УДК 32.327.83

БЕЗОПАСНОСТЬ И РИСКИ ПОЛИТИЧЕСКОЙ ДЕФРАГМЕНТАЦИИ КИБЕРПРОСТРАНСТВА

Леви Дмитрий Андреевич, кандидат политических наук, доцент кафедры «Европейских Исследований»
Санкт-Петербургский государственный университет
(191060, Россия, Санкт-Петербург, ул. Смольного 1/3 8 подъезд, e-mail: d.levi@spbu.ru)

Аннотация. Понятие информационной безопасности сегодня, в период информационных столкновений, как никогда воспринимается неоднозначно. Очевидно, что за последние годы содержание термина видоизменилось, а применение его существенно расширилось, заняв в первую очередь сферу электронной коммуникации, цифровых СМИ и киберпространства в целом. Для политологической оценки перспектив развития информационной безопасности в цифровой среде целесообразно разработать подходы к выделению элементов, из которых можно было «сложить» современное звучание понятия с одной стороны и оценить перспективы шагов, которые предпринимаются мировым сообществом по развитию данного явления. Вместе с тем как раз вопросы перспективы развития киберпространства и обеспечения его безопасности находятся в центре внимания статьи. Автор анализирует Парижский призыв Э.Макрона ноября 2018 года, оценивает его в контексте взглядов США, стран НАТО, России и Китая, а так же с точки зрения бизнес элит и корпораций. Не последнее место в исследовании уделяется особенностям переговоров по данным вопросам, проводимым в рамках ООН. Угроза дефрагментации связной системы интернета сегодня как никогда высока, в связи с чем автор приходит к выводу о том, что неожиданную роль медиатора - посредника между государствами и обществами могут сыграть корпорации, чьи финансовые интересы давно связаны с реализацией развития цифровой экономики.

Ключевые слова: кибербезопасность, информационная безопасность, управление безопасностью, кибер-пространство, управление интернетом, регулирование сети, дефрагментация интернета, CERT, криптовалюты, нетократия, ИКТ, Парижский призыв

CYBERSPACE SAFETY AND RISKS OF POLITICAL DEFRGAMENTATION

Levi Dmitri Andreevich, PhD in political science, associate professor of European Studies Chair
St.Petersburg State University
(191060, Russia, St.Petersburg, Smolny street 1/3, entrance 8, e-mail: d.levi@spbu.ru)

Abstract. Nowadays the concept of information security in the period of information collisions is perceived more ambiguously than ever before. Obviously, in recent years, the content of the term has changed, and its use has expanded significantly, taking first place in the field of electronic communication, digital media and cyberspace. New approaches should be developed for political assessment of the prospects for the evolution of information security in the digital environment. These approaches should seek to assist academic society to find new ways to deliver new meaning of information security and to assess future steps of the world community to develop this phenomenon. At the same time, the issues of the perspectives of cyberspace development and ensuring its security are at the center of attention of the article. The author analyzes the Paris appeal of E. Macron in November 2018, evaluates it in the context of the views of the United States, NATO countries, Russia and China, as well as from the point of view of business elites and corporations. Last but not least, the study focuses on the specifics of negotiations on these issues held within the UN. The threat of defragmentation of a coherent Internet system is now more than ever high, and therefore the author comes to the conclusion that corporations whose financial interests have long been associated with the realization of the development of the digital economy can play an unexpected role as a mediator - a mediator between states and societies.

Keywords: cybersecurity, information security, security management, cyberspace, Internet governance, network regulation, Internet defragmentation, CERT, cryptocurrency, netocracy, ICT, Paris Call

За последние десятилетия понятие государственной безопасности существенным образом изменилось. Из традиционного, т.н. «хардового» понятия, сочетающего в себе оценку рисков и угроз, связанных с традиционной деятельностью государств, понятие безопасности стало все больше включать в себя элементы «мягкой» безопасности, одной из составляющий которой является не менее неоднозначное понятие информационной безопасности. В различных исследованиях не раз предпринимались попытки разделить данное понятие на составляющие и предложить шкалы для измерения фактических угроз различным составляющим информационной безопасности, однако единого подхода, с которым согласилось бы большинство исследователей и практиков информационной безопасности выработано не было [например: 1, с. 34; 2, с.19; 3, с.41; 4, с. 45]. И дело не только в том, что прочтение информационной безопасности для государств с разным уровнем развития, с разным уровнем экономики различно. Ключевым для данного понятия является степень вовлеченности государств в международную информационную среду, киберпространства, а также отсутствие терминологического единства понятия информационной безопасности.

