УДК 004.056

Биндас Дмитрий Валерьевич

соискатель кафедры философии
университет МГИМО
Россия, Москва
723266@qx.com

РАССМОТРЕНИЕ СОЦИАЛЬНОГО РЕГУЛИРОВАНИЯ И САМОКОНТРОЛЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕРЕЗ ПРИЗМУ ФИЛОСОФИИ

Аннотация

Современное развитие информационного пространства и параллельно с ним контроль и обеспечение безопасности стоит в приоритете у любого современного государственного аппарата. Однако, не все принимаемые меры способны работать должным образом и обеспечивать необходимую защиту общества. В данной статье мы рассмотрим влияние социального регулирования цифровой экосистемы с целью защиты информационного общества, а также постараемся ответить на ключевой вопрос безопасности существования духовных пользователей в бездуховном мире.

Ключевые слова:

Информационная безопасность, цифровое пространство, информационное противоборство, онлайн общество

Dmitriy V. Bindas

Competitor of the Department of Philosophy
MGIMO University
Russia, Moscow

CONSIDERATION OF SOCIAL REGULATION AND SELF-CONTROL IN THE SPHERE OF INFORMATION SECURITY THROUGH THE PRISM OF PHILOSOPHY

Abstract

The modern development of the information space and, in parallel with it, control and security is a priority for any modern state apparatus. However, not all measures taken are able to work properly and provide the necessary protection to society. In this article, we will consider the impact of social regulation of the digital ecosystem in order to protect the information society, and also try to answer the key question of the security of the existence of spiritual users in a non-spiritual world.

Keywords:

Information Security, digital space, information confrontation, online society

Действие информационных технологий должно быть безопасным не только для государства, но еще для общества и человека. Поэтому в данном исследовании мы подробно рассмотрим участие информационного российского общества в формировании и защите пространства. Здесь необходимо важное уточнение, когда мы говорим о развитии информационного пространства и его защищенности в основном речь идет о международном уровне (и большинство научных трудов и колоссальная теоретическая база посвящена этим вопросам), а вот проблематики развития именно внутренне-региональной системы ИБ не уделяется никакого внимания. Но это было свойственно до 2022 года, хотя на наш взгляд с этого надо было начинать. Более того, материалов об общественных инициативах и других независимых участников, разбирающихся в вопросах по информационной безопасности практически нет. Поэтому перейдем от общего к частному.

Большой интерес представляет исследование Зиновьевой Е.С. о международной информационной безопасности. Она подробно рассматривает историческое становление и другие политические процессы, предпринятые Россией с 2000-х годов по выстраиванию

международных связей с Западными и Восточными странами в рамках глобальной системы МИБ. Опираясь на такие документы, как «Стратегия развития информационного общества, «Концепции внешней политики», «Стратегию национальной безопасности», «Доктрину информационной безопасности России», программу «Информационное общество» и другие документы, Зиновьева подробно расписывает процесс становления информационного общества, важность Российского рынка ИКТ в мире, развитие отечественного сегмента Рунета, отмечает взаимную кооперацию с крупнейшими международными компаниями: IBM, Cisco, SAP, Alcatel, Microsoft, Oracle, Google, Nokia, Siemens и другими, а также приводит огромное количество мировых политических организаций с которыми сотрудничает Россия в рамках создания МИБ (ООН, ICANN, ЮНЕСКО, «Группа восьми», Совет Европы, СНГ, ОДКБ, ШОС, ОБСЕ, МЭС и др.) [1, с. 125-149]. В заключении автор приходит к следующему выводу, что Россия активно участвует и принимает важные инициативы в вопросах регулирования Интернета, однако этого недостаточно, необходима большая кооперация в этом вопросе. Также во многих других организациях и структурах, в качестве постоянного члена Россия не представлена, например, в ICANN, W3C, IETF, более того, России не передают функцию технической кооперации с Международным союзом электросвязи (специализированный орган ООН). Автор утверждает: «В настоящее время управление Интернетом в значительной степени находится под контролем США… Управление Интернетом в рамках межправительственного подхода в рамках МСЭ позволит защищать государственный суверенитет во Всемирной сети. Россия также выступает за необходимость контроля государствами собственного сегмента глобального информационного пространства и невмешательство во внутренние дела посредством использования ИКТ» [1, с. 156]. Елена Сергеевна подчеркивает и разнице подходов между США, России и Китаем. Если США стремится к частной модели регулирования, то Российская Федерация с Китаем за государственную. По утверждению Зиновьевой США очень долгий период оценивала возможности ИБ на террористических и преступных компонентах. Исходя из многих характеристик видно, что западные страны не заинтересованы в развитии системы МИБ. Несмотря на неактуальность многих вопросах в труде Е.С. Зиновьевой, автор выделили ключевые проблемы, которые актуальны в настоящее время. Ее книга, опубликованная в 2014 году, еще до событий присоединения Крыма в состав РФ, конфликта на Донбассе, введению санкций и исключению России из большинства европейских организаций, а также уход западных партнеров из России в 2022 году. А основополагающий документ ее работы – стратегия национальной безопасности на момент нашего исследования дважды

