СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
ЧЕТЫРНАДЦАТОГО МЕЖДУНАРОДНОГО ФОРУМА

«ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

7–9 ДЕКАБРЯ 2020 г.,
МОСКВА, РОССИЯ

УДК 334.021(082)
ББК 65.291я43
П18

АННОТАЦИЯ

В сборнике представлено большинство выступлений участников Четырнадцатого международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», проходившего в г. Москве в период с 7 по 9 декабря 2020 г[1].

Форум, организованный Национальной Ассоциацией международной информационной безопасности (далее -Ассоциация), был посвящен обсуждению приоритетных направлений экспертной проработки проблем сотрудничества государств в использовании ИКТ-среды и путей их решения для обеспечения международного мира и экономического процветания государств мира.

В рамках Форума состоялось пленарное заседание, посвященное обсуждению современных проблем обеспечения международного мира и поддержания устойчивого развития в глобальном информационном обществе. Кроме того, была организована работа пяти круглых столов, на которых эксперты обсудили следующие вопросы:

- международное право и меры доверия в ИКТ-среде: политические и правовые проблемы;
- международное право и меры доверия в ИКТ-среде: проблемы технического регулирования в ИКТ-среде;
- проблемы разрешения международных споров, обусловленных инцидентами в ИКТ-среде, мирными средствами;
- проблемы международного сотрудничества в целях безопасности бизнеса в ИКТ-среде;
- правовые механизмы противодействия использованию ИКТ-среды для вмешательства во внутренние дела суверенных государств, включая гуманитарное измерение.

Форум проходил в условиях возрастания риска возникновения масштабной конфронтации в цифровой сфере. Несмотря на огромные усилия, которые прилагает международное сообщество для предметного изучения проблем международной информационной безопасности (МИБ), напряжение в отношениях между государствами в области безопасности использования ИКТ не уменьшается. Обостряются и разногласия в подходах государств к определению приоритетов в противодействии угрозам МИБ.

В докладах участников Форума уделено существенное внимание обсуждению проблем налаживания государственно-частного партнерства при обеспечении безопасности объектов критической инфраструктуры, включая объекты кредитно-финансовой сферы, а также безопасности использования ИКТ-среды коммерческими компаниями. Отмечена важность обсуждения имеющихся в этой области проблем с участием представителей бизнеса, с использованием опыта обеспечения информационной безопасности, накопленного коммерческими организациями. Подтверждена актуальность расширения сотрудничества представителей международного экспертного сообщества в поиске средств противодействия угрозам использования ИКТ в военно-политических целях. Высказана заинтересованность в более широком обсуждении вопросов применения международного права к обеспечению свободы волеизъявления граждан в процессе национальных выборов. Была подчеркнута важность изучения путей парирования возможного негативного влияния использования ИКТ на сохранение цивилизационных ценностей общества, а также активизации разъяснения российских подходов к решению проблем обеспечения МИБ. Отмечена необходимость расширения деятельности высших учебных заведений страны по подготовке кадров в области международной информационной безопасности.

В работе Форума, проходившего в комбинированном формате – онлайн и оффлайн – приняли участие более 120 экспертов из 10 государств и ряда международных организаций.

Перевод докладов зарубежных участников на русский язык осуществлен сотрудниками Ассоциации А. Цветковой, К. Бойко и Е. Осечкиным.

ISBN 978-5-6044055-1-2

Оргкомитет Четырнадцатого международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

1 Ряд выступавших участников не представили тезисы своих выступлений

ПРИВЕТСТВИЕ ЗАМЕСТИТЕЛЯ МИНИСТРА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Организаторам, участникам и гостям XIV Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Уважаемый Владислав Петрович!

Сердечно приветствую организаторов, участников и гостей XIV Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»!

За годы своего существования Форум по праву зарекомендовал себя в качестве авторитетной международной площадки по обмену опытом в области международной информационной безопасности. Мероприятие отличает внушительный состав участников — экспертов в области международной информационной безопасности, представляющих российские органы государственной власти, научные и деловые круги, а также иностранных специалистов.

В условиях усиливающихся киберугроз, представляющих опасность перерастания в глобальную киберпандемию, важно продолжать активную деятельность по выработке адекватного и жизнеспособного механизма противодействия этим губительным вызовам.

Ярким свидетельством того, что российские подходы отвечают устремлениям международного сообщества по выстраиванию как национальной, так и глобальной системы информационной безопасности являются итоги голосования 9 ноября нынешнего года в Первом комитете 75-й сессии Генеральной ассамблеи ООН, где большинством голосов был принят российский проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Соавторами российской резолюции стали 27 стран.

Данный успех налагает на российскую дипломатию, важной составной частью которой являются современные научные школы, включая возглавляемую Вами Национальную Ассоциацию международной информационной безопасности, серьезную моральную ответственность за совместную выработку и реализацию концептуальных позиций по вопросам международной информационной безопасности.

Высоко оцениваем участие бизнеса, неправительственных организаций и научного сообщества в международной дискуссии по вопросам обеспечения безопасности в сфере использования ИКТ. Технологические наработки и интеллектуальный вклад этих институтов востребованы в контексте наращивания цифрового потенциала и создания мер реагирования.

Надеемся, что и в этом году эксперты внесут весомый практический вклад в международную дискуссию по тематике безопасности ИКТ-среды.

Желаю организаторам и участникам Форума плодотворной и успешной работы.

г. Москва, «2» декабря 2020 года

О. СЫРОМОЛОТОВ

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Ведущий:
Шерстюк В.П., Сопредседатель оргкомитета Форума, советник Секретаря Совета Безопасности Российской Федерации, Президент Национальной Ассоциации международной информационной безопасности

В.П. Шерстюк

Сопредседатель оргкомитета Форума, советник Секретаря Совета Безопасности Российской Федерации, Президент Национальной Ассоциации международной информационной безопасности

Уважаемые участники конференции!
Уважаемые гости!
Дамы и господа!

1. Позвольте мне открыть заседание очередного Четырнадцатого Международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Хотелось бы начать со слов искренней признательности всем участникам и гостям, которые несмотря на сложную эпидемиологическую ситуацию и разницу во времени смогли найти возможность и желание принять участие в обсуждении, на наш взгляд, наиболее сложных и интересных проблем формирования системы международной информационной безопасности. С учетом сложившейся обстановки мы проводим Форум в основном в новом формате – видеоконференции.

Мы благодарны нашим немецким партнерам за возможность ежегодно в течение 13 лет собираться в г. Гармиш-Партенкирхен для открытых, доброжелательных дискуссий по всем существующим в области использования ИКТ проблемам.

Объективные обстоятельства вынуждают нас изменить этой традиции. Наше заседание проходит в г. Москве, в здании Дипломатической академии МИД России – соучредителя нашей Ассоциации. В связи с этим хотелось бы поблагодарить руководителей Академии и, прежде всего, ректора – Чрезвычайного и Полномочного посла Российской Федерации Александра Владимировича Яковенко и сотрудников Академии, которые оказали огромную помощь в подготовке Форума.

Мы благодарны аппарату Совета Безопасности Российской Федерации, Заместителю Секретаря Совета Безопасности Российской Федерации Олегу Владимировичу Храмову за поддержку и помощь в подготовке Форума, а также руководителям всех федеральных органов исполнительной власти России, представители которых принимают участие в нашей работе.

Но не только это характеризует настоящий Форум. К большому сожалению, нельзя сказать, что за прошедший год мир изменился в лучшую сторону, что он стал более устойчивым, а отношения между государствами – более доверительными.

Несмотря на огромные усилия, напряжение в отношениях между государствами в области безопасности использования ИКТ не уменьшается. При этом международное сообщество обсуждает проблемы международной информационной безопасности на ежегодных сессиях Генеральной Ассамблеи ООН, на созданных для предметного изучения этих проблем площадках – Рабочей группы открытого состава, Группе правительственных экспертов, на региональных площадках, например, ОБСЕ и других, на многосторонних и двусторонних встречах руководителей государств и других официальных лиц. Более того, в официальном докладе Госдепартамента США ситуация в ИКТ-среде рассматривается как создающая условия для снижения порога применения вооруженной силы, включая ядерное оружие.

Как известно, Президент России Владимир Путин 25 сентября 2020 г. предложил властям США возобновить сотрудничество в сфере международной информационной безопасности, которое завязалось еще в 2013 году, но было заморожено из-за разногласий вокруг Украины и якобы имевшего место вмешательства России в выборы президента США в 2016 году. Данное предложение о перезагрузке отношений было отвергнуто, в т.ч. госсекретарем США М. Помпео. В ходе участия В. Путина на заседании Валдайского клуба 22 октября с.г. у президента спросили о возможном установлении перемирия в киберпространстве. Президент В. Путин ответил: «Я считаю, что не нужно выставлять какие-то предварительные условия для того, чтобы начать этот диалог. Нужно немедленно сесть и договариваться. Ну что здесь плохого? Мы ведь не предлагаем ничего плохого, что не соответствует интересам наших партнеров».

Вышеуказанное, естественно, влияет на тематику Форума. Равно как оказывает влияние и современная международная обстановка, отличительной характеристикой которой являются непрекращающиеся попытки некоторых стран мира использовать свои преимущества в экономическом развитии и превосходстве в вооруженной силе для:

- навязывания другим государствам представлений о должном международном порядке;
- разрушения международного права и его замены стандартами и правилами, удобными, прежде всего, некоторым западным государствам и отражающими их представления о добре и зле, как основании для применения силы в нарушение Устава ООН, в обход Совета Безопасности ООН.

Угрозы миру стали еще более опасными, в том числе и в области использования ИКТ.

Обостряются и разногласия в подходах государств к определению приоритетов в противодействии этим угрозам, к поиску взаимоприемлемых компромиссов, в частности, в работе Групп правительственных экспертов ООН по достижениям в области информатизации и коммуникаций в контексте международной безопасности, работавших в 2016–2017 и 2018–2019 гг., а также сессий Генеральной Ассамблеи ООН (2018 и 2019 гг.).

Проявляя единство в понимании необходимости применения международного права к регулированию отношений в ИКТ-среде, государства существенно расходятся в представлениях о путях решения этой задачи. Даже в вопросе о создании условий для практической реализации, рекомендованных Группой правительственных экспертов консенсусом в Докладе 2015 года, правил ответственного поведения государств в ИКТ-среде, не удается достичь согласования позиций.

Отсутствует общее видение подходов к разрешению противоречий в вопросе о методах и способах применения международного права в ИКТ-среде.

Все это позволяет сделать вывод, что мы по-прежнему далеки от цели, поставленной Генеральной Ассамблеей ООН и заключающейся в создании открытой, безопасной, стабильной, доступной и мирной среды информационно-коммуникационных технологий.

Как отметил 26 ноября 2020 г. на заседании коллегий министерств иностранных дел Российской Федерации и Белоруссии Министр иностранных дел Сергей Лавров: «В нашей повестке дня стоит вопрос международной информационной безопасности. <…> Очевидно, что без универсальных договоренностей мир рискует погрузиться в киберхаос, последствия которого могут оказаться катастрофическими».

Единственной позитивной подвижкой в области формирования системы международной информационной безопасности можно считать появление новой площадки для инклюзивного обсуждения данной проблематики – Рабочей группы открытого состава. Работа Группы безусловно будет способствовать не только учету мнений всех заинтересованных государств – членов ООН при обсуждении проблем создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, но и расширению возможности более активного подключения к данному процессу международного экспертного сообщества.

Полагаем, что Форум будет способствовать консолидации усилий экспертного сообщества на изучении проблем создания открытой, безопасной, стабильной, доступной и мирной среды информационно-коммуникационных технологий, а также на подготовке предложений по решению этих проблем.

Со своей стороны, организаторы Форума сделают все возможное для того, чтобы участники могли свободно и открыто обсуждать наиболее острые вопросы международного сотрудничества в области обеспечения национальной и международной безопасности.

2. Уважаемые коллеги!

Мы собрались на Форум, чтобы обсудить мнения экспертов различных государств по наиболее актуальным проблемам международной информационной безопасности:

- практическое применение правил ответственного поведения государств в ИКТ-среде;
- совершенствование нормативного регулирования отношений в ИКТ-среде;
- меры укрепления доверия между государствами в ИКТ-среде;
- сотрудничество в области предотвращения использования ИКТ способами, приводящими к нарушению международного мира и безопасности, предотвращения конфликтов, обусловленных инцидентами в ИКТ-среде;
- применение международного права к отношениям в ИКТ-среде как единственной возможности остановить сползание человечества к катастрофе, обусловленной злонамеренным или агрессивным использованием информационных и коммуникационных технологий.

Актуальность этих проблем подтверждается, в том числе, и содержанием дискуссий, проведенных в рамках Рабочей группы открытого состава ООН, и ходом обсуждения проекта итогового документа по результатам работы Рабочей группы.

Думаю, что в своих докладах участники **пленарного заседания** затронут вопросы:

- международного правового регулирования безопасности объектов критической информационной инфраструктуры, деятельность которых носит глобальный характер (система корневых серверов сети «Интернет», международные платежные системы, системы продажи авиабилетов и др.);
- дадут свою оценку существующим и потенциальным угрозам международной безопасности, способам противодействия этим угрозам на основе принципа суверенного равенства государств в информационном пространстве;
- поделятся видением подходов к сотрудничеству государств по вопросам предотвращения включения в ИКТ скрытых вредоносных функций, которые могут использоваться для подрыва безопасности и надежности использования ИКТ, противодействия вмешательству во внутренние дела других государств.

Наверняка будут затронуты и другие актуальные проблемы.

3. К числу таких проблем, безусловно, относится применение международного права в ИКТ-среде. Эти проблемы будут обсуждены на **Круглом столе № 1 «Международное право и меры доверия в ИКТ-среде: политические и правовые проблемы».**

Несмотря на то, что со времени одобрения докладов Групп правительственных экспертов 2013 и 2015 гг., в которых отмечалась применимость международного права к ИКТ-среде, прошло более пяти лет существенных изменений в области формирования общего понимания того, как именно нужно применять международное право для регулирования соответствующих международных отношений не произошло.

Международное право пока не стало инструментом, способным на основе международного сотрудничества, предотвращать использование ИКТ для нанесения ущерба правам и свободам человека и гражданина, законным интересам коммерческих и некоммерческих организаций в области информационной деятельности, а также деятельности государственных органов по обеспечению безопасности использования глобальной информационной инфраструктуры, которая является общественным благом глобального характера.

Ответ на вызов, с которым столкнулось человечество в области правового регулирования международных отношений в ИКТ-среде, на наш взгляд, должен базироваться на сотрудничестве всех государств мира в двух основных направлениях:

- приспособление принципов и норм международного права к ИКТ-среде;
- приспособление ИКТ-среды к применению принципов и норм международного права.

Технические и политические аспекты этой проблемы, надеюсь, будут более подробно обсуждены на круглых столах Форума.

Рад сообщить участникам Форума, что в 2020 году при активной поддержке Национальной Ассоциации международной информационной безопасности удалось обеспечить завершение проекта Международного исследовательского консорциума информационной безопасности. Начало проекту было положено в 2018 году в рамках работы XII заседания Форума в г. Гармиш-Партенкирхен (Германия). Его целью было изучение методических вопросов применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды на примере трех правил, регулирующих отношения в области безопасности объектов критической информационной инфраструктуры.

В реализации проекта приняли участие эксперты московского государственного университета имени М.В. Ломоносова (Российская Федерация), Института киберполитики (Эстония), Института «Восток-Запад» (США), Фонда «ИКТ для мира» (Швейцария). К нашему сожалению, по объективным причинам не удалось удержать в проекте Центр киберправа Университета Корe (Южная Корея). Отчет о результатах исследования Международного исследовательского консорциума информационной безопасности размещен на сайте нашей Ассоциации.

По мнению участников проекта, для ликвидации указанных пробелов в нормативном регулировании целесообразно направить добровольные усилия государств на:

- установление или закрепление структуры национальной информационной инфраструктуры (например, перечней объектов, входящих в национальную инфраструктуру);
- определение порядка проведения совместных расследований по признакам инцидентов в национальной ИКТ-среде, связанным с нарушением стабильности функционирования этой среды.
- уточнение содержания понятия «инцидент в ИКТ-среде»;
- развитие стандартов технического регулирования в области безопасности критической информационной инфраструктуры.

Участники проекта не смогли выработать согласованную позицию по вопросу о целесообразности развития норм и принципов международного права для его адаптации к ИКТ-среде как новому пространству международного сотрудничества. Эксперты организаций западных государств полагают прогрессивное развитие в этих целях международного права излишним, в то время как российские эксперты считают, что такое развитие международного права является реальным направлением снижения международной напряженности в ИКТ-среде.

В рамках дискуссий на этом Круглом столе предполагается обсудить вопросы: целесообразности создания универсальных стандартов отграничения зон ответственности государств в ИКТ-среде при применении правил ответственного поведения государств; природы и содержания суверенитета государств в ИКТ-среде; содержания международных обязательств государств в области использования ИКТ, вытекающих из норм и принципов международного права; юрисдикции государств над ИКТ-инфраструктурой, расположенной на их территории, а также содержания международного правового режима безопасности объектов критической информационной инфраструктуры.

4. Интересные дискуссии предстоят участникам **Круглого стола № 2 «Международное право и меры доверия в ИКТ-среде: проблемы технического регулирования в ИКТ-среде».** В рамках этого Стола будут обсуждены вопросы совершенствования международного сотрудничества в области использования технического регулирования для следующего:

- международное правовое закрепление границ зон ответственности государств в ИКТ-среде;
- закрепление границ объектов национальной критической информационной инфраструктуры;
- закрепление сведений о нарушении норм, принципов и прав ответственного поведения государств в ИКТ-среде;
- закрепление сведений, необходимых для атрибуции государств, затронутых инцидентом в ИКТ-среде.