Очередной шаг на пути сближения подходов различных государств на международном уровне к данной проблеме в ноябре 2018 года предприняла Франция, когда на Всемирном форуме по вопросам управления интернетом президент Э.Макрон предложил общественности французский вариант декларации правил работы государственных и частных акторов в сети. «Парижский призыв к обеспечению доверия и безопасности в киберпространстве», - такое название получил документ, успешно включив в себя все необходимые ключевые слова, чтобы быть заметным на информационном поле, но содержательно, увы, остался декларативным политическим документом, отмечающим скорее политическую заявку Франции на более интенсивное участие в вопросах глобальной повестки дня, чем на предложение практического свойства. Идеологически документ предлагает развитие и сотрудничество по девяти ключевым направлениям, среди которых можно перечислить универсальные задачи по противодействию злонамеренным действиям в онлайн - пространстве, обеспечение доступности и целостности Интернета, защита прав интеллектуальной собственности, защита от распространения вредоносного программного обеспечения, рост и укрепление безопасности цифровой продукции услуг и прочее. Франция, разумеется, не могла пройти мимо актуальной повестки, поэтому «вишенкой на торте» стали положения, призывающие к сотрудничеству для избежа-

ние вмешательства в избирательные процессы, а также тезисы о необходимости защиты от кибер-наемничества и иных агрессивных действий со стороны различных акторов. Отдельные государства и многие международные компании в единодушном порыве одобрили данный документ, вместе с тем целый ряд государств отказались в нем участвовать. Является ли это участие или неучастие самостоятельным политическим заявлением или частью концептуальной логики, постепенно разрывающей кибер-пространство на несколько информационных блоков - один из ключевых вопросов, который определит развития интернета, цифровой коммуникации, политики и экономики на ближайшие годы.

Как было ранее отмечено, информационная безопасность, как термин, за последние годы оказался в заложниках сразу нескольких концептуальных направлений: технологического, общественно-информационного и политического. Технологический уровень представляется достаточно понятным и проработанным с точки зрения инструментариев международного сотрудничества и логики целеполагания. [5, с. 77-79] Действительно, с технологической точки зрения информационная безопасность представляет собой набор задач, связанных с ликвидацией угроз разрыва технической передачи данных и предотвращение угроз технической подмены информации или сообщений. В этой связи, ценности обеспечения информационной безопасности достаточно универсальны: трудно предположить компанию или государство, которое будет настаивать на целесообразности наличия уязвимостей, инструментов взлома, хищения или подмены данных. Сотрудничество по техническому направлению успешно сложилось за долго до прихода государства в посудную лавку ИКТ, в первую очередь за счет сотрудничества экспертных центров. Хотя можно по-разному относиться к системе относительно независимых центров по борьбе с инцидентами (CERT / CSERT), разветвленность данных лабораторий, активность их взаимодействия, формальная независимость (центры как правило существуют при независимых крупных ИТ компаниях или при лидирующих мировых Университетах), сделали возможным оперативный обмен данными о наличии угроз и де факто создали систему оперативного оповещения о наличии проблем, уязвимостей и очагах возникновения вирусных угроз. На базе данной системы успешно функционировали центры безопасности ведущих ИТ компаний, оперативно исправляя найденные уязвимости и обеспечивая информацией своих клиентов.

Технологический уровень борется с угрозами хакерских атак, хищениями, при этом составы данных угроз сравнительно легко квалифицируются национальным уголовным правом, что в целом обеспечивает достаточно быстрое взаимопонимание между экспертными центрами и местными управлениями спецслужб и полиции по противодействию преступлениям в кибер-пространстве.

