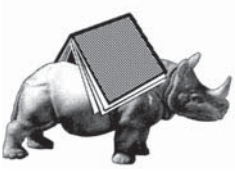

ОБ ИКТ, НЕ РАСТЕКАЯСЬ МЫСЛЬЮ ПО ДРЕВУ, — ПРОБЛЕМЫ, ЦЕЛИ И, ГЛАВНОЕ, РЕКОМЕНДАЦИИ

Олег Демидов. Глобальное управление Интернетом и безопасность в сфере использования ИКТ. Ключевые вызовы для мирового сообщества. М.: ПИР-Пресс, Альпина Паблишер. 2016. 198 с.

Рецензия — Елена Волчинская

Олег Демидов, работая в ПИР-Центре, более пяти лет занимается вопросами глобальной безопасности в сфере использования информационно-коммуникационных технологий (ИКТ). Он известен как информированный эксперт и думающий человек. Поэтому выход этой книги представляет безусловный интерес для всех, кто понимает, какие глобальные преимущества и, одновременно, какие глобальные вызовы национальной и международной безопасности несет применение ИКТ.

Книга отличается сжатым содержательным текстом, информативность обеспечивается привлечением большого количества разнообразных источников, а анализ тенденций и проблем в сфере использования ИКТ сопровождается выводами и предложениями. Книга написана очень хорошим, богатым русским языком, который нынче, к сожалению, в дефиците не только в публицистике, но и в научной литературе.

Структура монографии позволяет автору обратить внимание читателя на важные аспекты повестки дня — рассмотрение ИКТ в качестве критического фактора глобального развития. К ним относятся прежде всего вопросы безопасности в развитии и применении ИКТ, угрозы бесперебойному функционированию объектов критической информационной инфраструктуры и стратегии реагирования на эти угрозы, правовые и политические проблемы глобального управления интернетом, а также защита права на частную жизнь в Сети.

Каждый из восьми разделов книги построен по единой схеме: на основе анализа ситуации постулируются основные проблемы и формулируются цели и рекомендации. Эта жесткая конструкция не позволяет автору *растекаться мыслью по древу*, дисциплинирует повествование и является, по моему мнению, одним из достоинств монографии. Другое достоинство — редкая для такого издания актуальность привлекаемого материала. Наконец в качестве главного достоинства я бы определила авторские рекомендации (предложения). Они представляют интерес даже в том случае, если читатель с ними не соглашается. Остановлюсь на некоторых из них.

В разделе I «ИКТ — критический фактор глобального развития» автор справедливо, на мой взгляд, указывает на необходимость формирования на государственном уровне режима максимального благоприятствования для ИКТ-сектора.

В последнем обращении к Федеральному Собранию Президент России Владимир Путин впервые поставил задачу «запустить масштабную системную программу развития экономики нового технологического поколения, так называемой *цифровой экономики*[1]». При реализации этой программы приоритет будет отдаваться российским компаниям, а также научным, исследовательским и инжиниринговым центрам страны. Подобная постановка вопроса вселяет надежды. Однако многое будет зависеть от способа реализации амбициозных задач. К сожалению, необходимо признать, что институциональные механизмы формирования и реализации государственной политики в области развития и применения ИКТ недостаточно эффективны. В связи с этим содержащиеся в книге предложения о необходимости создания межведомственной координационной площадки для диалога между многочисленными регуляторами сферы ИКТ представляются целесообразными.

Анализируя проблемы выработки единых подходов к обеспечению безопасности при использовании ИКТ, автор обращает внимание на принципиальные разногласия в терминологии, имея в виду различия в содержании понятий *кибербезопасность* (используется в документах США, стран Европы, ряда стран Азии, НАТО, ОБСЕ, ОЭСР и др.) и *информационная безопасность* (используют Россия, СНГ, ШОС, ОДКБ). Автор понимает, что проблема разных подходов только внешне выглядит терминологической, на деле же она глубже, системнее. Автор книги предлагает, в частности, в целях ухода от терминологического конфликта применять нейтральный термин *обеспечение безопасности при использовании ИКТ*, который используется группой правительственных экспертов ООН в резолюциях Генеральной Ассамблеи ООН. Вместе с тем автор высоко оценивает опыт работы экспертного сообщества под эгидой Совета Федерации над проектом стратегии кибербезопасности Российской Федерации. Этот документ так и остался в статусе проекта, он не был поддержан органами государственной власти и частью экспертов. Но терминологические разногласия не были единственной и, тем более, определяющей проблемой. Например, я в своем отзыве на проект стратегии обращала внимание на недостаточную конкретизацию круга проблем, на решение которых направлен проект, на внутренние противоречия при формулировании направлений обеспечения кибербезопасности, а также на недостаточно продуманные принципы стратегии и механизмы координации деятельности по ее реализации. Наконец, в проекте не была обоснована целесообразность разработки стратегии кибербезопасности — нового доктринального документа, который был задуман как самостоятельный документ наряду с уже имеющимися. Полаю, что опыт создания стратегии подобного уровня был интересен и полезен для участников процесса, однако, к сожалению, для большинства из них этот опыт был первым, а он редко бывает удачным.