Исходя из того, что ИКТ-среда является новым пространством сотрудничества и представляет собой совокупность технических средств автоматизации обработки и передачи информации, расположенную в различных национальных юрисдикциях, принципиально важным становится вопрос о совершенствовании системы технического регулирования.

Техническое регулирование могло бы охватить отношения, связанные со следующим:

- обеспечение достаточного уровня защищенности объектов ИКТ, находящихся в зоне ответственности тех или иных государств, например, объектов критической информационной инфраструктуры;
- обеспечение международной юридической значимости сведений об инцидентах в ИКТ-среде, добываемых национальными правоохранительными органами;
- поддержание международного правового режима границы зоны ответственности государств в ИКТ-среде;
- надежное закрепление в протоколах взаимодействия устройств ИКТ, признаков их принадлежности к зоне ответственности того или иного государства и другие.

Совершенствование системы технического регулирования в ИКТ-среде, на наш взгляд, способно создать определённый потенциал не только для разрешения опасных международных ситуаций, связанных с инцидентами в ИКТ-среде, но и содействовать налаживанию взаимовыгодного сотрудничества в области противодействия компьютерной преступности как внутри страны, так и в глобальном масштабе.

По мнению многих государств мира, вредоносный потенциал ИКТ, предназначенных для использования в рамках «силового» разрешения межгосударственных противоречий, продолжает увеличиваться. Еще недавно к числу таких ИКТ эксперты относили, прежде всего, использование специального программного и технического обеспечения для нарушения деятельности критически важных объектов информационной инфраструктуры и других объектов, оказывающих существенное влияние на жизнедеятельность общества, на реализацию военного потенциала государства.

Активно развиваются системы искусственного интеллекта, внедряемые в системы вооружения и военную технику. Развиваются способы и методы боевого применения автономных боевых роботов различного назначения. ИКТ широко применяются для повышения боевой эффективности средств ведения вооружённой борьбы. Увеличивается количество объектов инфраструктуры государства, поражение которых способно привести к возникновению межгосударственных конфликтов. К таким объектам теперь относят не только объекты военной инфраструктуры государства, но и целый ряд объектов экономической и социальной инфраструктур общества.

В вооруженных силах многих государств создаются специализированные структуры для управления использования ИКТ в ходе вооруженного противоборства, для информационного обеспечения систем управления войсками и оружием.

Тенденции создания в вооруженных силах государств структурных подразделений, ориентированных на использование ИКТ для ведения «силового» противоборства, особенно опасны в условиях, когда отсутствует опыт применения принципов и норм международного права для мирного разрешения международных споров по поводу инцидентов в ИКТ-среде.

Конкурентное развитие средств ведения «силовых» действий в ИКТ-среде, называемое обычно «гонкой вооружения», повышает риск возникновения конфликтов, обусловленных инцидентами в ИКТ-среде, при отсутствии правовых средств разрешения соответствующих международных споров. Такие инциденты могут иметь самые серьезные последствия для международного мира и безопасности.

По существу, в процессе развития ИКТ-среды человечество столкнулось с необходимостью применять международное право для регулирования отношений в принципиально новой среде существования, в которой пока не представляется возможным объективными способами зафиксировать как признаки нарушения международных обязательств, так и установить субъекты международного права, причастные к этим нарушениям.

Отсутствие механизмов обеспечения международного признания сведений о злонамеренном или враждебном использовании ИКТ государствами создает практически непреодолимые препятствия не только для регулирования международных споров в ИКТ-среде, но и определения субъектов этих споров.

Еще раз хочу отметить, что сложившаяся ситуация способствует возникновению у некоторых юристов и политиков иллюзии свободы «силовых» действий в ИКТ-среде.

Представляется, что этим путем нельзя достигнуть закреплённой в Уставе ООН цели – избавить грядущие поколения от бедствий войны.

Решение этих вопросов позволит придать юридическую надежность сведениям о международных инцидентах в ИКТ-среде и создать условия для применения правовых средств разрешения соответствующих опасных ситуаций.

5. Коллеги!

На наш взгляд, основным направлением поддержания международного мира и безопасности все-таки должно остаться международное право и, соответственно, – использование для разрешения спорных ситуаций средств, предусмотренных Уставом ООН. Именно эти вопросы будут в центре внимания участников **Круглого стола № 3 «Проблемы разрешения международных споров, обусловленных инцидентами в ИКТ-среде, мирными средствами».**

В настоящее время основным средством реагирования государств на инциденты в ИКТ-среде является введение на основе суверенитета односторонних санкций на государство, которое, по мнению пострадавшего субъекта международного права, виновно в возникновении данного инцидента. Предусмотренные Уставом ООН средства мирного разрешения споров, создающих угрозу международному миру и безопасности, практически не используются. Во многом сложившаяся ситуация обусловлена «виртуальностью» процесса применения информационно-коммуникационных технологий, наблюдение которого не представляется возможным.

Невозможно избавиться от ощущения, что это так понравилось некоторым государствам, что они уже начали переносить этот подход и на события, возникновение которых имеет определенную материальную основу. Примером могут служить инциденты в Солсбери, так называемое «отравление» Навального, и некоторые другие. Государства не считают нужным обременять себя предъявлением каких бы то ни было доказательств вины, но громогласно предъявляют публичные обвинения другим суверенным государствам, да еще требуют от них оправданий.

На наш взгляд, некоторыми государствами проводится системная кампания по слому системы международного права и замене его некими стандартами, типа Таллиннского руководства по информационным операциям или системе стандартов, разрабатываемых, по данным СМИ, экспертами США и некоторых стран Европы по практическому применению правил ответственного поведения государств в ИКТ-среде.

Характерной чертой этих работ является демонстративное приглашение к осуществлению проектов только экспертов из «одинаково думающих» государств, которые и будут продвигать предлагаемые стандарты. Остальные государства, видимо, должны просто присоединиться к уже подготовленным стандартам. В такой манере государства приглашаются к участию в Европейской (Будапештской) конвенции по киберпреступлениям (2001 г.).

6. В рамках **Круглого стола № 4 «Проблемы международного сотрудничества в целях безопасности бизнеса в ИКТ-среде»** будут обсуждаться вопросы взаимодействия организаций бизнес-сообщества, находящихся в различных юрисдикциях, в целях обеспечения информационной безопасности, а также вопросы взаимодействия с государством при обеспечении безопасности критической информационной инфраструктуры.

Одной из фундаментальных особенностей ИКТ-среды является то, что само ее существование является продуктом применения норм международного частного права. Применение таких норм позволяет создавать и развивать информационную инфраструктуру, обеспечить использование данной инфраструктуры для оказания информационных и коммуникационных услуг как единого, глобального, связанного технического пространства.

Использование таких возможностей создает потенциал развития бизнеса в условиях глобального информационного общества, цифровой трансформации всех сфер жизни общества, в том числе обеспечения прав и свобод человека и гражданина, экономики, политики, государственного управления, обеспечения обороноспособности страны.

В этих условиях является почти очевидной необходимость участия организаций бизнес-сообщества в решении задач обеспечения безопасности использования инфраструктуры. Такое сотрудничество называется частно-государственным партнерством. Дан-

ное партнерство, как правило, базируется на системе национальных нормативных правовых актов, которые регулируют отношения в области безопасности организаций бизнеса, критической информационной инфраструктуры, а также использования в этих целях потенциала центров реагирования на чрезвычайные ситуации в среде информационных и коммуникационных технологий.

По мнению многих экспертов, за последние годы опасность злонамеренного использования информационных технологий для нападения на критическую информационную инфраструктуру, осуществления других преступных деяний продолжает расти. В докладе Группы правительственных экспертов ООН 2013 года отмечалось, что «угрозы частным лицам, компаниям, национальной инфраструктуре и государственным органам приобретают все более острый характер, и соответствующие инциденты имеют все более тяжелые последствия». В 2015 году Группа правительственных экспертов ООН пришла к выводу, что «к числу наиболее пагубных нападений с использованием информационных и коммуникационных технологий относятся нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств. Опасность вредоносных нападений с использованием информационных и коммуникационных технологий на критически важную инфраструктуру является реальной и серьезной».

Взаимодействие государства с организациями бизнес-сообщества, с собственниками соответствующих объектов критической информационной инфраструктуры сможет обеспечить безопасность использования ИКТ в финансовой области, экономике, социальной жизни, управлении государством.

7. Все более острой становится и ситуация в области использования ИКТ для вмешательства во внутренние дела суверенных государств. При этом складывается парадоксальная ситуация. Например, США бездоказательно обвиняя Российскую Федерации во вмешательстве в выборы в 2016 г., не делали большой тайны из того, что практически открыто вмешивались в выборы Президента Российской Федерации в 2018 г., в голосование по поправкам в Конституцию в 2020 г. и другие политические мероприятия. Аналогичным образом поступают некоторые Европейские государства.

Сложившаяся ситуация чревата серьезными угрозами международному миру и безопасности. По этой причине мы предложили обсудить некоторые аспекты проблемы на отдельном **Круглом столе № 5 «Правовые механизмы противодействия использованию ИКТ-среды для вмешательства во внутренние дела суверенных государств, включая гуманитарное измерение».**

8. В заключение доклада хочу сообщить, что в работе нашего Форума принимает участие более 30 ученых и специалистов из 20 государств мира (*Австрия, Белоруссия, Германия, Италия, Канада, Киргизия, Китай, Республика Корея, Словакия, США, Финляндия, Франция, Украина, Швейцария, Эстония, ЮАР, Япония* и *Российская Федерация*) а также представители *Конференции ООН по торговле и развитию, Института ООН по исследованию проблем разоружения и некоммерческой организации США ICANN (Международная корпорация по присвоению доменных имен и номеров).*

Благодарю за внимание.

С.М. Бойко
Начальник департамента обеспечения безопасности в области информации и информационных технологий аппарата Совета Безопасности Российской Федерации

ОСНОВНЫЕ ПОДХОДЫ К ФОРМИРОВАНИЮ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Базовые положения государственной политики Российской Федерации в области международной информационной безопасности представлены в главном профильном документе стратегического планирования – Основах государственной политики.

Со дня утверждения в июле 2013 года Президентом Российской Федерации действующих Основ прошло более семи лет, но ключевые положения документа по-прежнему сохраняют актуальность.

Этот семилетний период характеризовался нарастанием угроз в информационной сфере, приданием им системного, наступательного характера и увеличением масштабов последствий реализации этих угроз.

И если раньше эти угрозы в основном исходили от террористов, экстремистов, других преступных элементов, то сегодня привычными становятся звучащие из уст государственных деятелей прямые угрозы в адрес суверенных государств. Становится нормой политика силового диктата, основанная на научно-технологическом превосходстве ведущих мировых держав.

Предметный профессиональный разговор, практическое взаимодействие компетентных органов, обмен объективной информацией подменяются на государственном уровне бездоказательными обвинениями в адрес оппонентов в совершении компьютерных атак и другой противоправной деятельности в информационном пространстве.

На этой основе отдельными странами строится политика санкционного давления в отношении государств, не желающих поступаться собственным суверенитетом, в том числе и в информационной сфере.

В этих условиях сложно говорить о консолидации усилий мирового сообщества в борьбе с информационными угрозами. Поэтому безрезультатными становятся многие конструктивные идеи и инициативы, нацеленные на формирование мирного, безопасного и стабильного глобального информационного пространства.

Однако даже в таких непростых условиях Россия не отступает от своих принципов и придерживается подходов к формированию системы международной информационной безопасности, заявленных более 20 лет назад на площадке Организации Объединенных Наций.

Для реализации этих подходов важно сделать все возможное, чтобы создать эффективные международные правовые механизмы, способные предотвратить межгосударственные конфликты в глобальном информационном пространстве.

Сегодня российская государственная политика в рассматриваемой области – это, прежде всего, совокупность скоординированных мер в интересах обеспечения национальной безопасности и содействия формированию указанной системы.

В выступлении неоднократно упоминался ставший уже привычным термин «международная информационная безопасность». Что же стоит рассматривать под данным понятием? Это, прежде всего, такое состояние глобального информационного пространства, которое способно обеспечить поддержание

международного мира, безопасности и стабильности на основе равноправного стратегического партнерства.

Безусловно, обеспечить международную информационную безопасность отдельными разрозненными мерами невозможно. Необходима системная платформа, основу которой должна составить совокупность международных и национальных институтов, регулирующих деятельность различных субъектов глобального информационного пространства во имя главной цели – предотвращения угроз информационной безопасности.

В рамках государственной политики Российской Федерации сформулированы основные угрозы в указанной области.

На первый взгляд, они не отличаются новизной. Это – ставшие уже привычными угрозы, вызванные использованием информационных и коммуникационных технологий в различных противоправных целях.

Прежде всего, в военно-политических целях, противоречащих международному праву. Кроме того, в террористических и экстремистских целях.

Одновременно стремительно нарастают угрозы, связанные с использованием ИКТ преступниками. И это не только неправомерный доступ к компьютерной информации, но и многочисленные мошенничества.

Компьютерные атаки на информационные ресурсы государств, их критическую информационную инфраструктуру сегодня исчисляют уже миллионами.

Но перечень угроз был бы не полным без упоминания о стремлении отдельных государств использовать свое технологическое доминирование для монополизации различных сегментов рынка ИКТ. Сегодня это влияние активно распространяется на основные информационные ресурсы, критическую информационную инфраструктуру, ключевые технологии, продукты и услуги в данной сфере.

Кроме того, указанные страны делают все возможное для противодействия доступу других государств к новейшим технологиям, под якобы благовидными предлогами создают условия для технологической зависимости и неравенства в сфере информатизации.

Ставшие привычными угрозы информационной безопасности, сохраняя свое содержание, активно меняют свои формы, становясь все более изощренными и опасными для различных сфер жизнедеятельности как отдельных граждан, так и государств в целом.

В сложившихся условиях логичными выглядят российские подходы к формулированию цели государственной политики в области международной информационной безопасности.

Это – содействие обеспечению национальной безопасности путем установления международного правового режима, направленного на предотвращение межгосударственных конфликтов в глобальном информационном пространстве и на создание условий для формирования сбалансированной и эффективной системы международной информационной безопасности.

Достижению обозначенной цели будет способствовать участие России в решении основных задач.

Во-первых, формирование системы международной информационной безопасности путем межгосударственного взаимодействия на различных уровнях: двустороннем, многостороннем, региональном и глобальном.

Во-вторых, создание условий, обеспечивающих снижение риска использования ИКТ в целях подрыва суверенитета и нарушения территориальной целостности государств. Важно исключить возможность действий, угрожающих международному миру, безопасности и стабильности в глобальном информационном пространстве.

Еще одна задача – формирование механизмов международного сотрудничества, позволяющих противодействовать угрозам использования ИКТ в террористических и экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств.

Также в числе основных задач – повышение эффективности сотрудничества в целях противодействия использованию ИКТ в преступных целях, создание необходимого для этого международного правового режима.

Важное значение придается совершенствованию межгосударственного взаимодействия в области реагирования на компьютерные инциденты, а также предотвращению компьютерных атак на критическую информационную инфраструктуру.

Новым содержанием наполнена задача по созданию условий для обеспечения технологического суверенитета государств и преодоления информационного (цифрового) неравенства.

Решение перечисленных задач неразрывно связано с основными направлениями реализации российской государственной политики в области международной информационной безопасности.

Каждое из этих направлений характеризует комплексный подход, позволяющий обеспечить решение упомянутых задач.

Примером могут служить направления государственной политики, связанные с решением задачи по формированию системы международной информационной безопасности, к ключевым из которых относятся следующие направления.

Первое – создание условий для принятия Конвенции об обеспечении международной информационной безопасности.

Второе – содействие организации регулярного институционального диалога для обеспечения под эгидой ООН демократического, инклюзивного и транспарентного переговорного процесса по вопросам обеспечения безопасности в сфере использования ИКТ.

Также важным является направление, связанное с содействием в выработке учитывающих специфику ИКТ принципов и норм международного права в интересах регулирования деятельности в глобальном информационном пространстве.

Безусловно, все указанные направления реализуемы только при условии развития различных форм сотрудничества России в области обеспечения международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях.

В следующем, 2021 году, планируется утвердить новые Основы государственной политики Российской Федерации в области международной информационной безопасности, которые станут стратегическим ориентиром на данном направлении на среднесрочную перспективу и придадут новый импульс продвижению российских подходов и инициатив.

Чарльз Барри
Независимый эксперт (США)

РАЗЛИЧНЫЕ ПОДХОДЫ К МЕЖДУНАРОДНОМУ СОТРУДНИЧЕСТВУ В КИБЕРПРОСТРАНСТВЕ

Введение

Я благодарю профессора доктора Шерстюка и Национальную Ассоциацию международной информационной безопасности (НАМИБ) за организацию данной конференции и за возможность вновь внести свой вклад в наши дискуссии на 14-м международном ежегодном форуме. Виртуальный формат мероприятий этого года действительно является новшеством, свидетельствующим о способности киберпространства служить всем нам в новой «разделенной» среде, продиктованной COVID. Как всегда, в рамках форума в Гармише, сегодня я излагаю исключительно свои персональные размышления. Мое внимание будет сосредоточено на прогрессе, достигнутом в направлении основательного международного сотрудничества в киберпространстве. Я также предложу эффективный способ дополнить текущую работу группы правительственных экспертов ООН (ГПЭ ООН), рабочей группы открытого состава (РГОС) и многих других инициатив, направленных на освоение киберпространства в качестве среды мирного существования для всех.

Международное сотрудничество в киберпространстве

За последние 20 лет была проделана большая напряженная работа по развитию международного сотрудничества в киберпространстве, включая значительные достижения НАМИБ в Гармише за эти годы. Максимальный успех в вопросе технических аспектов сотрудничества был достигнут в рамках IANA («Администрация адресного пространства Интернет»), IETF/IRTF (Инженерный Совет Интернета / Исследовательская группа Интернет-технологий) и МСЭ. С юридической стороны мы наблюдали сотрудничество в рамках Будапештской конвенции о киберпреступности 2001 года (64 страны) и комплексных Таллиннских руководств 1.0 и 2.0. Региональных инициатив было много – АС, АСЕАН, ЕС, ЛАГ, ОАГ, ОБСЕ и ШОС. Частный сектор обнародовал свой опыт в рамках Цифровой Женевской конвенции Microsoft (2017) и Хартии доверия Siemens (2018).

