в рамках «интернета вещей» и возможность актуального, экономико-культурного участия удаленного субъекта практически в любых формах коммуникации (развлечение, обучение, производство, собственно общение, творчество и т. д.) позволяют в ближайшей перспективе говорить:

— о неизбежной и окончательной атомизации субъекта, который все меньше будет нуждаться для своего выживания в таких

устоявшихся формах, как семья, род, община, нация, государство; следовательно, о неизбежном упадке и отмирании этих форм в обозримой перспективе (например, категории «нации», «национальной культуры», «национальной памяти» будут неизбежно терять актуальность с ростом возможностей адекватного машинного перевода и, соответственно, с нивелированием языкового барьера);

— о формировании в коммуникативной среде новых общностей, связанных прежде всего с общностью способа вовлечения субъекта в глобализированный производственный процесс (это может быть не только сообщество сотрудников транснациональной корпорации, но и, например, сообщество фрилансеров), но также и с предпочтительными для субъекта формами досуга, религиозных верований, сексуального поведения и т. п.; при этом подобные сообщества принципиально будут находиться между собой в слабо иерархизированных горизонтальных связях, предполагая экономически обусловленную толерантность как базовую идеологию, возможность вовлеченности субъекта в неопределенно множественное количество подобных сообществ и одновременно конкуренцию за преимущественное внимание субъекта, осуществляемую через формирование максимально приемлемого для него дискурса (причем принцип «приемлемости» будет определенно доминировать над принципом «достоверности» во всех случаях, где принцип достоверности не является производственно необходимым; равным образом, эстетическая приемлемость, оформленность, подача, дизайн информации становятся для субъекта более значимыми, нежели точность, логическая выстроенность и непротиворечивость, при условии гарантированного наличия в инфосфере множественных взаимодополняющих дискурсов);

— о развитии механизмов «обратной связи» как формы взаимодействия субъект/техносфера, субъект/инфосфера, субъект/сообщество, сообщество/сообщество, субъект/субъект, а также, вероятно, взаимодействия субъекта с самим собой в процессе образования и саморазвития. Именно механизмы обратной связи и тотальной коммуникации, вовлеченности в дискурсы, приобретут статус новых форм политической активности как напрямую влияющие на коммуникативный (а соответственно, и экономический) статус субъекта

(в современной политической мысли эта тенденция реализуется в концепции ***делиберативной политики*** Д. Дьюи и др.)[56];

— о разрушении потребности в «privacy» как избыточной в ситуации тотальной вовлеченности субъекта в инфосферу и в конечном счете о разрушении категории личности как устойчивого и стереотипизированного комплекса реакций на любые возможные вызовы информационной среды; субъект инфосферы по преимуществу становится фокусом восприятия непрерывно возрастающих объемов информации, что в близкой перспективе указывает на осознанную недостаточность врожденных возможностей биологического человека и на переход к целенаправленному расширению этих возможностей с использованием технологических средств — имплантов и др. — и одновременно точкой преломления информационных потоков, придающего экономическую целесообразность его активности;

— о развитии и распространении механизмов совместной творческой и производственной деятельности во всех сферах, включая единичное и массовое производство, проектную деятельность, управление, науку, «высокую» и «массовую» культуру; о размывании границ между «элитарным» и «массовым» как в культуре, так и в потреблении, об отказе от уникальности (неизбежно тиражируемых в инфосфере) объектов, которая трансформируется в уникальность потребления как переживания и акта коммуникации; об отмирании категории авторства и, соответственно, «авторского права»;

— о прогнозируемом болезненном столкновении «сетевой» эпистемологии с традиционными формами мировосприятия, в том числе в сознании самого субъекта.

В книге «Война и мир в глобальной деревне» М. Маклюэн говорит, что появление новых технологий изменяет сенсорное восприятие окружающей среды, разрушая самоидентификацию человека и вынуждая к адаптации и видению мира в «зеркале заднего вида».

---

[56] *Dewey J.* The Public and its Problems. Chicago, 1954. 195 p. ; *Cohen J.* Deliberation and Democratic Legitimacy // A. Hablin, B. Pettit, The Good Polity. Oxford, 1989. 204 p. ; *Habermas J.* Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Frankfurt am Main, 1998. 704 p.

То есть человек не может осознать процесс, внутри которого находится, и описывает его в категориях, порожденных предшествующим этапом развития. Автор называет такой процесс перехода от одного сенсорного восприятия к другому само-ампутацией, сравнивая нивелируемые технологиями сенсорные способности с ампутированным органом, который продолжает вызывать фантомные боли. Таким образом, уже утратив традиционные ценности, человек испытывает тоску по ним и пытается вернуть их, в ряде случаев разрушая собственное существование (отсюда феномен возрастающего влияния религиозного фундаментализма). Согласно Маклюэну, попытки восстановить утраченную самоидентификацию приводят к войнам, в то время как любая война стимулирует новые технические разработки, которые оказываются внедренными в среду и провоцируют новую утрату самоидентификации. Таким образом, любая (в том числе информационная) война является не средством утверждения тех или иных идей, но скорее средством разрушения любых идей (прошлого!) как основы устоявшихся общностей, одновременно заставляя генерировать новые идеи, адекватные настоящему и предваряющие будущее[57].

С другой стороны, инфосфера как сфера экономического и политического со-творчества впервые создает адекватную и всеобще значимую среду для «коммуникативных действий» Ю. Хабермаса, предполагающих:

— ориентацию на взаимопонимание как механизм координации действий;

— разведение ситуации действия и ситуации речи;

— «фон жизненного мира», задающий условия и ресурсы взаимопонимания;

— «сферы референций» или «притязания высказываний на значимость»: взаимопонимание подразумевает достижение согласия на уровне знания, нормы, оценок и чувств[58].

---

[57] См.: *Маклюэн М.* Война и мир в глобальной деревне / М. Маклюэн, К. Фиоре ; пер. с англ. М., 2012. 219 с.

[58] См.: *Хабермас Ю.* Моральное сознание и коммуникативное действие / пер. с нем. СПб., 2001. С. 324–340.

Принцип обратной связи и опредмечивающаяся информация «интернета вещей» допускают не просто свободный выбор субъекта между возможными дискурсами (как показывает тот же Хабермас[59], в этом случае даже формально неструктурированная и неструктурируемая множественность дискурсов-«подсфер» Интернета оказывается в конечном счете подконтрольна государству и рынку, превращая частного субъекта в нарциссирующего потребителя), но коммуникативную активность субъекта, непосредственно участвующего в формировании дискурса — в рамках произвольно выбранной субъектом стратегии, но необходимо с ориентацией на взаимопонимание, что в конечном счете снимает с повестки дня проблему отчуждения. В свою очередь, это позволяет говорить о соединении классической веберовской эпистемологии социума, ориентированной на интересы, и эпистемологию публичной сферы Хабермаса и его учеников, ориентированную на достижение взаимопонимания, поскольку именно в инфосфере взаимопонимание и взаимодополнение приобретают характер осознанной, экономически обусловленной необходимости, причем субъект одновременно получает для этих целей максимально представимую инструментально-техническую поддержку со стороны программной и аппаратной инфраструктуры. Дискурс, в свою очередь, приобретает свойство прямого воздействия на реальность, ограниченного, однако, волей конечного субъекта, то есть становится сферой онтологии морали. «Идея ***дискурсивной этики*** несет в себе простую и ясную практическую установку, которая призвана служить адекватным ответом перед лицом глобальных вызовов современности: быть универсальной этикой коллективной ответственности за будущее человечества. Только в ходе свободного и ответственного обсуждения проблем своего самосохранения человечеству могут открыться неведомые прежде возможности и силы для их преодоления, для управления своей собственной судьбой»[60].

---

[59] См.: *Habermas J.* Further Reflections on the Public Sphere // ed. C. J. Calhoun. Habermas and the Public Sphere. Cambridge Mass, 1992. P. 425–429.

[60] *Назарчук А. В.* Указ. соч.

В сфере экономической активности дискурсивная этика реализуется прежде всего в интегративной, личностно ориентированной корпоративной культуре, которая предполагает:

— восприятие сотрудником себя как субъекта, чья профессионально-трудовая деятельность влияет на общую результативность деятельности предприятия и определяет стратегию его развития;

— осознанное принятие личной ответственности за общий продукт совместной деятельности организации;

— ориентацию сотрудника на самостоятельный поиск, разработку, выбор и воплощение наиболее оптимальных способов осуществления своей деятельности при максимуме ответственности и минимуме влияния вертикальных структур (в результате корпорация как метасубъект приобретает черты менеджера проектов), творческий и инновационный характер экономической активности субъекта, позитивное влияние трудовой деятельности на личностное развитие субъекта;

— ощущение взаимоадекватности личных и коллективных критериев оценки, формирующее для творчески активного субъекта комфортную психологическую среду[61].

Характерной чертой деятельности современных лидеров IT-рынка, наиболее завязанных на инфосферу, становится не только системой гласных внутренних принципов компании по организации внутренних коммуникаций и взаимодействию по линии корпорация/сотрудник или сотрудник/сотрудник, но и базовой установкой по взаимодействию с внешними субъектами коммуникативного пространства[62]. Google Inc провозглашает своей миссией стремление «организовать всю имеющуюся в мире информацию, сделав ее доступной и удобной для использования»: «Миссия такого рода придает осмысленность работе всех и каждого, потому что ее формулировка — скорее моральная истина, а не деловая цель. В подоплеке самых мощных подвижек в истории лежали моральные стимулы,

---

[61] См.: *Абрамова С. Г., Костенчук И. А.* О понятии «корпоративная культура». URL: http://www.emcon.ru/420-087.html (дата обращения: 25.08.2018).

[62] О корпоративной политике Google Inc см. напр., URL: http://www.efko.ru/kadry/international_corporate_culture/10564/ (дата обращения: 25.08.2018).

будь то стремление к независимости или равные права. И будет справедливо заметить, что именно в этом кроется причина того, что революции — это прежде всего идеи, а не прибыли или доли рынка. А главное — миссия Google недостижима, поскольку постоянно будет поступать новая информация, которую нужно организовать, и новые способы извлечь из нее пользу. Это создает стимулы для непрерывного обновления и продвижения в новые, неизведанные области. Миссия „стать лидером рынка“ уже не вдохновляет, как только она реализована»[63].

В подобном и даже более радикальном направлении движется Facebook. «В 2011 г. разработчики и менеджеры Facebook'а для описания своих „радикальных“ инноваций придумали термин „социальный дизайн“. По их замыслу, отныне в любом продукте, если он желает иметь успех у потребителя, должно быть выделено социальное измерение. На одной из конференций Марк Цукерберг сказал: „Игры — это по природе своей социальная вещь. Фильмы, телевидение, новости, книги — это тоже вещи, которые люди потребляют вместе с друзьями. В последующие несколько лет эти индустрии станут более социальными“»[64]. То есть аспект коммуникации, потребительской оценки, взаимных рекомендаций, обмена практически полезной или эмоционально значимой информацией должны стать не просто нормой, но неотъемлемой частью повседневного существования субъекта — миссия Facebook заключается в достижении добровольной и социально функциональной «прозрачности» общества (термин Д. Брина)[65]: «Тогда же Марк Цукерберг ввел понятие seamless или frictionless sharing — сверхгладкого шеринга, то есть моментального, автоматического транслирования в фейсбук-ленте любых телодвижений пользователя в сети, которое полностью снимает вопрос о том, следует о чем-то сообщать миру или нет. Цукерберг уверен, что все люди хотят социализировать каждый свой

[63] Там же.

[64] Цит. по: *Кушнарева И.* Ко всему приделать лайки. URL: http://www.intelros.ru/pdf/logos/2012_2/01.pdf (дата обращения: 25.08.2018).

[65] См.: URL: https://www.wired.com/1996/12/fftransparent/ (дата обращения: 25.08.2018).

шаг — то, что читали, слушали, смотрели, где и с кем были и т. д. Из этой концепции вырисовывается образ абсолютно прозрачного для окружающих существа, совершенно не нуждающегося в том, чтобы что-то скрывать <…>. У такого существа все аспекты жизни и ипостаси личности идеально подогнаны друг к другу: например, нет никакого разрыва между работой и частными интересами или разными эпизодами биографии. Однородная личность в однородной среде, выстроенной на горизонтальных связях при полном отсутствии вертикали»[66]. Спорность действий компании Цукерберга заключается, в сущности, не в том, что здесь неверно оцениваются свойства человека информационного, но только в том, что Facebook через систему актуальных горизонтальных связей пытался подтолкнуть формирование «прозрачного» общества посредством необсуждаемого (то есть обошедшего этап коммуникативного действия!) внедрения интерфейсных настроек, то есть вместо дискурсивного подхода применив командно-административный и настроив тем самым против себя существенную часть собственной аудитории.

В сфере политического самосознания аналогом «позитивного» корпоративного подхода становится концепция ***открытого общества*** (наиболее полно описана К. Поппером[67]), в сфере политического управления близка к нему концепция «открытого государства», предполагающая соблюдение следующих базовых принципов:

— **Freedom of Information**. Свобода доступа к государственной информации для граждан.

— **Open Government Data**. Открытые государственные данные. Свободное использование государственных данных разработчиками и сотрудниками НКО.

— **Open Dialog**. Открытый диалог между гражданами и обществом. Возможность граждан влиять на государственные структуры.

— **Open Spending**. Открытость государственных расходов[68].

---

[66] *Кушнарева И.* Указ. соч.

[67] *Поппер К. Р.* Открытое общество и его враги. URL: https://e-libra.ru/read/179137-otkrytoe-obschestvo-i-ego-vragi.html (дата обращения: 25.08.2018).

[68] По: Открытое государство. Чем оно является и чем быть не может / А. Аксенова и др. URL: http://polit.ru/article/2012/02/22/open/ (дата обращения: 25.08.2018).

Определяющим элементом «открытого государства» становится смещение технологии достижения легитимности власти за счет свободной и прозрачной публичной соревновательности множества партий, платформ и программ, а также «народного аудита» результатов деятельности государственных структур. Важным элементом такой открытости предполагается выведение большинства процедур, предполагающих личное взаимодействие субъекта с государственными органами, в электронную форму, создание структур общественного контроля и поощрение гражданской инициативы. В 2011 г. с целью утверждения идеалов открытого государства (развития административного профессионализма, открытого гражданскому контролю) создана международная организация Open Government Partnership (OGP). В РФ данный формат развивается с 2012 г.; так, в 2014 г. распоряжением Правительства РФ была принята Концепция открытых данных Российской Федерации[69]; в 2012 г. для взаимодействия госструктур с экспертным сообществом был организован Экспертный совет при Правительстве РФ; в состав кабинета министров входит ответственный за организацию работы правительственной комиссии по координации деятельности Открытого правительства» и т. д. Однако в целом состояние дел в данной области обычно описывается как малосистематизированная деятельность отдельных государственных и общественных структур.

Вообще, стоит отметить, что концепция инфосферы как зоны свободного и взаимодополняющего сосуществования и свободной морально ограниченной конкуренции множества горизонтально связанных дискурсов выглядит скорее идеализированной перспективой, чем актуальной стадией развития общества. Транснациональные корпорации успешно используют инфосферу как поле боя за внимание потребителя, то есть фактически ведут в ней вполне традиционные информационные войны с применением новых медийных технологий, современных средств коммуникации и обрат-

[69] См.: URL: http://docs.cntd.ru/document/499073612 (дата обращения: 25.08.2018).

ной связи[70]; «геополитический идеализм» со времен В. Вильсона и Лиги Наций приводил к достаточно сомнительным результатам, наталкиваясь на последствия Realpolitik и «разделения принципов и интересов», а разоблачения Э. Сноудена продемонстрировали систематическое стремление правительственных структур США и их союзников (то есть государств, постулирующих свою миссию как либерально-прогрессистскую) использовать коммуникативные каналы по преимуществу как средство тотального контроля — для усиления эффективности командно-административных рычагов, для сбора информации, пропаганды, сокрытия данных, то есть в конечном счете для попыток остановить движение общества к открытости. Инфосфера из инструмента формирования взаимопонимания превращается в агрессивную среду, провоцирущую разделение общества, причем не только на межэтническом, межконфессиональном или межгосударственном уровне, где мы вправе ожидать упомянутых «фантомных болей», связанных с разрушением традиционной самоидентификации.

Культуролог О. Мороз в видеовыступлении для сайта «Пост-Наука» говорит о феномене hate speech. «Hate speech — это понятие, которое на русский язык переводится двумя способами: либо „язык вражды“, либо „риторика ненависти“ <…> Hate speech — это проявление дискриминации на вербальном или дискурсивном уровне, на уровне общения по отношению к какому-то человеку, которого мы считаем принадлежащим к группе, недостойной нашего качественного и равноправного отношения. В этом смысле hate speech — это вариант дискриминации любого миноритария, любой группы, которую мы называем меньшинством, того самого „другого“, о котором говорил Вебер»[71]. Важно отметить, что hate speech — явление универсальное для инфосферы, носит интернациональный характер и, по мнению исследователя, не сводим

[70] См., напр., URL: http://web.snauka.ru/issues/2016/02/64315 ; URL: https://delovoymir.biz/informacionnye-voyny-v-biznese-i-ne-tolko.html (дата обращения: 25.08.2018) ; *Цыганов В. В., Бухарин С. Н.* Информационные войны в бизнесе и политике. М., 2007. 336 с. и др.

[71] URL: https://postnauka.ru/video/68876 (дата обращения: 25.08.2018).

к трансляции агрессии, характерной для «фона жизненного мира» Хабермаса. Практика показывает, что «коммуникативное действие» может быть направлено на изоляцию и/или подавление субъекта или группы субъектов с тем же успехом, что и действие социальное, а возможность использования инфосферы для организации прямых социальных действий (например, террористических актов), а также (см. гл. 3) для проведения киберпреступных актов и кибератак дает основания говорить о взаимном перетекании «холодной» информационной войны в войну «горячей фазы». Взаимные обвинения политиков Украины и РФ, РФ и США, представителей российской правящей элиты и «Фонда борьбы с коррупцией» А. Навального и т. д. в распространении в пропагандистских целях различных фейк-ньюс[72] военного, политического, экономического и социально-поведенческого характера, показательны именно своей взаимностью — в результате пользователь, имеющий доступ к нескольким альтернативным коммуникационным каналам, должен либо выбрать какой-либо из них, опираясь на выбор референтной группы или другие подобные небезусловные критерии, либо с высокой вероятностью перейти в цинический модус восприятия, соответственно, вообще отказываясь от «коммуникативного действия» как возможности. Информационная агрессия может представлять реальную опасность (как для отдельных субъектов, так и для легитимных сообществ) — следовательно, на наш взгляд, государственные структуры просто обязаны оценивать инфосферу как источник разного рода угроз и действовать соответственно, прежде всего средствами ограничения, регулирования, контроля, а при необходимости — проявлять встречную или превентивную агрессию. Даже сама концепция «открытого общества» вполне может быть непротиворечиво описана как инструмент экономической экспансии транснациональных корпораций и геополитических амбиций идеологов «атлантизма»; соответственно, мы можем найти полярные оценки деятельности представителей института «Открытое общество» фонда Дж. Сороса как добросовестных филантропов-модернизаторов, буквально

[72] См., напр., URL: https://ura.news/news/1052334517 (дата обращения: 25.08.2018) и др.

