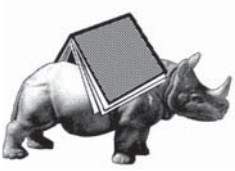

НЕНОВЫЙ ВЗГЛЯД НА НЕИЗВЕСТНОЕ

О.В. Демидов, М.Б. Касенова. Кибербезопасность и управление интернетом: документы и материалы для российских регуляторов и экспертов. — М.: Статут, 2014.

Рецензия — Александр Федоров

О безопасности в информационном обществе говорят уже более полувека, причем начали задолго до того, как даже наиболее развитые страны в полной мере[1] вступили в эту стадию развития. Однако до сих пор редкостью являются монографические издания, прямо относящиеся к этому вопросу.

Передо мною, человеком, полжизни посвятившим проблеме международной информационной безопасности (МИБ), математику по первому образованию, получившему на этом поприще дипломы и степени, и политологу по профессии, много лет занимающимся исследованием различных глобальных угроз и путей их предотвращения, лежит, вне всякого сомнения, нужная книга, претендующая на то, чтобы для таких, как я, стать настольной. И это в ней — главное.

БИБЛИОТЕКА

Рецензии пишут не тогда, когда хотят похвалить, да и серьезному автору это не нужно, разве что потешить самолюбие. Самая высокая похвала для исследователя — индекс цитируемости. Если на работу ссылаются, значит, она востребована, и автор не зря трудился. Многие ученые считают, что вершиной публикаций является справочник. В социальных науках это еще и сборник документов. И в этом смысле, невзирая на ту ложку дегтя, которую я пролью ниже, книга «Кибербезопасность и управление интернетом: документы и материалы для российских регуляторов и экспертов», подготовленная О. В. Демидовым и М. Б. Касеновой, представляет безусловную ценность.

Даже без учета авторской части читателю предоставляется возможность получить систематизированную подборку основных ныне действующих документов, определяющих нормативное поле, в котором работают исследователи, политики и все, кто так или иначе связан с регулированием отношений в сфере интернета и его применения.

Авторы проделали очень важную и непростую работу. Ограничение временного периода выпуска документов последними 5 годами, вероятно, оправданно. Предшествующие документы, хотя их и существенно меньше, носили бы для читателя скорее академическое значение, но значительно увеличили бы объем и без того не маленькой (464 с.) книги. Кроме того, ряд документов впервые публикуется на русском языке.

Следует приветствовать и нацеленность авторов-специалистов на сопровождение документов комментариями к состоянию и основным проблемам международного дискурса. Как показывает (в том числе и мой) опыт, большинство практиков, работающих в сфере компьютерной безопасности и использования интернета, не говоря уже о рядовых пользователях, строят свою позицию в вопросах информационной и кибербезопасности на базе публикаций СМИ. Причем последние

представляют собой либо статьи в прессе общей направленности (раньше такую называли *общественно-политические издания*), подготовленные журналистами, ни в коей мере не претендующими считаться специалистами в научно-технической составляющей предмета обсуждения, либо комментарии в сугубо специальных, в основном технического характера журналах, столь же далеких от политики, как первые от техники. Поэтому заложенная в книгу Демидова и Касеновой идея показать, как технико-программный феномен интернета отражается на политической ситуации (и не только отражается, но и в отдельных случаях определяет ее), безусловно, заслуживает всяческой поддержки.