Однако, следует задать отрезвляющий вопрос: была ли эффективность этих инвестиций достаточной? Удалось ли в результате наших усилий добиться сколько-нибудь заметного прогресса в решении неотложной задачи построения совместного управления в киберпространстве? Инвестиции были огромными. Эффективность этих инвестиций была незначительной и неопределенной. Как верно задал вопрос проф. Шерстюк в своем вступительном слове – почему прогресс идет так медленно?

Семь реалий усложняют сотрудничество при управлении международным киберпространством

Семь реалий бросают вызов любым усилиям по достижению международного сотрудничества в вопросах управления киберпространством. Во-первых, киберпространство стало широко распространенным на всех предприятиях. Все современные системы связаны между собой, и многие отрасли, например, коммуникационные и банковские сети, практически неразделимы. Чрезвычайно трудно «распаковать» одно из другого – либо системы из других систем внутри секторов, либо даже применить отдельные руководящие идеи к одному сектору, который тесно переплетен с другими. Следующий фактор заключается в том, что для каждой потенциально сотрудничающей страны большая часть инфраструктуры национальной безопасности частично зависит от ее гражданского сектора. Это утверждение справедливо почти всегда. Третий фактор касается тех международных служб, от которых страны зависят в целом, таких как системы контроля за воздушным движением. И хотя сотрудничество в сфере надзора за международными операциями в киберпространстве может рассматриваться позитивно, каждая система в конечном счете находится в пределах одного или нескольких суверенных государств. Это затрудняет трансграничное сотрудничество.

Четвертый осложняющий фактор заключается в том, что, хотя возможное управление киберпространством может быть определено и обеспечено государственными органами, системы, которые там функционируют, находятся в руках частных собственников, которые часто являются международными корпорациями. Еще одна усложняющая данность заключается в том, что надежность системы требует не только киберустойчивости, но и физической устойчивости. Двойственная природа требуемой защиты означает, что для достижения желаемой цели недостаточно сосредоточиться только на кибернарушениях.

Вышеприведенные факторы достаточно пугают. Однако, последние два обстоятельства являются, пожалуй, самыми серьезными препятствиями на пути построения устойчивого управления киберпространством. Во-первых, сотрудничество в киберпространстве осуществляется не изолированно, а в контексте более широких международных отношений – экономических, дипломатических, политических, информационных и военных. Когда государства переживают серьезную напряженность в одной сфере отношений, они все еще могут продолжать обмениваться идеями (как мы в рамках НАМИБ), однако, редко бывает так, что фактические соглашения могут быть достигнуты без преодоления серьезных разногласий в других сферах отношений. Наконец, в определенные периоды – в том числе, возможно, и в настоящее время – наблюдается серьезная нехватка доверия между государствами, которые должны объединиться для реализации сотрудничества. Все эти усложняющие, критические реалии препятствуют достижению прогресса в сфере управления.

Возможно, мы слишком сосредоточились на достижении управления киберпространством сверху вниз. Другим способом может стать объединение сотрудничества и достижение консенсуса по схеме снизу-вверх. Это может создать прочную основу для достижения более высоких целей.

Эффективное управление, достигнутое очень давно в других областях

Мы можем надеяться на будущее регулирование киберпространства исходя из множества прошлых соглашений между государствами по управлению различными доменами. Все они хорошо послужили международному сообществу. Сегодня они действуют под эгидой ООН в структурах, обеспечивающих доступность для всех сторон. Первая из таких структур – международная организация гражданской авиации (ИКАО), образованная в 1947 году и расположенная в Монреале. ИКАО – это учреждение, в рамках которого международное сообщество устанавливает правила безопасного воздушного движения в международном воздушном пространстве. Сегодня 193 государства – члена соблюдают правила ИКАО, которые никогда не отменяют национальных правил.

В 1958 году в Лондоне была создана Международная морская организация (ИМО), в которую на сегодня входят 174 государства, они разрабатывают и контролируют правила, а также реализуют такие договоры, как последние поправки (1974 г.) к Международной конвенции по охране человеческой жизни на море (СОЛАС). И ИКАО, и ИМО являются недоговорными организациями ООН, которые хорошо зарекомендовали себя в качестве основных институтов, представляющих международное регулирование в своих предметных областях.

Две другие сферы регулируются менее структурными, но, тем не менее, значимыми международными соглашениями, отражающими управление. Договор об Антарктике 1961 года (САР), подписанный 54 государствами, является единственным соглашением, регулирующим данную международную территорию, а договор о космическом пространстве 1967 года (его подписали 100 государств) является наиболее заметным из нескольких со-

International Cooperation in the Cyber Domain

Highlights of 20 year governance efforts thus far:

- Technical cooperation entities: ITU, ICANN, IETF/IRTF, etc.
- 2001 Budapest Cybercrime Convention – 64 countries
- UNGGE – 2005, 2010, 2013, 2015, 2017, 2021
- 2019 OEWG: sessions Sep/Dec 2019, Feb 2020, Mar 2021
- Regional Initiatives: AU, ASEAN, EU, LAS, OAS, OSCE, SCO
- Private sector: 2017 "Digital Geneva Convention" (MS); 2018 "Charter of Trust" (Siemens), Tallinn Manuals, etc.

Progress yes, but slow. Why?

7 Realities Complicate Cooperation on International Governance

Progress is challenged by:

1. **Interdependence** among systems and sectors.
2. Civil and national security systems **intertwined** in cyberspace.
3. Most infrastructure operates from/in **sovereign nations**.
4. Cyberspace will be State governed but **private ownership**.
5. Reliability demands a **duality of protection** across cyber and physical domains.
6. **Broader Disputes** in International State Relations
7. Most significant complicating factor: the ***dearth of wider trust among the states*** that must cooperate.

Long-agreed Governance in Every Other Global Domain

International Cooperation in other Domains

- 1958 International Maritime Organization (IMO) – 174 members.
- 1947 International Congress of Aviation Organizations (ICAO) – 193 members
- 1967 Outer Space Treaty (OST) – 100 signatories
- 1961 Antarctica Treaty System (ATS) – 54 parties (only international land territory on earth)

History shows these agreements grew from the bottom up, i.e., from regional or special interest groups to global.

Might a future 'International Cyberspace Organization' emerge in the same way?

The Shared Global Commons are:

- *Beyond national territory, territorial waters and airspace.*
  - *Protection in national areas are national responsibilities*
- *International or high seas, international airspace, space and cyberspace.*
- *The essential conduits for global trade and commerce.*
- *Open to all and the responsibility of all to protect.*
- *Essential Services in these regions must be protected in common, including the enterprises of national or multinational providers.*

A Gambit to Further Cyberspace Cooperation

An additional bottom-up path to complement UNGGE & OEWG top-down approach.

- ***Concept***: Collective Protection of select services essential to global commerce, benefiting all states.
- Discreet technologies within worldwide transportation and finance sectors
- Protection for System Reliability and Safety
- International Commerce versus National Security
- Protecting Shared Services in the Global Commons.
- Complementary also to national protections.
- Fence off niche cooperation from larger disputes.

Examples of Technical Services Essential to Global Commerce

- Automated Information Systems (**AIS/AIS-S**) maritime collision avoidance. IMO required for all ships over 300 tons in international waters.
- Automatic Dependent Surveillance-Broadcast (**ADS-B**) aviation safety reporting system. ICAO advocated, spreading rapidly across world.
- Society for Worldwide Interbank Financial Telecommunication (SWIFT) Network.

All States would be severely damaged by cyber attacks on these common use networks

Automated Information System AIS/S-AIS

- IMO Mandated since 2002 for all vessels 300 tons or more transiting international waters, plus all passenger ships.
- Initial phase was short range near shore and in proximity to any vessel.
- Connects ships with land controllers and other ships.
- More and more ocean coverage with satellite augmentation (AIS-S).
- Critical in busy, narrow channels and bad weather.
- Some suspected incidents of misuse
- Overall a positive safety, collision avoidance systems with future promise.

Society for Worldwide Interbank Financial Telecommunication SWIFT Network

- SWIFT - used by 11,000 banks in 200 countries - 32 million times/day.
- The primary secure method for completing financial transaction worldwide.
- Approximately half of all high value cross border payments in international financial worldwide are verified via Belgium-based SWIFT each day.
- A breech of security will have a major impact on global commerce for all nations.
- SWIFT is dependent on the reliability of the fiber cable system.

глашений, устанавливающих международные правила деятельности в космическом пространстве. Учитывая эти соглашения, можно с оптимизмом ожидать, что когда-нибудь страны придут и к соглашению о том, как управлять киберпространством. Примечательно, что все эти соглашения начинались с небольшого регионального сотрудничества в конкретных областях, где общие обеспокоенности позволили достигнуть соглашения.

Общее Глобальное Достояние

То, что можно назвать «Общим глобальным достоянием», – это совокупность международных территорий суши, моря, воздуха, космоса и киберпространства. Все эти области признаются всеми как выходящие за пределы суверенной юрисдикции любого государства. Многие жизненно важные услуги осуществляются вне пределов границ, даже если все они оказываются с национальных территорий. Операторы берут на себя предполагаемую международную ответственность за поддержание этих систем на общее благо всех стран.

Новый шаг к дальнейшему сотрудничеству в киберпространстве

Здесь предлагается создать дополнительную инициативу по сотрудничеству, которая будет осуществляться параллельно и комплементарно к более масштабным, формализованным ГПЭ ООН и РГОС, а также расширять национальные киберструктуры и режимы безопасности. Как и в других сферах, где полномочия накладываются друг на друга, здесь они также обязательно должны быть согласованы и скоординированы.

Три примера важнейших услуг и технологий, незаменимых для глобальной торговли

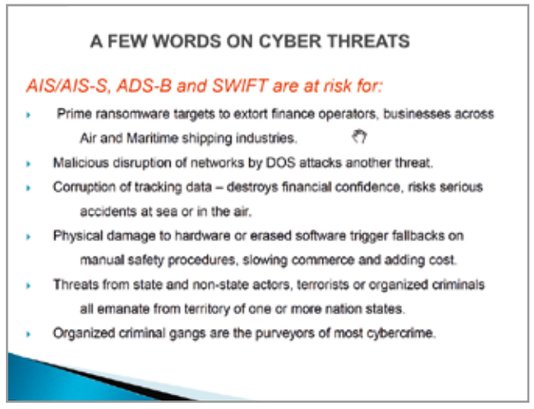
Следуя методу «Построения международного сотрудничества в киберпространстве с нуля», аналогичному предшествовавшей эволюции в других сферах (особенно морской и воздушной), мы начинаем с поиска взаимодействия в области киберуправления и защиты трех важнейших сервисных технологий, которые должны быть относительно бесспорными с точки зрения международного соглашения о защите. Причина в том, что эти технологии и услуги важны для экономики почти каждой страны. Это следующие технологии: система предотвращения морских столкновений, известная как AIS (Автоматическая идентификационная система), и ее новая космическая версия S-AIS; система безопасности воздушных судов под названием ADS-B (Автоматизированная система наблюдения и трансляций) и ее обновленная версия ADS-C (Автоматизированная система наблюдения и контроля); и, наконец, сеть SWIFT (Сообщество международных межбанковских финансовых телекоммуникаций), бельгийская система безопасной проверки транзакций. Глобальная торговля и, следовательно, международное сообщество понесут огромные экономические потери, если любая из этих систем подвергнется кибератаке или физическому разрушению. Таким образом, все нации должны объединиться, чтобы предотвратить эти события.

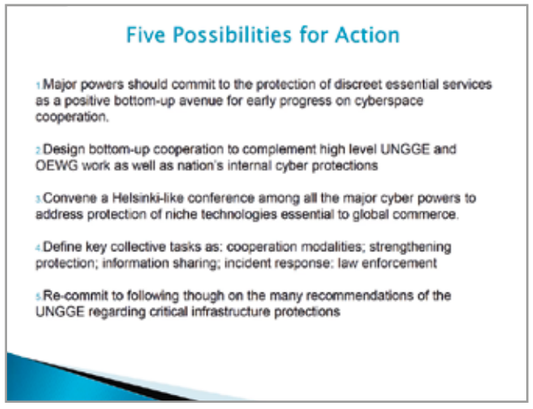
Автоматическая идентификационная система (AIS/S-AIS)

Береговая AIS и дополнительные космические AIS формируют архитектуру слежения за судами для предотвращения столкновений на море. Отдельные корабли передают данные AIS из бортовых систем в наземные центры управления, которые участвуют в маршрутизации трафика. Каждый корабль также использует AIS и бортовой радар для обнаружения и избегания других судов. AIS требуется для всех судов водоизмещением более 300 тонн или перевозящих пассажиров в международных территориальных водах. Эта сетевая система особенно важна, когда суда находятся в зонах интенсивного движения вблизи портов или в узких проливах, а также при работе ночью или в плохую погоду.

Автоматизированная система наблюдения и трансляций (ADS-B) и контроля (ADS-C)

ADS-B/ADS-C обеспечивает безопасность там, где ее в настоящее время недостаточно или нет совсем – в международном воздушном пространстве за пределами досягаемости наземных радаров. Это огромная территория, в основном пролегающая над океанами. Система относительно новая (существует около 10 лет) и заменяет радар в качестве более





эффективного и точного способа доподлинно определить местоположение и высоту самолета. Система настолько точна, что дополнительно позволяет более эффективно использовать воздушное пространство (меньше разделения между самолетами для обеспечения безопасности), а также обеспечивает более прямую маршрутизацию, сокращая эксплуатационные расходы. Как и AIS, система ADS-B/ADS-C имеет сетевую основу и подвержена нарушениям и атакам.

Сообщество международных межбанковских финансовых телекоммуникаций (сеть SWIFT)

SWIFT отличается от AIS и ADS-B/ADS-C. Эти системы в первую очередь направлены на обеспечение безопасности в международном транспортном секторе. SWIFT же обеспечивает безопасность информации о финансовых транзакциях. Это не менее важно для мировой торговли. Услугами SWIFT пользуются 11 000 банков в 200 странах, и они ежедневно отправляют между своими участниками около 32 миллионов сообщений. Как и AIS и ADS-B/ADS-C, сеть SWIFT является важнейшей сервисной технологией, поддерживающей глобальную торговлю. Ее подрыв или потеря окажет значительное влияние на мировые рынки и, таким образом, отразится на интересах многих стран.

Несколько слов о киберугрозах

Фактически, как уже отмечалось, те самые державы, которые чаще всего осуждают кибератаки, – Китай, Россия и США – неоднократно обвинялись в совершении кибератак на критическую инфраструктуру. Северная Корея, Иран и Израиль – три другие державы, также обвиняемые в разрушительных кибератаках на чувствительную инфраструктуру. Эти и другие страны должны объединиться для защиты вышеописанных систем на базе организованных совместных усилий. Атаки на все три системы либо проводились, либо были продемонстрированы в качестве возможных. Они являются основными целями для программ-вымогателей или атак типа «Отказ в обслуживании». Они также могут быть подвержены искажению данных в ходе атак, которые способны замедлить глобальную торговлю, подорвать финансовую стабильность или привести к серьезным авариям на море или в воздухе. Физический ущерб также должен приниматься во внимание. Однако, все эти нападения – будь то со стороны государства или негосударственного субъекта, террористов или организованных преступников – обязательно совершаются с территории одного или нескольких государств – государств, обладающих правовой юрисдикцией в отношении незаконных действий, совершенных с их территории.

Пять возможностей для действий

Нижеследующие рекомендации – это, опять-таки, мои персональные идеи о том, как можно было бы сформировать новую программу международного сотрудничества в киберпространстве.

1. Крупные державы должны взять на себя обязательства по защите чувствительных жизненно важных услуг в качестве позитивного расширяющегося направления для скорейшего достижения прогресса в сотрудничестве в киберпространстве.
2. Разработать сотрудничество снизу-вверх, так, чтобы дополнить работу высокого уровня ГПЭ ООН и РГОС, а также механизмы внутренней кибербезопасности стран.
3. Созвать конференцию, подобную Хельсинки, – среди всех крупных кибердержав, для решения проблемы защиты узкоспециализированных технологий, имеющих существенное значение для глобальной торговли.
4. Определить ключевые совместные задачи следующим образом: условия сотрудничества; усиление защиты; обмен информацией; реагирование на инциденты: правоохранительные органы
5. Вновь принять на себя обязательство следовать многочисленным рекомендациям ГПЭ ООН, касающимся защиты критической инфраструктуры.

Заключение

Цель этого доклада состоит в том, чтобы предложить эффективный путь вперед при построении будущего режима совместного управления киберпространством. Подобная организация может быть похожа на ИКАО или ИМО, но непременно должна быть уникальна во многих отношениях. Киберпространство имеет уникальные отличия от других областей, но не тотальные. Данная инициатива могла бы быть предпринята параллельно с ГПЭ ООН и РГОС. Не нужно начинать с формирования бюрократии. Она могла бы начаться по-Хельсинкски, как конференция высокопоставленных чиновников, а не ученых. Это может перерасти в длительный продуктивный и прозрачный процесс, опять же подобный Хельсинкскому. Мы должны искать, с помощью этого или другого метода, способ выйти за рамки простых добровольных норм. Начав с малого, коллективно согласившись защищать важнейшие, не вызывающие споров технологии, которые служат всем странам, мы можем найти возможность для достижения прогресса.

Еще раз спасибо профессору Шерстюку и НАМИБ за честь говорить с вами сегодня здесь. А также, мои слова благодарности нашим переводчикам за их удивительное мастерство и терпение. Наконец, моя признательность всем вам, кто слушает эти идеи. Я с нетерпением жду любой обратной связи, которую вы пожелаете мне предложить. Спасибо.