спасших российскую культуру, науку и образование в кризисную постперестроечную эпоху,[73] и как коварных «агентов влияния Запада», целенаправленно разрушавших устои российской духовности и продолжающих действия в этом направлении[74]. Таким образом, сама множественность точек зрения опять-таки оказывается не поводом для открытой дискуссии и по результатам сознательной трансформации описываемой реальности во взаимовыгодном для субъектов коммуникации направлении, но средством актуализации и усиления конфликта. Несмотря на близкие к идеальным технические условия, создаваемые для многонаправленной коммуникации в современном киберпространстве, «коммуникативное действие» Хабермаса остается утопией. В чем причина?

Мы говорим о построении «информационного общества» как о революции, принципиально меняющей систему производственных отношений и как следствие — социокультурную среду. На этом основании мы можем выстроить аналогию между современным состоянием инфосферы и информационными процессами периода предыдущей производственной революции — периода формирования индустриального мира, который, к счастью, хорошо задокументирован. Обратим внимание на трансформацию мировосприятия европейцев XVI–XVII вв. Мы обнаружим:

— распад устоявшегося к концу Средневековья «христианского мира» и напряженное противостояние между католиками и протестантами в религиозной сфере, обернувшееся рядом гражданских и международных, в том числе общеевропейских войн;

— нарастающее среди различных социальных групп ощущение «конца времен», затерянности человека в реальности, воплотившееся в философии неоскептиков (Монтень, Паскаль и др.), в эстетике барокко, в эмпирической методологии естественных наук; сюда же отнесем формирование и поддержку обществом авантюристической модели поведения (Кортес, Дрейк, У. Рэйли и др.) как замены

---

[73] См., напр., URL: https://meduza.io/feature/2015/12/01/chto-sdelal-fond-sorosa-v-rossii (дата обращения: 25.08.2018).

[74] См, напр., URL: http://www.politonline.ru/provocation/22887327.html (дата обращения: 25.08.2018).

устойчиво-сословной, а также бескомпромиссное преследование инакомыслящих (равным образом в католическом и протестантском лагерях) и ряд масштабных патологических социокультурных эксцессов таких, как «охота на ведьм»;

— попытки реставрации идеальных ценностей прошлого — от более или менее условно понимаемой античности до евангельского христианства в различных протестантских течениях;

— расцвет социальной, политической, экономической, юридической и философской мысли, формирование публицистики, появление СМИ, восстановление и признание социально-политической значимости театра как массового искусства и средства пропаганды; актуальность социально-политического дискурса для широких слоев населения и активный совместный поиск новых форм социокультурной общности, который закладывается в коммуникативном действии, неощутимо для его участников формирующем общеевропейскую повестку Нового времени.

Таким образом, информационные войны XVI–XVII в., при всей разнице в плотности информационных потоков и степени охвата коммуникативных средств той и нынешней эпох, демонстрируют нам сходные тенденции, вполне укладывающиеся в маклюэновскую концепцию «фантомных болей», тоски по утраченной самоидентификации. Причем массовый и, по-видимому, глобально значимый характер нынешних контентных войн — прямое указание на переходный характер эпохи. Информационное общество складывается как экономическая необходимость, интегрируя и трансформируя актуальные концепты разрушающихся дискурсов (как была инкорпорирована «ретроградная» протестантская теология, ставшая основой этики, правового, политико-экономического мышления и бытового сознания индустриальной эпохи) и необратимо отторгая элементы нежизнеспособные (как была отторгнута концепция «трех сословий» и вообще сословный принцип организации общества). При этом принципиально невозможно однозначно определить, какие из концептов предыдущей эпохи обречены, а какие, напротив, станут базой нового общественного договора. Хотя теоретики постиндустриализма и продемонстрировали замечательные примеры социального прогнозирования (см. гл. 1), однако любые прогнозы

в данном случае упираются в непросчитываемость большинства аспектов ближайшего будущего в условиях очередной научно-технической и производственной революции[75]. Если переход к информационному обществу действительно является одним из последних и определяющих шагов на пути «Мир — Системы» к стадии технологической сингулярности[76], это предположительно означает, что даже ближайшее будущее человечества принципиально непостижимо, неописуемо посредством имеющихся эпистем. Тем не менее, если информационная война как феномен есть именно фрустрация Настоящего, переживающего (неосознанную до конца) утрату осознаваемого и ценностно комфортного Прошлого, то, не отказываясь от тактической реакции на безусловные ***угрозы***, исходящие из инфосферы (терроризм, деструктивные секты, заведомо преступные сообщества и т. п.), на стратегическом уровне человечеству следует сосредоточиться на предоставляемых ей ***возможностях***, использование которых во все возрастающей степени становится основным способом актуального присутствия в политике, экономике и культуре.

Российский философ и методолог П. Щедровицкий анализирует ситуацию следующим образом: «Есть горизонтальное и вертикальное разделение труда. Горизонтальное — это разделение труда по производству продукта, а вертикальное — это разделение труда по производству всех тех знаний, которые нужны для производства этого продукта <…>. Если вы не перестроите технологию деятельности, то никакая „цифра“ вам не поможет. Само наличие цифровых технологий намекает на направление перестройки, но не замещает ее, а это очень сложный процесс.

---

[75] См. подборку графических прогнозов о будущем европейских государств, сделанных на рубеже XIX–XX вв. URL: https://www.moya-planeta.ru/travel/view/budushhee_glazami_predkov_14089/ (дата обращения: 25.08.2018).

[76] См., напр.: *Новоселов А.* Технологическая сингулярность как ближайшее будущее человечества. URL: http://transhuman.ru/biblioteka/tekhnologicheskaya-singul ; *Коротаев А. В.* Новые технологии и сценарии будущего, или Сингулярность уже рядом? URL: http://cliodynamics.ru/index.php?option=com_content&task=view&id=117&Itemid=49 ; *Диринг М.* Рассвет Сингулярности URL: https://web.archive.org/web/20110908052319/http://transhumanism.org/languages/russian/dawnofsingularity/Deering.htm (дата обращения: 25.08.2018) и др.

Есть, по крайней мере, три следствия того, что вертикальная система разделения труда определяет горизонтальную. Первое: вы должны иметь семиотические (знаковые) инструменты, например деньги, которые бы поддерживали предпринимательскую деятельность на этом этапе промышленной революции. Новая промышленная революция поменяет семиотические инструменты, эксперименты с биткоином и есть работа в этой сфере.

Второе: новая промышленная революция поменяет «клеточку» экономики <…>. Кандидатная клеточка Новой промышленной революции — это так называемые «платформы с открытой архитектурой», которые шире, чем ТНК. И те ТНК, которые не смогут перейти к новой платформе, исчезнут с лица земли.

И, в-третьих, нужна новая технология мышления, которая станет достаточно массовой и сквозным элементом войдет в систему деятельности по производству любого нового продукта. В ходе „нулевой“ промышленной революции такой технологией стала инженерно-конструкторская деятельность, в ходе первой — проектирование, в ходе второй — исследование. У той технологии мышления, которая становится ведущей, сегодня также есть свое название — „программирование“ (только не нужно сводить к компьютерному программированию, это только один из видов)»[77].

Соответственно, моментами, определяющими саму возможность присутствия России как дискурса в медиапространстве будущего, П. Щедровицкий полагает:

— развитие модульного подхода как основы реформы системы образования, в перспективе отказ от «уровнего», транслирующего образования к проектному;

— упор в образовательных программах на развитие «мягких» навыков (навыки работы с клиентом (то есть коммуникации), навыки командной работы (как в больших коллективах, так и в малых группах), умение справляться с проблемами, находить проблемно ориентированные решения (не решения вообще, а решение, которое

[77] *Щедровицкий П.* Революция уже произошла, мы просто этого не видим. URL: https://www.znak.com/2017-12-12/petr_chedrovickiy_pochemu_rossiyskaya_

решает конкретную проблему), умение переучиваться и, наконец, навыки психофизической самоорганизации);

— развитие горизонтальных связей между образованием и производством, при сокращении сроков проведения и внедрения образовательных программ, в перспективе переход к концепции непрерывного образования, интегрированного с проектно-экономической деятельностью.

Упор, соответственно, делается не на развитие тех или иных политических институтов, которые должны служить неким маркером принадлежности к современному человечеству, но развитие базиса, перевод его на уровень, когда культура, научно-техническое знание и производство неразделимы и перетекают друг в друга, развитие в направлении, в котором современность будет онтологическим статусом России. А политическая активность через систему осознанных коммуникативных действий приобретет те формы, которые будут наиболее адекватны новым реалиям. Впрочем, данный аспект развития информационного общества отнюдь не общепринят. Ф. Джордж, к примеру заявляет, что «техническое изменение детерминирует экономическое изменение, и экономическое изменение детерминирует социальные перемены»[78]. У. Дайзард подходит к вопросу более осторожно: «Совершенно ясно, что при всем своем могуществе технологические и экономические силы сами по себе не обеспечат социальных условий, при которых коммуникационные и информационные ресурсы максимально эффективно служили бы нашим потребностям. Необходимые нам решения выходят далеко за пределы технологической и экономической проблематики. В конечном итоге главные проблемы — политические»[79]. Рассмотренные выше аспекты информационной составляющей «арабской весны» позволяют говорить скорее о сонаправленном, многостороннем и комплексном подходе. Более того, опыт КНР показывает, что

---

ekonomika_i_obrazovanie_ne_uspevayut_za_ostalnym_mirom (дата обращения: 25.08.2018).

[78] Цит. по: *Негодяев И. А.* На путях к информационному обществу. URL: http://udik.com.ua/books/book-584/ (дата обращения: 25.08.2018).

[79] Там же.

даже жестко авторитарные системы государственного управления способны эффективно стимулировать инновационное развитие экономики и повышение информационной компетентности субъектов. Однако во всех описанных случаях мы так или иначе говорим о взаимодействии уже оформленных политических концептов (национально-государственного, демократического и т. д.) со становящейся новой реальностью. Мы можем оценивать эти концепты как более или менее способствующие развитию информационного общества, как более или менее успешно позволяющие субъекту инфосферы и человечеству в целом использовать себе на благо возможности наступающей эпохи и нивелировать ее очевидные или неочевидные, но потенциально возможные угрозы, однако не можем требовать, чтобы эта реальность обслуживала существующие политические институты, не трансформируя их (тем более ошибочно будет, вслед за А. И. Ракитовым, говорить о принципиальной несовместимости с новыми реалиями произвольно оцениваемого как антиинновационное «культурного ядра» Российской нации[80]). Так или иначе трансформация неизбежна: разумеется, человек как моральное, культурное, осознающее себя как часть исторического процесса существо, не может рассматриваться как слепой заложник экономического процесса. Однако сама история учит нас, что и в этих сферах экономическая необходимость и экономическая возможность в конечном счете становятся определяющими, хотя подобное воздействие не является ни мгновенным, ни линейным. Собственно, специфика информационного общества заключается, в частности, именно в том, что человечество как глобальный автокоммуницирующий субъект впервые получил возможность осознания происходящих социокультурных процессов, апробации их в различных, но сосуществующих, пересекающихся и взаимопроникающих эпистемологических системах и, соответственно, в актуальном со-участии при выборе вектора развития цивилизации.

Следует отметить, что российские государственные структуры, по-видимому, достаточно адекватно оценивают как инфраструктур-

[80] См.: *Ракитов А. И.* Цивилизация, культура, технология и рынок. // Вопросы философии. 1992. № 5. С. 3–15.

ный, экономико-производственный аспект цифровой революции, так и определяющую роль «человеческого капитала». Правительством РФ в июле 2017 г. утверждена программа «Цифровая экономика Российской Федерации», где утверждается следующее:

«В связи с тем, что эффективное развитие рынков и отраслей (сфер деятельности) в цифровой экономике возможно только при наличии развитых платформ, технологий, институциональной и инфраструктурной сред, настоящая Программа сфокусирована на два нижних уровнях цифровой экономики — базовых направлениях, определяя цели и задачи развития:

— ключевых институтов, в рамках которых создаются условия для развития цифровой экономики (нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технологических заделов);

— основных инфраструктурных элементов цифровой экономики (информационная инфраструктура, информационная безопасность). <…>

Основными целями направления, касающегося кадров и образования, являются:

— создание ключевых условий для подготовки кадров цифровой экономики;

— совершенствование системы образования, которая должна обеспечивать цифровую экономику компетентными кадрами;

— рынок труда, который должен опираться на требования цифровой экономики;

— создание системы мотивации по освоению необходимых компетенций и участию кадров в развитии цифровой экономики России»[81].

Программа предусматривает тесную кооперацию образовательной и исследовательской деятельности с потребностями бизнеса и производства, а также государства и общественных организаций, стимулирование образовательных потребностей населения в области ИКТ и развитие перспективных областей, таких как робото-

[81] URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 25.08.2018).

техника, виртуальная реальность, квантовые компьютеры, системы искусственного интеллекта и обработки big data и т. д. Особое внимание уделяется созданию соответствующей инфраструктуры. Разумеется, программа сформулирована в рамках очевидного для государственных органов командно-административного подхода. Эксперт Аналитического центра И. Каракчиева, выступая на VIII Международной конференции по вопросам правового регулирования в электронной среде «Право и информация: вопросы теории и практики», заявила: «Действующие нормативные регуляторы не успевают за изменениями в образовании, вызванными цифровой революцией, внедрением искусственного интеллекта, робототехники и „умных" систем <…>. Парадокс — инструменты для стратегического, прорывного развития регулируются старыми нормами по управлению и контролю»[82]. Тем не менее установка программы совпадает с предложениями П. Щедровицкого — стимулирование коммуникативной компетентности и инновационной активности субъекта, гибкость образовательных и научных программ, смена вектора производственного развития.

В сущности, парадоксальным образом централизованное патерналистское государство ставит перед собой и последовательно реализует программу, которая предоставляет гражданам через развитие информационных компененций максимальную свободу, максимальную вовлеченность в дела общества при максимальной же открытости политической и экономической структуры на всех уровнях, максимальную коммуникативную компетентность, мобильность и адаптируемость к стремительно меняющимся производственным и общественным требованиям, как следствие, экономическую и психологическую независимость, то есть полный набор условий для отказа от патерналистского восприятия реальности. Очевидно, что выбор данного вектора трансформации государства и общества осознан как необходимое средство выживания государства и общества, и это тот случай, когда благо человека становится не просто лозунгом предвыборной компании: Россия

[82] Цит. по: URL: http://ac.gov.ru/events/016719.html (дата обращения: 25.08.2018).

как дискурс, Россия как общность действительно получает шанс выжить даже в случае, если Россия как политическое объединение окажется в новой реальности избыточной для самих россиян. Выбор в пользу подобной трансформации будет сделан (если будет) самими ее гражданами — свободными и компетентными людьми, способными оценить последствия своих действий в новой реальности, а осознанная активность субъектов коммуникации в конечном счете определит облик этой реальности на всех уровнях, при том что на сегодня описание и анализ этого облика остается уделом фантастов и футурологов, более фантазией, нежели уверенно ожидаемым будущим человечества. Вот, например, как описывает наступающую эпоху С. Переслегин: «Единый информационный мир моноцивилизации исчезнет, рассыпавшись на сотни ПЕРЕСЕКАЮЩИХСЯ игровых миров. По улицам городов будут бродить люди и чудовища, сами города будут постоянно меняться, превращаясь для одних — в средневековый замок, для других — в пустыню, для третьих — в страну-фантазию.

Жизнь в таком мире будет весьма рискованной (уже потому, что граница между смертью и жизнью в нем размывается до предела), а какой-либо порядок и определенность отсутствует. Следует учесть, что, во-первых, будет происходить взаимодействие между ВСЕМИ играми, существующими в Сети и, во-вторых, сетевые квазиличности также будут субъектами игр, что внесет в жизнь пользователей дополнительную неопределенность.

Это приведет к „феодализации сознания“ — делению мира на небольшую ойкумену, понятную, доступную и для каждого индивидуальную и внешних территорий, скрытых в тумане полной неизвестности, территорий, где, возможно, все и где законы природы, усвоенные дома, не обязательно действуют. И в этом хаотическом, непонятном, рискованном и интересном мире, где не провести четкой границы между сном и явью, фантазией и реальностью, игрой и жизнью, единственный элемент порядка вносит таинственная, сказочная фигура Программиста, странствующего мага будущего»[83].

---

[83] *Переслегин С.* Общество и эволюция информационной сети. URL: http://www.igstab.ru/materials/black/Per_ScNet.htm (дата обращения: 25.08.2018).

Героико-параноидальный подход как концепция осознанного и целенаправленного вмешательства в исторический процесс может быть рассмотрен как частный случай экономически обусловленного и культурно модифицированного «коммуникативного действия» акторов инфосферы: не являясь в собственном смысле неактуальным, он, по-видимому, является лишь одним из сосуществующих в инфосфере дискурсов и так или иначе будет неизбежно трансформирован самими акторами под влиянием экономической необходимости. С другой стороны, рассмотренная в настоящем разделе ***эволюцитонная*** модель *опять-таки* позволяет системно и (в рамках репрезентации) непротиворечиво описать реалии инфосферы, причем, хотя и востребована более в интернационально-глобалистском либертарианском дискурсе, вполне успешно адаптируется и дискурсом патриотическим. Как система управленческих концептов, эта модель укладывается в канон «***Школы человеческих отношений» и «японской модели» в теории управления***.

Объект: коллектив. *Цель:* доминирование с поглощением. *Ценности:* безопасность, корпоративность, толерантность. *Принципы:* децентрализация, делегирование, партнерство, мотивация, обратная связь, моральная состоятельность. *Структура:* неизменная, сетевая, матричная. *Личность:* универсальна, развиваема, взаимозаменяема, адаптивна. *Тип развития:* экспансионистский. *Практика:* экономический подход, подвижность норм, профессионализм менеджеров, воспитание исполнителей, психологическое сопровождение. *Боги (создатели концептов):* К. Маркс, А. Маслоу, Н. Винер, К. Поппер, Э. Мэйо, И. Оу, К. Исикава. *Утопия:* Ф. Гладков «Цемент», М. Шолохов «Поднятая целина». *Антиутопия:* О. Хаксли «Прекрасный новый мир», Д. Эггерс «Сфера».