Однако уже первая фраза предисловия повергла меня в глубокое уныние: «Интернет явился концентрированным отражением информационной революции конца XX — начала XXI в. Становится очевидным, что интернет интегрирует не только коммуникационные и технологические, но и материальные, финансовые, интеллектуальные, гуманитарные, политические и прочие ресурсы, формирует и диверсифицирует процессы социальной регуляции» (с. 3). Едва ли это мог написать математик (а интернет, являясь технико-программным комплексом, все-таки порождение математики[2], остальное в нем вторично или относится к электросвязи, что, по сути, автор и констатирует на с. 12, правда, с другой целью) или социолог, исследующий процессы социальных регуляций на указанных направлениях. Я уж не говорю об *информационной революции* — такие фразы в настоящее время едва ли простительны даже журналистам заводских многотиражек. Хотя, если интернет «интегрирует... политические... ресурсы» и «формирует... процессы социальной регуляции», то последующие две главы посвящены опровержению авторами самих себя. Но это, я думаю, просто досадная недоработка, на которую можно было бы не обращать внимания. Есть и более существенные и весьма спорные моменты.

Авторская часть книги, к сожалению, пронизана каким-то *религиозным* преклонением перед интернетом, что лишает авторов способности различать глобальную сеть как действительно яркое творение совокупной мысли математиков, физиков, химиков, связистов, инженеров, лингвистов и др. и использование этого творения обладателями «материальных, финансовых, интеллектуальных, гуманитарных, политических и прочих ресурсов» в том числе с целью «формирования и диверсификации процессов социальной регуляции». Такая апологетика интернета сродни поклонению электричеству первой половины XX в.[3]. Конечно, эта *болезнь* у составителей тоже пройдет, как прошла у их предшественников вера в чудодейственную силу электричества. Но пока она сильно мешает авторам и омрачает впечатление от первой части книги, которая, по замыслу, должна показывать читателю назначение и место в национальном и международном правовом поле приведенных во второй части документов. И если бы она была только одна. Собственно, именно это и побудило меня, говоря известным литературным штампом, взяться за перо.

Книга по сути представляет собой сборник документов. В данном случае — содержащий редкую, если не единственную и весьма актуальную с учетом даты выхода подборку материалов. Предваряющие сами материалы главы должны были бы нести объективные комментарии, вводящие неспециалиста в проблему, а специалисту объясняющие, почему сделана именно такая, а не иная выборка из всего множества официальных или неофициальных материалов. И если вторая глава в целом отвечает этой задаче, то назначение первой остается загадкой. Хотя не исключаю, что, по замыслу авторов, именно эта интрига и призвана стимулировать читателя обратиться к текстам как к первоисточникам.

Основная черта (можно сказать, квалифицирующий признак) правоведа — точность в терминологии и цитировании. Здесь мы наблюдаем полную свободу. Можно перепутать статьи 5 и 6 Североатлантического договора (с. 4), перевести словосочетание *Information and Telecommunication* и как *информационно-коммуникационные*, и как *информационные и коммуникационные*[4] (с. 11), забыв, кроме того, при этом, что приставка *теле-* имеет самостоятельное и немаловажное значение не только в романских, но и в современном русском языке. Но апофеозом

является понимание слова *технология*. Вероятно, авторы не вполне понимают, что это. Ограничусь лишь одним примером: на с. 12 книги автор говорит о «правовом регулировании технологий», забыв, вероятно, что право как важнейший элемент социальной сферы, по определению, регулирует отношения между субъектами или субъектами и вещами. Интересно технология в понимании автора — субъект или вещь, если вещь, то кто субъект?

К сожалению, такое отношение к терминам является качественной чертой данной работы и несказанно снижает впечатление от нее. Термины *кибербезопасность* и *информационная безопасность* во всех основных языках мира суть обозначение разных понятий, и они не могут восходить к одному греческому источнику *kyber-*. Обратимся, в частности, к электронному словарю Министерства обороны США, где последние 20 лет присутствуют как самостоятельные словарные статьи *cybersecurity* и *information security*[5]. Первая из них, как и полагается в современном английском языке, относится к компьютерным сетям и системам, а вторая — ко всей информационной сфере, включая ее психологическую составляющую (отсюда военные термины армии США *психологические операции* и *информационно-психологические операции* как вид *информационных операций*[6]) и техническую сферу обработки информации — информационные системы (необязательно компьютерные, но и они в том числе) и сети передачи данных. Так что кибербезопасность не синоним, а часть информационной безопасности, что полностью соответствует российскому подходу. В российской нормативной правовой лексике такой термин вообще отсутствует. Фактически насильственное насаждение в русскоязычные материалы этой синонимии действительно имеет отчасти политическую мотивацию, но в основном связано с недостатком знаний тех, кто это делает. Кстати, в документах ООН сначала в 1998 г. появился термин *информационная безопасность* и лишь год спустя, в 1999 г., *кибербезопасность*, причем в сочетании *культура кибербезопасности*, т. е. в другом контексте.