Представляется, что в процессе формирования и реализации государственной политики в сфере ИКТ необходимо обеспечить баланс интересов как минимум трех групп субъектов: государства, производителей ИКТ и связанных услуг, а также пользователей технологий. Так, принцип баланса интересов был провозглашен еще на Тунисском этапе Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО). Принцип замечательный, но его реализация оказалась сложной задачей. Рассуждая о том, как этот принцип может быть реализован, Олег Демидов задается вопросом: «Нужен ли сообществу российских интернет-пользователей собственный представитель, наделенный полномочиями

и имеющий доступ к публичным каналам выражения мнений?» (с. 29). Создание поста советника Президента России по вопросам развития интернета и назначение на этот пост Германа Клименко рассматривается как необходимый, но недостаточный шаг. С этой позицией я соглашусь, поскольку в существующих реалиях советник не имеет полномочий — по крайней мере он сильно проигрывает в статусе аналогичной фигуре в администрации президента США. Однако далее Олег Демидов, отвечая на свой вопрос, предлагает в качестве «условного прототипа» коллективного представителя российское общественно-политическое объединение «Пиратская партия». По моему мнению, эта организация не ставит перед собой задачу достижения баланса интересов или поиска компромисса. На мой взгляд, вопрос обеспечения баланса интересов даже не заключается в выборе конкретного ответственного субъекта, который бы представлял интересы интернет-сообщества. Убеждена, что внимание стоит сконцентрировать на выстраивании процесса принятия решений, в рамках которого: а) появится возможность представлять различные интересы; б) будут существовать механизмы их отстаивания; в) представители разных субъектов смогут участвовать в выработке проектов решений. Последний пункт представляется актуальным, поскольку в настоящее время большинство таких решений принимается кулуарно в органах власти, а экспертные советы Минкомсвязи России практически не работают. Кроме того, информация о готовящихся решениях иногда появляется слишком поздно, тексты проектов на портале regulation.gov.ru[2] размещаются в неактуальной редакции, а стадия разработки законопроектов зачастую указывается неверно. В таких условиях о балансе интересов говорить не приходится.

Подробно освещаемые в книге вопросы кибербезопасности объектов критической информационной инфраструктуры (КИИ) получили в настоящее время особую актуальность в связи с внесением в Государственную Думу 6 декабря 2016 г. пакета законопроектов, разработанных и направленных на обеспечение безопасности КИИ России. В базовом законопроекте под КИИ Российской Федерации понимается совокупность объектов КИИ, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой. Таким образом, российская терминология относит телекоммуникационные системы, сети и системы связи к КИИ, так же как и в других странах. В связи с этим к значимым объектам КИИ предъявляются повышенные требования по обеспечению их безопасности.

Автор делает акцент на вопросах международного взаимодействия в сфере обеспечения безопасности КИИ, справедливо полагая, что выработка базовых механизмов обмена информацией об угрозах безопасности объектов КИИ, а также формирование общей системы классификации таких объектов будут способствовать повышению эффективности их систем безопасности. Достижение результатов в этой сфере отвечает интересам всего мирового сообщества, потому что эффект техногенных катастроф, вызванных атаками на системы управления объектами КИИ, выходит за рамки границ одного государства.

Конечно, автор не мог обойти вниманием вопросы использования ИКТ в военно-политических целях. Обсуждение подобных угроз ведется достаточно давно, а в настоящее время можно наблюдать, как они стали воплощаться в реальность. Тем не менее говорить о существовании компьютерных войн преждевременно, поскольку, как верно указывает Олег Демидов, «использование ИКТ в военно-обо-

ронительных целях не охвачено какой-либо системой международных договоров, конвенций или иных соглашений» (с. 100). Это означает, что любая квалификация компьютерных инцидентов как военных конфликтов уязвима с точки зрения международного права. Конечно, отсутствие признанных классификаций зачастую не останавливает акторов от использования подобных определений. Недавний пример: администрация США обвинила российских хакеров в проигрыше Демократической партии на выборах президента Соединенных Штатов.