Если героико-параноидальная модель принципиально воспринимает «Другого» как угрозу, а Будущее — как пространство угроз и в этом смысле ретроспективна и проигрышна, то в данном случае мы говорим о множественности, гибкости, взаимодополнении, открытости будущему, то есть о перспективах. Это, однако, не делает предложенную модель безупречной, скорее напротив высвечивает ряд проблемных моментов, актуальных, в том числе и при соотне-

сении с описанной ранее «проигрышной» модели. Эти моменты можно обозначить следующим образом:

Экономический фатализм. При всех приведенных выше оговорках исследователей в конечном счете речь идет о неомарксистской вере в неизбежность трансформации будущего, жестко детерминированной экономической необходимостью. Оставляя за пределами данного исследования вопрос о корректности подобного исторического детерминизма, отметим только, что большая часть рассуждений о перспективах очередной технологической революции основана на использовании производственных процессов и возможностей инфосферы и цифровых технологий, которые фактически существуют либо как нереализованные проекты (искусственный интеллект, квантовые компьютеры, полноценная виртуальная реальность, гуманизированная система поиска информации, полноценный эффект присутствия, полноценный синтез продуктов питания, дешевая общедоступная энергия, тем более трансгуманистические и биомодифицирующие технологии), либо как проекты, находящиеся в начальной стадии завоевания рынка, хотя и обладающие, по всей видимости, большим экономическим потенциалом (возобновляемые источники энергии, роботизация, 3D-печать, нанотехнологии). Если учесть, что критике подвергается даже концепция непрерывно ускоряющегося технологического развития (а значит, о неизбежности «технологической сингулярности» если и возможно будет говорить с научной достоверностью, то только после ее наступления!), очевидно, что рассматриваемая точка зрения на инфосферу является более догадкой, художественным образом, социально-философским размышлением, идеологемой, в крайних формах — религиозной догмой, нежели научно корректным описанием прогнозируемого будущего человечества. Реальность, как и у марксистов, подменяется концепцией реальности, а все элементы реальности оцениваются с позиций соответствия или несоответствия этой концепции (то есть по степени адекватности концепция «информационного общества» в рамках данной модели столь же уязвима, сколь и в рамках модели героико-параноидальной). Соответственно, выбор в пользу этой концепции возможен для субъекта, но сам по себе он не дает ни явного экономического

преимущества, ни гарантии актуальности выбора при прохождении точки бифуркации.

Подмена мотивировок. Концепция Апеля и Хабермаса предполагает определенную этически ориентированную перезагрузку человеческих отношений посредством инфосферы как инструмента сознательной коммуникации. Однако сам принцип экономической детерминированности перемен предполагает, что моральные основания социального действия, как минимум на первых порах, будут отодвинуты на второй план. Ж. Аттали в историософском трактате «Линия горизонта» (1992) описывает будущее как общество «новых кочевников»: «Покончив с любой национальной привязкой, порвав семейные узы, заменив все это миниатюрными микропроцессорами, такие граждане — потребители из привилегированных регионов мира, превратятся в „богатых номадов“. Они смогут принимать участие в освоении либеральной рыночной культуры, руководствуясь при этом своим политическим или экономическим выбором, они будут странствовать по планете в поисках путей использования свободного времени, покупать информацию, приобретать за деньги острые ощущения и такие товары, которые только они могут себе позволить, хотя и будут испытывать тягу к человеческому участию, тоску по уютной домашней обстановке и сообществу людей — тем ценностям, которые прекратили свое существование, так как их функции устарели. Подобно жителям Нью-Йорка, которым ежедневно приходится сталкиваться с бездомными бродягами, слоняющимися у банков-автоматов и выклянчивающими у прохожих мелочь, такие состоятельные странники повсюду будут сталкиваться с мириадами „бедных кочевников“ — этих хватающихся за соломинки в планетарном масштабе людей, которые бегут прочь от испытывающей нужду периферии, где по-прежнему будет жить большая часть населения Земли. Эти обнищавшие пираты будут курсировать по планете в поисках пропитания и крова над головой, их желания станут еще острее и навязчивее благодаря созерцанию роскошных и соблазнительных картин безудержного потребления, которые они увидят на экранах телевизоров в спутниковых телепередачах из Парижа, Лос-Анджелеса или Токио. В тщетной попытке перейти,

по выражению Элвина Тоффлера, от замедленного к ускоренному миру им придется вести жизнь живых мертвецов»[84].

Опять-таки перед нами радикальная точка зрения, построенная на концепции экономической неизбежности. Однако характерным моментом здесь становится ожидание не экономического и социокультурного выравнивания, гармонизации экономических условий существования человечества, но, напротив, глобальное утверждение окончательного социально-экономического (и как следствие, коммуникативного — см. выше об «Арабской весне») расслоения. Более того, внедрение подобных месседжей в инфосферу де-факто становится пропагандой неизбежности подобного разделения — субъекту предлагается либо вскочить в уходящую лодку информационной цивилизации, либо деградировать, при этом его идентичность будет уничтожена в обоих случаях и представляется, соответственно, неактуальной. Но даже приведенные выше исторические аналогии, используемые как обоснование неизбежности формирования человеком информационным новой идентичности, демонстрируют нелинейность, неоднозначность и непрогнозируемость культурных изменений изнутри процесса. Опять-таки можно сослаться на опыт КНР, демонстрирующий совместимость командно-административного управления, авторитарной политический системы, с одной стороны, и технологизации общества с упором на частную инициативу, информационно-коммуникативные навыки и инновационность — с другой.

Показательно, что именно попытки традиционалистских структур, опираясь на принципы «открытого общества», вступить в коммуникацию с этим обществом по предложенным правилам, отстаивая свой дискурс как возможный и — в рамках концепции множественности взаимодополняемых дискурсов — приемлемый, встречают агрессивное сопротивление как противоречащие идеалам толерантности и открытости. Снисходительно считая, что оно стоит «над» проявлениями шовинизма, расизма и т. д., «открытое

---

[84] Цит. по: *Аттали Ж.* На пороге нового тысячелетия. URL: https://www.rulit.me/books/na-poroge-novogo-tysyacheletiya-read-60972-1.html (дата обращения: 28.08.2018).

общество» не способно воспринимать возможность той же терпимости или отстраненности со стороны других культур. В результате элиты и идеологи, формирующие консервативную повестку, и их сторонники воспринимают доктрины открытости, мультикультурализма и т. п. не как реальную (или хотя бы формирующуюся) социокультурную перспективу, но как манипулятивную идеологическую конструкцию, как попытку средствами пропаганды, провозглашающей терпимость к «Другому», де-факто уничтожить «Другого» как самоподдерживающийся и потенциально конкурентный дискурс, разрушить его культурную и политическую онтологию, что позволит инкорпорировать максимальное количество субъектов в среду экономически комфортных для ТНК легкоуправляемых потребителей, то есть в конечном счете превратить рассуждения Аттали о «богатых номадах» в самосбывающееся пророчество. Речь, таким образом, идет не о гипотетической сингулярности в ближайшем будущем, а исключительно о стабильном и безопасном извлечении сверхприбылей из глобализировавшегося рынка в настоящем. Вполне естественной реакцией в данном случае становятся отторжение и агрессия; следовательно, как раз навязываемый западными масс-медиа образ абсолютно толерантного и абсолютно коммуницирующего субъекта не способствует, но исключает формирование среды «коммуникативного действия», а это, в свою очередь, вообще ставит под вопрос возможность построения общественной системы, основанной на принципах взаимодополнения дискурсов.

Релятивизм. Принцип свободной конкуренции и взаимодополнения дискурсов в инфосфере приводит не только к свободному «горизонтальному» взаимодействию морального и аморального, легального и нелегального, но и к конкурентности дискурсов антинаучных (теория «плоской Земли», «новая хронология» Фоменко, «волновая генетика» и мн. др.), антитехнологических (в том числе представляющих прямую социальную опасность, таких как ВИЧ-диссидентство и различные формы радикальной натуропатии) и антиинформационных. Поскольку деиерархизированное размещение и взаимодействие дискурсов охватывает также пространство культуры и истории (которые, очевидно, в свою очередь превращаются в модифицируемый и множественный дискурс, в среду про-

извола, свободного со-творчества акторов), то конкретный актор, по-видимому, лишается возможности для минимально рационального выбора между дискурсами, что лишает его и возможности осознанного и ответственного действия как в коммуникативной, так и в социальной сфере. Удаленность взаимодействия, необязательность последствий и непредсказуемость совместно генерируемого результата любой активности превращают человека информационной эпохи из супертворца в суперпотребителя, ориентирующегося только на собственный произвол и не признающего морали и ответственности, если моральность и ответственность не являются частью сиюминутно актуального дискурса. Собственно, адепты информационной революции в конечном счете апеллируют к гедонистическим установкам субъекта.

Гедонизм. Развитие мультимедийных каналов передачи информации, тем более встроенных в систему интерактивного взаимодействия с инфосферой, несомненно, невообразимо расширяет горизонт восприятия субъекта. В результате, однако, человек оказывается в ситуации не вообразимой в предшествующие эпохи информационной перегрузки: собственно, даже эстетическое восприятие предлагаемой информации становится невозможным в условиях, когда субъект последовательно воспринимает бесконечное множество бесконечно качественных и сенсорно безупречных информационных объектов, не располагая, соответственно, ни временем, ни возможностью, ни желанием даже для осознанного эстетического, тем более для аналитического восприятия. Познавательная активность субъекта (тем более в условиях релятивизма) или продуктивная творческая, тем более социальная активность (если эти действия в рамках необязательного дискурса не поддержаны существующими вычислительными возможностями, то есть не подменяются машинным анализом данных) представляется в этих условиях невозможным. Реальность превращается в калейдоскоп игровых действий, не предполагающих ответственного подхода и выбираемых по критериям сиюминутного желания и максимального ожидаемого удовольствия. «Человек информационный» из осознающего себя актора инфосферы превращается в «человека наслаждающегося», для которого разницы между экономически/морально/социально/

культурно допустимым и НЕдопустимым не существует по определению, для которого очевидна его экономическая неуязвимость (обеспеченная трудом роботов либо представителей низшего уровня стратифицировавшегося общества «номадов» — кем именно, принципиально несущественно) и поведенческая вседозволенность. В сущности, «сингулярность» такого рода проанализирована и описана очень давно, как электрод, воткнутый в центр удовольствия в мозге.

Подмена реальности. Любая технология оцифровки предполагает на входе интерпретацию данных через более или менее сложные процессы квантования сигнала, что приводит к неизбежным и неустранимым при анализе цифрового сигнала погрешностям квантования. В информационной среде мы можем сталкиваться с невообразимо высоким качеством звука, изображения, видеозаписи, причем качество съемки, обработки и трансляции уже, по-видимому, превосходит пределы, доступные лишенному инструментов аналоговому человеческому восприятию (это, к примеру, касается получившей распространение в последние годы гигапиксельной графики). В результате у субъекта неизбежно возникает ощущение знания реальности, основанное не на самой реальности, но на ее образе, транслированном другим субъектом посредством разработанного третьим субъектом (или вообще искусственным интеллектом?) инструмента интерпретации; при этом инструментарий модификации и обстановка релятивизма позволяет без труда переделывать любые данные в любом желаемом направлении. Если сравнивать возможности субъекта инфосферы с теми, которыми обладали его недавние предшественники, то окажется, что в низовом и даже среднем сегменте качество информационного потока (особенно в невербальной сфере) непредставимо возросло, однако это достигнуто ценой нивелирования элитарного сегмента восприятия. Как и релятивизм в критериях оценки информации, цифровая медиализация инфосферы де-факто препятствует сколь-нибудь адекватной познавательной деятельности субъекта.

Псевдоморфоз. Последовательная реализация радикально либеральных принципов в инфосфере систематически оборачивается их противоположностью, что заставляет говорить о сомнительной

достоверности исходных установок. Так, множественность информационных потоков сопровождается генерализацией контроля над каналами коммуникации (критической точкой в данном случае можно считать проект Илона Маска по созданию глобальной бесплатной беспроводной интернет-инфраструктуры — сценарий, неоднократно описанный в фантастических сюжетах как шаг к завоеванию мира). Во всяком случае, контроль за каналами коммуникации и одновременно за технологиями big data, потенциально позволяющими анализировать персональные данные и коммуникационные предпочтения ***каждого*** субъекта инфосферы, действительно выглядит как свобода в частностях при просчитанном тотальном контроле — за образом мира в существенных его элементах. На это работает и принцип открытости, отказ от privacy, облегчающий подобный анализ (но также и концепция государственного контроля над персональными данными). Подобным же образом индивидуализация производства просто переводит стандартизацию на более глубокий уровень — на уровень разработки модульных схем любых потребительских товаров, от продуктов до автомобилей, по типу конструктора LEGO или производства для 3D-принтеров сырья, как обычно пишут в рекламных буклетах, «идентичного натуральному или превосходящего натуральный продукт по потребительским качествам».

Размывание политических, религиозных, этнических и культурных границ, мультикультурализм и толерантность выглядят в этом случае не неизбежным логическим следствием смены способа производства (который по факту остается индустриальным), но идеологическим симулякром, призванным адаптировать передел экономической и политической власти в пользу ТНК. Важно отметить, что наличие «всемирного заговора» корпораций, целенаправленно зомбирующих субъектов инфосферы, логически избыточно; вероятнее всего, в каждой конкретной ситуации речь идет о профессиональных управленцах, работающих на благо своей компании (и даже, в меру своего понимания, на благо человечества) и не задумывающихся о глобальных перспективах в терминологии «власти над миром». Упомянутые издержки развития инфосферы — не более чем логическое следствие движения в направлении

тотальной информатизации, которое, например, требует громадного (и затратного) ресурсного и экономического потенциала для возможности появления и развития (что под силу корпорациям и/или государственным структурам, реже общественным — и все в меньшей степени отдельным субъектам). Здесь, кстати, возникает еще один любопытный парадокс: если бы информационное общество действительно являлось бы свободным и децентрализованным, то есть какого-либо центра, контролирующего информационные и экономические потоки в инфосфере, не существовало бы в принципе, подобное общество было бы неспособно сконцентрировать и выделить сколько-нибудь существенные ресурсы для технологического или научного развития цивилизации: таким образом, даже в случае успешной децентрализации образования, медицины и логистики человечество получило бы на выходе стагнацию, остановку в развитии, в конечном счете опять-таки тепловую смерть.

Итак, при анализе человека информационной эпохи вместо социально ответственно актора коммуникативного действия, сознательно и целенаправленно строящего для себя и окружающих цифровой рай, перед нами, как упоминалось во вступлении, предстает классический диссоциативный психопат с разбалансированной пирамидой потребностей, отсутствием критериев оценки реальности, лишенный как ощущения подлинности Настоящего, так и сколь-нибудь постоянных и достоверных знаний о чужом и собственном Прошлом, соответственно, неспособный и к развитию, к движению в Будущее, но стохастически дрейфующий от иллюзии к иллюзии, погруженный в гедонистические грезы о собственном всемогуществе и паразитирующий на труде рабов-роботов, точнее, на данный момент мечтающий о подобном паразитизме, поскольку на практике для подавляющего большинства населения Земли подобное существование находится далеко за гранью возможного (а для многих — и за гранью приемлемого). Если для существования подобного общества необходим искусственный интеллект, то более чем вероятно, что этот искусственный интеллект сочтет такое человечество сообществом экономически избыточных цифровых паразитов и избавится от них, возможно, вежливо сказав «спасибо» за собственную разработку.

§ 3. Авантюрно-невротический подход. От фактчекинга к принципу неопределенности

Проведем промежуточные итоги. Для условных сторонников «героического» подхода инфосфера — прежде всего среда интенсифицирующегося по мере технического развития и роста охвата глобальных коммуникаций глобального столкновения цивилизационных концептов. Установки этих концептов зачастую непримиримы, к тому же в ряде случаев они оказываются лишь прикрытием для (неизбежно ввиду ограниченности физического мира и его ресурсов) антагонистичных друг другу геополитических стремлений. В результате явно или неявно, осознаваемо для акторов или нет, но коммуникативное взаимодействие преобразуется в тотальную информационную войну. В качестве оружия рассматриваются идеи и истинные либо ложные сообщения (информация и дезинформация), в качестве ресурса — каналы коммуникаций, в качестве цели — сохранение и утверждение цивилизационных концептов как базовой ценности, определяющей культурное бытие субъекта. Поскольку концепты сформированы историческим прошлым, то данная эпистемология принципиально ретроспективна и оценивает настоящее по критерию соответствия/несоответствия идеализируемому Прошлому, а Будущее — по критерию возможности/невозможности воспроизведения этого Прошлого на технически продвинутом уровне.

Соответственно, для условных сторонников «эволюционного» подхода само появление и развитие инфосферы существенно как этап становления идеализируемого Будущего. В этом же ключе оценивается вообще Настоящее, в то время как прошлое превращается в пространство временных, исторически обусловленных заблуждений и обладает ценностью только в той степени, в которой предваряет Будущее. Прошлое при этом обладает определенной властью над субъектами инфосферы (через традиции/привычки/предрассудки, а также посредством административного и пропагандистского ресурса отмирающих элит), и отмирающие элиты также стремятся быть представленными в инфосфере, оценивая ее как оружие борьбы за власть, и, соотвественно, глобальные комму-

никации действительно приобретают характер военных действий, однако этот момент, значимый на тактическом уровне, пренебрежим стратегически, поскольку человечество в осязаемой перспективе неизбежно должно прийти к массовому использованию коммуникаций именно как инструмента преодоления подобных коллизий в принципе. Развитие инфосферы есть необходимый (хотя и не единственный) аспект экономического развития человечества, а значит, это направление изменений является неизбежным, хотя его результирующие формы на данный момент непредставимы.

Для нас существенно обратить внимание на то, что обе концепции а) преподносятся как взаимоисключающие, хотя на практике используются в риторике одних и тех же акторов; б) в процессе контентных войн маркируются как ценностно ориентированные, противопоставляются друг другу и произвольно присваиваются акторами (при том, что оппоненты лишаются права на обладание подобными ценностями или же объявляются носителями «антиценностей» — вплоть до появления термина «античеловечество», не обязательно связанного с очередной «теорией заговора»); в) последовательно игнорируют Настоящее как профанное по отношению к сакрализованному Прошлому либо Будущему, что придает этим эпистемологическим системам стройность, цельность, непротиворечивость, и ведет их носителей к игнорированию реального положения дел. Ведется ли глобальная информационная война или же нет, она в любом случае ведется не теми, не так, не с той целью и не теми средствами, как следует из данных моделей, и именно поэтому построенные на них оценки и/или прогнозы на ближайшую или отдаленную политическую перспективу по всему миру в подавляющем большинстве оказываются несостоятельными (от «разорванной в клочья экономики России» до бесконечных ожиданий «смены вектора» американской политики и истерического информационного «со-участия» россиян в выборах каждого очередного президента США). Именно этот, последний параметр может быть использован для описания еще одной эпистемологической системы, также обладающей и авторитетом, и распространенностью, и актуальным присутствием в коммуникативной среде. Речь идет о различных проявлениях теории неопределенности.