Весьма спорен, на мой взгляд, подход авторов к пониманию термина *информационное (кибер-) пространство*. Этот термин действительно пока сложен для понимания, по нему не удалось достичь договоренностей ни в научном, ни в политическом экспертных сообществах. Вместе с тем его важность трудно переоценить. Во всяком случае, нельзя говорить о понятиях *суверенитет*, *агрессия*, *границы*, *терроризм* и многих других, включая *преступление*, в информационном (кибер-) пространстве, если мы не знаем, что такое это пространство. Дискуссии в международном официальном и конференциальном формате ведутся, что называется, *при общем понимании...*

Конечно, это не первый случай в истории. Не определены до сих пор понятия *оружие*, *война*, *сила*, да и понятие *безопасность* также не имеет понятных и общепринятых нормативных определений. Вся наука строится на аксиоматиках, включающих исходные неопределяемые понятия. В математике это *точка*, *прямая* и ряд других. В политике, включая вопросы безопасности, также не удается определить все. Именно по этой причине некоторые исследователи (и я в этом готов с ними солидаризироваться) считают, что именно в области безопасности прошло время глобальных договоров — слишком многое в них надо определить. На их смену приходят так называемые *инициативы*, где государства объединяются вокруг идеи, понимая, что надо делать, но не пытаясь все это формально описать. На смену *участникам договор*а приходит *коллектив единомышленников*. Однако и здесь все не просто: идею и ее толкование определяет сильнейший, и совместная борьба, оказывается, ведется на его пользу. Примером может служить Инициатива по борьбе с распространением ОМУ (ИБОР).

Может быть, интуитивно (поскольку никаких прямых экивоков в этом направлении в тексте нет) ощущая сложность соотнесения вопросов информационной (кибер-) безопасности с договорным правом, авторы как бы оставили его *за скобками*. А жаль, это было бы интереснее и свежее, чем в очередной раз выступать в поддержку западного, надо признать, весьма прямолинейного и по этой причине

нередко выглядящего несерьезным подхода к применимости к информационной (кибер-) безопасности положений гуманитарного права.

Хочется верить, что авторы внимательно прочитали «Таллинское руководство». Однако видно, что это не было, говоря словами М. Горького, *чтение осмысленное и продуманное*, а — главное — авторы находятся в плену западного подхода. Безусловно, следует согласиться с приведенной на с. 62 оценкой, что «Таллинское руководство представляет собой… попытку заполнить международно-правовой вакуум в части поведения государств как непосредственных участников конфликтов в киберпространстве». Однако отнюдь не первую и едва ли серьезную. На эту тему проходило множество конференций, в том числе в том же НАТО, выпущено множество работ. Однако они не были так, говоря языком шоу-бизнеса, раскручены.

Мне сейчас не хотелось бы отвлекать внимание читателя на частности, но разве можно считать серьезными правила, определяющие суверенитет, юрисдикцию и территорию государств в ходе киберконфликтов, если сами понятия *суверенитет* и *территория* в киберпространстве не определены и то же НАТО против его определения, хотя при этом распространяет статью 5 Вашингтонского договора на кибернападения. А правило 17, предписывающее в ходе конфликта представлять отчеты о кибероперациях в СБ ООН. Кто и как реально себе это представляет? Я уже не говорю о правилах, посвященных комбатантам, военнопленным, журналистам, священникам и пр.