Несмотря на альтернативные подходы к развитию норм международного права, в конечном итоге все акторы заинтересованы в том, чтобы был принят юридически обязательный международный документ, направленный на запрет и предотвращение использования ИКТ в военно-политических целях. Однако автор книги считает, что принятие такого международного акта вряд ли возможно, пока не решены вопросы атрибуции, т. е. пока не выработаны критерии для квалификации использования ИКТ в качестве средства вооруженного нападения в определении статьи 52 Устава ООН. Олег Демидов предлагает *тактику малых шагов*, позволяющую максимально адаптировать существующие основополагающие нормы международного права, включая Устав ООН, нормы международного гуманитарного права и права вооруженных конфликтов для использования этих положений в разрешении вопросов военного использования ИКТ. Не отрицая целесообразность такой деятельности, я все же не соглашусь с тем, что подобных усилий будет достаточно. Занимаясь вопросами правового регулирования сферы ИКТ, я нередко убеждалась в том, что привычные нормы права дают сбой и не работают в виртуальной реальности. Это касается как национального законодательства, так и международного права. По этой причине создание новых норм международного *компьютерного права* наряду с возможным развитием и адаптацией норм международного гуманитарного права не только полезно, но и необходимо.

Два раздела книги посвящены проблемам глобального управления Интернетом. Автор подробно анализирует функции основных технических организаций глобального интернет-сообщества, так или иначе участвующих в управлении Интернетом, а также трансформацию подходов к его управлению за последние 10–15 лет. При этом в качестве одной из тенденций рассматривается нарастающее присутствие государства в Сети. В России эта тенденция очевидна — доказательством тому служит обнародованный в 2014 г. проект Минкомсвязи России, который предусматривает, по словам российского интернет-омбудсмена Дмитрия Мариничева, возможность отключения Рунета от глобальной сети при определенных условиях. «Речь идет не о каких-либо блокировках и ограничении доступа к интернет-ресурсам, а о выработке плана действий в экстренных случаях»[3], — сообщил представитель Минкомсвязи России, комментируя появившуюся в СМИ информацию. Несмотря на отсутствие признанных определений международных компьютерных преступлений, как указывает Олег Демидов, мы действительно являемся свидетелями использования ИКТ в военно-политических целях, в целях экономического шпионажа и иных противоправных целях, и это неизбежно стимулирует страны к разработке защитных мер на государственном уровне.

Тема защиты персональных данных в Сети и, шире, защиты права на тайну частной жизни в течение 10 лет после принятия Федерального закона «О персональных данных» не покидает повестку дня в России. Автор анализирует, как изменилось понимание этой проблемы после разоблачений Эдварда Сноудена 2013 г. и утвержда-

ет, что международно-политический итог этих разоблачений «не сводим к удару по авторитету США, он фундаментальнее, поскольку позволил констатировать, что «ИКТ и Интернет являются инструментом систематического одностороннего контроля государства над обществом и внешними контрагентами» (с. 167). Действительно, потенциальные возможности для подобного контроля со стороны государства при помощи использования ИКТ существуют, но, по моему мнению, не все государства озабочены таким контролем, и он не является всеобъемлющим, поскольку для государства его реализация трудноосуществима и затратна. Тем не менее задача создания механизмов защиты права на тайну частной жизни, безусловно, востребована, и автор предлагает несколько направлений действий для мирового сообщества, в частности распространение на программно-аппаратное обеспечение подобной слежки механизмов Вассенаарских договоренностей по экспортному контролю за обычными вооружениями и товарами и технологиями двойного применения.

Как уже было указано выше, монография изобилует предложениями, и многие из них могут быть учтены как при формировании российской стратегии в отношении применения ИКТ или при модернизации Стратегии развития информационного общества в России, так и в рамках развития международно-правовых институтов. Однако можно с уверенностью сказать, что свое отношение к указанным рекомендациям читателю следует формировать только после прочтения этой интересной книги.

Примечания

1 Послание Президента Федеральному Собранию, 1 декабря 2016 г. http://kremlin.ru/events/president/news/53379 (последнее посещение — 22 января 2017 г.).

2 Официальный сайт для размещения информации о подготовке федеральными органами исполнительной власти проектов нормативных правовых актов и результатах их общественного обсуждения.

3 Минкомсвязь: рунет не планируется отключать от глобальной сети. Ведомости. 2014, 19 сентября. http://www.vedomosti.ru/technology/news/2014/09/19/minkomsvyaz-runet-ne-planiruetsya-otklyuchat-ot-globalnoj (последнее посещение — 23 января 2017 г.).