Другие два уровня гораздо менее очевидны и нейтральны. Общественно-информационный уровень затрагивает вопросы распространения контента - т.е. информации в сети. Безопасность общественно-информационного уровня цифрового пространства - это не безопасность хранения и передачи «ноликов и единичек», это смысловая безопасность, связанная с наличием в информационном обществе конкурентных взглядов, альтернативных точек зрения, инструментов их продвижения и консолидации цифровой аудитории - цифрового нетократического коммьюнити - вокруг данных взглядов и тематических порталов/групп. Общественно-информационный уровень тесно связан с ценностями ядра общества, в зависимости от уровня раздражения и способности к толерантному отношению общественно-информационный уровень крайне уязвим к значительному количеству внешних раздражителей и остроте обсуждаемых тем. Появление новых религиозных взглядов, новые социальные раздражители, новая мода или молодежные маргинальные движения и флеш-мобы провоцируют ощущение угрозы на общественно-информационном уровне, заставляя национальный контент взрываться обсуждениями тех или иных явлений, искать «предателей», «отступников» или хотя бы «виноватых». Состояние «небезопасности» понимается как наличие любого агрессивного инакомыслия, как следствие этот уровень практически никогда не может быть оценен как спокойный или безопасный, кроме как в периоды экономического подъема и комфортного потребительского довольства.

Политический уровень во многом является производным от общественно-социального, но завязан на вопросы политики, политической конкуренции, политические ценности и, в последнее время особенно, оценку возможностей для развития иностранного влияния на национальные политические процессы. Понятие безопасности политического уровня очень сильно завязано на общественное восприятие собственной целостности и собственного единства. Политическая безопасность - это нередко не приходящее состояние, скорее состояние самооценки, связанное с манерой организации внутренней политической жизни, наличием или отсутствием внутренних противопоставлений «свой - чужой», «национальный - иностранный», «южный - северный» и т.п. Нередко на ощущении политической небезопасности паразитируют многие политические процессы, что приводит к симбиотическому непротивлению небезопасности. Близки по смыслу риски политической безопасности столкновению интересов государств, проводящих различные действия в рамках цифровой дипломатии. [6; 7, с.97]

Очевидно, для разных государств при комплексной оценке информационной безопасности различные элементы становятся более значимыми и менее значимыми. США, Китай и Россия - отдельные игроки, к позициям которых еще стоит вернуться, но если пройтись по по национальным стратегиям безопасности некоторых европейских государств, исследователь с удивлением обнаружит, что в своем большинстве они ориентированы на развитие технологического сотрудничества, где терминологическое противоречие - что хорошо, что плохо, с чем боремся - сведено к нулю.

Действительно, даже до появления координационной системы ENISA - Европейского Агентства по сетевой и информационной безопасности - в 2005 году координация в ЕС велась по линии CERT-центров. ENISA не заменила CERTы, но предложила систему информационных бюллетеней открытого свойства - публикацию Good practice guides (Инструкций по правильной организации) и работу по формированию единой проницаемой на территории ЕС правовой позиции по всем вопросам, связанным с компьютерными преступлениями. Даже бурное вниманием, уделяемое в последние годы цифровой безопасности со стороны НАТО, также не отменило сотрудничество по линии CERT. [4, с. 200-214] Последнее особенно тесно переплетается с вопросом развития и гармонизации стратегий кибербезопасности в странах-членах ЕС. Так, например, для Эстонии, где стратегия по кибербезопасности 2014-2017 года была недавно фактически заменена на проект создания сил киберзащиты в рамках Европейской программы постоянного структурного сотрудничества PESCO, в центре внимания находятся вопросы координации и безопасности инфраструктурных объектов и сетей. До 2008 года, правда, в стратегии кибербезопасности говорилось о гражданском характере рекомендуемых мер, в 2018 говорят уже о наличии инструментов почти силового контроля. Но во всех случаях основная масса документов копирует положения друг друга, оценивает риски безопасности информационных систем в первую очередь и лишь немного о разработке внешней политики в сфере кибербезопасности.