«Война — область недостоверного: три четверти того, на чем строится действие на войне, лежит в тумане неизвестности, и следовательно, чтобы вскрыть истину, требуется прежде всего тонкий, гибкий, проницательный ум <…> Недостоверность известий и постоянное вмешательство случайности приводят к тому, что воюющий в действительности сталкивается с совершенно иным положением вещей, чем ожидал; это не может не отражаться на его плане или по крайней мере на тех представлениях об обстановке, которые легли в основу этого плана. Если влияние новых данных настолько сильно, что решительно отменяет все принятые предположения, то на место последних должны выступить другие, но для этого обычно не хватает данных, так как в потоке деятельности события обгоняют решение и не дают времени не только зрело обдумать новое положение, но даже хорошенько оглядеться. Впрочем, гораздо чаще исправление наших представлений об обстановке и ознакомление с встретившейся случайностью оказываются недостаточными, чтобы вовсе опрокинуть наши намерения, но могут все же их поколебать. Знакомство с обстановкой растет, но наша неуверенность не уменьшается, а напротив — увеличивается.

Причина этого заключается в том, что необходимые сведения получаются не сразу, а постепенно. Наши решения непрерывно подвергаются натиску новых данных, и наш дух все время должен оставаться во всеоружии»[85].

Казалось бы, глобальное развитие информационных сетей позволяет получать информацию мгновенно. Проблема, однако, заключается в том, что а) информационные войны по определению нацелены прежде всего не на профессионалов, принимающих стратегические или тактические решения, а на те или иные группы населения, не имеющие доступа к каналам гарантированно достоверной информации, особенно в случае, когда в определенной оценке информации насущно заинтересована как минимум одна из сторон конфликта; б) как показано выше, глобальный характер медиасферы создает у субъекта ощущение непосредственного при-

[85] *Клаузевиц К. фон.* О войне. М., 1934. URL: http://knigosite.org/library/read/27370 (дата обращения: 25.08.2018).

сутствия, однако в большинстве случаев это иллюзия, более того, иллюзия, которую современные медиатехнологии позволяют создать (и по желанию модифицировать) намеренно (таким образом, субъект готов к непосредственной реакции на информацию, но не может быть уверен в достоверности этой информации, что заставляет выбирать не критерии достоверности, а скорее критерии доверия к источнику); в) будучи удален от места событий, субъект реагирует прежде всего в медиасфере, тем самым увеличивая количество привязанной к событию информации, то есть повышая общую зашумленность информационного фона, создавая симулякры события второго или третьего порядка; г) при этом актуальность медиасферы в социально-политическом контексте современности заставляет элиты рассматривать эти симулякры как актуальную часть реальности и в большей или меньшей степени реагировать на них как на реальность объективную. В результате сколь-нибудь продуктивная открытая дискуссия, в том числе в среде профессиональных политиков, становится предельно малопродуктивной, превращаясь в бесконечный обмен бездоказательными по сути встречными обвинениями, как правило, прежде всего обвинениями в сознательном искажении истины, создании так называемых фейк-ньюс или прямой лжи; таким образом, развитие коммуникативной сферы повышает уровень шума в канале и все более препятствует не только коммуникации как таковой, но, вероятно, также и принятию более или менее ответственных стратегических решений.

См., например, освещение в прессе и официальных политических заявлениях таких событий, как катастрофа «боинга МН-17» по вине России/ополченцев ЛНР/ДНР/армии Украины/американских спецслужб; применения либо неприменения режимом Асада в Сирии химического оружия против населения и войск оппозиции; виновность/невиновность российских спецслужб в отравлении семьи Скрипалей; взаимные претензии РФ и США в нарушении договора РСМД; участие/неучастие российских хакеров и информационных агентств во вмешательстве в выборы президента США; доминирование экономических или же политических интересов РФ в планах строительства газопровода «Северный поток — 2»; законность/незаконность присоединения Крыма к РФ; ответственность

СССР/ответственность стран Запада в ситуации вокруг оккупации Польши и заключении «Пакта Молотова — Риббентропа», признание/непризнание так называемого «голодомора» целенаправленным геноцидом украинского народа и мн. др.: характерно, что понятие «историческая дистанция» в нынешних информационных войнах, кажется, окончательно теряет актуальность: исторические дискурсы становятся не менее актуальными, чем дискурсы, посвященные текущим политическим конфликтам. Поскольку в большинстве случаев анализ информации (опять-таки с противоположными выводами) осуществляют в том числе субъекты, маркированные в инфосфере как профессионалы, представители экспертного сообщества — ситуация подрывает общее доверие не только к журналистам и политикам (что традиционно), но и к экспертам.

В 1991 г. Жан Бодрийяр объявил, что «Войны в заливе» не было, имея в виду, что эта война в том виде, в котором ее представляет обыденное сознание, существовала только как феномен инфосферы, как симулякр; в реальности речь шла о масштабном военно-политическом преступлении, определенным образом интерпретированном СМИ[86]. Чтобы не допустить попадания в ловушку фейк-ньюс и симулакров, современная журналистика прибегает к методике ***фактчекинга*** (от англ. «проверка фактов»)[87]. В общем виде фактчекинг предполагает:

— стремление к беспристрастности при оценке источников информации; отказ от эмоциональной составляющей и оценки потенциального эффекта информации в глазах публики в пользу достоверности исследуемого факта;

— обязательный поиск первоисточника любой актуальной, тем более претендующей на сенсационность, информации; оценка текста первоисточника с позиций заинтересованности и информи-

---

[86] *Бодрийяр Ж.* Дух терроризма. Войны в заливе не было. URL: http://avidreaders.ru/read-book/duh-terrorizma-voyny-v-zalive-ne.html (дата обращения: 25.08.2018).

[87] См., напр., подборку академических исследований по проблеме политического фактчекинга. URL: https://ballotpedia.org/Academic_studies_of_political_fact-checking (дата обращения: 25.08.2018).

рованности субъекта, сопоставление предложенной им информации и ее референций;

— сравнение информации из разных источников, желательно независимых друг от друга, в идеале — сравнение описаний, предлагаемых разными сторонами конфликта;

— осторожное использование социальных сетей (вплоть до проверки наличия за аккаунтом реального субъекта), проверка оригинальности сообщений очевидцев, проверка оригинальности мультимедийной информации (фото- и видеоматериалов, в том числе с помощью сверки метаданных файла)[88].

Для проверки фактов работают специализированные проекты и сервисы типа Storyful.com, FactCheck.org, PolitiFact.com или The Fact Checker, созданного редакцией Washington Post; рекомендуются также приложения Trooclick, Truth Goggles, Lazy Truth, Skeptive, Genius. Установка на публикацию достоверной информации закреплена в Кодексе принципов Международной сети фактчекинга (International Fact-Checking Network) и подтверждена отечественными документами, такими как «Медиаэтический стандарт — 2015», разработанный Общественной коллегией по жалобам на прессу; рядом национальных законодательств, в том числе российским, предусмотрена ответственность за публикацию заведомо ложной информации без соответствующего бэкграунда, позволяющего опознать новость как шутку или псевдотекст, публикуемый, например в рамках социологического исследования. Тем не менее объем заведомо недостоверной информации в медиасфере продолжает возрастать.

Следует отметить, что методика фактчекинга, помимо того, что она требует от журналиста труднодостижимого уровня бесстрастности и добросовестности, обладает существенным логическим недостатком. Построенная на индуктивной оценке ситуации, на соответствии или несоответствии частных деталей и оценок и общего информационного фона, эта методика в ряде случаев позволяет субъекту отсеять заведомо ложную информацию. Однако она

[88] По: *Корнев М.* Фактчекинг: 5 надежных способов проверить информацию. URL: http://mediatoolbox.ru/factchecking/ (дата обращения: 25.08.2018).

не позволяет реконструировать истинное положение дел, и этот момент становится критичным в ситуации, которая представляется субъекту требующей немедленного проявления активности, как минимум коммуникативной. «Туман войны», описанный Клаузевицем, приобретает в инфосфере онтологический статус: инфосфера становится не только сферой знания и деятельности, но и сферой вероятной недостоверности, сферой разрушения доверия и обрушения эпистемологических систем.

Н. Н. Талеб, анализируя взаимодействие доминирующих эпистемологий с реальностью, вводит понятие «черного лебедя»: «То, что мы будем называть Черным лебедем (с большой буквы), — это событие, обладающее следующими тремя характеристиками.

Во-первых, оно аномально, потому что ничто в прошлом его не предвещало. Во-вторых, оно обладает огромной силой воздействия. В-третьих, человеческая природа заставляет нас придумывать объяснения случившемуся после того, как оно случилось, делая событие, сначала воспринятое как сюрприз, объяснимым и предсказуемым»[89].

История, по Талебу, кишит «черными лебедями» и во многом определяется именно ими. Ряд факторов, порождаемых информационным обществом, например скорость обмена информации и нарастание информационного давления, приводит к усложнению системы взаимодействий, повышение рекурсивности социума, что, как следствие, многократно повышает количество совершаемых социально значимых действий с непредсказуемыми последствиями; то есть история последних десятилетий порождает «лебедей» чаще, чем в предыдущие эпохи, а их воздействие на сознание становится более интенсивным, что, впрочем, вероятно, должно нивелироваться ростом их количества и возникновением эффекта привыкания к сенсации. Тем не менее обе приведенные выше эпистемологические модели выстроены таким образом, как если бы подобных событий не происходило в принципе: «Неспособность предсказывать аномалии ведет к неспособности предсказывать ход истории, если

[89] *Талеб Н. Н.* Черный лебедь. Под знаком непредсказуемости / пер. с англ. 2-е изд., доп. М., 2012. С. 5.

учесть долю аномалий в динамике событий <…> Но мы ведем себя так, будто можем предсказывать исторические события, или даже хуже — будто можем менять ход истории. Наша неспособность к прогнозам в среде, кишащей Черными лебедями, вместе с общим непониманием такого положения вещей, означает, что некоторые профессионалы, считающие себя экспертами, на самом деле таковыми не являются»[90].

Талеб рассуждает о непроницаемости истории как ввиду скрытости подлинных причин, так и ввиду склонности нашего сознания к некорректным обобщениям, построенным по индуктивному принципу; однако, говоря о некорректности обобщающих ретроспекций в оценке состоявшегося прошлого, мы должны тем более ожидать ошибочных оценок при анализе происходящего Настоящего и становящегося Будущего. «Американский метеоролог Лоренц — первооткрыватель странных аттракторов — вводил в свои расчеты менее десяти переменных (обычно шесть), в то время как на погодные условия влияют миллионы неизвестных нам параметров. В метеорологии прогнозисты, в общем-то, смирились, что не только долгосрочные, но и среднесрочные прогнозы погоды невозможны, так как все переменные невозможно учесть никогда и ни при каких условиях. Невозможно даже приблизиться к приемлемому уровню достоверности. Более-менее точным считается прогноз погоды на три дня вперед. Дальше точность снижается на порядок»[91]. Эмпирический опыт не предсказуем и не прогнозируем; инфосфера непредсказуема и изменчива; надежность и стабильность конструкций (например, социально-политических, экономических или военно-стратегических) иллюзорна (примером может служить «Доктрина Дуэ», не реализуемая на практике). Субъект инфосферы стоит перед выбором. Он может оставаться гражданином «Среднестана», получая гарантированное центрами силы и статистически выверенное благополучие, не имея при этом гарантий, что это благополучие не будет обрушено

[90] *Талеб Н. Н.* Указ. соч. С. 7.

[91] *Прохватилов В. В.* Против математиков (К вопросу о кризисе оснований в отечественной теории информационных противоборств) // Информ. войны. 2013. № 2 (26). С. 93–101.

в результате появления очередного «Черного лебедя», либо что этот «лебедь» не окажется таковым только для него, «среднего» субъекта, в то время как в реальности период «благополучия» изначально являлся неким подготовительным этапом, разрушающим жизнь субъекта А во благо запланировавшего это разрушение субъекта Б: «Представьте себе индюшку, которую кормят каждый день. Каждый день кормежки будет укреплять птицу в убеждении, что в жизни существует общее правило: каждый день дружелюбные представители рода человеческого, „заботящиеся о ее благе“, как сказал бы политик, насыпают в кормушку зерно. Накануне Дня благодарения с индюшкой произойдет нечто неожиданное. Это нечто повлечет за собой пересмотр убеждений»[92] (вариация на тему «Курицы Рассела»).

Другой вариант — переход на позиции жителя «Крайнестана», оценивающего мир с позиций эмпирика-скептика и умеющего использовать непредсказуемые трансформации воспринимаемой и осознаваемой реальности для собственной пользы: подход, который повышает ожидаемую вероятность проигрыша, но одновременно — единственный из всех — дает шанс на выигрыш по результатам кризиса. Собственно, изначальным (не идеологизированным в либеральном политическом дискурсе) смыслом термина «открытое общество» Поппера была последовательно-скептическая установка на отказ от окончательных смыслов как цели познания и социального конструирования: сознание «человека информационного» прежде всего открыто изменению — и сомнению. При этом следует помнить, что под «выигрышем» в данном случае не обязательно подразумевается, допустим, финансовая отдача от вложенных усилий. «Исследователь Томас Астебро установил, что отдача от независимой новаторской идеи гораздо меньше, <…> чем от венчурных инвестиций. Чтобы предприятие функционировало, предприниматель должен закрывать глаза на законы вероятности или вдохновляться верой в своего, счастливого, Черного лебедя. А пенки снимает венчурная компания. Экономист Уильям Баумоль называет это „сумасшедшинкой“. То же относится к любой „концентрированной“ деятельности: издатель зарабатывает больше писателя, дилер — больше художника, а науке

[92] *Талеб Н. Н.* Указ. соч. С. 36.

живется лучше, чем ученым (около половины всех научных работ, которые писались месяцы или годы, так никто и не прочтет до конца). Играющий в эту игру получает не материальное вознаграждение, у него другая валюта — надежда»[93]. При этом только субъект, принявший на себя ответственность за последствия собственного выбора и лично рискующий в рамках собственного представления о ценности, способен принимать по-настоящему адекватные решения — просто в силу гносеологической и психологической готовности к непредсказуемым изменениям в ткани реальности. Любые другие основания, положенные в основу эпистемологии, однозначно приводят субъекта к одной из трех базовых ошибок описания:

— нарративное заблуждение: постфактум событие описывается так, что не кажется беспричинным;

— заблуждение игрока: уподобление системы случайностей игры бессистемным случайностям в жизни;

— заблуждение обратной статистики: уверенность, что события в будущем предсказуемы через изучение событий в прошлом.

Эти ошибки приводят актора инфосферы к заведомой утрате возможности правильного анализа, тем более правильного прогноза ситуации (хотя такой прогноз по стечению обстоятельств может оказаться — в системе координат заблуждающегося субъекта СЛУЧАЙНО верным; см. пример с курицей Рассела). Тем самым из субъекта осознанных коммуникативных действий актор так или иначе неизбежно превращается в объект манипуляции других акторов, то есть по определению в жертву информационной войны, но не в «бойца» или тем более «полководца».

В качестве противовеса «лебедям», которые не обязательно негативны по своей природе, но, вероятнее всего, принесут негативные последствия в случае, если субъект не готов их использовать (ср. ситуацию ухудшения жизненных обстоятельств в результате неожиданной крупной удачи, многократно обыгранную в литературе и кинематографе и систематически воспроизводящуюся в жизни) Талеб предлагает доктрину «антихрупкости» как способность к извлечению выгоды из неудач, потерь, ошибок; умение закаляться,

[93] *Талеб Н. Н.* Указ. соч. С. 68.

развиваться и становиться сильнее при столкновении с хаосом[94]. Уникальность антихрупкости состоит в том, что она позволяет работать с неизвестностью, делать что-то в условиях, когда отсутствует понимание, что именно делается, и добиваться успеха. Ее цель — не построение непроницаемого щита от возможных и невозможных угроз, но уменьшение потерь при столкновении с Неизвестностью. Идеал антихрупкости — децентрализация, ставка на риск, выживание в агрессивной среде, адаптивность, инновационность, опора на практические правила. Антихрупкость в социальной политике — «самостоятельность сильных» и «поддержка слабых» (но не укрепление привилегий «среднего класса»). Носитель Антихрупкости — прежде всего авантюрист, представитель мира «сильных» (рыцарь), слабых (разбойник, пират), либо актор внешней экспансии (конкистадор), которые способны действовать осознанно и успешно в ситуации, пониманием которой не обладают. «Из античной культуры я вынес понятие „мегалопсихон“ (от др.-греч. „великая душа“) <…>, величественную концепцию, смененную позже „христианским смирением“. На романские языки это слово не переводится, в арабском таких людей называют „шхм“ — что можно перевести как „не ничтожный“. Если вы рискуете и встречаете судьбу с достоинством, ничто не может сделать вас ничтожным; если вы не рискуете, ничто не сделает вас великим, вообще ничто на свете. И когда вы принимаете риск, оскорбления полулюдей (ничтожных людей, которые ничем не рискуют) схожи со звериным лаем: пес оскорбить не может»[95]. Важный аспект: тот, кто не рискует собой в большей или меньшей степени, не способен (кроме как на словах) отказаться от принципа выгоды, перерасти уровень homo economicus, именно потому, что он, сознательно или нет, делает выбор в пользу ситуации, в которой его выбор ничего не значит, а его комфортное существование выглядит максимально гарантированным. Впрочем, такой выбор, очевидно, не следует считать однократным и окончательным: субъект может не сделать подобного выбора, не нуждаясь в нем по обстоятельствам жизни,

[94] *Талеб Н. Н.* Антихрупкость. Как извлечь выгоду из хаоса. 768 с.
[95] Там же. С. 259.

но в определенный момент сделать «героический» выбор, осознав его необходимость, в результате обыватель должен превратиться в героя либо злодея (см., например, хоббитов Толкина). Наивысшей ценностью в глазах общества обладает риск, означающий потенциальное или реальное самопожертвование во имя блага «Другого» (ситуация, когда субъект, по Талебу, «ставит на кон свою душу»), именно эти люди могут оказаться героями в глазах общества (что не исключает: а) ошибок общества, неверно определяющего «героя»; б) незамеченного обществом героизма; в) наконец, ошибок «героического» субъекта, в результате которых самопожертвование оказывается бесполезным или вредным). С другой стороны, выбор в пользу отказа от риска, в пользу стабильности и предсказуемости, выбор «ничтожных» Данте, «последних людей» Ницше или «полулюдей» Талеба — это в конечном счете выбор социальной позиции «лоха», жертвы сторонней информационной активности и чужих авантюр. Гражданин «Среднестана» может быть в инфосфере пешкой или фигурой, но никогда — игроком.