пересматривался. Мы не критикуем прекрасный труд Елены Сергеевны, мы просто хотим подчеркнуть, что все положения, касаемые вопросов МИБ, выстраиваемые с 2000-х годов, в 2022 перестали быть актуальными по политическим соображениям западных партнеров.

Мы косвенно затронули проблематику пересмотра стратегии национальной безопасности. Сама концепция была утверждена в 1997 году, в 2000 году она была принята [2]. В 2009 году была представлена первая стратегия до 2020 года, в 2015 она была пересмотрена, а в 2021 году она еще раз была доработана [4]. То есть, этап становления и реализации данной стратегии очень ранний. С другой стороны такой пересмотр крайне полезен, учитывая релевантность развития информационного пространства. Проанализировав, все три стратегии с 2009 по 2021 год, можно увидеть, насколько важность приоритетов цифровых технологий и защиты информационного пространства выросла и перешла на первостепенные направления в списке задач. Сложно давать предсказание столь ранней стратегии, однако результаты по реформированию информационного поля необходимы прямо сегодня.

Мы выяснили, что в современных реалиях формирование глобальной системы МИБ – невозможно. Поэтому создание локальной сеты – самое необходимое, что мы можем представить в действующих условиях. Откровенно говоря, те позиции, на которых настаивал Китай и Россия не были интересны. В очередной раз мы наблюдаем о формирование однополярного мира только в информационной среде, возвращаясь к геополитике, такие уже исторические моменты были в истории человечества. Зиновьева пишет, что не раз Евразия и Азия настаивали на исключение военных действий в интернет-пространстве. Но, Запад в очередной раз применил новый пакет санкций, который в корне отразился на сфере IT после начала проведения специальной военной операции на территории Украины. Эти деструктивные манипуляции в очередной раз возвращают нас к политической философии и размышлениям о том, почему западные страны стремятся применять рычаги влияния не только на конкурентов, но и на союзников. Философ В.В. Ильин в своей монографии подробно разбирает, противоречия взглядов между Западом и Востоком, а также отдельной роли России между двумя континентами – именно эти вопросы являются камнем преткновения в обеспечении информационной безопасности.

Ильин выделяет рад особенностей, свойственных для Востока, например, властность, волюнтарность, коллективность, гражданственность, исполнительность, традиционность, затратность и др. Для Запада – либеральность, правосообразность, индивидуальность, конфликтность, инициативность, модернизированность, эффективность и другие. Виктор