В.А. Шин

Заместитель директора ДМИБ МИД России

Уважаемые участники Форума, коллеги!

Год назад – 28 декабря 2019 г. – Указом Президента Российской Федерации в структуре МИД России было создано новое подразделение – Департамент международной информационной безопасности (ДМИБ). Позвольте кратко поделиться основными итогами работы ДМИБ за прошедший период и рассказать об основных задачах на перспективу.

Появление ДМИБ, безусловно, является примечательным событием, поскольку свидетельствует об особом внимании российского руководства к решению всего комплекса вопросов, связанных с развитием и обеспечением безопасности информационно-коммуникационных технологий (ИКТ), и было обусловлено необходимостью адекватного оперативного реагирования дипломатическими методами на новые вызовы и угрозы, возникающие в этой сфере.

По состоянию на сегодня можно констатировать, что несмотря на объективные трудности, связанные с эпидемическими ограничениями, организационное становление ДМИБ в основном завершено: практически полностью укомплетован кадровый оперативно-дипломатический состав, завершен процесс переезда и обустройства департамента в выделенных для него помещениях, в штатном режиме функционируют вспомогательные технические подразделения. Средний возраст Департамента составляет лишь 38 лет, что несколько отличает нас от других подразделений МИД России. ДМИБ – молодой департамент как в институциональном плане, так и по возрасту работающих в нем сотрудников.

Несмотря на это, в субстантивном плане ДМИБ с первых дней своего существования является абсолютно боеспособным подразделением, ежедневно доказывающим свою эффективность и востребованность. Понятно, что ДМИБ возник не на пустом месте: его интеллектуальный костяк составили сотрудники отдела МИБ ДНВ МИД России во главе со Специальным представителем Президента по вопросам МИБ А.В. Крутских. Но и новые члены команды, к коим относится и ваш покорный слуга, полноценно влились в работу, «заболев» (в хорошем смысле) тематикой МИБ.

Тематическая одержимость коллектива играет важную роль в обеспечении результативности его работы. Совместными усилиями удалось создать в коллективе уникальную атмосферу интеллектуальной креативности, ориентированной на достижение весомых практических результатов и основанной на осознанной дисциплине исполнителей. Считаем это одним из главных своих достижений и намерены и впредь культивировать такую атмосферу контролируемой креативности.

В субстантивном плане, несмотря на все уже упомянутые сложности, связанные с организационным становлением департамента в условиях пандемии, к главным достижениям ДМИБ в уходящем году можно отнести следующее.

9 ноября с.г. Первым комитетом 75-й сессии Генассамблеи ООН был одобрен проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Принятие этой инициированной Россией резолюции является крупной внешнеполитической победой нашей страны. Наш документ поддержало внушительное большинство государств-членов ООН: 27 государств стали соавторами нашей инициативы, 104 проголосовали «за». В целях обеспечения позитивных итогов голосования ДМИБом была развернута активная работа по продвижению нашего документа – как из Центра посредством видеоконференций, так и в Нью-Йорке по постпредствам и по столицам – силами роспосольств.

В чем же заключается важность упомянутой резолюции?

В соответствии с резолюцией в следующем году сроком на пять лет будет учреждена новая Рабочая группа открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ. Будущая РГОС будет действовать на основе консенсуса. Приоритетом ее работы останется дальнейшая выработка норм, правил и принципов ответственного поведения государств в информационном пространстве и путей их имплементации. Новая РГОС будет также уполномочена рассматривать инициативы государств, направленные на обеспечение безопасности в сфере использования ИКТ, организовывать под эгидой ООН регулярный институциональный диалог с широким кругом государств-участников, а также продолжать исследования существующих и потенциальных угроз в сфере информационной безопасности, включая такие аспекты, как применимость международного права к использованию ИКТ государствами, меры укрепления доверия и наращивания потенциала и т.д.

Несмотря на ожесточенное сопротивление наших идеологических оппонентов, России не только удалось гарантировать международному сообществу сохранение, а также непрерывность и преемственность инклюзивного, транспарентного и подлинно демократического переговорного процесса по вопросам обеспечения информбезопасности, но и в очередной раз доказать свое интеллектуальное лидерство в глобальном диалоге по проблематике МИБ.

Я уже упомянул про активное противодействие со стороны наших оппонентов. В этом году оно носило беспрецедентно ожесточенный характер. Наши заклятые партнеры в лице всего западного лагеря во главе с США «пустились во все тяжкие» и использовали даже процедурные уловки: впервые за время продвижения нашей резолюции по МИБ в Первом комитете Генассамблеи ООН проходило раздельное голосование по отдельным пунктам нашего документа. Весьма показательно, что накануне голосования американский киберкоординатор М. Маркофф через замгенсекретаря ООН О. Накамицу обещала не делать этого, но спустя пару дней вероломно нарушила свои обещания.

До голосования по нашей резолюции Первый комитет Генассамблеи ООН должен был рассмотреть внесенный (причем в обход процедуры) американской стороной проект их резолюции, единственной целью которой было блокировать возможность принятия Генассамблеей ООН каких-либо решений по дальнейшей работе на направлении МИБ до завершения итогов нынешних РГОС и ГПЭ. Данное препятствие нам удалось обойти, предприняв ряд упреждающих маневров.

9 ноября в Первом комитете была выиграна важная битва, но борьба за принятие нашей резолюции еще не окончена: в конце декабря – начале января предстоит окончательное голосование по нашему проекту резолюции в Генеральной Ассамблее ООН. В связи с этим продолжаем активную работу с единомышленниками и колеблющимися – как с помощью роспосольств, так и напрямую, посредством видеоконференций.

Накал борьбы вокруг РГОС отражает обостряющуюся борьбу за создание идейных контуров будущего мироустройства, прежде всего в информационном пространстве, которое США и их единомышленники рассматривают как новый «театр военных действий». Сфера МИБ стремительно превращается в еще одно направление стратегического противостояния наряду с традиционными вооружениями и становится одним из ключевых элементов глобальной стратегической стабильности.

В условиях отсутствия общепризнанных правил поведения в киберпространстве наши оппоненты, прежде всего, США, стремятся обеспечить себе «свободу рук», включая право произвольно трактовать и применять выгодные для них нормы международного права, произвольно определять «виновных» в совершении кибератак и наказывать их путем контрмер и санкций, при этом не утруждая себя излишними доказательствами, умышленно нагнетают процессы хаотизации внешнего мира и фактического отказа от обязательств по конструированию стабильности в киберсреде.

В противовес нашим подходам, направленным на предотвращение противоборства в ИКТ-среде, обеспечение стабильности и безопасности глобального информпространства, а также на достижение равноправного стратегического партнерства, американцы упорно пытаются навязать международному сообществу свои концепции мира с опорой на силу и соперничество великих держав.

В данном контексте очевидно, что одним из ключевых условий выработки стратегического статус-кво в киберсфере является достижение принципиальных договоренностей с Вашингтоном, основывающихся на системе взаимоприемлемых мер доверия.

В этих целях ДМИБом была разработана инициатива по нормализации диалога по МИБ с Соединенными Штатами. 25 сентября Президент Российской Федерации В.В. Путин выступил с заявлением о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. Суть инициативы сводится к принятию комплекса практических мер по перезагрузке двусторонних отношений в сфере использования ИКТ, направленных на повышение уровня доверия между нашими государствами и обеспечение безопасности наших народов. Особое внимание в заявлении посвящено аспектам, касающимся гарантий невмешательства во внутренние дела друг друга, включая избирательные процессы, а также необходимости начала профессионального экспертного диалога и особой ответственности ключевых игроков за предотвращение масштабной конфронтации в цифровой сфере.

Кроме того, в заявлении содержался призыв России ко всем странам выйти на заключение глобальной договоренности о принятии политического обязательства государствами о ненанесении первыми удара с использованием ИКТ друг против друга.

К сожалению, реакция Вашингтона (а точнее, по сути, ее фактическое отсутствие) свидетельствует о неспособности американской стороны, по крайней мере, на данном этапе, к какому-либо конструктивному, субстантивному диалогу. Исходим из того, что период внутриполитической неразберихи в США должен когда-то окончиться, готовы проявить стратегическое терпение. Иллюзий по поводу тональности будущего диалога не имеем. Вместе с тем рассчитываем на трезвость, прагматизм и элементарный инстинкт самосохранения американских партнеров.

Другим важным направлением деятельности ДМИБ является трек противодействия киберпреступности.

Россия выступила инициатором разработки под эгидой ООН первой в истории универсальной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях. Эта идея была оформлена резолюцией Генассамблеи ООН, за принятие которой в 2019 г. проголосовали 79 стран. Она предусматривает запуск работы специального комитета открытого состава по разработке конвенции. В 2020 г., несмотря на серьезные ограничения, связанные с пандемией, начали активную совместную работу по реализации этой важной инициативы. В настоящее время активно готовимся к созыву первой (организационной) сессии спецкомитета в январе 2021 года.

Одним из главных направлений деятельности ДМИБ является обеспечение межгосударственного сотрудничества по вопросам МИБ на региональном (прежде всего, в таких форматах, как СНГ, ОДКБ, ШОС, БРИКС, АСЕАН) и двустороннем уровнях.

Важным достижением в год председательской вахты России в Шанхайской Организации Сотрудничества, несмотря на внесенные в связи с эпидемией коронавируса изменения в планы совместной работы, стало принятие 10 ноября заявления Совета глав государств-членов ШОС о сотрудничестве в области обеспечения МИБ. В документе отражены принципиальные подходы стран к этой сфере, отмечено общее стремление к сотрудничеству в вопросах предотвращения конфликтов в информационном пространстве, подчеркнута ключевая роль ООН в борьбе с угрозами в сфере МИБ, выражена поддержка осуществляемой в ней деятельности по выработке правил, норм и принципов ответственного поведения государств в информационном пространстве, подтверждено намерение продолжить совместную работу и координацию усилий государств-членов ШОС на этом направлении в рамках ключевых профильных переговорных площадок ООН.

Главы государств заявили о необходимости усиления координации в рамках ШОС по вопросам совершенствования управления сетью Интернет, в том числе обеспечения равных прав государств на участие в процессе управления сетью Интернет и повышения роли Международного союза электросвязи. Стороны выступили за всеобъемлющую реализацию Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г.

В рамках СНГ согласовывается аналогичное заявление глав государств Содружества, планируемое к принятию в ходе предстоящего саммита Содружества.

Активно работали в уходящем году и в формате БРИКС: особое внимание традиционно уделяли проблематике противодействия угрозам в информационном пространстве, а также развитию практического сотрудничества «пятерки». Провели 6-е заседание Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ (в этом году – впервые в режиме видеоконференции). Обсуждение всего комплекса пятистороннего взаимодействия в области МИБ, в том числе обзор хода реализации принятой по инициативе китайского председательства в БРИКС в 2017 г. «Дорожная карта практического сотрудничества в области обеспечения безопасности в сфере использования ИКТ», вновь подтвердило востребованность профильного профессионального диалога экспертов наших стран. В итоговом коммюнике саммита БРИКС зафиксированы важные договоренности стран-участниц объединения в сфере МИБ.

На направлении АСЕАН одно из главных достижений уходящего года – согласование со всеми странами-участницами Ассоциации концептуального документа о запуске Диалога Россия-АСЕАН по вопросам использования ИКТ, который призван стать основным механизмом по рассмотрению всего спектра вопросов обеспечения информбезопасности.

С 2017 г. по инициативе России действует механизм межсессионных встреч по безопасности в сфере использования ИКТ и самих ИКТ (МВ-ИКТ) Регионального форума АСЕАН по безопасности (АРФ). В сентябре с.г. министрами иностранных дел Регионального форума АРФ утверждены российские проекты концептуальных документов АРФ по терминологии в области безопасности в сфере использования ИКТ и самих ИКТ и о проведении семинара по противодействию использования ИКТ в преступных целях. Российская инициатива по выработке терминологии имеет принципиально важное значение с учетом отсутствия в международном дискурсе общепринятых терминов в сфере МИБ, не говоря уже об их юридическом закреплении.

Прорабатываются организационые аспекты проведения первых региональных встреч по тематике МИБ в таких форматах, как Россия – Африканский союз, Россия – Лига арабских государств и Россия – государства Южной части Тихого океана.

В 2020 г., несмотря на пандемию, развернулась глобальная работа в двустороннем формате с государствами, заинтересованными в развитии двустороннего сотрудничества с Россией в области МИБ.

В развитие договоренностей между президентами В.В. Путиным и Э. Макроном в 2020 г. был запущен российско-французский механизм Межведомственного стратегического диалога по кибербезопасности. Его первый раунд, состоявшийся в сентябре 2020 г. в Париже, продемонстрировал высокую заинтересованность обеих стран в деполитизированном профессиональном разговоре по самому широкому кругу вопросов в сфере МИБ.

По состоянию на сегодня полностью готовы к подписанию пять двусторонних межправительственных соглашений с рядом государств Центральной, Западной и Юго-Восточной Азии, а также Латинской Америки. В стадии проработки находятся еще порядка десятка аналогичных соглашений.

В развитие уже заключенных соглашений подписываются планы реализации основных направлений двустороннего сотрудничества в области обеспечения МИБ на предстоящие годы (в частности, с Вьетнамом).

Активно ведется работа по продвижению российского кандидата на пост Генерального секретаря Международного союза электросвязи (МСЭ) в ходе выборов на Полномочной конференции МСЭ (ПК-22, Бухарест, 26 сентября – 14 октября 2022 г.), а также по подготовке намеченного на 2025 г. Форума по управлению Интернетом.

Завершая, хотел бы выразить мнение, что итоги уходящего года свидетельствуют о растущей актуальности проблематики МИБ (находящейся сейчас, пожалуй, не просто на острие, а на самом кончике острия глобальной повестки дня), своевременности решения о создании ДМИБ, а также эффективности и результативности деятельности нового Департамента.

Безусловными приоритетами ДМИБ в ближайшей перспективе станут участие в работе текущих РГОС и ГПЭ, запуск новой РГОС и спецкомитета по разработке конвенции по противодействию киберпреступности, работа на региональном и двустороннем уровнях. Обязательными условиями достижения успеха на этих и других направлениях считаем плотную межведомственную координацию, регулярную «сверку часов» с ближайшими единомышленниками, а также активизацию взаимодействия с отечественным бизнесом, академическими и экспертными кругами. Считаем наше сегодняшнее мероприятие важным шагом в этом направлении.

Благодарю за внимание!

Дэниел Штауффахер

Президент Фонда «ICT4Peace» («ИКТ для мира»), Швейцария

Высокоуважаемые дамы и господа, уважаемые коллеги!

Для меня большая честь получить приглашение выступить на этом пленарном заседании по теме “Актуальные проблемы обеспечения международного мира и поддержания устойчивого развития в глобальном информационном обществе”.

Я с теплотой вспоминаю свое участие в международной конференции по Киберстабильности в Москве, которая состоялась в декабре 2019 года в Министерстве иностранных дел Российской Федерации. Тогда же мы обсуждали наш совместный проект и отчет под названием “Методологические вопросы применения норм, правил и принципов ответственного поведения государств” под редакцией проф. А. А. Стрельцова и д-ра Энекен Тикк. Данный отчет уже опубликован. Фонд ICT4Peace гордится тем, что принял участие в этой редкой коллективной работе российских и западных экспертов по изучению будущего кибернорм с партнерами из России, США, Эстонии и Швейцарии.

Вас не удивит, если я, будучи президентом организации гражданского общества ICT4Peace, подойду к этому вопросу с той позиции, которая изначально вдохновляла ICT4Peace, – с видением киберпространства, предназначенного для мирной деятельности. Несмотря на печальную статистику злонамеренных и наступательных кибероперaций, проводимых как государствами, так и негосударственными субъектами, мы никогда не должны забывать, что уникальная, созданная человеком среда киберпространства может быть сохранена в мирных целях, если мы сообща выступим за это.

Одним из немногих достижений Организации Объединенных Наций в части сдерживания наступательных кибероперaций стало соглашение 2015 года, устанавливающее свод норм ответственного поведения государств в киберпространстве. Эти одиннадцать норм были приняты на основе консенсуса группой правительственных экспертов ООН (ГПЭ ООН) и впоследствии были поддержаны в Резолюции Генеральной Ассамблеи ООН (также принятой консенсусом), которая призвала государства руководствоваться итогами работы ГПЭ при использовании ими информационно-коммуникационных технологий (ИКТ).

Важнейшей среди этих норм была запрещающая кибератаки на критическую инфраструктуру, от которой зависит общество. Тот факт, что эта норма была разработана членами ГПЭ, в которую вошли представители всех пяти постоянных членов Совета Безопасности ООН (все державы, обладающие значительным наступательным киберпотенциалом), давал основания надеяться, что данная ограничительная норма будет соблюдаться на практике.

К сожалению, эта надежда, по-видимому, не оправдалась, поскольку едва ли не ежедневно поступают достоверные сообщения о киберпреступлениях и, периодически, о реальном повреждении критической инфраструктуры в результате наступательных кибероперaций, многие из которых спонсируются или проводятся государствами.

Тот факт, что сектор здравоохранения был масштабно атакован во время текущей пандемии COVID-19, стал причиной оправданного возмущения со стороны многих людей во всем мире. Но мы не должны сводить общий запрет на атаки в адрес критической инфраструктуры только к тем элементам, которые наделены медицинским логотипом.

Безусловно, сектор здравоохранения является ключевым элементом критической ин-

фраструктуры, но, если мы будем ссылаться на него исключительно как на общегосударственную услугу, заслуживающую защиты, мы отвлечемся от обязательства охранять всю критическую инфраструктуру. Не нужно быть специалистом по кибербезопасности, чтобы понять, насколько разрушительными для общества могут быть кибератаки на инфраструктуру, подобную энергетическим сетям, водоочистным заводам, транспортным узлам и ядерным объектам.