«Антихрупкий» субъект Талеба скептичен, рефлективен и эмпирически ориентирован (то есть обращает внимание на многообразную и многоуровневую конкретику опыта Настоящего, а не на обобщения Прошлого или ожидания Будущего), а значит, менее прочих подвержен типичным когнитивным сдвигам. Характерно, что эпистемологические ошибки Талеба, в принципе, выстраивают похожую модель искажений восприятия, к которой мы можем отнести:

— персонализацию, когда все события интерпретируются преувеличенно личностно;

— дихотомическое мышление, когда все события могут быть либо только хорошими, прекрасными, либо плохими, ужасными;

— выборочное абстрагирование, когда оценка одной детали начинает трактоваться как оценка всего события;

— произвольные умозаключения, когда бездоказательные умозаключения становятся определяющими (например, фраза: «Я ужасная мать!»);

— сверхгенерализацию, когда обобщение строится на основании единичного случая (типа «Все мужчины одинаковы», «я всегда все делаю неправильно»);

— преувеличение («катастрофизация») как переоценка значения, масштаба или последствий какого-либо события.

Состояние инфосферы позволяет с высокой точностью отслеживать типичные для целевой группы когнитивные сдвиги и избирательно воздействовать на ситуацию, используя, например, «вирусную» коммуникацию или «вбросы» сенсационного характера безотносительно к их истинности либо ложности (см. историю «распятого мальчика» на Украине; см. также ситуацию с «советскими/российскими подводными лодками у берегов Швеции»). И если обыденное сознание принципиально тяготеет к однозначности, определенности и введенного в инфополе смысла происходящих событий (нарративное заблуждение по Талебу), то провоцирование этой ошибки должно стать (и становится) осознанно применяемым инструментом пропаганды, например прием «блистательная неопределенность» и другие пропагандистские приемы, в общем виде сводимые к подмене факта предварительно заданной оценкой, искажающей реальность в пользу актора пропаганды.

Однако и акторы инфосферы оказываются в заведомо неравных условиях. Описывая ключевые эпистемы, характерные для героического и эволюционного подхода, мы обнаруживаем в обоих случаях стабильность как сверхцель. В первом случае можно говорить о необходимости обеспечить стабильное процветание, во втором — стабильное развитие, но в обоих идеалом для субъекта полагается достижение посредством принятия «правильной» системы ценностей некоего гармоничного равновесия между миром внутренним (эго, душа, личность) и миром внешним (социум, сверх-Я, этнос, мир Божий и т. п.), интерпретируемого как высшее благо. Проблема в том, что подобное равновесие благом, по-видимому, не является.

Известна серия экспериментов американского этолога Дж. Кэлхуна «Вселенная-25»[96], в которых группа мышей, размещенная в (предположительно) оптимальных для стабильного процветания и размножения условиях, выработала систему форм девиантного

[96] См.: *Calhoun J. B.* Death Squared: The Explosive Growth and Demise of a Mouse Population. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1644264/pdf/procrsmed00338-0007.pdf (дата обращения: 25.08.2018).

поведения и, в конце концов, прекратила размножение, деградировала и вымерла. Условия эксперимента и чистота его проведения подвергались критике, однако применительно к стратегиям субъектов инфосферы мы также не можем говорить о «безусловной чистоте эксперимента»: даже если мы примем как аксиому искреннюю приверженность акторов декларируемым ими целям (что в реальности не обязательно), речь в обоих случаях идет о навязывании инфосфере «единственно верной» эпистемологии, которая должна исключить саму возможность появления «черных лебедей», в том числе в рамках гегелевской диалектики, через инкорпорирование противоречия в систему как необходимого структурного элемента и, соответственно, постулирование необходимых сломов мироописания.

В случае концепции технологической сингулярности мы вообще говорим о «предсказанной непредсказуемости», готовя восприятие субъекта к этой (и никакой другой) перспективе как единственно возможной. Следовательно, обе модели в качестве сверхзадачи ставят нивелирование субъектов инфосферы как минимум по одному ключевому показателю — по адаптированности к «единственно правильному» варианту реальности. Но проблема не столько в том, что оппонирующая сторона, естественно, воспринимает такую «адаптацию» как давление, пропаганду, попытку разрушения ключевых эпистем. Важнее то, что в ситуации незавершенного и небезусловного познания мира концепция единственно адекватной эпистемологии по определению неадекватна, так как человечество если и нуждается в «абсолютном и неограниченном благе», то, во всяком случае, не в «единственно возможном» благе. Если для отдельного человека нормально (но не обязательно!) стремиться к личному счастью и благополучию, то человечество как популяция, как сверхорганизм для предохранения от деградации нуждается в наличии внутреннего (конфликты) и внешнего (вызовы) давления. Сбалансированное, «последовательно эволюционное» развитие неизбежно порождает концепцию преемственности, недискутируемости базовых ценностей, неуязвимости (Рим как «Вечный город»; «Москва — Третий Рим»; «Союз ***нерушимый*** республик свободных», концепт США как сверхценного лидера демократического мира и т. п.), то есть

хрупкость и стагнацию. Движение человечества вперед осуществляется посредством катастроф[97]. (Катастрофа понимается в значении, принятом в физике динамических систем как резкое качественное изменение объекта при плавном количественном изменении параметров, от которых он зависит.) Соответственно, задача, стоящая перед субъектом инфосферы, не предотвращение катастроф, но формирование готовности к катастрофам и умение использовать их потенциал для интенсификации собственного развития. Стратегическое планирование должно усвоить принципы теории хаоса.

С. Манн определяет эти принципы следующим образом:

— теория хаоса прилагается к динамическим системам — системам с очень большим количеством подвижных компонентов;

— внутри этих систем существует непериодический порядок, по внешнему виду беспорядочная совокупность данных может поддаваться упорядочиванию в разовые модели;

— подобные «хаотические» системы показывают тонкую зависимость от начальных условий; небольшие изменения каких-либо условий на входе приведут к дивергентным диспропорциям на выходе;

— тот факт, что существует порядок, подразумевает, что модели могут быть рассчитаны как минимум для более слабых хаотических систем[98].

Работу Манна в отечественной политологической традиции обычно рассматривают как свидетельство аморализма американского политического истеблишмента, ориентированного на направленное провоцирование политического хаоса как средства сохранения однополярного мира под контролем США. В реальности Манн изначально отказывается от концепции «полярности» как

---

[97] См.: *Арнольд В. И.* Теория катастроф // Итоги науки и техники. Сер. Соврем. проблемы математики. Фундаментальные направления. 1986. Т. 5. С. 219–277 ; *Арнольд В. И., Афраймович В. С., Ильяшенко Ю. С., Шильников Л. П.* Теория бифуркаций // Итоги науки и техники. Сер. Соврем. проблемы математики. Фундаментальные направления. 1986. Т. 5. С. 5–218 ; *Мясников А. А.* Синергетические эффекты в современной экономике: введение в проблематику. М., 2010. С. 27.

[98] См.: *Манн С.* Теория хаоса и стратегическое мышление. URL: http://spkurdyumov.ru/what/mann/ (дата обращения: 25.08.2018).

избыточно линейной и механистической. «Сейчас, когда мы отошли от сдерживания, начинаются разговоры о правильной концепции полярности — является ли мир многополярным, однополярным или триполярным, он уже более не двуполярный. Эти разговоры являются примером того, как мы не замечаем очевидных вещей. В политическом плане мир имеет слишком много различных акторов, чтобы осмыслять его в терминах полярности. Мы еще пытаемся использовать метафору из механицистского лексикона, дающего нам комфортабельно ощущение, что мы действительно понимаем новый мир»[99]. Манн, разумеется, говорит о «вирусном» распространении американской идеологии как способе достичь максимальной выгоды для лагеря, к которому принадлежит, но не путем «распространения хаоса», а путем внедрения в хаос международной политики идеологических «аттракторов», точек притяжения, завязанных прежде всего на права и возможности личности.

По мнению Манна, этот подход является формой «мягкой силы», поскольку в краткосрочной перспективе позволяет уменьшить конфликтность международной обстановки и уровень направленной против США агрессии ввиду формирования у политически активных субъектов сходной системы ценностей. Хаос не нужно создавать — он существует априори, но его следует использовать как ресурс, при этом доминирование в инфосфере становится инструментом, обеспечивающим выживание структуры (США). В противном случае хаос неизбежно разрушает структуру, причем в отдаленной перспективе это, по Манну, произойдет в любом случае — грамотные действия в условиях доминирующей неопределенности позволят лишь отсрочить неизбежную трансформацию общества и сгладить формы и последствия катастрофы. По сути, речь идет о возобновлении в современных условиях «византийской модели»: стратегически значимая часть структуры Римской империи успешно переживает социокультурную катастрофу, уничтожившую античность, и на несколько столетий становится одним из определяющих центров силы в Средиземноморском регионе и в глобальной (на тот момент) экономике. Структура, таким образом, успешно

[99] *Манн С.* Указ. соч.

проходит «зону хаоса» и погибает уже при многократно изменившейся внешней и внутренней парадигме, полностью исчерпав изначально запасенный ресурс выживания — за пределами «горизонта событий». Показательно здесь именно осознание современности как эпохи глобального структурного кризиса, при котором подобная постановка задачи приобретает первостепенное значение как едва ли не единственное возможное средство выживания структуры. В кризисную эпоху именно известные и признанные центры силы становятся первостепенной зоной притяжения, первостепенным раздражителем и очевидным объектом агрессии. При этом объективная военная, экономическая, политическая и демографическая мощь сформированных ранее структур в эпоху системного кризиса сама по себе значения не имеет, поскольку адаптирована к известным и систематизированным угрозам, а не к действиям в условиях катастрофы. Границу Римской империи на рубеже IV в н. э. пересекли, по разным источникам, от 10 до 40 тыс. гуннов. Совершенно очевидно, что никакой угрозы римскому могуществу эти нищие, голодные, полудикие варвары не несли.

Использование принципа неопределенности как точки отсчета позволяет по-новому взглянуть на уже рассмотренные ранее феномены инфосферы:

— Информационная война в обыденном понимании есть норма существования человеческого сообщества. Информационные войны в политическом пространстве обращают на себя особое внимание, поскольку вовлеченность субъекта в процесс является одним из инструментов достижения доминирования. Это не отменяет, однако, информационных войн как обыденности во всех сферах личного, социального, экономического, политического и культурного взаимодействия между субъектами разных типов и уровней — от личности до государства или мегакорпорации.

— Нарастание интенсивности «информационных войн» — типичное когнитивное искажение, известное как «систематическая ошибка выжившего» (жертвам геноцида тутси в Руанде абсолютно все равно, какую оценку задним числом дадут этим событиям мировые новостные каналы): погружаясь в инфосферу (что возможно при ожидаемой гарантированной безопасности на материальном

уровне), субъект предполагает именно информационную реальность определяющей, в то время как столкновения в ней были и остаются только частью «гибридных» конфликтных взаимодействий между акторами. Реально здесь нужно говорить об общей интенсификации межсубъектного взаимодействия в глобальной перспективе, что приводит к нарастанию общей конфликтности, находящей отражение в инфосфере. Переоценка роли информационных войн ведет к фантасмагорическим построениям в духе «российские СМИ с государственным участием и кремлевская „Фабрика троллей“ помогли Трампу выиграть президентские выборы», либо «к распаду СССР привела литературная деятельность Солженицына и пропаганда ВВС»: инфосфера — только один из факторов существования субъекта, не единственный и далеко не всегда определяющий.

— Соответственно, информационные войны — не печальный, неизбежный, но преходящий этап становления технологического сверхчеловечества и не попытка подмены культурных стереотипов противника с целью достижения глобального доминирования (хотя ситуативно они могут быть и тем, и другим, особенно в восприятии акторов инфосферы). Информационная война вообще не имеет собственной онтологии, этот термин имеет смысл только методологически — как описание определенной совокупности приемов взаимодействия с хаотически изменяющейся реальностью, но, несомненно, важен как концепт, используемый для такого взаимодействия. Термин «информационные войны» тем более осмыслен, чем ближе его применение к среде профессионалов, владеющих инструментарием подобного рода взаимодействий; показательно при этом, что именно профессионалы предпочитают избегать использования термина, отдавая его на откуп медийным фигурам.

— При этом инфосфера однозначно приобретает определяющее значение как инструмент сбора и обработки информации обо всех уровнях существования человечества вообще и актуальной структуры в частности; соответственно, такая обработка может позволить выделить ключевые для ситуативной адаптации структуры параметры глобальных и локальных систем, в которые она включена, и в результате с высокой вероятностью спрогнозировать возникновение экстремальной ситуации и (при возникновении)

преодолеть ее с наименьшими возможными потерями. Однако это возможно только при выполнении четкой программы управленческих решений, ориентированной на методики стратегического планирования и управления в кризисной ситуации:

а) определение ключевых ценностей, конституирующих структуру и, соответственно, подлежащих по возможности сохранению или трансформации до тех пор, пока само их сохранение не будет признано угрозой существования структуре;

б) создание и совершенствование механизмов мониторинга всех уровней реальности: наблюдение в реальном времени вплоть до спутниковой съемки, биометрическое документирование, цифровой документооборот, цифровое образование, цифровая медицина, цифровая экономика, цифровое правительство, хранение и каталогизация информации (технологии big data), фреймирование (SWOT-анализ и др.), ситуативное определение ключевых параметров (развитие искусственного интеллекта); междисциплинарность, описание мира как многоуровневой, многофакторной динамической системы;

в) подготовка аналитических групп, вырабатывающих модели и сценарии развития ситуации в условиях кризиса. Характеристики: мобильность, креативность, инновационность, адаптивность. Технологизация творческих процессов (например, по методике ТРИЗ). Свободная конкуренция между группами. Развитие дистантного, модульного образования, внедрение концепции непрерывного образования. В современной России центрами подготовки кадров по этой модели, по-видимому, являются ВШЭ, инновационный центр «Сколково», образовательный центр «Сириус»;

г) подготовка лидеров, психологически адаптированных к критическим ситуациям, к активным действиям в условиях неопределенности, и способных принимать ответственные решения, выбирая из вариантов, предложенных креативными группами. В современной России центрами подготовки кадров по этой модели, по-видимому, являются программа «Лидеры России», «Кадровый резерв Президента РФ», до 2014 г. — Всероссийский молодежный образовательный форум «Селигер». Группы разработки сценариев и группы принятия решений не пересекаются. Здесь сохраняет актуальность принцип

Форда «исполняющий не решает, решающий не исполняет»: производство по заказ моделей и сценариев есть работа исполнителя, основной процесс; предложенные сценарии становятся основой для принятия решений, но не становятся напрямую решениями; штаб не эквивалентен командованию;

д) работа по критическим точкам — структура реагирует на экстеремум информационного потока, срезая угрожающие стабильности пики и одновременно обеспечивая нормальное функционирование в крайних точках социальной кривой («принцип штанги» по Талебу: усиливай сильных, поддерживай слабых, придерживайся принципа невмешательства («Laissez-faire») на среднем уровне)[100];

е) диверсификация ресурсов и направлений деятельности, формирование стратегического резерва на случай экстремальной ситуации.

Анализ политики РФ последних десятилетий позволяет с высокой долей уверенности предполагать, что принцип неопределенности и осознание актуального распада устоявшихся структур экономического, политического и социального миропорядка, что знаменует глобальное «расторжение общественного договора» и делает задачу выживания структуры первоочередной, не является прерогативой американского истеблишмента. Настоящее России целенаправленно и последовательно используется как ресурс, позволяющий сформировать готовность к Будущему. Готовность, предполагающую не просто сохранение России как над-персональной структуры, транслирующей будущим поколениям культурные ценности Прошлого, но и накопление и преумножение потенциала для получения комфортной позиции в новой реальности какой бы эта реальность в конечном счете не оказалась.

Теория неопределенности вновь выдвигает на первый план личность, героя, однако героя иного склада, чем структурно интегрированный «сакральный правитель» героической модели. В ситуации, когда количество факторов неисчислимо, когда ключевой параметр может быть определен ошибочно и когда катастрофа может быть

[100] См.: *Талеб Н. Н.* Черный лебедь. Под знаком непредсказуемости.

отложена, но не исключена, а сверхзадача — не избежать волны, а взобраться на ее гребень, героем становится харизматический лидер, авантюрист, искатель приключений. Его действия могут выглядеть хаотичными, непредсказуемыми — однако сама эта непредсказуемость обладает признаками четкой организации, соотносимой с принципами *системного подхода* и *кризис-менеджмента* в теории управления. Инфосфера, коммуникации, субъекты коммуникаций приобретают для такого актора статус изучаемых и используемых ресурсов, а реальность в целом описывается по следующим параметрам.

Объект: кейс. *Цель*: стабильное доминирование. *Ценности*: адаптация, развитие, мобильность. *Принципы*: системность, стратегическое планирование, актуальность внутренней структуры, неопределенность внешней среды. *Структура*: дискретная, конфликтогеничная, подвижная, адаптивная. *Личность*: универсальна, развиваема, автономна, амортизируема. *Тип развития*: интенсивный. *Практика*: авантюрно-экономический подход, подвижность структуры, инновационность, креативность, лидерство. *Боги* (*творцы концептов*): Чжуань-цзы, К. Клаузевиц, А. Богданов, Л. фон Берталанфи, Г. Саймон, П. Друкер, А. Чандлер, Г. Щедровицкий. *Утопия и антиутопия*: Ф. Херберт «Дюна».

На первый взгляд, эпистемология неопределенности, ориентированная прежде всего на адекватность мирописания мира, на деконструкцию мифологий и инструментальный характер знания, представляется (особенно в условиях глобального кризиса сознания, не отрицаемого и в других моделях) наиболее корректной и перспективной. Это, однако, не означает отсутствия у нее критических недостатков:

Невротизм. Благополучие иллюзорно. Нахождение в «зоне комфорта» — источник недооценки возможностей изменчивой реальности (в том числе и потенциальных угроз), попытка удержаться в этой зоне — источник страданий. Нормальным состоянием субъекта является актуальное осознание давления среды — это дает стимул развития. Развитие себя также не самоцель, но обновляемый ресурс в ситуации неопределенности. Мы получаем классическую рекурсию, при которой «необходимо бежать очень быстро, чтобы

просто остаться на месте». При этом, поскольку субъект изначально рассматривает себя как ресурс выживания, и так же расценивают его внешние структуры, с которыми он так или иначе связан (хотя бы как потенциальная жертва), то мы должны говорить о неизбежной амортизации человеческого ресурса, то есть субъект принципиально работает на истощение, на самоуничтожение и знает об этом, что не может не оказывать влияния на его эмоциональное состояние. Герой изменчивого мира — эмоционально нестабильный невротик с принципиально непредсказуемой, но, как правило, неоправданно агрессивной реакцией на любой кейс. В гости к Эгилю Скаллагримсону, великому исландскому скальду и знаменитому викингу, приехал его друг и привез в подарок богато украшенный щит. Не застав дома Эгиля, он оставил подарок и отправился восвояси. Вернувшийся Эгиль возмутился: значит, этот человек надеялся, что он, Эгиль, всю ночь будет сидеть и сочинять в честь дарителя хвалебную песню? Дайте коня — я догоню и убью его! Догнать дарителя не получилось (тот успел сесть на корабль), так что пришлось все-таки сочинять хвалебную поэму. Эгиль — типичный авантюрист-невротик переходной эпохи.[101]

Цинизм. Ресурсом выживания по определению является ***все***. Например, ценности, нормы и идеалы, культурные мифы и клише, этические категории, религиозные верования — в той степени, в которой они могут быть использованы в построении сценария выживания. Принципы принимаются не потому, что субъект их разделяет (его личное мнение в данном случае несущественно), но потому что здесь и сейчас они выгодны для выживания. Поскольку нет оснований полагать, что эта логика не общепринята вне субъекта, то любую попытку коммуникации следует рассматривать именно как попытку амортизации «Я» как ресурса для выживания «не-Я». На практике это означает глобальный *кризис доверия*[102] к любым внешним

[101] См.: Исландские саги: Сага об Эгиле. URL: https://www.litmir.me/br/?b=101844&p=44.