Васильевич, точно разделяет Восток и Запад, приводя контраргументы в виде цитирования Дефо, Монтескье, Вальтера и Кенэ. Ильин пишет: «Ключ к западному и восточному небу, – дивергенция античной общины с выделением индийского и греческого производительных укладов. На Востоке возникла властная корпоративность, на Западе – правовое собственничество. На Востоке утвердился подданный, на Западе – гражданин. Отмеченное предопределило складывание долгосрочных линий в социальном развитии, выработку специфических стандартов существования» [7, с. 60-63]. Все вышеописанное мы сегодня наблюдаем на внешнеполитической арене. Но как быть с Россией? Этот вопрос последние 20 лет стоит очень остро в вопросах самоидентичности, ответом на который будет частично считаться свой собственный путь. И действительно, в политике, в военных вопросах и даже в информационном медиа мире, мы выстраиваем свой абсолютно уникальный подход. Наверно, это все и является ответом, почему мы ведем борьбу с терроризмом и экстремизмом, реагируем на вызовы и угрозы, диктуемыми информационной войной, обеспечиваем информационную безопасность с русской оригинальностью, так часто критикуемой исключительно Западом [8, с. 46-51]. А аргументы в пользу того, что меры, принятые действующим политическим руководством, ведут к угнетению и притеснению собственного народа – выглядят абсурдными, просто из-за различности культурологических и национальных подходов. Пример, президент США – Джой Байден, за время своего президентского срока несколько раз называл президента В. В. Путина «убийцей», «тираном» и «военным преступником» [9]. В то время, как Россия никогда не позволяла себе такую риторику оскорблений. И Восточноазиатские страны тоже придерживаются подобной философии. Мы видим, что западные правительства очень резки и критичны в своих высказываниях. Тем не менее, коррупционные и другие скандалы в их регионе далеко не исключение. Кстати, тактика не реагирования на подобные провокации – тоже еще одна тема для обсуждения нашего собственного «пути» в вопросах ведения информационной войны.

Ответы официальных представителей политического руководства России всегда сдержаны и спокойные, в особенности, это касается провокаций и обвинений администрации западных партнёров. И тому подтверждение – примеры, когда на объективное обвинение Запада, Россия либо умалчивала, либо реагировала, не переходя на эмоции. Например, когда крупнейшие европейские и американские медиа (CNN, BBC и другие) чья авторитетность и доверие высоко ценилось сообществом журналистов всего мира. Начали запускать откровенную провокацию в 2008 году, представляю Россию агрессором напавшим на Грузию,

не раз обвиняли в применении жестокости по отношению к сирийской оппозиции с 2017 по 2019 года и бездоказательные обвинения в убийстве и насилии гражданского населения в Буче во время проведения специально военной операции на Украине в 2022 году. На все акты порицания Западом имеют агрессивный настрой и если обобщать, то в целом политика доминирования в информационном пространстве и проведении информационной войны по отношению к России довольно часто применяется. В это время Российская Федерация к подобным заявлением подходит с позиции не контраргументов, а с позиции защиты. Именно такая медиа политика внутри общественности и породила мнение о том, что мы проигрываем информационную войну. Но мы склонны считать, что это не перехват инициативы в медиа важен, скорее всего мы возвращаемся к той же теме собственного российского пути в исследовании цифрового мира.

Возвращаясь к труду В.В. Ильина, где он объясняет, почему мы не отвечаем на вбросы, вызовы и другие агрессивные выпады западных медиа. «В России жизнь ориентирована не на право, а на правду, не на формальные принципы, а на содержательные начала — ценности. Причем если на Западе вопросы ценностей вследствие атомарности сосредоточены в частной сфере, в России вследствие синкретичности – во властно-государственной» [7, с. 248]. Также автор убежден, что в России правит не закон, а воля, если возвращаться к западной культуре, то в их системе ценностей закон обеспечивает заведённый порядок вещей, у нас же, «не правовая договоренность (отсутствие регистрационной системы сказывается), а добрая воля» [7, с. 261]. Исходя из его теории, в информационном поле мы теряем инициативу, исключительно потому что нами движет добрая воля. Если Запад показывает кадры как они отправляют оружие на Украину (при этом утверждая, что необходимо мирное регулирование вопроса), то Россия показывает, как раздает гуманитарную помощь гражданскому населению, оказавшемуся в трагических условиях.

Все, вышеописанное показывает не только особенный подход России к формированию информационного пространства и обеспечения медиа безопасности, но подчеркивает социокультурные различия в том, почему из ранее так называемого информационного противоборства отношения переросли в уже фактическую информационную войну.