Финляндия и Словакия примерно на одном уровне воспринимают угрозы кибербезопасности, не отражая в основных документах политические и внешнеполитические риски. В основном кибербезопасность понимается с точки зрения технологических угроз и угроз для бизнеса, но не для государства и национальных ценностей. Национальное законодательство Чехии оценивает риски атак в цифровом мире как с точки зрения злонамеренных действий по совершению компьютерных преступлений, так и с точки зрения рисков прекращения свободного доступа к информационным сервисам в киберпространстве республики. Надо отметить, что кибер-стратегия Чехии достаточно эффективно вписана в систему национального права и не выглядит декларативным документом. Что нельзя сказать, например, о Франции, где национальное регулирование 2011 года сильно изменилось в части модернизации наборов слов и терминов. Последний кибер-ноябрь 2018 года с цепочкой выступлений и упомянутым выше документом, отличный пример работы Франции в этом направлении. Однако, если говорить содержательно, несмотря на упоминание информационных и политических рисков, в ключевых стратегиях прописаны исключительно опоры на технические средства защиты информации, целесообразность развития кибер-гигиены и необходимость горизонтального сотрудничества с другими государствами и экспертными центрами.

Одной из наиболее проработанной стратегий организации и осуществления безопасности в киберпространстве является набор стратегий Германии. Здесь сделан акцент на развитие по двум направлениям - первое связано с расследованием уголовных преступлений в цифровом мире. [8, с.128-131; 9, с.246] Второе - направлено на предоставление государством или около государственными сервисами (например на базе банков) базовых функциональных сервисов, способных предоставлять безопасность для проведения определенных действий. Причем понимается, что данные сервисы более защищены и проверены на предмет надежности, а значит и расследования инцидентов с ними представляется более простым и быстрым. [10] Например, модули авторизации пользователей, наподобие российских сервисов авторизации Госуслуги, аукционных сервисов Сбербанка, ВТБ и др.

Наконец, максимальной с точки зрения критичности общественно-информационной и политической составляющих в информационной безопасности, можно назвать национальную стратегию Великобритании, где еще с 2011 года говорилось о наличии в информационно-коммуникационном пространстве террористов, способных сделать киберпространство небезопасным для граждан и экономики.

Разночтения в восприятии кибербезопасности даже в Европейском Союзе, при наличии ENISA делают невозможным договориться о единой терминологии и даже на техническом уровне нередко создают проблемы для работы European Cypercrime Center EC3 - с 2013 года институциональной части Европола, института по борьбе с киберпреступлениями. В мировом масштабе ситуация усугубляется еще наличием двух проблем: разнородным восприятием ценностей свободной коммуникации и кризисом доверия.

Парижский призыв Макрона в какой-то степени стал иллюстрацией к текущему состоянию нарастания недоверия: появление пунктов о противодействию вмешательству в выборный процесс и призывы обеспечить защиту «опорной инфраструктуры интернета» как раз и говорят о недоверии государств друг другу. Вместе с тем Парижский призыв прозвучал как раз вовремя - в момент, когда официальные международные переговоры по линии ООН о будущем организации киберпространства оказались в тупике. Впервые с 2005 года участники Группы правительственных экспертов ООН зашли в тупик в ходе переговоров в рамках переговоров пятого созыва группы. Итогом работы стал абстрактно-декларативный документ, не содержащий даже графика продолжения работы и конкретных планов. По оценке некоторых обозревателей причиной тупика стало предложение регламентировать режим использования киберпространства в случае военных действий, США при поддержке ряда союзников предложили проект такого документа и связали его с текущими нормами гуманитарного права. Решительно против регламента выступила Россия и Китай, официально мотивируя это необходимостью защитить киберпространство от понятия военных действий. Неофициальная аргументация сводилась к тому, что при проведении военных действий ключевой актив киберресурсов - интернет-сайтов, социальных сетей и проч. находится в ведении компаний, находящихся под юрисдикцией США, а предоставление исключительных возможностей доступа к персональным данным пользователей для конкретного государства противоречит интересам других стран. Эта же логика лежит в основе разночтений в оценках конвенции Совета Европы по борьбе с киберпреступностью: Россия отказывается от участия в данном документе с 2001 года, опасаясь, что предоставление правоохранительным органам стран-участников права получать оперативную информацию с территории другой страны может быть лазейкой для кибершпионажа.