Эта жизненно важная норма по ограничению поведения государств в киберпространстве должна быть поддержана во всей ее полноте, и организации гражданского общества наряду с ответственными правительствами и компаниями должны публично настаивать на этом защитном статусе для всей критической инфраструктуры.

ICT4Peace выступает за проактивное подтверждение государствами своей приверженности соблюдению нормы отказа от атак на критическую инфраструктуру. Прошлой осенью мы инициировали "Призыв к правительствам" – для засвидетельствования того, что их государства соблюдают эту ключевую норму.

В то время, когда международное сообщество занято пандемией, крайне важно, чтобы норма по защите критической инфраструктуры была скорее усилена, нежели чем подорвана.

Общепризнанным является тот факт, что желательно создать некий механизм привлечения государств к ответственности за кибероперации, затрагивающие другие государства. Такой механизм можно было бы рассматривать как совместный процесс, который был бы ориентирован на государства, но который также предусматривал бы участие других заинтересованных сторон.

Среди существующих моделей механизм Универсального периодического обзора Совета по правам человека мог бы стать актуальным в контексте кибербезопасности в сочетании с совместным изучением под руководством государств и одновременным обеспечением вклада и участия частного сектора и гражданского общества.

В связи с этим, ICT4Peace в своем предложении Рабочей группе открытого состава ООН (РГОС) выдвинул идею – "Механизм равноправного рассмотрения киберпространства", представляющий собой один из способов обеспечения отчетности государств о поведении в киберпространстве. Эти базовые рамки будут уважать принцип прозрачного рассмотрения, проводимого под руководством государств и учитывающего вклад гражданского общества и частного сектора.

Это также позволило бы растущему числу государств, обладающих наступательным киберпотенциалом, убедить международное сообщество в том, что этот потенциал используется в соответствии с международным правом и согласованными ООН нормами ответственного поведения государств.

Создание механизма равноправного рассмотрения киберпространства было бы ценной рекомендацией, сформулированной РГОС ООН. Мандат РГОС только что был продлен еще на пять лет, но мы полагаем, что государства могли бы уже сейчас инициировать многосторонние переговоры, которые принесли бы конкретные результаты. Несколько государств-участников РГОС предложили "Программу действий" по кибербезопасности. Переговоры по данной Программе лучше начать раньше, чем позже. Наше предложение о механизме равноправного рассмотрения наряду с другими элементами, усиливающими или дополняющими первоначальный свод норм, может быть включено в этот процесс.

Дальнейшие усовершенствования мер укрепления доверия (МД) в целях придания прозрачности и предсказуемости могли бы фигурировать в потенциальной Программе. Меры укрепления доверия уже давно содействуют снижению недоверия между государствами, находящимися в противоборствующих отношениях. Процесс ГПЭ ООН уже привел к формированию ряда МД, а также региональные организации, такие как ОБСЕ, ОАГ и АСЕАН, разработали ряд МД в области кибербезопасности.

Убедить государства согласовать набор мер укрепления доверия – это не то же самое, что заставить их фактически реализовать их на практике. Именно поэтому ICT4Peace подчеркивает важность механизмов подотчетности и институциональной поддержки для стимулирования государств к выполнению своих политических обязательств по обеспечению реализации МД в политике и на практике.

Заметная поддержка наращивания потенциала в области кибербезопасности также заслуживает включения в любую возможную Программу действий. В этой связи ICT4Peace выступает за то, чтобы Комитет содействия развитию (КСР) Организации экономического сотрудничества и развития (ОЭСР) признал расходы на укрепление потенциала приемлемыми для кредитования в рамках Официальной помощи в целях развития (ОПР).

Если мы серьезно настроены на преодоление цифрового разрыва и предоставление развивающимся странам возможности участвовать в многосторонних форумах по кибербезопасности на равных, то международные организации должны предпринять шаги по стимулированию финансирования со стороны стран-доноров.

Любая возможная Программа действий по международной кибербезопасности будет вынуждена столкнуться с существующим зияющим пробелом в вопросах подотчетности. Для того чтобы заинтересовать кибердержавы в ответственном поведении при проведении кибероперациий за пределами своих границ, международному сообществу необходимо будет разработать всеобъемлющий механизм рассмотрения действий государств и, с помощью прозрачности и многостороннего участия, обеспечения подотчетности.

Подотчетность и атрибуция кибератак идут рука об руку – мы не можем достичь одного без другого. Вполне понятно, что суверенные государства хотят сохранить атрибуцию в качестве национальной прерогативы, но с учетом свойственной им предвзятости сугубо национальный подход будет лишен доверия.

Нам необходимо разработать независимый механизм получения результатов атрибуции, основанный на фактических доказательствах. Исходя из многочисленных отчетов о киберугрозах, подготавливаемых компаниями по кибербезопасности, очевидно, что существуют широкие возможности для обращения к потенциалу частного сектора в этом отношении.

В начале работы РГОС ICT4Peace представила предложение с зарисовкой возможных подходов, учитывающих технические и политические проблемы, связанные с эффективной атрибуцией, и представила простое предложение по усовершенствованию, а именно – создание независимой сети организаций, вовлеченных в экспертную оценку атрибуции. Нам нужно продумать, как подобную автономную сеть атрибуции можно связать с официальными многосторонними процессами по принятию решений в связи с инцидентами на основе эмпирических данных.

Когда мы смотрим на современный киберландшафт, деформированный постоянно растущими киберзлоупотреблениями в адрес человеческой безопасности и нарушениями согласованных норм, становится ясно, что у глобального общества более чем достаточно "текущих проблем" для решения. И в то же время сегодня есть растущая группа действующих лиц в правительствах и за их пределами, разрабатывающих творческие решения этих проблем. Если мы хотим отвоевать киберпространство для мира и устойчивого развития, нам потребуются согласованные усилия всех заинтересованных сторон.

Спасибо!

А.В. Яковенко
Ректор Дипломатической академии МИД России

ЦИФРОВОЕ БУДУЩЕЕ И РОССИЙСКАЯ ДИПЛОМАТИЯ

Уважаемые участники конференции!
Уважаемые гости!
Дамы и господа!

Сегодня доминирующим фактором мирового развития становятся информатизация и информационные технологии, охватывающие самые различные области социальной, духовной, материальной жизни человека. Наряду с имеющими трансграничную природу новыми вызовами, угрозы информационной безопасности в современном мироустройстве выходят на первый план. В условиях прорывного развития передовых информационных технологий актуализировалось информационное противоборство, возрос риск возможного перерастания противостояния в информационную войну, провоцирующую создание принципиально нового оружия – информационно-технологического, при ужесточении очередного витка гонки вооружений и сфер враждебной деятельности. Исходя из реального характера угрозы, еще в 1998 году Россия вышла в ООН с инициативой предметного и целенаправленного обсуждения темы международной информационной безопасности.

По инициативе нашей страны проблематика международной информационной безопасности неоднократно обсуждалась нашими дипломатами в рамках ОБСЕ, ОДКБ, ШОС, Международного союза электросвязи (МСЭ), в ходе Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), в рамках СНГ и Регионального содружества в области связи (РСС). Постоянная работа ведётся и на площадках, как «Группа восьми», «Группа двадцати», БРИКС. В настоящее время более 140 государств разрабатывают свои программы кибервойны. Это значительно подрывает информационную стабильность, поскольку оперативно обнаружить источник информационной атаки достаточно сложно, а последствия её могут стать причиной ответного удара, в том числе с использованием обычных вооружений. В таких условиях позиция России, предлагающей выработать конструктивные правила поведения государств в информационном поле и демилитаризировать информационное пространство с целью обеспечения его безопасности, представляется актуальным. Перед внешнеполитическим ведомством нашей страны встают задачи совершенствования инструментария внешней политики для более эффективного проведения работы на различном международном уровне с целью продвижения российской позиции по вопросам международной информационной безопасности (МИБ).

В статье Сергея Викторовича Лаврова “Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью” подчеркивается, что “именно российские принципиальные установки пользуются самой широкой поддержкой в мире. В 2018 году 73-я сессия Генеральной Ассамблеи ООН подавляющим большинством голосов приняла нашу резолюцию, которая не только сформулировала первоначальный перечень правил поведения государств в информационном пространстве, но и создала под эгидой ООН эффективный переговорный механизм в формате профильной рабочей группы открытого состава для практического решения проблемы обеспечения МИБ. Все более насущной становится задача оперативного согласования правил ответственного поведения государств, закрепляющих в цифровой среде принципы уважения суверенитета, невмешательства во внутренние дела, неприменения силы и угрозы силой, права на индивидуальную и коллективную самооборону, уважения прав и основных свобод человека, а также равные права для всех государств на участие в управлении сетью Интернет”.

Острые вопросы международного сотрудничества в сфере информации ставят перед высшей школой задачу подготовки специалистов в области обеспечения международного мира и поддержания устойчивого развития в глобальном информационном обществе, готовых продвигать инициативы по информационной безопасности в ООН и на других международных переговорных площадках. Магистральная цель таких переговорных усилий, как подчеркнул министр, – “предотвращение конфликтов в информационном пространстве и обеспечение использования ИКТ исключительно в мирных целях”.

На постоянной основе Дипакадемия проводит международные научно-практические конференции по злободневным вопросам современности и узловым темам международной повестки дня, в том числе и по вопросам цифрового будущего нашей планеты.

В 2018 году Дипакадемия стала соучредителем НАМИБ наряду с МГУ, МГИМО, РАНХИКС и др. Главной целью ассоциации является координация и содействие реализации государственной политики РФ в области кибербезопасности как на национальном уровне, так и на международной арене. За этот недолгий период НАМИБ стала национальным центром научных и методических компетенций в сфере информбезопасности, который вырабатывает соответствующие научные и экспертные рекомендации для органов принятия решений.

Мы приветствуем в наших стенах участников Четырнадцатого международного Форума “Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности”, который проходит в условиях обострения противоборства в мировом информационном пространстве на фоне пандемии, буквально за несколько месяцев изменившей привычный мир и ставшей суровым испытанием для всего мира. В условиях обострившейся эпидемиологической обстановки на различных уровнях решается проблема по переводу в т.н. “цифру” многих сфер повседневной жизни социума, включая государственную и общественную деятельность, деловую активность, образование и культуру. Своевременное и устойчивое обеспечение международной информационной безопасности стало как никогда раньше актуальной задачей человечества.

Позвольте пожелать всем участникам Форума успешной и творческой работы на площадке Дипломатической академии МИД России!

Чен Жимин

Председатель Китайской народной ассоциации дружбы с зарубежными странами

Уважаемый Владислав Петрович!

Всекитайская Ассоциация по содействию дружбе свидетельствует Вам глубокое уважение.

Очень приятно получить от Вас приглашение. Разрешите выразить горячие поздравления проведению Четырнадцатого международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», это большая честь для нас. Как известно, что это важное событие научного круга, пользуется прекрасной репутацией и оказывает значительное влияние на мир. Как я помню в 2018 году, на каждой конференции были собраны многие специалисты и таланты, и получены крупные результаты.

Как Вам уже известно, что кроме в ВАСД, я еще работаю в НПКСК. По плану работы с декабря я буду возглавлять рабочую группу по исследованию в разных регионах. Очень жаль, что не смогу принять участие в Вашей конференции. Заранее поздравляю Вас с успешным проведением конференции.

Охватившая планету пандемия COVID-19, к сожалению, оказала влияние на наше сотрудничество, но перспективы дальнейшего сотрудничества в будущем все еще весьма обширны. Нас весьма интересует Сетевая безопасность и мы ожидаем дальнейшего сотрудничества в подходящее время после эпидемии.

С уважением, Председатель Всекитайской Ассоциации по содействию дружбе

В.О. Запивахин

Эксперт Минобороны России

МИЛИТАРИЗАЦИЯ КИБЕРПРОСТРАНСТВА – ГЛАВНАЯ УГРОЗА МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

По оценкам Минобороны России, угроза милитаризации киберпространства[2] ставит ее на одно из первых мест в ряду существующих угроз и вызовов международному миру и стратегической стабильности.

Страны НАТО в 2016 году, объявив о признании киберпространства новой сферой ведения военных действий, создают боевые «киберкомандования», готовятся к проведению наступательных «кибероперациий» на тактическом, оперативном и стратегическом уровне или систематически проводятся «киберучения». Выделяются значительные финансовые средства на развитие наступательного «киберпотенциала» и разработку различных видов «кибероружия».

Наиболее далеко в деле милитаризации киберпространства продвинулись США. Особенно наглядно эта тенденция проявилась в годы правления нынешней администрации Д. Трампа, принявшей и реализующей на практике целый пакет военно-политических документов, определяющих планы военного строительства в киберпространстве как новой сфере ведения военных действий[3].

Поводом, побудившим Вашингтон к этой работе была объявлена якобы ведущаяся против США «информационная война». Противниками объявлены Россия, Китай, Иран и Северная Корея.

В чем она заключается, так и остается вопросом для мирового сообщества. Информационная война с этими странами признана в Белом доме более важной задачей, чем борьба с региональными противниками и террористами, которая была в центре внимания предыдущих американских стратегий в области обороны и безопасности.

За последние четыре года США предприняли ряд первоочередных мер:

- создана система киберкомандований, применение которых планируется в сфере наступательных и оборонительных операций;
- усилена интеграция дипломатических, экономических, финансовых, разведывательных, правоохранительных, военных и информационных инструментов проведения внешней политики;
- проведена оценка киберустойчивости систем управления силами ядерного и неядерного сдерживания;
- получила развитие национальная система кибероборонь;
- в интересах сдерживания стратегических конкурентов в мирное время и проведения военных действий в киберпро-

1 Статья подготовлена коллективом авторов в составе: генерал-лейтенант Дылевский И.Н., генерал-майор Базылев С.И., полковник Запивахин О.В., полковник в отставке Комов С.А., полковник Песчаненко К.О., полковник Юниченко С.П.

2 Киберпространство (cyberspace) - глобальный домен в пределах информационной среды, состоящий из взаимозависимых инфраструктур информационных сетей с хранящимися и циркулирующими в них данными, включая Интернет, сети передачи данных, компьютерные системы и используемые в них процессоры и контроллеры. (JP 3-12 Cyberspace Operations, 8 June 2018, p.100).

3 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, № 13800, The White House, Washington, DC, May, 11 2017; National Security Strategy of the United States of America, The White House, Washington, DC, December 2017; Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command, March, 2018; Summary of the National Defense Strategy. The United States of America. Sharpening the American Military's Competitive Edge, 2018; U.S. Department of Homeland Security. Cybersecurity Strategy. May 15, 2018.

странстве на тактическом и стратегическом уровнях;

- публично предъявлены ложные обвинения ряду юридических и физических лиц иностранных государств в совершении противоправных политически мотивированных действий (вмешательство в выборы, кибератаки на критическую информационную инфраструктуру, распространение дезинформации, пропаганда);
- проведены исследования новых форм и способов межгосударственного противоборства в киберпространстве, ориентированных на достижение победы даже при отсутствии превосходства в воздухе, на море, на земле и в космосе.

Для того чтобы достичь поставленных военно-политических целей правительство США использует весь диапазон имеющихся средств от привлечения государственных органов и неправительственных организаций, устанавливающих технические стандарты, до прямого дипломатического и санкционного воздействия, а также демонстрации и применения военной силы, в том числе с использованием созданной в США системы киберкомандований.

Подходы США к проведению операций в киберпространстве включают ряд новаций, к которым можно отнести:

1. Условное разделение киберпространства на синюю (американскую), красную (вражескую) и серую (нейтральную) зоны.
2. Разрешено на «законном основании» проводить кибероперации в любом иностранном киберпространстве («красной» и «серой» зонах) без уведомления органов власти этих государств на том основании, что киберпространство не имеет государственных границ.
3. Определено, что операции в киберпространстве могут проводиться не только в ответ на «злонамеренную деятельность» противника, но также в превентивном порядке с целью создания препятствий для осуществления противником такой деятельности.
4. Установлена прямая взаимосвязь и взаимозависимость между операциями в киберпространстве и информационными операциями, опирающаяся на положение о том, что киберпространство является частью информационного пространства.
5. Введено понятие «атаки в киберпространстве» (кибератаки), под которой понимаются действия в киберпространстве, приводящие к значимым негативным последствиям (деградации, разрушению или уничтожению) как в самом информационном пространстве, так и в других сферах жизнедеятельности человека. Такая атака приравнена к огневому поражению.

Внесение американскими стратегами в военный лексикон последнего термина следует считать весьма серьезным фактором.

По сути, американские военные специалисты признали, что проведение «атак в киберпространстве» является таким же применением военной силы, как и нанесение огневых ударов.

В настоящее время в школе СВ США в Форт-Гордоне (штат Джорджия) проводится подготовка специалистов связи, кибер- и радиоэлектронной борьбы, которых планируется задействовать в работе первого объединенного командования. Его оперативное развертывание планируется завершить в 2028 году[4].

Авторы новой американской стратегической парадигмы много внимания уделяют ее внешнеполитическому обеспечению. При этом усилия Госдепа США направлены не на предотвращение милитаризации киберпространства, а на обеспечение ее легитимности и поддержки государствами мирового сообщества, транснациональными корпорациями и мировой общественностью.

Таким образом, считаем, что запущенный по инициативе США процесс милитаризации глобального киберпространства неизбежно приведет к эскалации военной напряженности между членами мирового сообщества. Если он не будет остановлен, а разрушительный военный кибернетический потенциал продолжит наращиваться, в обозримой перспективе возможно появление вполне реальных людских и материальных потерь в результате его применения. В свою очередь, это будет свидетельствовать о том, что информационные технологии превратились в новое оружие, а киберпространство – в новую сферу ведения военных действий.

Минобороны России традиционно рассматривает глобальное информационное пространство в качестве зоны мира и добрососедских отношений между всеми членами мирового сообщества.