Теперь, переходим к частным случаям саморегулирования и контроля в новом образовавшемся цифровом медиа поле России. Учитывая важность обеспечения информационной безопасности российского общества, важно упомянуть отдельное

ведомство – Минцифры. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации было создано в 2018 году, в структуру организации входит большое количество департаментов. Один из них - департамент обеспечения кибербезопасности. В 2020 году была представлена справка, в которой осуждался перечень перспективных технологий и оценки федерального проекта «Информационная безопасность» и национальной программы «Цифровая экономика Российской Федерации». В ней, рассматривается вопросы искусственного интеллекта, виртуальная и дополнительная реальность, распределительный реестр Блокчейн, квантовые технологии, технологии Роботизированной Автоматизации процессов, Интернет вещей и Большие данные. В заключении, специалисты приводят аргументы о необходимости создания российской системы контроля больших баз данных. В исследовании дана аналитика подобных конкурентных систем, например – голландский комплекс Kesida или продукт AdaptiveDefense от Panda Security – который до недавнего времени был представителем на рынке ИТ в России, но после введения санкций со стороны США и Евросоюза, прекратил свою деятельность. Аналитические инструменты комплексов позволяют, базируясь на больших данных поводить цифровые расследования и выявлять нарушения в различных областях жизнедеятельности, а также успешно и эффективно используются большие данные и машинное обучение в инструментах безопасности [10]. Более свежих отчетов и справок о обеспечении безопасности ИТ сферы в России, на официальном сайте Минцифры не опубликовано. Безусловно, в России хватает своих собственных продуктов для обеспечения безопасности, ярким представителем которой, например является лаборатория Касперского. Но пока, совершить массово переход на исключительно отечественное сырье и программное обеспечение в такой короткий срок невозможно. Поэтому мы считаем, что участие государственных институтов важно и необходимо в обеспечении таких серьезных задачах как ИБ, но по непонятным причинам, ставку на информационное общество России в стратегиях, никто не делает. А на наш взгляд, это и является уязвимым местом любой стратегии безопасности.

В 2002 году Билл Гейтс пишет письмо своим пользователем, в котором говорит о новых взглядах политики Microsoft на вопросы обеспечения информационной безопасности. Он признает проблемы в экосистеме. Гейтс начинает с того, что ИБ держится на четырех столпах (безотказность, безопасность, конфиденциальность и бизнес-этика). Он перечисляет первые шаги, которые планирует реализовать компания (прописывание программного кода, быстрое восстановление системы, изменение инструментов SUS и

многое другое) [11]. В конце своего письма, он обращается к пользователям и просит их о помощи в виде обращений в клиентский сервис и обмен информации и отчетами об ошибках встроенных в Office XP и Windows. При этом, в 2022 году на официальном сайте компании было представлено исследование, в котором представлялись шаги по противодействию России в различных новостных и цифровых областях [12]. Следовательно, за двадцать лет Microsoft совершило скачок от формирования безопасности личного сервиса к откровенному противостоянию на мировом уровне.

В 2022 году американская аналитическая компания Гартнер представила доклад, в котором 88% членов совета директоров отнесли кибербезопасность к деловым рискам; только 12% назвали это технологическим риском. Тем не менее, опрос 2021 года показал, что ИТ-директор и директор по информационной безопасности (CISO) заявляли, что эквивалент ответственности за кибербезопасность составляет 85% из всех опрошенных организаций [13]. Разница между этими двумя письмами двадцать лет, и мы видим, что проблемы как были «головной болью» мирового информационного общества, так ей и остаются в 2022 году. Гартнер относит к деловым рискам 88% - касательно юридических лиц. Но реальные случаи незаконных операций в отношении физических лиц не просто имеют высокие показатели, но и в большинстве случаев остаются проблемой самих пользователей. Кибермошенничество, взломы приложений, хакерство и незаконное приобретение ПД – до настоящего времени остается актуальной проблемой незащищенности российского информационного общества. Торговля персональными данными и базой пользователей особенно распространена в России, так как на данный момент за это деяние - не предусмотрена ответственность. Безусловно факты и судебные прецеденты уже есть, но как правило они направлены исключительно на продавца, а не на покупателя. И случаев реального обращения в компетентные органы по данному вопросу достаточно мало [14]. Государство делает прекрасные вещи по защите цифрового и информационного общества, но на наш взгляд этого недостаточно, потому что акцент должен был сделать именно на пользователей с их участием в этом глобальном процессе. Как минимум, их помощь будет полезной в выявлении, написании в клиентский сервис отчетов и в тестах пилотных проектов по защите данных.