В целом в отношении положений, касающихся международного права, у авторов наблюдаются явный крен к позитивной оценке западных инициатив и необоснованное принижение действий России на переговорном треке. Упрощенно такую позицию можно было свести к схеме: все, что делают США хорошо, потому что это делают США, а все, что делает Россия, плохо, потому что это делает Россия, исключением является только то, что Россия делает совместно с США.

С этих позиций нетрудно понять осуждение авторами всего, что Россия делает в интересах установления международной информационной безопасности, даже самого термина *международная информационная безопасность*. И, напротив, явное непонимание того, почему российские официальные эксперты и чиновники до сих пор никак не могут понять, что все, что предлагают США, НАТО и их партнеры разумно и просто ждет принятия.

И якобы российский бизнес тоже в недоумении. Однако известный российский предприниматель и специалист в области IT-технологий генеральный директор компании *Ашманов и партнеры* Игорь Ашманов думает по-другому. Фактически в ответ на этот вопрос он в своем интервью интернет-изданию *D-Russia* 25 декабря 2013 года, когда рассматриваемая книга еще писалась, заявил: «Превратить информационное пространство страны [России. — **А. Ф.**] в черное пятно для АНБ — это государственная задача»[7]. Не надо противопоставлять государство и бизнес. Разумный бизнес заинтересован в сильном государстве, способном выполнять делегированные ему обществом, включающим бизнес-сообщество, функции, в первую очередь обеспечение безопасности. Так думают не только в России. В Америке давно уже крылатой стала фраза: «Сила Силиконовой долины основана на мощи армии США».

Вопрос вызывает и реализуемый в книге подход к проблеме управления интернетом. Авторы явно отталкиваются от традиционной пространственной модели. Они упорно используют термин *трансграничное управление*, то ли забыв о своей позиции глобальности и безграничности интернета и признавая возможность установления в нем каких-либо границ, то ли перенося в интернет-пространство географические границы государств, то ли что-то третье. В условиях неопределенности самого предмета рассмотрения — управления — такой подход подрывает и другого священного *кита* авторов — мультистейкхолдеризм.

В контексте рассматриваемой книги эта модель управления интернетом тоже лишена предмета. Вряд ли несколько миллиардов пользователей могут решать вопрос по типу новгородского вече или собрания граждан в греческих полисах. В древних Афинах такой способ управления назывался демагогия. Выработанные в то время и унаследовавшие это название приемы и сейчас широко используются в политике и рекламе.

Еще вопрос. А *отдельный заинтересованный пользователь* (также входящий в круг *стейкхолдеров*) — это кто: человек, компьютер, а может быть, просто идентификатор, которых у каждого человека, регулярно использующего интернет, десяток? А может быть, это программа, которая формирует нужную кому-то репрезентативную статистическую выборку? Такие примеры формирования *общественного мнения* уже есть, и такие программы известны. И это только первый вопрос, открывающий лишь самый верхний слой проблем. Дальше идут более сложные слои: бизнес, научное сообщество, государство, гражданское общество.

Однако для авторов книги, вероятно, все это ясно. Было бы очень интересно, если бы они сумели это объяснить читателям. А ведь те, прочитав приведенный на с. 81 пример «участия в управлении интернетом» такого стейкхолдера, как АНБ США, могут усомниться в оптимальности подобной модели. Понятно, в любом сообществе равных есть более и менее равные. Не ясно только, почему авторы вслед за *более равными* так упорно и бездоказательно рекламируют мультистейкхолдеризм. Кстати, американцы не скрывают своего подхода и, говоря о передаче полномочий ICANN и IANA другим структурам, заверяют, что дадут на это согласие, только в том случае, если те будут устраивать Вашингтон.