Только конструктивный диалог на различных международных площадках по всем вопросам использования информационных и коммуникационных технологий, затрагивающих проблемы в области МИБ, позволит сохранить мир и стабильность, не позволяя конфликтным ситуациям в информационном пространстве перерасти в реальное вооруженное противостояние между государствами.

Безусловно, одной из таких площадок является, созданная по инициативе Российской Федерации Рабочая группа ООН открытого состава, в которой может принять участие абсолютно любое государство в независимости от уровня развития ИКТ конкретных стран, являясь при этом полноценным членом мирового информационного пространства.

4 'Desperate Need For Speed' As Army Takes On Chinese, Russian, ISIS Info Ops, Sydney J. Freedberg JR., August 21, 2019, https://breakingdefense.com/2019/08/desperate-need-for-speed-as-army-takes-on-chinese-russians-isis-trolls/;
Army To Build New Info War Force – Fast, Sydney J. Freedberg JR., August 22, 2019, https://breakingdefense.com /2019/08/the-armys-information-warfare-build-up/

А.А. Воробьев
Директор, Координационный центр доменов .RU/.РФ

О ПРАКТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ КООРДИНАЦИОННОГО ЦЕНТРА ДОМЕНОВ .RU/. РФ В ЦЕЛЯХ УКРЕПЛЕНИЯ ДОВЕРИЯ И СТАБИЛЬНОСТИ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

Правила ответственного поведения государств в ИКТ-среде, как известно, одобрены резолюциями Генеральной Ассамблеи ООН. Вопросы практического применения этих правил сегодня выходят на первый план в связи с реальной угрозой потери принципов доверия и стабильности привычного всем нам Интернета как Глобальной сети. Такие опасения, в частности, содержатся в заключительном отчете Глобальной комиссия по стабильности киберпространства (GCSC) по результатам трехлетней работы. Драматизм содержания его первого абзаца – свидетельство важности документа и глубокого понимания его разработчиков своей ответственности за будущее одного из величайших изобретений человечества – киберпространства.

«Мы подошли к концу двадцатипятилетнего периода стратегической стабильности и относительного мира между крупными державами. Конфликты между государствами приобрели новые формы, и кибератаки играет ведущую роль в этой новой нестабильной среде. За последнее десятилетие количество и изощренность кибератак со стороны государственных и негосударственных субъектов увеличились, что угрожает стабильности киберпространства. Проще говоря, люди и организации не могут больше быть уверены в своей способности безопасно и надежно использовать киберпространство или быть уверенными в доступности и целостности услуг и информации».

Специалисты Координационного центра доменов .RU/.РФ принимают активное участие как в международных мероприятиях, посвященных вопросам управления Интернетом и обеспечения международной информационной безопасности, так и организуют площадки для обсуждения указанных вопросов в России. Эта работа на протяжении последних нескольких лет проводится в тесном партнерстве с Национальной Ассоциацией международной информационной безопасности (НАМИБ).

По итогам 10-го юбилейного национального Российского форума по управлению Интернетом (RIGF 2019) можно отметить следующее:

1. После многолетнего перерыва государство вновь присутствует на форуме как один из ключевых стейкхолдеров. Выступивший на открытии форума первый заместитель руководителя администрации Президента Российской Федерации Сергей Кириенко отметил, что Россия открыта для всех международных компаний, но при условии, что они соблюдают российское законодательство, в особенности законодательство о хранении персональных данных и налоговое.
2. Сохраняется большой интерес со стороны зарубежных стейкхолдеров, что подтверждено присутствием на форуме их представителей, – ООН и Совет Европы, ICANN и RIPE NCC (партнеры форума), национальные правительства, академическое сообщество (международное), гражданское общество (ISOC) и бизнес-сообщество.
3. Программа форума отражала все основные тренды, в ходе дискуссии были поставлены важнейшие вопросы и предложен российский взгляд, российские подходы к решению этих вопросов. Так, в полном соответствии с мировыми тенденциями в России создается стратегия развития искусственного интеллекта, мы работаем над повышением инклюзивности и возможностей равного доступа к вопросам управления Интернетом, рассматриваются вопросы информационной безопасности и защиты персональных данных.

В итоговой резолюции форума, которая была представлена на Глобальном форуме по управлению Интернетом в Берлине в ноябре 2019 года, отмечается, что представители многостороннего сообщества, следуя принципам взаимного уважения и доверия, подчёркивая свою приверженность высоким стандартам в области защиты прав и основных свобод человека как оффлайн, так и онлайн, отмечая важность использования новых эффективных форм взаимодействия между государством, компаниями, техническим сообществом и пользователями в целях построения открытой, стабильной и безопасной экосистемы Интернета, договорились соблюдать «общественные договорённости» в Интернете с чётким распределением ролей и ответственности всех заинтересованных сторон на основе следующих принципов:

1. Российское интернет-пространство является неотъемлемой частью глобальной сети, которая должна сохранить своё единство и открытость под равноправным управлением государствами её критическими ресурсами.
2. Государство гарантирует гражданам защиту в своей юрисдикции, обеспечивает управление, стратегическую устойчивость и безопасность своей инфраструктуры, защиту национального рынка ИТ-продукции и в то же время гарантирует его инновационность и открытость.

Развивает контакты по линии бизнес-структур всех стран, укрепляет государственно-частное партнёрство, активно развивает интернет-экономику, улучшает правила торговли в информационном пространстве, принимает шаги по разработке международных правил и стандартов в этой сфере.

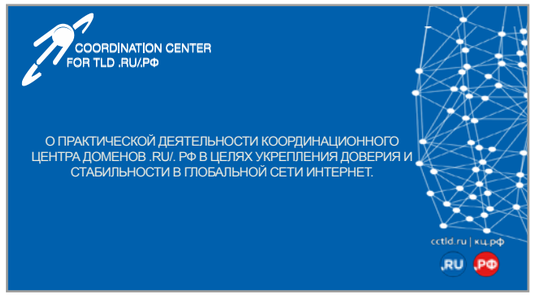
3. Государство создаёт прочную сбалансированную нормативно-правовую основу в сфере интернет-регулирования, которая, с одной стороны, поддерживает безопасное и устойчивое развитие экосистемы Интернета, предоставляет гарантии защиты граждан, национальных компаний и государства в целом, а с другой стороны – создаёт стимулы для инновационного развития, технологического прорыва, конкурентной и открытой среды для всех заинтересованных сторон. Разработка инструментов «мягкого права», саморегулирования, руководящих принципов, этических кодексов приветствуется и является важной частью «общественных договорённостей».
4. Транснациональные корпорации добросовестно выплачивают местные налоги соразмерно количеству пользователей и объёму оказанных услуг в этом государстве, на равных участвуют в развитии инфраструктуры, в том числе через налоговые отчисления.

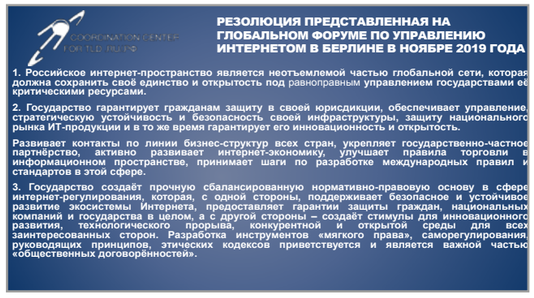
Уважают и соблюдают национальные законы, нормы этики и морали, менталитет государства (традиции, многообразие культур, религий, языков). Работают в условиях честной конкуренции, не монополизируя национальные рынки.

5. Государство эффективно защищает в Интернете персональные данные, принадлежащие его гражданам, регулируя их обработку на национальном уровне и при трансграничной передаче.

Транснациональные корпорации не пренебрегают правами человека и общественной безопасностью. Они подотчётны и ответственны перед государством и пользователями в отношении сбора, хранения и анализа персональных данных и несут ответственность за любые незаконные действия в отношении таких данных.

Государство и транснациональные корпорации совместными усилиями формируют систему доверия в Интернете, сохраняющую конфиденциальность





и личную безопасность пользователей и их информации.

Пользователи имеют право самостоятельно управлять своим личным пространством в Интернете, исключающим навязывание информации и влияние на его информационное поле. На любом этапе обработки данных запрашивается добровольное, чётко выраженное, информированное и однозначное согласие субъекта этих данных.

6. Государство обеспечивает равный и максимально широкий доступ к ресурсам Интернет всех населённых пунктов, учреждений и граждан, уделяя особое внимание уязвимым группам населения (дети, женщины, пожилые люди, инвалиды, люди с ограниченными возможностями и т.д.).

Совместно с заинтересованными сторонами повышают уровень цифровой грамотности населения, разрабатывают и внедряют специализированные программы и курсы для различных категорий населения (дети и молодёжь, предприниматели, женщины, население, проживающее в удалённых территориях), оказывают содействие населению в адаптации к новым технологиям.

7. Государство, транснациональные корпорации, пользователи формируют культуру доверия в Интернете, принимают меры по противодействию дезинформации, использованию сети для манипулирования общественным сознанием. Создают правовые, общественные фильтры для предотвращения попадания в Интернет любой противоправной, вредоносной, токсичной для пользователей информации, особенно для незащищённой детской аудитории. Усиливают защиту детей в Интернете, принимают законодательные и иные меры по противодействию порнографии, педофилии и насилию в отношении детей; создают в этих целях альянсы.

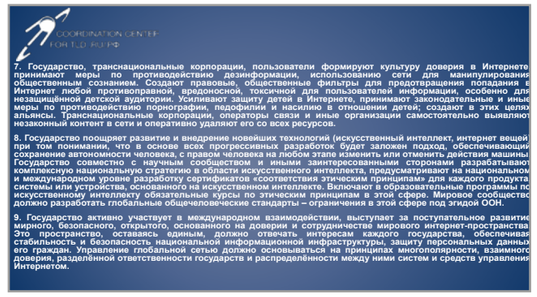
Транснациональные корпорации, операторы связи и иные организации самостоятельно выявляют незаконный контент в сети и оперативно удаляют его со всех ресурсов.

8. Государство поощряет развитие и внедрение новейших технологий (искусственный интеллект, интернет вещей) при том понимании, что в основе всех прогрессивных разработок будет заложен подход, обеспечивающий сохранение автономности человека, с правом человека на любом этапе изменить или отменить действия машины.

Государство совместно с научным сообществом и иными заинтересованными сторонами разрабатывают комплексную национальную стратегию в области искусственного интеллекта, предусматривают на национальном и международном уровне разработку сертификатов «соответствия этическим принципам» для каждого продукта, системы или устройства, основанного на искусственном интеллекте. Включают в образовательные программы по искусственному интеллекту обязательные курсы по этическим принципам в этой сфере. Мировое сообщество должно разработать глобальные общечеловеческие стандарты – ограничения в этой сфере под эгидой ООН.

9. Государство активно участвует в международном взаимодействии, выступает за поступательное развитие мирного, безопасного, открытого, основанного на доверии и сотрудничестве мирового интернет-пространства. Это пространство, оставаясь единым, должно отвечать интересам каждого государства, обеспечивая стабильность и безопасность национальной информационной инфраструктуры, защиту персональных данных его граждан.

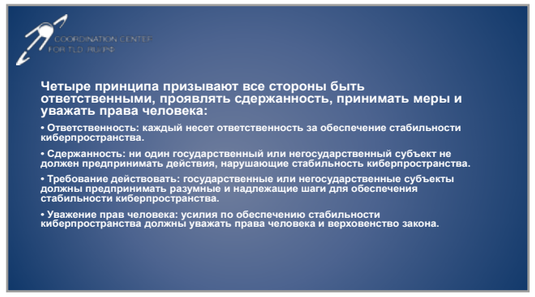
Управление глобальной сетью должно основываться на принципах многополярности, взаимного доверия, разделённой ответственности государств и распределённости между ними систем и средств управления Интернетом.



Очевидно, что нам есть с чем выходить к международному сообществу, мы не только не отгораживаемся и вовсе не пытаемся стать автономными, мы являемся полноправными участниками процесса, мы предоставляем площадку для конструктивного диалога, подчёркивая свою приверженность высоким стандартам в области защиты прав и основных свобод человека как оффлайн, так и онлайн. Нельзя недооценивать при этом важность использования новых эффективных форм взаимодействия между государством, компаниями, техническим сообществом и пользователями в целях построения открытой, стабильной и безопасной экосистемы Интернета.

Россия с успехом принимала во Владивостоке региональный Азиатско-Тихоокеанский форум по управлению Интернетом, голос России звучит на WSIS в Женеве, традиционно на высоком уровне наша страна представлена на Глобальных форумах по управлению Интернетом, к участию в которых всё активнее привлекаются депутаты российского парламента.

Россия выбрана страной проведения Глобального IGF в 2025 году, проводятся переговоры по проведению после пандемии в нашей стране и международной конференции ICANN – под это мероприятие рассматривается Москва, Санкт-Петербург и Сочи.



Говоря о вопросах обеспечения информационной безопасности, нельзя не отметить необходимость ответственного подхода к развитию системы DNS как важного элемента публичного ядра Интернета. Форум в Гармиш-Партенкирхене по праву занимает одно из ведущих мест в рейтинге мероприятий, посвященных обсуждению вопросов кибербезопасности. Это своего рода Давос в сфере информационной безопасности, важная часть международного диалога в области МИБ. Важнейшей темой пленарных заседаний последних лет остается проблема подорванного доверия государств в сфере информационно-телекоммуникационных технологий. Доверие – основа всех социальных институтов. Развитие ИКТ базировалось именно на доверии. Сегодня в области международной информационной безопасности в российских подходах особое место также уделено мерам по укреплению доверия. Гармишевский процесс нацелен на поиск направлений перспективного сотрудничества в тех сферах, где у всех заинтересованных сторон есть согласие, но нет реально работающего инструмента, помогающего достижению глобальных целей развития информационного общества.

Мы благодарим Национальную Ассоциацию международной информационной безопасности (НАМИБ) за предоставленную возможность обсудить на высоком экспертном уровне вопросы развития системы интернет-адресации как важного элемента публичного ядра Интернета и роли регистратуры национальных доменов в повышении цифровой грамотности пользователей. Для достижения последнего Координационный центр в партнерстве со специалистами в области информационной безопасности успешно реализует ряд социально-просветительских проектов, направленных на повышение цифровых компетенций интернет-пользователей, в том числе в сфере обеспечения информационной безопасности.

Особого внимания заслуживает обсуждение на площадке НАМИБ результатов выполнения международного исследовательского проекта, направленного на изучение вопросов практического применения норм, правил и принципов ответственного поведения государств в среде информационно-коммуникационных технологий. В этой работе приняли участие эксперты Института проблем информационной безопасности МГУ имени М.В. Ломоносова, Института «Восток-Запад» (США), Института кибербезопасности (Эстония) и Фонда «ИКТ для мира» (Швейцария). Экспертам удалось выявить основные проблемы, препятствующие применению международного права к ИКТ-среде. Для формирования системы международной информационной безопасности на основе суверенитета государств, необходимо более активно изучать правовые и технические аспекты делимитации и демаркации зон ответственности государств в ИКТ-среде. Решение этой задачи позволит приступить к созданию системы получения объективной информации об опасных инцидентах в ИКТ-среде, и системы атрибуции государств, вовлеченных в эти инциденты. На этой основе можно будет обеспечить применение норм Устава ООН, регулирующих отношения в области мирного разрешения международных споров, к инцидентам в ИКТ-среде.

Результаты реализации международного проекта могут быть использованы для совершенствования системы международного регулирования отношений в ИКТ-среде в направлении, способствующем снижению эскалации напряженности в глобальном информационном пространстве, повышению эффективности применения международного права для разрешения опасных ситуаций на объектах критической информационной инфраструктуры. Проделанная работа оказывает большое позитивное влияние на расширение сотрудничества экспертного сообщества в области формирования системы международной информационной безопасности.

Вставка:

Концепция Cyberstability из семи элементов представлена на рисунке.

Эта структура включает:

(1) взаимодействие с участием многих заинтересованных сторон;
(2) принципы кибербезопасности;
(3) разработка и внедрение добровольных норм;
(4) соблюдение норм международного права;
(5) меры доверия;
(6) наращивание потенциала;
(7) открытое обнародование и широкое использование технических стандартов, обеспечивающих устойчивость киберпространства.

После определения этой концепции Комиссия тщательно изучила три ее элемента:

- взаимодействие с участием многих заинтересованных сторон;
- принципы кибербезопасности;
- нормы.

Многостороннее взаимодействие требуется во многих международных соглашениях, но оно все еще не достигло компромисса. Некоторые продолжают считать, что обеспечение международной безопасности и стабильности почти полностью является обязанностью государств. На практике, однако, поле битвы в киберпространстве разрабатывается, развертывается и управляется в основном негосударственными субъектами, и мы считаем, что их участие также необходимо для обеспечения стабильности киберпространства. Более того, их участие неизбежно, поскольку негосударственные субъекты часто первыми реагируют на кибератаки и даже приписывают их себе.

Комиссия пришла к выводу, что эти негосударственные субъекты не только критически важны для обеспечения стабильности киберпространства, но и что они тоже должны руководствоваться принципами и соблюдать нормы.

Четыре принципа отражают эту точку зрения, призывая все стороны нести ответственность, проявлять сдержанность, принимать меры и уважать права человека:

- Ответственность: каждый несет ответственность за обеспечение стабильности киберпространства.
- Сдержанность: ни один государственный или негосударственный субъект не должен предпринимать действия, нарушающие стабильность киберпространства.
- Требование действовать: государственные или негосударственные субъекты должны предпринимать разумные и надлежащие шаги для обеспечения стабильности киберпространства.
- Уважение прав человека: усилия по обеспечению стабильности киберпространства должны уважать права человека и верховенство закона.