Возвращаясь к философским аспектам, почему проблема защиты и безопасности так важная для информационного общества. На новом этапе развития и становления информационного поля и сообществ внутри него, уверенность каждого пользователя в защите его данных обусловлена не только геополитическими и нравственными аспектами,

а проблемой бездуховности цифрового мира. С подсоединением к сети интернет, человек становится юзером, но при этом сохраняет все свои базисные функции (культурную идентичность и философское самосознание), которое и помогает ему отличать позитивные и негативные воздействия информационных средств, а также противодействовать манипуляциям с его сознанием [15, с. 149-150]. Именно безопасность и защищенность информационного общества поможет решить человечеству проблему поиска духовного в «бездуховном мире».

Список использованных источников

1. Зиновьева Е.С. Международная информационная безопасность: монография. / Е.С. Зиновьева. – М.: МГИМО-Университет. 2013. С. 125-149. – Текст: непосредственный

2. Указ Президента РФ от 17 декабря 1997 г. № 1300. «Об утверждении Концепции национальной безопасности Российской Федерации». – Текст: электронный // Президент России: официальный сайт. – URL: http://www.kremlin.ru/acts/bank/11782 (дата обращения: 04.05.2022)

3. Указ Президента РФ от 10 января 2000 г. № 24. «О Концепции национальной безопасности Российской Федерации». – Текст: электронный // Президент России: официальный сайт. – URL: http://www.kremlin.ru/acts/bank/14927 (дата обращения: 04.05.2022)

4. Указ Президента РФ от 12 мая 2009 г. № 537. «О Стратегии национальной безопасности Российской Федерации до 2020 года». – Текст: электронный // Президент России: официальный сайт. – URL: http://kremlin.ru/acts/bank/29277 (дата обращения: 04.05.2022)

5. Указ Президента РФ от 31 декабря 2015 г. № 683. «О Стратегии национальной безопасности Российской Федерации». – Текст: электронный // Президент России: официальный сайт. – URL: http://kremlin.ru/acts/bank/40391 (дата обращения: 04.05.2022)

6. Указ Президента РФ от 2 июля 2021 г. № 400. «О Стратегии национальной безопасности Российской Федерации». – Текст: электронный // Президент России: официальный сайт. – URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 04.05.2022)

7. Ильин В.В. Теория познания. Социальная эпистемология. Социология знания: монография. М.: Академический проект, 2014. С. 60-63. – Текст: непосредственный

8. Поляков В.П. Развитие информационной подготовки в контексте стратегии национальной безопасности Российской Федерации. // Наукоград наука производство общество.2016. – №2. – С. 46-51. – Текст: непосредственный

9. Шейхман М.М. «И такая дребедень каждый день. Байден взял за правило обзывать Путина». – Текст: электронный // Радио Sputnik. – URL: https://radiosputnik.ria.ru/20220318/bayden-1778881346.html (дата обращения: 05.05.2022)

10. Департамент обеспечения кибербезопасности Минцифры. Справка по вопросу определения перечня перспективных технологий для их инвестиционной поддержки и оценки информационной безопасности (федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»). – Текст: электронный // Департамент обеспечения кибербезопасности Минцифры. – URL: https://digital.gov.ru/uploaded/files/spravka-dlya-publikatsii-na-sajte.pdf (дата обращения: 05.05.2022)

11. Дергунова О.К. Стратегии корпорации Microsoft по автоматизации государственных служб. – Текст: электронный // Информационное общество. 2002. С.50 – 53. – URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/6405e081ec9d2fbfc3256d5700404cba (дата обращения: 05.05.2022)

12. Brad Smith. Defending Ukraine: Early Lessons from the Cyber War. – Текст: электронный // Microsoft On the Issues. Jun 22, 2022. – URL: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (дата обращения: 05.07.2022)

13. Gartner. What does cybersecurity mean for your business? – Текст: электронный // Gartner. – URL: https://www.gartner.com/en/topics/cybersecurity (дата обращения: 05.05.2022)

14. Грамматчиков А. «Бот выходит на охоту». – Текст: электронный // Журнал Эксперт. – URL: https://expert.ru/expert/2021/40/bot-vykhodit-na-okhotu/ (дата обращения: 05.05.2022)

15. Понарина Н.Н., Губанова М.А., Рудых С.А. Духовность человека информационного общества. // Вестник Армавирского государственного педагогического университета. 2021. №4. С.149-150. – Текст: непосредственный