Исходя из материалов книги, можно подумать, что проблема, которой она посвящена, появилась не ранее как в последние 5–7 лет. Это далеко не так. Хотелось бы порекомендовать интересующимся читателям самостоятельно исправить пробел и посмотреть более раннюю библиографию на эту тему. Кроме политологических работ, появившихся еще в середине XX в. (см. сноску в начале статьи), с начала 1990-х гг. было множество предметных публикаций в США, а с середины 1990-х и в России. Параллельно шло множество конференций и круглых столов, материалы которых публиковались. В мае 1996 г. в Мидранде (ЮАР) прошла Международная конференция по глобальному информационному сообществу, в которой участвовали представители более 60 стран. В 1998 г. стартовал переговорный процесс в рамках ООН. Ситуация того времени нашла отражение в большой коллективной монографии[8], изданной тем же ПИР-Центром еще в 2001 г.

Это были лишь отдельные мысли, возникшие у меня при чтении книги. Я не ставил перед собой задачу разбирать текст и заставлять читателя судить, кто прав, а кто нет. Мой вывод достаточно тривиален: книгу надо читать, а с документами работать. И большое спасибо авторам за то, что они выдвинули очень интересную идею и реализовали ее. Не ошибается, как известно, только тот, кто ничего не делает. И каждый вправе высказывать свое мнение, даже если оно удивительно похоже на ранее высказанное сильными мира сего.

Примечания

[1] Т. Рона еще в 1976 г. опубликовал книгу *Weapons System and Information War*. В той или иной степени вопросов безопасности в информационном обществе касались работы 70–80-х годов прошлого столетия Д. Белла, А. Гидденса, М. Либики, Л. Хиршхорна, Д. Нейсбита, И. Масуды и др. Некоторые, в том числе российские эксперты, считают, что все вопросы сетевой безопасности решены в работах С. Шеннона еще в начале 1960-х гг.

[2] Ревнителей *computer science* я попрошу не волноваться — я ни в коей мере не собираюсь умалять их права и заслуги, хотя пока никто мне не сумел объяснить, в чем состоят собственные предмет и метод этой *науки* и на какой теории, отличной от математических, она построена. Как известно, именно уникальность этой триады определяет науку как самостоятельную ветвь *древа познания.*

[3] В одной из студенческих песен 1930–1950-х гг. пелось: «Нам электричество сделать все сумеет. Нам электричество и вспашет, и посеет. Нам электричество любой заменит труд. Нажал на кнопку — чик-чирик — все будет тут как тут». Да и тогда это воспринималось как социальная сатира.

[4] Ссылка на употребление здесь не корректна — употребление не есть перевод, если автор-юрист пишет переводится, значит речь идет о переводе, а не об «употреблении в значении…».

[5] U. S. DOD. Dictionary of Military Terms.

[6] На этот счет есть целый ряд доступных посредством того же интернета документов Комитета начальников штабов армии США и военных наставлений родов войск, например, Joint Doctrine for Information Operations. Joint Pub. 3–13. W.: Joint Chiefs of Staff, 1998 или Joint Information Operations: Planning Handbook. AF InfoDiv, 2001. Кроме того, этим вопросам посвящено много статей, в частности, в журналах *Военная мысль* и *Международная жизнь*, да и в том же *Индексе Безопасности (Ядерном Контроле)*.

[7] Игорь Ашманов: «Превратить внутреннее пространство страны в черное пятно для АНБ — да, это государственная задача». 2013, 25 декабря, http://d-russia.ru/igor-ashmanov-prevratit-vnutrennee-prostranstvo-strany-v-chernoe-pyatno-dlya-anb-da-eto-gosudarstvennaya-zadacha.html (последнее посещение — 5 ноября 2014 г.).

[8] Информационные вызовы национальной и международной безопасности/И. Ю. Алексеева и др. Под общей редакцией А. В. Федорова и В. Н. Цыгичко. М.: ПИР-Центр, 2001. 328 с.