[102] См., напр.: *Хан Е.* Всемирный кризис доверия. URL: https://cont.ws/@jeckhan/668132 (дата обращения: 25.08.2018) ; *Ермолин Е.* Глобальный кризис доверия и перспективы актуальной журналистики. URL: http://yspu.org/imag-

структурам и к любым провозглашаемым ценностям, призывам, идеалам и нормам — и, как следствие, не столько переключение субъектов на героический модус действия, сколько, напротив, развитие безразличия, социокультурной пассивности, отсюда «Цинизм есть просвещенное ложное сознание» П. Слотердайка. «Цинизм как восхождение на „гордую и одинокую высоту“ ненавидящей мир интроспекции — это позиция избыточной сентиментальности, которая на самом деле не такая уж пренебрежительная и не такая уж „глубокая“. Зависть, которую она испытывает к „метафизической невинности“ — к тем, кто благоденствует благодаря своей „свободе“ от метафизических забот интеллектуалов, это опять же признак ее связи с ценностями мира. И метафизическая невинность, и меланхоличный циник нуждаются в посредственности. Оба в определенном смысле признают представление о мире, предлагаемое миром в самом ходе отказа от него»[103]. Таким образом, за спиной «рыцаря, пирата или конкистадора» отчетливо проступает фигура удачливого биржевого спекулянта, тоскующего на историческом маскараде. Декларируемая готовность к крайним формам ответственности не эквивалентна этой готовности, а значит, цинический модус кризисного менеджмента построен на самоотрицании.

Отсутствие стратегической перспективы. Одним из любопытных аспектов культурологических эссе Талеба является пренебрежительное отношение к фундаментальной науке. Действительно, какой смысл тратить все возрастающие ресурсы на постижение давно уже никому неинтересных законов природы, которые, по мнению самих же ученых, непостижимы? Наука должна превратиться в новую магию, в чудотворчество, позволяющее лучше использовать мир как ресурс; то есть ценным является только знание, полезное здесь и сейчас — точно так же, как идеология, по утилитарным соображениям поддерживаемая здесь и сейчас. Показательно в этом смысле отношение общества и государственных структур к лунной

---

es/a/a1/Ермолин_Е.А._Глобальный_кризис_доверия_и_перспективы_актуальной_журналистики.pdf (дата обращения: 25.08.2018) и др.

[103] *Бьюз Т.* Цинизм и постмодерн / пер. с англ. С. А. Зеленского. М., 2016. С. 198.

и марсианской космическим программам и вообще к пилотируемой космонавтике: эти направления находятся в последние десятилетия в очевидном упадке, несмотря на громадный, по сравнению с 60-ми годами, рост технологических и производственных возможностей. Именно поэтому зачастую утилитарно используются в современной российской пропаганде «духовные скрепы» и историческое прошлое России (см. дискуссию о допустимом/недопустимом искажении истории, связанную, в частности, с фильмом «28 панфиловцев» или докторской диссертацией В. Р. Мединского). При этом структура может апеллировать к прошлому и/или будущему культурному, политическому, экономическому, военному и т. п. величию, однако следует иметь в виду, что в рамках цинического модуса — это во всех случаях не более чем выбранный структурой сценарий самосохранения, не предполагающий реального вложения в декларируемые ценности. Эпистемология хаоса может способствовать выживанию использующей ее инструментарий структуры, однако она контрпродуктивна в культурном плане, поскольку единственное, что она позволяет создавать — это воспроизведение действующей структуры в тех или иных формах; принцип неопределенности позволяет (при удачном стечении обстоятельств) вписаться в будущее — но не построить его. Соответственно, мы опять-таки сталкиваемся с рекурсией, при которой сохранение самоценной и самодостаточной структуры как высшая ценность подменяет, вытесняет и обессмысливает любые возможные формы социокультурного само-стояния.

Н. Талеб, апеллируя к авторитету У. Эко, говорит о перспективах доминирования неопределенности как о наступлении Нового Средневековья; однако вряд ли он имеет в виду тот период, который на самом деле последовал за падением Римской империи и известен историкам как «Темные века». Жак Ле Гофф, описывая становление средневековой цивилизации, характеризует ее ранний этап следующим образом: «Франкский король, возводимый на трон поднятием его на щите, в качестве инсигний, вместо скипетра или диадемы, имел лишь копье, а его отличительным знаком являлись длинные волосы („rex crinitus“). Этакий царь Самсон с гривой волос, переезжавший из одного своего владения в другое в сопровожде-

нии нескольких писцов, домашних рабов и гвардии антрустионов. И ко всему этому прилагались дивные титулы, позаимствованные из словаря поздней Римской империи. Старший конюх именовался „главным конюшим", или коннетаблем, личные охранники — „палатными графами", и все это сборище пьяных солдат и неотесанных служащих величалось „славными, или именитыми, людьми". Налоги более не поступали, и богатство короля было заключено в сундуках с золотыми монетами, стеклянными изделиями и драгоценностями, которые после его смерти оспаривали друг у друга его жены, наложницы, законные и незаконные дети, производя одновременно раздел земель и всего королевства»[104]. Структура, таким образом, действительно отчасти сохранилась, хотя изменились ее носители, но она сохранилась как содержательно мертвый ритуал, минимально камуфлирующий нефункциональность в эпоху победившего хаоса каких-либо структур вообще. Остатки структуры позволяют удерживать некоторое количество значимых для предыдущей эпохи ценностей. У ле Гоффа это золото, в новую эпоху в этой роли, вероятно, могла бы выступать информация, однако ценности утрачивают свое инструментальное значение в социуме и превращаются в сокровища, в символ статуса, то есть опять-таки ритуализируются — они утилитарно бесполезны в силу уничтожения рынка, но ценны в силу редкости и невоспроизводимости в случае утраты.

Структура, выбирающая в качестве базового ориентира принцип неопределенности, может некоторое время продержаться на плаву как подобное «варварское королевство» в эпоху крушения традиционного социума. Причем есть некоторая вероятность, что из хаотического столкновения подобных квазисоциальных общностей может родиться как новое эпическое повествование подобно тому, как «Темные века» породили европейский эпос эпохи Средневековья, так и новые устойчивые формы смыслообразования, такие, например, как концепция прав личности в европейском либерализме, опирающаяся более на «варварские Правды» и христианскую

[104] *Гофф Ж. ле.* Цивилизация средневекового запада. М., 1992. URL: http://www.danilov.lg.ua/author/7538/ebook/24894/le_goff_jak/tsivilizatsiya_srednevekovogo_zapada/read (дата обращения: 25.08.2018).

концепцию греха и воздаяния, нежели на римское право. Однако вряд ли это можно описать как созидательную активность самих рассматриваемых структур. Скорее их практика близка в основной части к схеме, описанной персонажем Е. Леонова в фильме «Джентльмены удачи»: «Украл — выпил — в тюрьму! Украл — выпил — в тюрьму! Романтика!..» Если у человечества есть хотя бы намек на возможность сознательного выбора цели и перспектив развития, то принцип неопределенности может быть использован как фактор, но не должен становиться целью, смыслом и предпочитаемой перспективой.

ЗАКЛЮЧЕНИЕ

— Солнце снова всходит и заходит,
снова камень имеет вес, а воздух не имеет.
Вода опять падает дождем и стекает
в море… Давайте строить планы.
Д. Вэнс. Когда планета сошла с ума.

Лукиан Самосатский, позднеантичный философ и писатель-сатирик II в. н. э., писал в монологе «О смерти Перегрина»:

«Христиане проявляют невероятную быстроту действий, когда случится происшествие, касающееся всей общины, и прямо-таки ничего не жалеют <…> Ведь эти несчастные уверили себя, что они станут бессмертными и будут всегда жить; вследствие этого христиане презирают смерть, а многие даже ищут ее сами. Кроме того, первый их законодатель вселил в них убеждение, что они братья друг другу, после того как отрекутся от эллинских богов и станут поклоняться своему распятому мудрецу и жить по его законам. Поэтому они одинаково ко всему относятся с презрением и все доходы считают общими, так как все подобное они принимают без какого-либо достаточного доказательства <…> Так вот, когда к ним приходит обманщик, мастер своего дела, умеющий использовать обстоятельства, — он скоро делается весьма богатым, издеваясь над простецами»[1].

[1] *Лукиан*. О кончине Перегрина (Отрывки). URL: http://lib.ru/POEEAST/LUKIAN/lukian1_6.txt (дата обращения: 28.08.2018).

Высокообразованный, ироничный, скептически настроенный интеллектуал, утонченный стилист, один из замечательнейших носителей культуры своей эпохи, Лукиан оказался не в состоянии увидеть в христианстве то, что станет основой крушения привычного ему мира и сформирует новую европейскую цивилизацию. Вряд ли эту ошибку можно поставить в вину Лукиану. Он видел в христианах то, что видели и другое его современники: сборище малообразованных, наивных, жалких людей, одержимых странными предрассудками и суевериями и легко идущих на поводу у бессовестных шарлатанов. Более того, вероятно, присоединившиеся к христианам носители высокой культуры античности (такие, как Августин Аврелий) должны были вызывать у современников подозрения либо в безумии, либо в попытке корыстно эксплуатировать доверчивость христиан — подобно тому, как использовал его «герой» лукиановского монолога мошенник Перегрин.

Любая новая историко-культурная парадигма — классический «Черный лебедь» Талеба: в исторической перспективе ее возникновение будет представляться как необходимость, как неизбежность, но до момента ее становления ее ключевые параметры неочевидны, хотя они, несомненно, существуют и развиваются внутри действующей системы отношений, накапливая потенциал для качественного скачка. Именно и только в этом смысле мы действительно можем говорить о сингулярности: признаки надвигающегося качественного скачка в развитии цивилизации не безусловны, но в любом случае математически точно спрогнозировать это развитие на данный момент не представляется возможным именно потому, что любой выбор ключевого параметра в условиях глобального системного кризиса носит сугубо гадательный характер.

Ошибкой рассмотренных выше моделей описания инфосферы является в каждом случае как раз попытка построить универсальный рецепт, технологию сохранения себя в условиях погружающейся в хаос реальности. Однако такая постановка задачи содержит явное противоречие в условиях, когда для сохранения себя в меняющейся реальности субъект обязан измениться, причем не имея гарантии, что выбранное им направление изменений будет актуальным после того, как трансформация закончится, — «поставить на кон душу».

Христианство не было единственным конкурентом античности в борьбе за будущее Европы; при этом, не зная будущего, субъект, способный к осознанному выбору, вынужден был выбирать по неявным параметрам. Здесь можно говорить о роли веры или интуиции, но методически точнее будет акцентировать внимание на самой необходимости выбора. И если катастрофа неизбежна, то инструмента, позволяющего сделать гарантированно правильный выбор, не существует, либо он избыточен, поскольку в конечном счете все определяет не инструмент, а сам выбор.

Воздержание от выбора ***какой-либо*** системы ценностей, предполагающей возможность превращения человека в нечто более значимое, чем то, кем он является здесь и сейчас, то есть в конечном счете выбор в пользу самосохранения — в «интересные времена» позиция онтологически проигрышная. «Среднестанец», считающий единственной актуальной ценностью собственное благополучие в вечном и незыблемом «Среднестане», вполне может уцелеть в катастрофе, но актором новой реальности, культурно значимым субъектом миротворчества он не станет по определению. «Крайнестанец» может победить или проиграть, причем его победа или поражение будут выглядеть по-разному в разных системах отсчета. Но в его действиях будет как минимум попытка заглянуть за горизонт событий, «танцующая звезда» Ницше, которая и делает человека человеком.

«Когда не знаешь, что делать, делай что должно, и будь что будет» (*Л. А. Сенека*).

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ И ИСТОЧНИКОВ

Абдеев Р. Ф. Философия информационной цивилизации / Р. Ф. Абдеев ; ред. Е. С. Ивашкина, В. Г. Деткова. М. : ВЛАДОС, 1994. 336 с.

Абдигалиева Г. К. СМИ как фактор манипуляции массовым сознанием / Г. К. Абдигалиева, Б. Токтаров. URL: https://articlekz.com/article/8154.

Абрамова С. Г. О понятии «корпоративная культура» / С. Г. Абрамова, И. А. Костенчук. URL: http://www.emcon.ru/420–087.html.

Открытое государство. Чем оно является и чем быть не может / А. Аксенова и др. URL: http://polit.ru/article/2012/02/22/open/.

Алексеева И. Ю. Информационное общество / И. Ю. Алексеева. URL: https://iphras.ru/page46589323.htm.

Алпеев А. С. Критически важные объекты. Терминология безопасности / А. С. Алпеев // Вопр. кибербезопасности. 2016. № 4 (17). URL: https://tinyurl.com/ycsnqgtd.

Антоненко В. И. Информационное единство мира : учеб. пособие / В. И. Антоненко. Монино : ВВА, 1996. С. 314.

Антонова Л. Г. Медиатексты в современной массовой коммуникации / Л. Г. Антонова // Ярослав. пед. вестн. 2012. № 2. С. 275–278.

Теория бифуркаций / В. И. Арнольд и др. // Итоги науки и техники. Сер. «Соврем. проблемы математики. Фундам. Направления». 1986. Т. 5. С. 5–218.

Арнольд В. И. Теория катастроф / В. И. Арнольд // Итоги науки и техники. Сер. «Соврем. проблемы математики. Фундам. Направления». 1986. Т. 5. С. 219–277.

Барабаш В. В. Государственная пропаганда и информационные войны : учеб. пособие / В. В. Барабаш, Г. А. Бордюгов, Е. А. Котеленец. М. : АИРО-XXI, 2015. 400 с.

Баранова Е. В. Образование в информационном обществе. Проблемы образования в России и пути их решения / Е. В. Баранова // Концепт : науч.-метод. электрон. журнал. 2015. Т. 5. С. 41–45.

Барбашин М. Ю. Технологии информационного воздействия и социальной вакцинации / М. Ю. Барбашин. 2012. URL: http://evrazia.org/article/1998.

Батуева Е. В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая : дис. … канд. полит. наук / Е. В. Батуева. М., 2014. URL: https://tinyurl.com/yaf26hq7.

Бедрицкий А. В. Информационная война: концепции и их реализация в США / А. В. Бедрицкий. М. : РИСИ, 2008. 187 с.

Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Д. Белл. М. : Academia, 2004. 790 с.

Бентли Л. Право интеллектуальной собственности: Авторское право / Л. Бентли, Б. Шерман ; пер. с англ. В. Л. Вольфсона. СПб. : Изд-во «Юр. центр Пресс», 2004. 535 с.

Бжезинский З. Великая шахматная доска: главенство Америки и ее геостратегические императивы / З. Бжезинский. М. : АСТ, 2018. 384 с.

Бжезинский З. Между двумя веками: роль Америки в эру технотроники / З. Бжезинский. М. : Прогресс, 1972. 308 с.

Боголюбов Л. Н. Обществознание : 10 кл. Базовый уровень / Л. Н. Боголюбов. М. : Просвещение, 2009. 351 с.

Бодрийяр Ж. Дух терроризма. Войны в заливе не было / Ж. Бодрийяр. URL: http://avidreaders.ru/read-book/duh-terrorizma-voyny-v-zalive-ne.html.

Бодрунова С. С. Медиакратия. Атлантические подходы к определению термина / С. С. Бодрунова // Материалы междунар. науч. конф. «Медиафилософия. Границы дисциплины». СПб., 2013. С. 91–105.

Бон Г. ле. Психология народов и масс / Г. ле Бон. URL: http://lib.ru/POLITOLOG/LEBON/psihologia.txt_with-big-pictures.html#25.

Бондаренко С. В. Модель социализации пользователей в киберпространстве / С. В. Бондаренко // Технологии информационного общества — Интернет и современное общество : труды VI Всерос. объед. конф. Санкт-Петербург, 3–6 ноября 2003 г. СПб., 2003. С. 5–7.

Борисов Н. В. Информационное пространство направления научных исследований «Культура и технологии» / *Н. В. Борисов, Д. Е. Прокудин* // Культура и технологии. 2016. Т. 1. Вып. 1. С. 1–14.

Бродель Ф. Материальная цивилизация, экономика и капитализм. XV–XVIII вв. Т. 1–3 / Ф. Бродель. URL: https://web.archive.org/web/20091123073344/http://www.i-u.ru/biblio/archive/brodel/.

Буряк В. В. Глобальное гражданское общество и сетевые революции / В. В. Буряк. Симферополь : ДИАЙПИ, 2011. 152 с.

Буряк М. А. Медиасфера: концептуализация понятия / М. А. Буряк // Вестн. СПбГУ. 2014. Сер. 9. Вып. 2. С. 200–212.

Бьюз Т. Цинизм и постмодерн / Т. Бьюз ; пер. с англ. С. А. Зеленского. М. : ИД «КДУ», 2016. 270 с.

Валери П. Проблема музеев / П. Валери. Об искусстве. М. : Искусство, 1976. 622 с.

Варакин Л. Е. Глобальное информационное общество: Критерии развития и социально-экономические аспекты / Л. Е. Варакин. М. : Междунар. акад. связи, 2001. 43 с.

Вартанова Е. Л. Медиасфера, медиасреда, медиапространство / Е. Л. Вартанова. URL: http://www.journ.msu.ru/blog/%20blog_vartanovoy/.

Вартанова Е. Л. Медиаэкономика зарубежных стран / Е. Л. Вартанова. М. : Аспект-Пресс, 2003. 336 с.

Василенко И. А. Геополитика современного мира: учебник для бакалавров / И. А. Василенко. 3-е изд., перераб. и доп. М. : Изд-во «Юрайт», 2014. 420 с.

Васильев В. Информационное общество и образование / В. Васильев, М. Сухорукова. URL: https://cyberleninka.ru/article/n/informatsionnoe-obschestvo-i-obrazovanie-2.

Васильев М. ИКТ как фактор «Арабской весны» / М. Васильев. URL: https://www.geopolitica.ru/article/informacionno-kommunikativnye-tehnologii-kak-faktor-arabskoy-vesny.

Ваховский А. М. Политико-правовые вопросы регулирования Интернета: мировой опыт и российская практика / А. М. Ваховский // Изв. Тульск. гос. ун-та. Гуманитарные науки. 2016. № 2. С. 3–11.