Комиссия также дала определение стабильности в киберпространстве:

«Стабильность киберпространства означает, что каждый может быть достаточно уверен в своей способности безопасно и надежно использовать киберпространство, где доступность и целостность услуг и информации, предоставляемых в киберпространстве и через киберпространство, как правило, гарантированы, где изменения управляются в относительном мире и где напряженность решаются без эскалации.

Публичное ядро имеет двойное назначение его можно использовать как в мирное время, так и в военное – для атаки. С ростом ядра и количества пользователей количество атак будет увеличиваться».

КРУГЛЫЙ СТОЛ № 1
МЕЖДУНАРОДНОЕ ПРАВО И МЕРЫ ДОВЕРИЯ В ИКТ-СРЕДЕ: ПОЛИТИЧЕСКИЕ И ПРАВОВЫЕ ПРОБЛЕМЫ

Модератор:
Стрельцов А.А., член Президиума Национальной Ассоциации международной информационной безопасности, Институт проблем информационной безопасности МГУ имени М.В. Ломоносова

В.П. Шерстюк
Сопредседатель оргкомитета Форума, советник Секретаря Совета Безопасности Российской Федерации, Президент Национальной Ассоциации международной информационной безопасности

А.А. Стрельцов
Член Президиума Национальной Ассоциации международной информационной безопасности, Институт проблем информационной безопасности МГУ имени М.В. Ломоносова

КЛЮЧЕВЫЕ ПРОБЛЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Международное сообщество прикладывает значительные усилия для создания открытой, безопасной, стабильной, доступной и мирной среды информационно-коммуникационных технологий (ИКТ-среды). Данный вопрос ежегодно рассматривается: на сессиях Генеральной Ассамблеи ООН; на заседаниях Группы правительственных экспертов, регулярно созываемой для предметного изучения угроз безопасности ИКТ-среды и поиска путей их решения; на региональных площадках (ОБСЕ, ШОС, ОДКБ, БРИКС, НАТО и других); на многосторонних и двусторонних встречах руководителей государств и других официальных лиц. В 2018 г. с целью обсуждения этих же проблем 73-ей сессией Генеральной Ассамблеи ООН создана Рабочая группа открытого состава.

Однако вся эта работа пока не приводит к снижению напряжения в отношениях между государствами в области безопасности использования ИКТ. Более того, в официальном докладе Госдепартамента США (от 20 октября 2020 г.), появляются намеки на возможность снижения порога применения вооруженной силы, включая ядерное оружие, в ответ на злонамеренное использование ИКТ против США.

Угрозы миру становятся все более опасными, в том числе и в области использования ИКТ. В то же время не прекращаются попытки некоторых государств мира использовать свое преимущество в экономическом развитии и превосходство в вооруженной силе для

разрушения основ международного права, для навязывания другим государствам представлений о должном международном порядке, базирующемся на неких правилах и представлениях о добре и зле, для придания легитимности применению силы в нарушение Устава ООН и, прежде всего, в обход Совета Безопасности ООН. Сохраняются разногласия между государствами по поводу подходов к определению приоритетов в области противодействия угрозам и взаимоприемлемым компромиссам. Это негативно отражается как на работе сессий Генеральной Ассамблеи ООН (2018 и 2019 гг.), так и Группы правительственных экспертов ООН по достижениям в области информатизации и коммуникаций в контексте международной безопасности (2016–2017 гг., 2018–2019 гг.).

Проявляя единство в понимании важности применения международного права к регулированию отношений в ИКТ-среде, члены международного сообщества существенно расходятся в представлениях о путях решения и этой задачи. Отсутствует общее видение подходов к разрешению противоречий в вопросе о методах и способах применения международного права в ИКТ-среде. Не удается согласовать позиции даже по вопросу о путях практической реализации правил ответственного поведения государств в ИКТ-среде, рекомендованных консенсусом Группой правительственных экспертов (2015 г.).

Все это позволяет сделать вывод о том, что цели, поставленной Генеральной Ассамблеей ООН и заключающейся в создании открытой, безопасной, стабильной, доступной и мирной среды информационно-коммуникационных технологий, остаются недостижимыми. Международное право пока не стало инструментом, способным на основе международного сотрудничества предотвращать использование ИКТ для нанесения ущерба правам и свободам человека и гражданина, законным интересам коммерческих и некоммерческих организаций в области информационной деятельности, а также деятельности государственных органов по обеспечению безопасности использования информационной инфраструктуры, которая является общественным благом глобального характера.

Как отметил 26 ноября 2020 г. на заседании коллегий министерств иностранных дел Российской Федерации и Белоруссии Министр иностранных дел Российской Федерации Сергей Лавров: «В нашей повестке дня стоит вопрос международной информационной безопасности. <…> Очевидно, что без универсальных договоренностей мир рискует погрузиться в киберхаос, последствия которого могут оказаться катастрофическими».

Одним из факторов, обусловливающим сложившееся положение, является новизна ИКТ-среды как пространства международных отношений и его существенные отличия от традиционных пространств международного сотрудничества.

С правовой точки зрения ИКТ-среда представляет собой юридическую фикцию, заключающуюся в том, что искусственной, технической инфраструктуре приписывают свойства территории государства и на нее распространяют государственный суверенитет. При этом при взаимодействии автоматизированные системы и объекты, другие объекты информационной инфраструктуры, включая технические устройства, системы и сети, использующие ИКТ для решения задач автоматизации процессов обработки и передачи информации, характеризуются цифровыми идентификаторами, которые не связаны международными нормативными актами с территорией того или иного государства.

Вследствие этого пространственные пределы суверенитета государств в ИКТ-среде остаются неопределенными. Каждое государство определяет эти пределы в соответствии с представлениями о границах распространения на объекты ИКТ-среды его национальной юрисдикции и возможностями применения.

Другим важным отличием ИКТ-среды от традиционных пространств применения международного права является виртуальный характер информации, обрабатываемой и передаваемой в этой среде, а также процессов реализации используемых для этого ИКТ. Следствием этого является сложность объективной фиксации нарушений функционирования объектов информационной инфраструктуры третьими лицами (свидетелями), а также установления причин возникновения таких нарушений.

Ввиду неопределенности международных обязательств государств в ИКТ-среде и отсутствия договоренностей о процедуре сбора сведений об инцидентах в ИКТ-среде сложившаяся модель применения международного права не предусматривает возможности использования закрепленных Уставом ООН средств обеспечения международного мира и безопасности (мирное разрешение споров, разбирательство дел Международным Судом, рассмотрение в Совете Безопасности ООН).

Наконец, третья особенность ИКТ-среды заключается в том, что отношения по поводу предоставления цифровых идентификаторов для включения объектов информационной инфраструктуры в систему глобального взаи-

Ключевые проблемы правового обеспечения МИБ

Key issues of legal support for International information security

Президент НАМИБ, Владислав Шерстюк
Vladislav Sherstyuk, NAIIS President

Член Президиума НАМИБ, заведующий отделом, ИПИБ МГУ имени М.В.Ломоносова, Анатолий Стрельцов

Anatoly Streltsov, Member of the NAIIS Presidium, head of Department, IPIS of of Lomonosov Moscow state University

Международное право в ИКТ-среде International law in the ICT-environment

- Международное право, и, в частности, Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной ИКТ-среды (Доклады ГПЭ ООН 2013, 2015 гг.)
- International law, in particular the United Nations Charter, is applicable and essential for maintaining peace and stability and building an open, secure, peaceful and accessible ICT environment (UN GGE Reports 2013, 2015)

Международные отношения в ИКТ-среде International relations in the ICT-environment

- Количество опасных ситуаций в ИКТ-среде ежегодно увеличивается, мир приближается к катастрофе. В то же время закреплённые в Уставе ООН мирные средства разрешения международных споров, возможности рассмотрения дел в Международном Суде и определения существования угрозы миру вследствие использования ИКТ, в Совете Безопасности ООН не реализуются.
- The number of dangerous situations in the ICT-environment is increasing every year, the world is going to a catastrophe. At the same time, the UN Security Council does not implement enshrined in the UN Charter peaceful means of resolving international disputes, the possibility of considering cases in the International Court of Justice and defining the existence of a threat to peace due to the use of ICTs.

Существующая модель применения МП Existing model of International law application

- Применение международного публичного права в ИКТ-среде базируется на суверенном праве государств определять существование угроз национальной безопасности и принимать меры противодействия этим угрозам. При отсутствии универсальных договоров для определения должного поведения государств в ИКТ-среде используется метод аналогии права.
- The application of public international law in the ICT-environment is based on the sovereign right of States to determine the existence of threats to national security and take measures to counter these threats. In the absence of universal treaties, the method of law analogy is used to determine the proper States behavior in the ICT-environment.

Причина кризиса модели применения МП The reason for the crisis of the International Law application model

- Существующая модель применения международного права государствами не предусматривает применение правовых средств обеспечения международного мира и безопасности в ИКТ-среде (мирное разрешение споров, разбирательство дел Международным Судом, рассмотрение в Совет безопасности ООН) - неопределенность обязательств государств и сведений об инцидентах).
- The existing model of International law application by States does not provide the use of legal means to ensure international peace and security in the ICT-environment (peaceful settlement of disputes, proceedings by the International Court of Justice, consideration by the UN Security Council)-uncertainty of State obligations and information about incidents).

Предложение Initiative

- Изменить модель применения международного публичного права в ИКТ-среде. Поставить в основу модели прогрессивное развитие МП одновременно с соответствующим развитием системы международного технического регулирования. Для применения правил ответственного поведения в ИКТ-среде необходимо решить следующие ключевые проблемы.
- To change the model of public international law application in the ICT-environment. To base the model on the progressive development of international law simultaneously with the corresponding development of the international technical regulation system. To apply the rules of responsible behavior in the ICT-environment, the following key issues need to be addressed.

Проблема 1 (демаркация и делимитация)

Issue 1 (demarcation and delimitation)

- Закрепление в международных договорах цифровых идентификаторов объектов ИКТ-среды, находящихся под суверенитетом государств и на которые распространяется международный правовой режим безопасности, а также создание международных норм технического регулирования, обеспечивающих надежную идентификацию этих объектов.
- Fixing in international agreements digital identifiers of ICT-objects that are under the States sovereignty and are objects to the international legal security regime, as well as creating international technical regulation norms that ensure reliable identification of these objects.

Проблема 2 (правовой режим безопасности объектов)

Issue 2 (legal regime for objects security)

- Закрепление в международных договорах обязательств государств по обеспечению безопасности использования и устойчивости функционирования объектов ИКТ-среды, находящихся под их суверенитетом, и создание международных норм технического регулирования, обеспечивающих безопасность и устойчивость функционирования объектов ИКТ-среды.
- Fixing in international agreements States obligations to ensure the safety of use and stability of the functioning for the ICT-objects that are under their sovereignty, as well as creating international technical regulation norms that ensure security and functioning stability for the ICT-objects.

модействия, регулируются нормами международного частного права. Отношения по поводу использования средств, устройств, систем и сетей информационной инфраструктуры для обеспечения информационной деятельности субъектов жизнедеятельности общества, регулируются нормами национального законодательства. Вследствие этого правовое регулирование отношений между субъектами информационной деятельности в глобальной ИКТ-среды, а также субъектами, обеспечивающими функционирование объектов ИКТ-среды в составе глобальной информационной инфраструкткры, носит сложный, мультиюрисдикционный характер.

Данные обстоятельства привели к возникновению нового явления в области международного регулирования отношений в ИКТ-среде – добровольные, необязательные нормы, правила и принципы ответственного поведения государств в ИКТ-среде, принятых консенсусом рекомендаций Группы правительственных экспертов (2015 г.), предложенных 70-ой сессией Генеральной Ассамблеи ООН для рассмотрения государствами.

Правила ответственного поведения условно могут быть объединены в группы, действие которых направлено на регулирование отношений в следующих областях:

- поддержание мира и безопасности;
- обеспечение прав человека;
- обеспечение безопасности объектов критической информационной инфраструктуры;
- обеспечение безопасности продуктов ИКТ.

Исходя из анализа резолюций 73-ей и 74-ой сессий Генеральной Ассамблеи ООН, Правила ответственного поведения в настоящее время рассматриваются государствами как приемлемая основа для развития международного регулирования отношений в ИКТ-среде. На данном этапе правила ответственного поведения не имеют характера правовых или политических норм и могут быть отнесены скорее к неким моральным ориентирам.

В то же время международным сообществом поставлена задача поиска способов обеспечения их практического применения в международных отношениях.

Как показывают исследования, выполненные институтом проблем информационной безопасности МГУ имени М.В. Ломоносова, а также международной группой экспертов в рамках реализации проекта Международного исследовательского консорциума информационной безопасности, на этом пути возникают существенные трудности. Предметом этих исследований были правила ответственного поведения государств в области обеспечения безопасности объектов критической информационной инфраструктуры.

Как показали эти исследования, для оказания позитивного воздействия на состояние международных отношений, практическое применение данных правил должно базироваться на нормах и принципах международного права.

Применительно к правилам ответственного поведения государств в области безопасности критической информационной инфраструктуры, возникают, не имеющие пока решения, вопросы:

- определение источников международного права для оказания помощи другим государствам в чрезвычайной ситуации в ИКТ-среде;
- приписывание государствам ответственности за осуществление злонамеренных действий в ИКТ-среде;
- проведение расследований международных инцидентов в ИКТ-среде;
- имплементация правил ответственного поведения государств в ИКТ-среде.

Анализ публикаций по вопросам применения международного права для регулирования отношений в ИКТ-среде, позволяет сделать вывод о том, что российские и зарубежные эксперты сосредоточились в основном на разработке двух направлений:

- применение аналогии права (например, так называемое «Таллиннское руководство по информационным операциям»);
- разработка новых мер укрепления доверия и правил ответственного поведения (например, итоговый отчет Глобальной комиссии по киберстабильности. 2019 г.).

Представляется, что при практическом применении предложений, полученных в рам-

ках разработок по этим направлениям, тоже потребуется найти взаимоприемлемые решения по определению пространственных пределов суверенитета государств в ИКТ-среде, сбору объективной информации об инцидентах, а также по международному правовому режиму безопасности объектов ИКТ-среды.

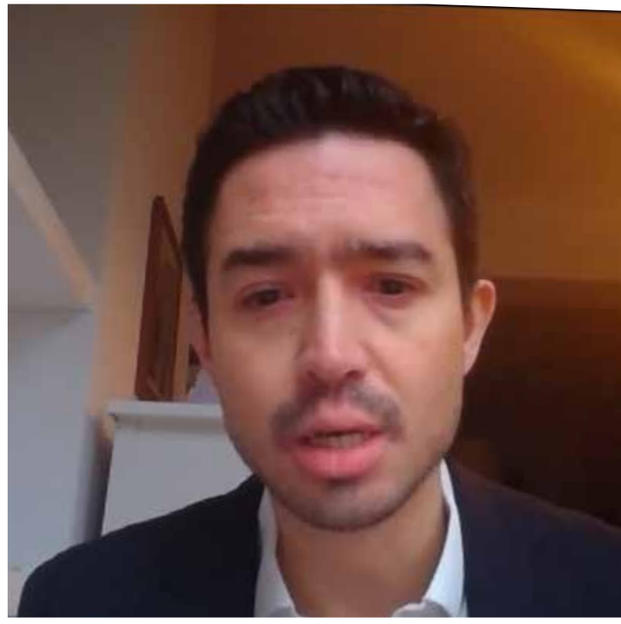
В связи с этим, более перспективным направлением исследований представляется прогрессивное развитие международного права в объеме, необходимом для решения конкретных задач международного сотрудничества.

Представляется, что для обеспечения безопасности объектов критической информационной инфраструктуры ключевое значение имеет создание универсальных источников международного права для регулирования следующих групп международных отношений.

1. Отношения в области демаркации и делимитации границ зон ответственности государств в ИКТ-среде. Применительно к отношениям в области безопасности объектов критической информационной инфраструктуры решение проблемы может быть осуществлено посредством закрепления в международном договоре цифровых идентификаторов объектов данной инфраструктуры, находящихся под суверенитетом государств и на которые распространяется международный правовой режим безопасности, а также создание международных норм технического регулирования, обеспечивающих надежную идентификацию этих объектов.
2. Отношения в области установления правового режима безопасности объектов критической информационной инфраструктуры. Проблема может быть решена закреплением в международном договоре обязательств государств по обеспечению безопасности использования и устойчивости функционирования объектов ИКТ-среды, находящихся под их суверенитетом, а также по применению международных норм технического регулирования, обеспечивающих безопасность и устойчивость функционирования объектов ИКТ-среды для мониторинга ситуации и сбора сведений для обмена с заинтересованными субъектами международного права.
3. Отношения в области фиксации фактов нарушения международного правового режима безопасности объектов критической информационной инфраструктуры. Проблема может быть решена посредством закрепления в международном договоре понятия «международный инцидент в ИКТ-среде» и обязательств государств по применению международных норм технического регулирования, обеспечивающих надежную идентификацию нарушения безопасности и устойчивости функционирования объектов ИКТ-среды.
4. Отношения в области применения средств мирного разрешения спорных ситуаций в ИКТ-среде. Проблема может быть решена посредством закрепления в международном договоре процессуальных норм выявления государств, вовлеченных в «международный инцидент в ИКТ-среде», и обязательств государств, которым приписана вовлеченность в «инцидент», участвовать в мероприятиях по мирному разрешению опасной ситуации, связанной с «инцидентом в ИКТ-среде», а также предоставлять имеющуюся информацию, собираемую в соответствии с международными нормами технического регулирования.

Для подготовки конкретных предложений по нормам международного права и нормам технического регулирования, которые могут быть закреплены в соответствующих универсальных международных нормативных актах, представляется важным проведение исследований с участием экспертов всех заинтересованных сторон.