Выработала ли свой лимит возможностей группа переговорщиков, - как заявил Томас Боссерт советник президента США по внутренней безопасности или это временное отступление не очевидно, вместе с тем Макрон явно воспользовался паузой и рассудил так, что раз он не может претендовать на то, чтобы Франция оказалась в локомотивах цифровой экономики, то тогда хотя бы по аналогии с проектом Пьера Дюбуа, неплохо бы Франции оказаться в локомотивах регулирования этой дивной цифровой экономики следующего века. Но интрига состоит не в способности переписать основные пункты деклараций, а в разработке действующих механизмов их исполнения. И в этой связи неучастие Ирана, Китая, России в подписании документа с одной стороны, экстренное возобновление дискуссии в формате ООН - ясные сигналы Франции о том, что возглавить процесс просто так не получится.

9 ноября 2018 года Россия и США внесли два конкурирующих проекта резолюций по вопросу формата работы Группы: A/C.1/73/L.27* и A/C.1/73/L.37 соответственно. Россия предложила расширить формат группы, привлечь бизнес-элиты и увеличить географическое представительство стран. США настаивают на сохранении формата. Сложно прогнозировать, чья точка зрения возьмет верх, однако очевидно, что каждая из сторон не собирается дожидаться оппонентов и уже начинает работы в рамках двусторонних соглашений - США по линии НАТО, Австралии, Японии и Украины. В свою очередь Россия по линии БРИКС с Китаем, странами Латинской Америки, странами СНГ и рядом других союзников. Отсюда слышны периодические проекты резервных ДНС систем, предлагаемых к строительству в отдельно взятых государствах или блоках государств и требования по перемещению серверов различных сервисов, оперирующих персональными данными, на территорию стран.

США и Россия придерживаются решительно различных взглядов на инструмент защиты государственного суверенитета в кибер-пространстве и ключевыми направлениями расхождения взглядов являются необходимость международного или государственного регулирования не только технологического, но и общественно-информационного, а также политического уровня информации, необходимость формирования юридически обязательных инструментов, классифицирующих и ограничивающих применение технологий машинной обработки информации и цифровой коммуникации. Результирующей может стать рост интереса бизнеса к

регулированию вопросов развития ИКТ. Ведь для крупных компаний государственные инициативы сродни цунами, которое, как известно, «приходит неожиданной и из ниоткуда и рушит построенное за многие годы». Не случайно, что на Парижский призыв активно откликнулись представители многих международных компаний, включая Microsoft и российские Kaspersky Labs и Group IB. Учитывая прохладное отношение к инициативе Э.Макрона со стороны официального Кремля, участие российских компаний с одной стороны - намек на непонимание ценностей бизнеса со стороны российского государства, а с другой символ отчаянного стремления российских ИТ компаний не остаться за бортом международного рынка после череды скандалов.

Если на минуту представить возможность реализации сценариев США и России в отдельно взятых регионах мира, но следует допустить и реализацию третьего пути, своеобразного «движения неприсоединения». Корпоративный сегмент очень осторожно смотрит на инициативы государств в сфере регулирования интернета и вскоре может предложить и самостоятельный сценарий регулирования, связанный с использованием корпоративных доменных пространств, корпоративных криптовалют (с большой натяжкой - Riple). [11, с. 148-152] Учитывая экономический вес, например, Alibaba Group, недовольство государственными стратегиями ряда других южноазиатских компаний, все это может принести на стол обсуждения понимаемый всеми фактор доверия. Сегодня система доверия разрушена и поэтому страны пытаются из пока технологически единого киберпространства вынуть «свой кусок» регулирования, посадить за стол с большой красной кнопкой «своего человека». Но делается это не для фактического контроля за возможностью отключения технически значимых устройств, а для возможности цензуры общественно-информационного и политически значимого контента. Понимание этого объясняет тот факт, почему доверие подорвано между государствами, но по отношению к государствам со стороны населения. Корпоративный сегмент в этой связи может представляться менее ангажированным и тем более находящимся в условиях большой конкуренции. Получается, что корпоративный сектор в последнее время обладает ресурсом, который стремительно теряет государство: доверие и ценность «goodwill», которые де факто могут позволить корпорациям совершить блиц-криг в этой сфере и вплотную подойти к роли государства.