Вербилович О. Теория коммуникативного действия: ключевые категории и познавательный потенциал / О. Вербилович. URL: https://tinyurl.com/y8du2s9p.

Виноградова Е. А. Информационная война: концептуальный анализ / Е. А. Виноградова. URL: http://www.nbpublish.com/library_get_pdf.php?id=30177.

Военная доктрина Российской Федерации // Рос. газета. Федеральный выпуск № 6570 (298). 30 декабря 2014 г.

Волковский Н. Л. История информационных войн : в 2-х ч. / Н. Л. Волковский. СПб. : Полигон, 2003.

Воробьев Г. А. Развитие информационного общества в России: проблемы и перспективы / Г. А. Воробьев. URL: https://www.pglu.ru/editions/un_reading/detail.php? SECTION_ID=2863&ELEMENT_ID=9891.

Воронина Т. П. Информационное общество: сущность, черты, проблемы / Т. П. Воронина. М. : ЦАГИ, 1995. 110 с.

Глазунов О. Н. Специфика правового регулирования сети Интернет в Китайской Народной Республике / О. Н. Глазунов, В. В. Авдеенко // Общество: политика, экономика, право. 2017. № 2. С. 93–96.

Гофф Ж. ле. Цивилизация средневекового запада / Ж. ле Гофф. М. : Изд. группа «Прогресс», «Прогресс-академия», 1992. URL: http://www.danilov.lg.ua/author/7538/ebook/24894/le_goff_jak/tsivilizatsiya_srednevekovogo_zapada/read.

Грачев Г. В. Информационно-психологическая безопасность личности: теория и технология психологической защиты : автореф. дис. … д-ра псих. наук / Г. В. Грачев. М. : РАГС, 2000. 56 с.

Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили. М. : ФИЗМАТЛИТ, 2010. 228 с.

Давыдов В. Н. Глобальные угрозы информационного общества / В. Н. Давыдов // Противодействие терроризму: Проблемы XXI века : информ.-аналит. и науч.-практ. журнал, 2012. URL: https://stategovernor.admhmao.ru/upload/iblock/47e/counter_terrorism_2012_3.pdf.

Давыдов Д. Развитие кибервойск США до 2020 г. / Д. Давыдов. URL: https://tinyurl.com/y8g8q47e.

Дебре Р. Введение в медиалогию / Р. Дебре. М. : Праксис, 2010. 368 с.

Дергачев В. А. Геополитика : учебник для вузов / В. А. Дергачев. М. : ЮНИТИ-ДАНА, 2004. 526 с.

Дерен Г. Грядущая цифровая война / Г. Дерен // Популярная механика. 2008. № 10. С. 78–80.

Директива МО США TS3600.I «Информационная война» от 21 декабря 1992 г.

Директива председателя КНШ МО США № 30 «Борьба с системами управления». 1993 г.

Диринг М. Рассвет сингулярности / М. Диринг. URL: https://web.archive.org/web/20110908052319/http://transhumanism.org/languages/russian/dawn-ofsingularity/Deering.htm.

Дискурс современных масс-медиа в перспективе теории, социальной практики и образования // Актуальные проблемы современной медиалингвистики и медиакритики в России и за рубежом : II Международ. науч.-практ. конф. Белгород, НИУ «БелГУ», 5–7 октября 2016 г. / под ред. Е. А. Кожемякина, А. В. Полонского. Белгород : ИД «Белгород» НИУ «БелГУ», 2016. 380 с.

Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

Документы Генеральной ассамблеи ООН по вопросу международной информационной безопасности // Информационные вызовы национальной и международной безопасности / И. Ю. Алексеева и др. / под общ. ред. А. В. Федорова, В. Н. Цигичко. М. : ПИР-Центр, 2001. 328 с.

Дугин А. Г. Основы геополитики / А. Г. Дугин. М. : Арктогея, 1997. URL: http://grachev62.narod.ru/dugin/chapt00.htm.

Дугин А. Г. Теория многополярного мира / А. Г. Дугин. М. : Евраз. движение, 2012. 532 с.

Дускаева Л. Р. Интенциональность медиаречи. Медиатекст как полиинтенциональная система / Л. Р. Дускаева. СПб. : С.-Петерб. гос. ун-т, 2012. 250 с.

Елизарова О. И. Разработка управленческих решений : учеб. пособие / О. И. Елизарова. М. : МГУП, 2009. 114 с.

Ельчанинова Н. Б. Проблемы совершенствования законодательства в сфере ограничения доступа к противоправной информации в сети Интернет / Н. Б. Ельчанинова. URL: https://cyberleninka.ru/article/n/problemy-sovershenstvovaniya-zakonodatelstva-v-sfere-ogranicheniya-dostupa-k-protivopravnoy-informatsii-v-seti-internet.

Еляков А. Д. Информационная перегрузка людей / А. Д. Еляков // Социол. исследования. 2005. № 5. С. 114–121.

Еремин А. Л. Оптимизация умственного труда и творчества: новые биоинформационные подходы и концепции / А. Л. Еремин // Жизнь без опасностей. Здоровье. Профилактика. Долголетие. 2013. № 4. С. 59–66.

Ермолин Е. Глобальный кризис доверия и перспективы актуальной журналистики / Е. Ермолин. URL: http://yspu.org/images/a/a1/Ермолин_Е.А._Глобальный_кризис_доверия_и_перспективы_актуальной_журналистики.pdf.

Ершов А. П. Информатизация: от компьютерной грамотности учащихся к информационной культуре общества / А. П. Ершов // Коммунист. 1988. № 2. С. 82–92.

Ершова Т. В. Информационная война и вечные ценности / Т. В. Ершова // Информ. общество. 2014. № 1. С. 3–4.

Жилкин В. В. Инфосоциализация. Сущность понятия / В. В. Жилкин // Общество. Среда. Развитие. 2007. Вып. 1. С. 37–47.

Жирков В. Предисловие // Н. Л. Волковский. История информационных войн : в 2 ч. Ч. 1 / В. Жирков. СПб. : Полигон, 2003. С. 4–6.

Засурский Я. Н. Система средств массовой информации России : учеб. пособие для вузов / Я. Н. Засурский, М. И. Алексеева. М. : Аспект Пресс, 2003.

Згоба А. И. Кибербезопасность: Угрозы, вызовы, решения / А. И. Згоба, Д. В. Маркелов, П. И. Смирнов // Вопр. кибербезопасности. 2014. № 5 (8). URL: http://cyberrus.com/wp-content/uploads/2015/02/vkb_08_05.pdf.

Ибрагимова Г. Стратегия КНР в области управления Интернетом и обеспечения информационной безопасности / Г. Ибрагимова // Индекс безопасности. 2013. № 1 (104). URL: http://www.pircenter.org/media/content/files/10/13559074100.pdf.

Иванов А. С. Информационное общество и институты демократии в постсоветской России / А. С. Иванов. URL: https://cyberleninka.ru/article/n/informatsionnoe-obschestvo-i-instituty-demokratii-v-postsovetskoy-rossii

Ивашов Л. Г. Россия или Московия? Геополитическое измерение национальной безопасности России / Л. Г. Ивашов. М. Эксмо, 2002. 416 с.

Казаков М. Ю. Интернет как сетевая публичная сфера / М. Ю. Казаков, В. А. Кутырев // Совр. проблемы науки и образования. 2013. № 3. URL: http://science-education.ru/ru/article/view?id=9328.

Калашников М. Третий Проект : в 3-х т. Т. II: Точка перехода / М. Калашников. URL: https://history.wikireading.ru/84840.

Кара-Мурза С. Г. Манипуляция сознанием / С. Г. Кара-Мурза. М. : Эксмо, 2005. 832 с.

Касаткин П. И. Современное образование: функции и предназначение / П. И. Касаткин. URL: https://cyberleninka.ru/article/n/sovremennoe-obrazovanie-funktsii-i-prednaznachenie.

Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе, обществе / М. Кастельс. М. : «У-Фактория», 2004. 328 с.

Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс. URL: http://www.gumer.info/bibliotek_Buks/Polit/kastel/index.php.

Кеннеди П. Вступая в двадцать первый век / П. Кеннеди. М., 1997. URL: https://www.gumer.info/bibliotek_Buks/Polit/Kenn/index.php.

Кириллова Н. Б. Медиакультура: теория, история, практика : учеб. пособие / Н. Б. Кириллова. М. : Академ. проект ; Культура, 2008. 496 с.

Киселев В. Кибервойна как основа гибридной операции / В. Киселев, А. Костенко // Армейский сб. 2015. № 11 (257). С. 3–6.

Клаузевиц К. фон. О войне / К. фон Клаузевиц. М. : Госвоениздат, 1934. URL: http://knigosite.org/library/read/27370.

Клингберг Т. Перегруженный мозг. Информационный поток и пределы рабочей памяти = The Overflowing Brain. Information Overload and the Limits of Working Memory / Т. Клингберг. М. : ЛомоносовЪ, 2010. 208 с.

Колин К. К. Философские проблемы информатики / К. К. Колин. М. : Бином, 2010. 264 с.

Концепция развития непрерывного образования взрослых в Российской Федерации на период до 2025 года // Союз руководителей учреждений и подразделений дополнительного и профессионального образования и работодателей : проект постановления. URL: http://www.dpo-edu.ru/?page_id=13095.

Корнев М. Фактчекинг: 5 надежных способов проверить информацию / М. Корнев. URL: http://mediatoolbox.ru/factchecking/.

Коротаев А. В. Новые технологии и сценарии будущего, или Сингулярность уже рядом? / А. В. Коротаев. URL: http://cliodynamics.ru/index.php?option=com_content&task=view&id=117&Itemid=49.

Коротков А. В. Государственная политика Российской Федерации в области развития информационного общества / А. В. Коротков, Б. В. Кристальный, И. Н. Курносов ; науч. ред. А. В. Коротков. М. : ООО «Трейн», 2007. 472 с.

Корсаков Г. Б. Роль информационного оружия в военно-политической стратегии США / Г. Б. Корсаков // США и Канада: экономика, политика, культура. 2012. URL: http://naukarus.com/rol-informatsionnogo-oruzhiya-v-voenno-politicheskoy-strategii-ssha.

Костина А. В. Тенденции развития культуры информационного общества: анализ современных информационных и пост-индустриальных концепций / А. В. Костина // Знание. Понимание. Умение : информ. гум. портал. 2009. № 4. Культурология. URL: http://zpu-journal.ru/e-zpu/2009/4/Kostina_Information_Society/.

Костина А. В. Культура информационного общества: тенденции и противоречия развития / А. В. Костина. URL: https://cyberleninka.ru/article/n/kultura-informatsionnogo-obschestva-tendentsii-i-protivorechiya-razvitiya.

Котенко И. В. Таксономии атак на компьютерные системы / И. В. Котенко // Труды СПИИРАН. Вып. 1 : в 3-х т. Т. 2. СПб. : СПИИРАН, 2002. URL: http://www.proceedings.spiiras.nw.ru/ojs/index.php/sp/article/download/1112/976.

Кристальный Б. В. Информационное общество, информационная политика, правовая информационная защита / Б. В. Кристальный, Ю. М. Нестеров. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/988e812f3502e63ac32575bd003028e3.

Кузьмина Н. А. Современный медиатекст : учеб. пособие / Н. А. Кузьмина. Омск : Полиграф. центр «Татьяна», 2011. 414 с.

Куликова С. А. Информационное право России : учеб. пособие / С. А. Куликова. Саратов : Изд-во гос. ун-та, 2010. 196 с.

Курбатов В. И. «Homo informaticus» — человек информационной эпохи: характерологические черты / В. И. Курбатов // Гум., соц.-эконом. и общ. науки. 2017. № 7/1. С. 46–51.

Кушнарева И. Ко всему приделать лайки / И. Кушнарева. URL: http://www.intelros.ru/pdf/logos/2012_2/01.pdf.

Лекторова Ю. Ю. Политические коммуникации в сетевом ландшафте: акторы и модели взаимодействия (на правах рукописи) : автореф. дис. …. канд. полит. наук / Ю. Ю. Лекторова. Пермь : ПГУ, 2011. 22 с.

Леонтьев М. Большая игра. Британская империя против России и СССР / М. Леонтьев. СПб. : Астрель, Астрель-СПб. 2012. 352 с.

Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография / Д. А. Ловцов. М. : РГУП, 2016. 316 с.

Ловцов Д. А. Информационное право : учеб. пособие / Д. А. Ловцов. М. : РАП, 2011. 228 с.

Луман Н. Реальность массмедиа / Н. Луман. М. : Праксис, 2005. 256 с.

Макиндер Х. Круглая Земля и обретение мира / Х. Макиндер // Космополис. 2007. № 16. URL: http://www.intelros.ru/index.php?newsid=357.

Маккиндер Х. Демократические идеалы и реальность / Х. Макиндер // Полис. Полит. исследования. 2011. № 2. С. 134–144.

Маклюэн М. Война и мир в глобальной деревне / М. Маклюэн, К. Фиоре ; пер. с англ. М. : АСТ: Астрель, 2012. 219 с.

Маклюэн М. Понимание медиа: внешние расширения человека / М. Маклюэн. М. : Кучково поле, 2011. 464 с.

Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк. М. : Горячая линия-Телеком, 2004. 280 с.

Манн С. Теория хаоса и стратегическое мышление / С. Манн. URL: http://spkurdyumov.ru/what/mann/.

Манойло А. В. Государственная информационная политика в особых условиях : монография / А. В. Манойло. М. : Изд-во МИФИ, 2003. 388 с.

Манойло А. В. Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта / А. В. Манойло // Информационные технологии и безопасность : материалы V Международ. науч.-практ. конф. Киев. 2005. Вып. 8. С. 73–80.

Манойло А. В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. 3-е изд. М. : Горячая линия-Телеком, 2012. 542 с.

Мартин У. Дж. Информационное общество : реферат / У. Дж. Мартин // Теория и практика общественно-научной информации : ежеквартальник / гл. ред. В. А. Виноградов. М. : ИНИОН РАН, 1990. № 3. С. 115–123.

Матвейчев О. Уши машут ослом: сумма политтехнологий / О. Матвейчев. М. : Алгоритм, 2011. 640 с.

Мониторинг информационного общества и цифровой экономики : материалы по проекту // Высшая школа экономики: Мониторинговые исследования. URL: https://issek.hse.ru/info_society.

Медийно-информационная грамотность в России: дорога в будущее // Медиа- и информационная грамотность в информационном обществе : сб. материалов Всерос. науч.-практ. конф. (Москва, 24–27 апреля 2013 г.) / сост. Е. И. Кузьмин, И. В. Жилавская, Д. Д. Игнатова ; под ред. И. В. Жилавской. М. : МЦБС, 2014. 232 с.

Мелюхин И. С. Информационное общество и баланс интересов государства и личности / И. С. Мелюхин. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/23d97560ce093100c32575bc002dfc6c.

Мелюхин И. С. 21 век: информация и общество / И. С. Мелюхин. М. : Изд-во МГУ, 1999. 208 с.

Мешкова Т. А. Безопасность в условиях глобальной информатизации: новые вызовы и новые возможности : автореф. дис. … канд. полит. наук / Т. А. Мешкова. М., 2003. 26 с.

Моисеева О. А. Россия в глобальном информационном пространстве : учеб.-метод. комплекс дисциплины / О. А. Моисеева. М.: МГУТУ им. К. Г. Разумовского, 2013. 126 с.

Мороз О. Феномен hate speech / О. Мороз. URL: https://postnauka.ru/video/68876

Мясников А. А. Синергетические эффекты в современной экономике: введение в проблематику / А. А. Мясников. М. : ЛЕНАНД, 2010. 160 с.

Назачук А. В. Этика глобализирующегося общества : учеб. пособие / А. В. Назачук. URL: https://studfiles.net/preview/593669/ (дата обращения: 05.07.2018).

Негодяев И. А. На пути к информационному обществу / И. А. Негодяев. URL: https://studfiles.net/preview/593864/.

Новиков В. К. Информационное оружие — оружие современных и будущих войн / В. К. Новиков. 2-е изд., испр. М. : Горячая линия-Телеком, 2013. 264 с.

Новоселов А. Технологическая сингулярность как ближайшее будущее человечества / А. Новоселов. URL: http://transhuman.ru/biblioteka/tekhnologicheskaya-singul.

Нордстрем К. Бизнес в стиле фанк. Капитал пляшет под дудку таланта / К. Нордстрем, И. Риддерстрале. СПб., 2002. URL: http://vitalik.info/pictures/photo/4484.pdf.

О'Рейлли Т. Что такое Веб 2.0 / Т. О'Рейлли // Компьютерра. 11 октября 2005 г.

Об утверждении Концепции открытости федеральных органов исполнительной власти : Распоряжение Правительства Российской Федерации от 30 января 2014 года № 93-р. URL: http://docs.cntd.ru/document/499073612.

Об утверждении Программы «Цифровая экономика Российской Федерации» : Распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

Овчинский В. Кибервойны XXI века: О чем умолчал Эдвард Сноуден / В. Овчинский, Е. Ларина. М. : Книж. мир, 2014. 352 с.

Окинавская Хартия глобального информационного общества // Офиц. сайт МИД Японии. URL: http://www.kremlin.ru/supplement/3170.

Орлов С. Роль социальных сетей в организации протестных выступлений населения в ходе «арабской весны» / С. Орлов // Зарубеж. военное обозрение. 2014. № 12. С. 51–54.

Орлова В. В. Глобальные телесети новостей на информационном рынке / В. В. Орлова. М. : Изд-во «РИП-холдинг», 2003. URL: http://zavantag.com/docs/427/index-2016694.html.

Паршин С. Взгляды научного комитета МО США на классификацию угроз в киберпространстве : в 2-х ч. Ч. 1 / С. Паршин // Зарубеж. воен. обозрение. 2017. № 5. С. 12–17.

Паршин С. Взгляды научного комитета МО США на классификацию угроз в киберпространстве : в 2-х ч. Ч. 2 / С. Паршин // Зарубеж. воен. обозрение. 2017. № 6. С. 29–34.

Паршин С. А. Кибервойны — реальная угроза национальной безопасности? / С. А. Паршин, Ю. К. Горбачев, Ю. А. Кожанов. М. : КРАСАНД, 2011. 96 с.

Паршуткин А. В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем / А. В. Паршуткин. URL: https://cyberleninka.ru/article/n/kontseptualnaya-model-vzaimodeystviya-konfliktuyuschih-informatsionnyh-i-telekommunikatsionnyh-sistem.

Переслегин С. Общество и эволюция информационной сети / С. Переслегин. URL: http://www.igstab.ru/materials/black/Per_ScNet.htm.

Переслегин С. Опасная бритва Оккама / С. Переслегин. М. : АСТ: Астрель ; СПб. : Terra Fantastica, 2011. 664 с.

Петров Р. В. Реонизм. Как информационные технологии делают репутацию сильнее власти, а открытость — безопаснее приватности / Р. В. Петров, И. А. Сименко. Одесса: ВМВ, 2012. 255 с.