Подводя итог отметим, что текущее состояние обеспечения кибербезопасности, несмотря на глобальные дискуссии, находится на весьма достойном уровне. Технологический уровень развит сегодня, как никогда. Несмотря на частичное охлаждение в рамках международного сотрудничества, фактические возможности по наблюдению за совершаемыми киберпреступлениями лишь нарастают в т.ч. за счет средств автоматизации по противодействию киберпреступлениям, а также участию отдельных государств в разработке систем сертификации - инструментов-гарантов безопасности совершения сделок. Вместе с тем, на социально-информационном и политическом уровнях ощущение безопасности постепенно уменьшается в первую очередь за счет снижения уровня взаимного доверия. Это тревожный симптом, преодоление которого связано не столько с развитием кибепространства, сколько с развитием общества и необходимостью перестроения политического направления развития общества. Медиаторами такого рода развития неожиданно могут выступить мировые корпорации, заинтересованные в прекращении «дележки» интернета по частям, но обладающие собственными интересами. Корпорации, способные тягаться с государствами - в части экономических ресурсов, в части криптовалют, в части диктата политической воли в сферах занятости и технологий, а теперь еще и в сфере опосредованного регулирования международных стандартов ИКТ - это интересное направление развития, изученное разве что в фантастических фильмах о будущем планеты, где корпорации полностью вытеснили государство. Не рассуждая об этом всерьез, следует понимать, что и общественно-информационный и политический уровни восприятия безопасности - это информационно-зависимые уровни. Институт политического комментирования в виде черного ящика Д.Истона и на смену ему пришел ящик со светодиодной подсветкой поисковой системы, контролируемый корпорацией, способный не только осуществлять комментирование и агрегацию информации, но и осуществлять мягкую цензуру - пессимизировать поисковую выдачу контента.

СПИСОК ЛИТЕРАТУРЫ:

1. Zinatullin L., The Psychology of Information Security : Resolving Conflicts Between Security Compliance and Human Behaviour. Ely, Cambridgeshire : IT Governance Publishing. 2016

2. Vacca J., Cyber Security and IT Infrastructure Protection. Waltham, MA : Syngress. 2014

3. Dykstra J., Spafford E. The Case for Disappearing Cyber Security // Communications of the ACM. Jul2018, Vol. 61 Issue 7, p40-42.

4. Gori U. Modelling Cyber Security : Approaches, Methodology, Strategies. Amsterdam : IOS Press. 2009 (HATO - 213)

5. van der Walt E., Eloff J., Grobler, J. Cyber-security: Identity deception detection on social media platforms // Computers & Security Sept. 2018, vol.78, pp. 76-89.

6. Цветкова Н.А., Ярыгин Г.О. Публичная дипломатия ведущих государств: традиционные и цифровые методы. Санкт-Петербург, 2014

7. Леви Д.А., Интернет-мобилизуемая политическая активность и феномен цифровой дипломатии // Азимут научных исследований: экономика и управление. 2015. № 4 (13). С. 96-99.

8. Орлова В.В. Киберпреступления и основные виды интернет угроз // Общество и человек. 2015. № 1-2 (11). С. 128-132.

9. Гасанова В.С. Киберпреступления в международном праве: понятие, содержание и меры регулирования // Юридическая наука: история, современность, перспективы Сборник материалов VII международной научно-практической конференции, посвященной Дню российской науки. 2016. С. 244-248.

10. Трунцевский Ю.В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения // Российский следователь. 2014. № 21. С. 19-22.

11. Леви Д.А. Перспективы признания и развития криптовалют в Европейском Союзе и странах Европы // Управленческое консультирование. 2016. № 9 (93). С. 148-158.

Статья поступила в редакцию 08.11.2018
Статья принята к публикации 27.11.2018