Поппер К. Р. Открытое общество и его враги / К. Р. Поппер. URL: https://e-libra.ru/read/179137-otkrytoe-obschestvo-i-ego-vragi.html.

Почепцов Г. Г. Информационные войны / Г. Г. Почепцов. М. : Релф-бук, К. : Ваклер, 2000.

Почепцов Г. Г. Информационные войны: Основы военно-коммуникативных исследований / Г. Г. Почепцов. URL: http://www.ligis.ru/library_2/049/02.html.

Почепцов Г. Г. Информационные войны: тенденции и пути развития / Г. Г. Почепцов. URL: https://psyfactor.org/psyops/infowar7.htm.

Почепцов Г. Г. Теория коммуникации / Г. Г. Почепцов. URL: https://studfiles.net/preview/2142041/

Пронина Л. А. Информационная культура как фактор развития информационного общества / Л. А. Пронина. URL: http://analiculturolog.ru/journal/archive/item/531-article_13–2.html.

Прохватилов В. В. Против математиков (К вопросу о кризисе оснований в отечественной теории информационных противоборств) / В. В. Прохватилов // Информ. войны. 2013. № 2. URL: http://pstmprint.ru/wp-content/uploads/2016/12/INFW-2–2013–12.pdf.

Пушкин А. С. Борис Годунов / А. С. Пушкин. Драматические произведения. Проза. М. : Просвещение, 1984. 351 с.

Развитие информационного общества в России : сб. ст., докладов и материалов : в 2-х т. / под ред. Н. В. Борисова, Ю. Е. Хохлова. СПб. : Изд-во С.-Петерб. ун-та, 2001.

Разумов Е. А. Политика КНР по обеспечению кибербезопасности / Е. А. Разумов. URL: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti.

Ракитов А. И. Постинформационное общество / А. И. Ракитов // Философ. науки. 2016. № 12. С. 7–19.

Ракитов А. И. Цивилизация, культура, технология и рынок / А. И. Ракитов // Вопр. философии. 1992. № 5. С. 3–15.

Ракитов А. И. Россия в глобальном информационном процессе и региональная информационная политика / А. И. Ракитов // Проблемы информатизации. М. : ИНИОН, 1993. Вып. 1–2. С. 20–26.

Раскин А. В. Некоторые философские аспекты информационной войны / А. В. Раскин // Информ. войны. 2015. № 3 (35). С. 18–21.

Расторгуев С. П. Информационная война / С. П. Расторгуев. М. : Радио и связь, 1999. 416 с.

Рашкофф Д. Медиавирус: Как поп-культура тайно воздействует на ваше сознание / Д. Рашкофф. URL: https://librolife.ru/g2003985.

Робертсон Д. С. Информационная революция: Наука, экономика, технология : реф. сб. / Д. С. Робертсон ; отв. ред. А. И. Ракитов. М. : ИНИОН РАН, 1993. С. 17–26.

Роговский Е. А. Американская стратегия информационного преобладания / Е. А. Роговский // Россия и Америка в XXI веке. 2009. № 3. URL: http://www.rusus.ru/?act=archive&edition=18.

Рябенко В. Образование и информационное общество / В. Рябенко. URL: http://magref.ru/obrazovanie-i-informatsionnoe-obshhestvo/.

Савчук В. Д. Медиареальность. Медиасубъект. Медиафилософия / В. Д. Савчук. URL: http://www.intelros.ru/pdf/mediafilosofia_2/31.pdf.

Скородумова О. Б. Отечественные подходы к интерпретации информационного общества: постиндустриалистская, синергетическая и постмодернистская парадигмы / О. Б. Скородумова // Знание. Понимание. Умение : информ. гум. портал. 2009. № 4. Культурология. URL: http://www.zpu-journal.ru/e-zpu/2009/4/Skorodumova/.

Слотердайк П. Критика цинического разума / П. Слотердайк. Екатеринбург : «У-Фактория» ; М. : АСТ, 2009. 800 с.

Смирнов А. В. Информационная глобализация и Россия. Вызовы и возможности / А. В. Смирнов. М. : Парад, 2005. 392 с.

Смирнов И. Противоборство в киберпространстве по взглядам военно-политического руководства ведущих зарубежных государств / И. Смирнов, Г. Алексеев // Зарубеж. воен. обозрение. 2017. № 6. С. 8–14.

Соловьев А. И. Политология: Политическая теория, политические технологии : учебник для студентов вузов / А. И. Соловьев. М. : Аспект Пресс, 2006. 559 с.

Соловьёв И. В. О Происхождении и содержании понятия «инфосфера». Инфосфера как объект исследования наук об информации / И. В. Соловьёв // Фундамент. исследования. 2013. № 6. С. 66–71.

Соловьёв Э. Г. Информационное общество / Э. Г. Соловьёв // Новая философская энциклопедия : в 4-х т. / предисл. В. С. Стёпина. 2-е изд. М. : Мысль, 2010.

Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики // Новая технократическая волна на Западе / Т. Стоуньер ; ред. П. С. Гуревич. М. : Прогресс, 1986. 453 с.

Стратегия развития информационного общества в Российской Федерации // Рос. газета. 16 февраля 2008 г. № 591(0). URL: http://rg.ru/gazeta/rg/2008/02/16.html.

Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года : утв. Распоряжением Правительства РФ от 01.11.2013 № 2036-р. URL: http://minsvyaz.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014–2020_2025.pdf.

Талеб Н. Н. Антихрупкость. Как извлечь выгоду из хаоса / Н. Н. Талеб. М. : ООО «Изд. Группа "Азбука Аттикус"», 2014. 768 с.

Талеб Н. Н. Черный лебедь. Под знаком непредсказуемости / Н. Н. Талеб ; пер. с англ. 2-е изд., доп. М. : КоЛибри, Азбука-Аттикус, 2012. 736 с.

Терин В. П. Государство — идеология — управленческие культуры и глобальная информатизация / В. П. Терин // Проблемы формирования государственных политик в России : материалы Всерос. науч. конф. Москва, 31 мая. М. : Научный эксперт, 2006. С. 204–215.

Ткаченко С. В. Информационная война против России / С. В. Ткаченко. СПб. : Питер, 2011. 224 с

Тоффлер Э. Метаморфозы власти: знание, богатство и сила на пороге XXI века / Э. Тоффлер. М. : ООО «Издательство АСТ», 2003. 669 с.

Тоффлер Э. Третья волна / Э. Тоффлер ; пер. с англ. М. : ООО «Издательство АСТ», 2009. 800 с.

Тоффлер Э. Шок будущего / Э. Тоффлер ; пер. с англ. М.: ООО «Издательство АСТ», 2002. 557 с.

Тоффлер Э. Война и антивойна / Э. Тоффлер, Х. Тоффлер. М. : АСТ, 2005. 416 с.

Тузовский И. Д. Светлое завтра? Антиутопия футурологии и футурология антиутопий / И. Д. Тузовский. Челябинск : Челяб. гос. акад. культуры и искусств, 2009. 312 с.

Тузовский И. Д. Утопия-XXI: глобальный проект «Информационное общество» / И. Д. Тузовский. Челябинск : Челяб. гос. акад. культуры и искусств, 2014. 392 с.

Тур Х. И. В поисках кибермира / Х. И. Тур // Постоянная группа по мониторингу информационной безопасности Всемирной федерации ученых. Январь 2011 года. URL: http://nauka.x-pdf.ru/17bezopasnost/507676–1-v-poiskah-kibermira-hamadun-ture-hamadoun-tour-generalniy-sekretar-mezhdunarodnogo-soyuza-elektrosvyazi-postoyannaya.php.

Ушаков А. Клод Шенон — создатель теории информации (к 100-летию со дня рождения) / А. Ушаков. URL: http://controlengrussia.com/retrospektiva/klod-shennon-sozdatel-teorii-informatsii-k-100-letiyu-so-dnya-rozhdeniya/.

Уэбстер Ф. Теории информационного общества / Ф. Уэбстер ; пер. с англ. М. В. Арапова и Н. В. Малыхиной ; под ред. д-ра филол. наук, проф. Е. Л. Вартановой. М. : АСПЕКТ ПРЕСС, 2004. 400 с.

Финько О. А. О развитии информационного пространства России / О. А. Финько // Информ. ресурсы России. 1998. № 1. С. 12–13.

Фролов Д. Б. Информационное противоборство: история и современное состояние / Д. Б. Фролов, Л. В. Воронцова. М. : Горячая линия — Телеком, 2004. 192 с.

Фролова Т. И. Гуманитарная повестка российских СМИ. Журналистика, человек, общество : монография / Т. И. Фролова. М. : МедиаМир, 2014. 352 с.

Фромм Э. Анатомия человеческой деструктивности / Э. Фромм. М. : АСТ ; Хранитель. 2018. 736 с.

Фукуяма Ф. Конец истории и последний человек / Ф. Фукуяма. М. : АСТ, 2005. 488 с.

Хабермас Ю. Демократия. Разум. Нравственность / Ю. Хабермас. М. : Академия, 1992. 256 с.

Хабермас Ю. Моральное сознание и коммуникативное действие / Ю. Хабермас ; пер. с нем. СПб. : Наука, 2001. 382 с.

Хан Е. Всемирный кризис доверия / Е. Хан. URL: https://cont.ws/@jeckhan/668132.

Хантингтон С. Столкновение цивилизаций / С. Хантингтон. М. : АСТ ; СПб. : Terra Fantastica, 2003. 603 с.

Харрис Ш. Кибервойн@: пятый театр военных действий / Ш. Харрис. М. : АНФ, 2016. 392 с.

Хаусхофер К. О геополитике. Работы разных лет / К. Хаусхофер. М. : Мысль, 2001. 426 с.

Ортега-и-Гассет Х. Восстание масс / Х. Ортега-и-Гассет. М. : АСТ, 2008. 352 с.

Цыганов В. В. Информационные войны в бизнесе и политике / В. В. Цыганов, С. Н. Бухарин. М. : Академ. проект, 2007. URL: https://studfiles.net/preview/2142006/.

Чалдини Р. Психология влияния / Р. Чалдини. 5-е изд. СПб. : Питер, 2012. 304 с.

Челышева И. В. Культурологический подход к проблеме медиареальности и медиакультуры / И. В. Челышева. URL: http://mic.org.ru/index.php/t-media/1-tm/27-chelysheva-1.

Черкасов В. В. Проблемы риска в управленческой деятельности / В. В. Черкасов. М. : «Рефл-бук» ; Киев : «Ваклер», 2002. 320 с.

Чернов А. Становление глобального информационного общества: проблемы и перспективы / А. Чернов. М. : Изд.-торг. корпорация «Дашков и К°», 2003. 232 с.

Шваб К. Четвертая промышленная революция / К. Шваб. М. : Эксмо, 2016. 138 с.

Шендрик А. И. Информационное общество и его культура: противоречия становления и развития / А. И. Шендрик // Знание. Понимание. Умение : информ. гум. портал. 2010. № 4. Культурология. URL: http://www.zpu-journal.ru/e-zpu/2010/4/Shendrik/.

Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. М. : Иностр. лит., 1963. 832 с.

Шестакова И. Г. Генезис средств коммуникации и трансформация социального тела / И. Г. Шестакова // Актуал. проблемы гум. и естеств. наук. 2013. № 2. С. 173–177.

Шкондин М. В. Информационный потенциал общества и концепты целостности медиасистемы / М. В. Шкондин // Вопр. теории и практики журналистики. 2015. Т. 4, № 4. С. 335–348.

Шпенглер О. Закат Европы. Образ и действительность / О. Шпенглер. Минск : Попури, 2009. 656 с.

Щедровицкий П. Революция уже произошла, мы просто этого не видим / П. Щедровицкий. URL: https://www.znak.com/2017–12–12/petr_che-

drovickiy_pochemu_rossiyskaya_ekonomika_i_obrazovanie_ne_uspevayut_za_ostalnym_mirom.

Яковлева Э. В. Современные информационные войны и политика. Обзор / Э. В. Яковлева // Молодой ученый. 2015. № 10. С. 1050–1053.

Ясперс К. Смысл и назначение истории / К. Ясперс. М. : Политиздат, 1991. 527 с.

Allard K. Co-operation, command and control / K. Allard // Co-operation, command and control in UN peace-keeping operations. A pilot study from the Swedish War College. Stockholm, 1996. P. 100.

Anderson Ch. Makers: The New Industrial Revolution / Ch. Anderson. N.Y. : Crown Business, 2012. 272 p.

Arquilla Jh. Cyberwar is Coming! / Jh. Arquilla, D. Ronfeldt. URL: https://www.rand.org/pubs/reprints/RP223.html.

Betz D. J. Cyberspace and the State: Towards a Strategy for Cyberpower (Adelphi series) / D. J. Betz, T. Stevens. London: Routledge, 2017. 162 p.

Calhoun J. B. Death Squared: The Explosive Growth and Demise of a Mouse Population / J. B. Calhoun. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1644264/pdf/procrsmed00338–0007.pdf.

Clarke R. A. Cyberwar. The Next Threat to National Security and What to Do About It / R. A. Clarke, R. K. Knake. Ecco, 2010. 290 p.

Cohen J. Deliberation and Democratic Legitimacy / J. Cohen // Hrsg. A. Hablin, B. Pettit. The Good Polity. Oxford, 1989. P. 17–34.

Collin B. The Future of Cyberterrorism: The Physical and Virtual Worlds Converge / B. Collin // Crime & Justice International Journal. 1997. Vol. 13. Is. 2. P. 15–18.

Connell M. Russia's Approach to Cyber Warfare / M. Connell, S. Vogler // CNA Corporation, March 2017. URL: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231–1Rev.pdf.

Deepak Sh. Integrated Network Electronic Warfare: China's New Concept of Information Warfare / Sh. Deepak. URL: https://idsa.in/system/files/jds_4_2_dsharma.pdf.

Department of Defense Strategy for operating in Cyberspace. July 2011. URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Dewey J. The Public and its Problems / J. Dewey. Chicago, 1954. 242 p.

Feakin T. Special Report — Enter the Cyber Dragon: Understanding Chinese intelligence agencies' cyber capabilities / T. Feakin. URL: https://www.aspi.org.

au/report/special-report-enter-cyber-dragon-understanding-chinese-intelligence-agencies-cyber.

Foerster H. von. Cybernetics of Cybernetics / H. von Foerster // Understanding Understanding: Essays on Cybernetics and Cognition. N. Y., 2003. P. 283–286.

Fritz J. How China will use cyber warfare to leapfrog inmilitary competitiveness / J. Fritz // Culture Mandala. The Bulletin of the Centre for East-West Cultural and Economic Studies. Vol. 8, № 1. P. 28–80.

Habermas J. Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats / J. Habermas. Frankfurt, 1998. 704 p.

Habermas J. Further Reflections on the Public Sphere / J. Habermas // ed. C. J. Calhoun. Habermas and the Public Sphere. Cambridge Mass. : MIT Press, 1992. P. 425–429.

Information Warfare and Information Operations (IW/IO). A Bibliography / compiled by G. E. Marlatt. Dudley Knox Library, Naval Postgraduate School, 2008. URL: http://edocs.nps.edu/npspubs/scholarly/biblio/Jan08-IWall_biblio.pdf.

Joint Vision 2000 — Joint Vision 2020. America's Military: Preparing for Tomorrow. Wash.: United States Department of Defense, 2000. URL: http://www.dtic.mil:80/jv2020/jvpub2.htm.

Libicki M. C. Conquest in Cyberspace: National Security and Information Warfare / M. C. Libicki. N. Y. : Cambridge University Press, 2007. 336 p.

Masuda Y. The Information Society as Postindustrial Society / Y. Masuda. Wash. : World Future Soc., 1983. 171 p.

Military Field Manual: Psychological Operations Techniques And Procedures. U. S. Government Printing Office, 1994. 315 c.

National Security Strategy 2015 — National Security Strategy. Wash. The White House. February 2015.

Technology, Policy, Law, and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities / eds. W. A. Owens, K. W. Dam, H. S. Lin // National Research Council: Computer Science and Telecommunications Board. 2009. URL: http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf.

Rippe K.-P. Ethikkommissionen in der deliberativen Demokratie / K.-P. Rippe // Hrsg. M. Kettner. Angewandte Ethik als Politikum. Frankfurt, Suhrkamp, 2000. 411 p.

Shannon C. E. A Mathematical Theory of Communication / C. E. Shannon // The Bell System Technical Journal. Vol. 27. P. 379–423, 623–656. July, October,

1948. URL: http://worrydream.com/refs/Shannon%20-%20A%20Mathematical%20Theory%20of%20Communication.pdf.

Stein G. H. Information Warfare / G. H. Stein // Airpower Journal. Spring 1995. P. 30–39.

Szafranski R. A. Theory of Information Warfare: Preparing for 2020 / R. A. Szafranski // World Air Power Journal. Spring 1995. Vol. 20. P. 56–65.

Thomas T. L. Chinese and American Network Warfare / T. L. Thomas. URL: https://library.uoregon.edu/ec/e-asia/read/netwar-1538.pdf.

Young T. The truth about post-truth politics / T. Young // The Spectator. 16 July 2016.

Wurman R. S. Information Anxiety / R. S. Wurman. N. Y., London : Doubleday, 1989. 356 p.

ОГЛАВЛЕНИЕ

Научное издание

Назаров Владимир Лазаревич
Жердев Денис Вадимович

«БОЛЬШАЯ ИГРА» v. 2.0:
Россия в глобальном информационном пространстве

Монография

Подписано в печать 21.12.2018. Формат 60×84 1/16.
Усл. печ. л. 17,44. Гарнитура Minion Pro.
Бумага офсетная. Тираж 60 экз. Заказ № 352.

Издательство Уральского университета
620000, Екатеринбург-83, ул. Тургенева, 4

Отпечатано в Издательско-полиграфическом центре УрФУ
620000, Екатеринбург-83, ул. Тургенева, 4
Тел.: +7 (343) 358-93-06, 350-90-13, 358-93-22, 350-58-20
Факс: +7 (343) 358-93-06
E-mail: press-urfu@mail.ru
http://print.urfu.ru

9 785799 624941

НАЗАРОВ ВЛАДИМИР ЛАЗАРЕВИЧ

Доктор педагогических наук, профессор кафедры организации работы с молодежью Института физической культуры, спорта и молодежной политики УрФУ, руководитель магистерской программы «Профилактика экстремизма в молодежной среде». Сфера научных интересов: профилактика экстремизма и противодействие идеологии терроризма в молодежной среде, геополитика, страноведение, Россия в глобальном информационном пространстве.

ЖЕРДЕВ ДЕНИС ВАДИМОВИЧ

Кандидат филологических наук, доцент кафедры филологического образования СУНЦ УрФУ. Сфера научных интересов: поэтика, герменевтика художественного текста, культурная антропология, творчество П. П. Бажова, информационное общество.