Адам Купер
Старший руководитель программы "Глобальное сотрудничество в киберпространстве", Центр гуманитарного диалога, Швейцария



ПРОБЛЕМА РАЗРАБОТКИ ЭФФЕКТИВНЫХ МЕР УКРЕПЛЕНИЯ ДОВЕРИЯ: НАБЛЮДЕНИЯ С ТОЧКИ ЗРЕНИЯ ПОСРЕДНИЧЕСТВА И ДИАЛОГА

Введение

- Всем доброе утро. Я поделюсь некоторыми размышлениями о мерах доверия (МД) с точки зрения посредничества и диалога. Я придерживаюсь данной позиции, поскольку именно на ней специализируется организация, в которой я работаю, – Центр гуманитарного диалога, также известный как HD. Штаб-квартира нашей организации находится в Женеве, и мы специализируемся на диалоговых процессах, направленных на мирное разрешение и урегулирование конфликтов. Мы выполняем эту работу в течение последних 20 лет в строго независимой и нейтральной манере.
- В рамках HD мы создали отдел, который занимается адаптацией посредничества и диалога к особым характеристикам конфликтов в киберпространстве, или международной информационной безопасности, которые, безусловно, значительно отличаются от традиционных форм вооруженных конфликтов.
- И мы полагаем, что существует целый ряд тем, по которым государствам необходимо вести откровенный диалог, включая МД.
- Мы придерживаемся реалистичного подхода к этой работе, осознавая, что существуют фундаментальные различия между государствами в части их концепций международной информационной безопасности, которые вряд ли будут устранены в ближайшее время.
- Но мы также считаем, что необходимо обсудить, существуют ли при этом и общие интересы. Это могут быть механизмы по преодолению той напряженности, которая действительно существует, или мирного урегулирования разногласий путем диалога.
- Я верю, что при наличии надлежащей политической воли и правильного технического подхода эти решения могут быть найдены.
- И в такое время, как сегодня, когда мир страдает от пандемии, международное сотрудничество необходимо как никогда.

Эффективные МД

- Конечно, тема МД не нова. Она обсуждается уже много лет. И было опробовано много различных подходов. И поэтому я задаю вопрос, который очень легко задать, но так трудно ответить: в действительности, сколько доверия на самом деле было сформировано мерами укрепления доверия? Насколько они эффективны?
- Я считаю, что до сих пор мы добились лишь ограниченного успеха, особенно в отношениях между великими державами, которые являются ключевыми для глобальной стабильности. Но я также считаю, что именно поэтому нам и нужен диалог для разработки более эффективных моделей на будущее. Я постараюсь высказать некоторые соображения по этому поводу и предложения на будущее.
- Во-первых, мы должны осознать, что на разных уровнях применялись раз-

ные подходы, и тщательно проанализировать их. Мы также должны признать значительные усилия, предпринятые многими государствами и организациями в ходе этой работы – многосторонние (РГОС, ГПЭ), региональные (ОБСЕ, ШОС, АРФ, АСЕАН и др.) и двусторонние.

- Эти усилия действительно преследуют некоторые общие цели. Часто МД направлены на повышение прозрачности, сотрудничества и стабильности. Но ключевой вопрос заключается в том, что это за МД, стремящиеся укрепить доверие.
- Работа на многостороннем и региональном уровнях важна по многим причинам и, несомненно, должна продолжаться. Но едва ли они станут платформами для урегулирования разногласий между великими державами.
- Это объясняется разными причинами. Эти государства обладают возможностями, превосходящими возможности других. У них хорошо развиты государственные институты и политика. И отношения между ними неизбежно приобретают более геополитический характер.
- И на данный момент, в текущей международной обстановке, уровень доверия между ними остается низким.
- Поэтому нам нужен метод, учитывающий эту реальность и ориентированный на конкретный подход к “МД в условиях низкого доверия”.

Позвольте мне предложить 5 принципов того, на чем должен основываться диалог по МД в условиях низкого доверия:

1. **Реализм.** Мы должны быть реалистами в отношении того, что МД могут и чего не могут достичь. Они не являются заменой политической воли. МД могут помочь предотвратить неумышленную или непреднамеренную эскалацию, но, если одно государство намерено обострить конфликт, МД не могут этого предотвратить. Когда я говорю о реализме, я также имею ввиду, что диалог должен основываться на откровенном понимании интересов государств. Более чем вероятно, что угрозы, которые одна страна воспринимает как наиболее важные, будут отличаться от тех, которые оцениваются таким образом другой страной. Но, лучше понимая приоритеты друг друга, мы с большей вероятностью сможем вести диалог, который удовлетворит основные интересы каждой стороны.
2. **Общее понимание прошлых соглашений.** Если мы не будем переосмысливать то, что было сделано до сих пор, мы не сможем это улучшить. Многое из того, что до сих пор предпринималось в отношении МД, заимствовано из традиционной практики контроля над вооружениями. Наличие горячих линий, обмен доктринами и так далее. Но перевести эти механизмы в область информационной безопасности было очень сложно. Поэтому мы должны иметь общее понимание того, что было эффективным, а что нет.
3. **Признание того, что обсуждение МД будет проходить по мере продолжения нормативных дебатов.** Под нормативными вопросами я имею в виду такие темы, как важность суверенитета, применимость международного права и так далее. Я бы предположил, что нам необходимо продолжать обмен мнениями по этим темам, поскольку они важны для определения того, что является допустимым поведением, а что нет, и влияют на то, как МД воспринимаются и применяются на практике. Но я бы также предположил, что мы вполне реалистично относимся к тому, что эти нормативные дебаты вряд ли будут урегулированы в ближайшее время и не должны ограничивать прогресс в других областях.
4. **Механизмы верификации.** Очевидно, что предыдущие соглашения пострадали из-за расходящихся представлений относительно их выполнения. Эту задачу решить трудно. Когда одно государство говорит, что другое нарушило соглашение, другое государство, как правило, просто отрицает это. Кроме того, трудно предоставить доказательства в области, которая по своей природе скрыта, поэтому прозрачность не всегда возможна. У нас нет четких стандартов и протоколов в этой области, поэтому нам нужен диалог, который касается этой темы и определяет, какие механизмы могут быть лучшими.
5. **Определение сфер общего интереса.** Вопросы, затрагиваемые ООН, такие как защита критической инфраструктуры, очень важны. Но их трудно решать, не найдя конкретных областей, которые в интересах государств должны быть защищены. Как и другие спикеры, я бы сказал, что мы должны начать с подхода “снизу-вверх” и сосредоточиться на конкретных инфраструктурах – особенно тех, которые являются общими для всей международной системы. Пандемия COVID-19 может быть одной из возможных сфер для сотрудничества – от защиты государственных медицинских учреждений до исследований и распространения вакцин.

Я считаю, что эти пять принципов помогут нам приблизиться к атмосфере международного сотрудничества. Прогресс будет нелегким – и он зависит от факторов, которые находятся вне нашего контроля, – но мы обязаны найти области сотрудничества там, где это возможно.

Санжай Гоэл
Профессор, Университет штата Нью-Йорк, США

УПРАВЛЕНИЕ МИЛИТАРИЗАЦИЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ОГРАНИЧЕНИЕ ЕЕ НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

Прямо перед нами развивается новая гонка вооружений, имеющая огромные стратегические последствия для военных факторов и общества, с подстерегающими опасностями, которые угрожают будущей стабильности мира. Искусственный интеллект (ИИ) стал ключевым катализатором развития новых технологий и, как и все великие технологические достижения, нашел свой путь в национальные вооруженные силы. Государства в настоящее время вовлечены в двустороннюю войну, чтобы получить стратегические рычаги воздействия: военные и экономические. Я хочу обсудить ключевые военные технологии, которые в настоящее время разрабатываются с использованием ИИ, а также потенциал погрешностей и ошибок, которые могут привести к непреднамеренным конфликтам.

Во-первых, ИИ широко применяется в разведке, наблюдении и рекогносцировке. При огромных объемах генерируемых видеоматериалов люди не могут проверить все визуальные данные. ИИ все чаще используется для проверки видеозаписей с беспилотных летательных аппаратов для выявления возможной враждебной деятельности. Это уже стало обычным явлением в полицейской работе, когда полиция активно использует беспилотники для выявления и отслеживания уличных преступников. Это, очевидно, имеет последствия для частной жизни простых граждан и поднимает вопросы о нашей возможности быть анонимными и иметь частную жизнь даже в публичных местах или во время участия в широкой социальной деятельности. Китай использует слежение на основе ИИ с программным обеспечением распознавания лиц для наблюдения за своими гражданами в более чем 70 городах. (Human Rights Watch, 2019, Scharre, 2019). Они также экспортируют эти возможности, обучая должностных лиц авторитарных режимов в более чем 30 странах инструментам и практикам мониторинга поведения и контроля общественного мнения на основе искусственного интеллекта (Scharre, 2019).

Второе распространенное применение ИИ заключается в разработке социальных ботов в целях дезинформации. Боты на основе ИИ, которые производят язык, подобный человеческому, используются для кампаний по дезинформации, что делает учетные записи, созданные с помощью ИИ, трудно отличимыми от обычных. Эти боты используются для дестабилизации иностранных правительств и вмешательства в выборы по всему миру.

В-третьих, военные учреждения встраивают инструменты на основе ИИ для защиты сети, чтобы автоматически и автономно искать отклонения, для более быстрой идентификации и реагирования, чем это было бы возможно с помощью обычных операторов. Кроме того, эти организации рассматривают возможность использования ИИ для интеграции информации в воздушное, космическое, морское, наземное и киберпространство, формируя единый источник оперативной информации благодаря датчикам в этих областях.

Возможно, наиболее значительным преобразованием военного использования ИИ является разработка автономных транспортных средств, где ИИ используется для разведки, чтобы распознавать препятствия, собирать данные сенсоров, планировать навигацию и общаться с другими транспортными средствами, часто в многочисленном составе. Они предназначены для обезвреживания самодельных взрывных устройств, наблюдения и навигации на суше. Разрабатываются автоматические противолодочные системы для слежения за подводными лодками противника. SeaHunter, разрабатываемый для ВМС США, работает за небольшую часть стоимости пилотируемого корабля и показывает фантастические результаты в рабочих испытаниях. Беспилотники используются для подавления сетей связи, в электронных атаках, для огневой поддержки и для уничтожения средств ПВО. Рои беспилотников уже тестируются в качестве ударной силы во время конфликтов, таких как армяно-азербайджанский конфликт, когда рои беспилотников израильского производства Harpy, Harop и Orbiter уничтожили противовоздушную оборону в Нагорном Карабахе. Военное использование, подобное этому, очевидно, побудит другие мировые державы вкладывать более значительные средства в аналогичные технологии.

Беспилотные летательные аппараты в настоящее время являются ключевым элементом возможностей для вооруженных сил – от сбора разведданных до применения в военных операциях. Но что произойдет, если наша собственная технология обернется против нас? Станут ли те же технологии доступны террористическим организациям и правительствам-изгоям для ведения этнических войн в своих собственных странах? Есть технологии, которые должны заставить нас всех задуматься, такие как беспилотники-убийцы, которые используются для уничтожения вражеских целей. Более ранние версии этой технологии использовали оператора-человека, который смотрел на изображения и нажимал кнопку “убить”, если это требовалось. Новые беспилотники используют программирование на основе ИИ для автоматического определения вражеских целей и совершения убийства без участия человека.

До 11 сентября беспилотники использовались исключительно для наблюдения, и их полезность была в значительной степени проигнорирована ВВС США. Военно-воздушные силы никогда не рассматривали беспилотные летательные аппараты (БПЛА) в качестве подлинных самолетов, так как на них не летали пилоты, подвергающие свою жизнь риску. Необходимость изменила этот образ мышления: Predator и, в конечном счете, его гораздо более крупный родственник, Reaper, были оснащены ракетами, которые могли стереть с лица земли гостиную, полную предполагаемых террористов, обычно сохраняя при этом дом по соседству нетронутым.

Планы ВВС заменить Reaper новым дроном-охотником-убийцей были раскрыты в рамках недавней публикации закона “О свободе информации”. Беспилотник повышенной мощности будет обладать комбинированными возможностями разведки, наблюдения и рекогносцировки при гораздо большей автономии. В то время как “Reaper” управляется экипажем из двух человек, сидящими в трейлере порой за тысячи миль от него, управляющими им через спутник, новый беспилотник, напротив, будет характеризоваться автономными возможностями благодаря Skyborg, передовому ИИ, который разрабатывается исследовательской лабораторией ВВС (Axe, 2020).

Представьте себе оборонительную операцию, в которой беспилотник направляется шпионить за территорией противника. Противник идентифицирует беспилотник, но вместо того, чтобы отключить его, компрометирует датчики (видение, сонар и т. д.), чтобы ввести ложные данные. Действия, основанные на таких данных, могут привести к ошибочной тактике, а в худшем случае даже к жертвам, которых можно было бы избежать.

Куда более важный вопрос заключается в том, ответственно ли позволять машинам принимать автономные решения с последствиями для человеческой жизни? Где же она кончается? Будем ли мы участвовать в целенаправленных убийствах; дадим ли свободу дронам и позволим ли им совершать необратимые и серьезные действия?

Что происходит во время открытой вражды между двумя странами, такими как Армения и Азербайджан? Будем ли мы от безысходности использовать беспилотники, чтобы сбрасывать ракеты на критически важные объекты инфраструктуры, такие как ядерные реакторы, электростанции и телекоммуникационные сети?

ПРОТИВОРАКЕТНАЯ ОБОРОНА

Управляемые человеком системы противоракетной обороны подвергаются угрозе

со стороны подавляющей силы кластерных ракетных атак. ИИ перешагнул в конструкторское мышление, чтобы способствовать автоматическому обнаружению кластерных ударов и запуску противоракет. Эти системы ИИ будут характеризоваться намного более быстрым временем реагирования и смогут нанести более эффективный оборонительный удар. Может ли оператор-мошенник инсценировать атаку, чтобы добиться ответа от системы противоракетной обороны? Хотя ИИ предлагает решения этих вопросов, при их реализации также возникают значительные риски.

Некоторые военные технологии искусственного интеллекта опираются на компьютерное зрение, которое способно распознавать цели для атаки по изображениям. Мы десятилетиями использовали одни и те же технологии слежки, но сейчас ставки гораздо выше. Например: 1) любая ошибка в ИИ может привести к уничтожению жизни и имущества гражданского населения, например, система ИИ ошибочно принимает школьный автобус за военную машину; 2) хакер может проникнуть в автономную систему вооружения и использовать ее в целях запугивания людей или разжигания конфликта; или 3) производители в сговоре с национальными правительствами могут оставить лазейки в импортных технологиях, точки доступа, которые могут быть задействованы в более поздний момент времени.

Системы искусственного интеллекта сталкиваются с риском внедрения мошеннических данных, злонамеренно отправленных для сбоя их классификационной модели (например, ошибочная классификация изображений для распознавания лиц может позволить злоумышленникам избежать обнаружения). Основной причиной этих уязвимостей безопасности является общая нехватка прозрачности в системах ИИ, что делает их доступными для использования в рамках конкурирующих методов машинного обучения, такими как уклонение, отравление и бэкдор-атаки (NIST, 2019). Недостаток прозрачности или понимания руководящих алгоритмов и механизмов, лежащих в основе функционирования ИИ, является ключевым риском систем ИИ, поскольку они не могут быть протестированы и исправлены, а только обучены и переобучены. Таким образом, подотчетность или ответственность за ошибки, как злонамеренные, так и безобидные, не может быть установлена. Например, злоумышленники могут внедрить вредоносные данные на этапе обучения, чтобы повлиять на выводы моделей ИИ, или добавить небольшое искажение к исходным образцам на этапе заключения, чтобы изменить его итог. Злоумышленники также могут внедрить бэкдоры в модели для запуска целевых атак или извлечения параметров модели или обучающих данных из результатов запросов. Затем параметры модели могут быть изменены, чтобы сделать систему некорректной или изменить ее целевую ориентацию.

Эта потребность в прозрачности стала очевидной для кибербезопасности, управляемой ИИ, особенно если учесть, что одни и те же инструменты, разрабатываемые и используемые для защиты информации конечных пользователей на индивидуальном и корпоративном уровнях, используются не только преступниками, но и военными, и разведывательными службами. Потенциальные последствия “решений”, принимаемых в масштабе автономных систем вооружения и войны, проясняют это. Как отмечает Тим Стивенс: “Алгоритмы и автоматизация также создают новые сферы генерации знаний, одновременно затрудняя точные вычисления, которые приводят к определенным результатам. Это привлекает внимание к проблемным аспектам делегирования мышления машинам, поскольку предвещает сокращение возможностей для содержательного надзора и регулирования” (Stevens, 2020).

ИНСТРУМЕНТЫ, ОСНОВАННЫЕ НА ИИ, МОГУТ КАК ОБЛЕГЧИТЬ ВЗЛОМ, ТАК И БЫТЬ ВЗЛОМАННЫМИ

Selex Galileo, многомиллиардный американо-итальянский технический военный подрядчик, разрабатывает небольшой беспилотник специально для ведения радиоэлектронной войны и сопутствующих кибератак. Главным образом он предназначен для электронного разрушения ракетных систем класса “Земля-воздух”. Имея на борту устройство для радиоэлектронной борьбы весом всего 8,8 фунта, он способен лететь со скоростью чуть ниже 150 миль в час и оставаться в воздухе по крайней мере час. За это время беспилотник способен нарушить работу систем связи, таких как Bluetooth, или нарушить работу Wi-Fi на объектах.

Израильская фирма Septier Communications разработала беспилотник для перехвата и прослушивания телефонных звонков и данных, проходящих через смартфоны. Он имеет 90-минутное время полета и максимальную скорость около 30 миль в час. Компания оснащает беспилотник одним из своих сетевых перехватчиков, который может прослушивать сети 2G, 3G и 4G. Максимальная дальность перехвата беспилотника составляет 1 км, что делает его физически незаметным для цели. (O’Neill, 2019).

Аналитики по безопасности продемонстрировали способность перехватывать и брать под контроль беспилотник пользователя, из которого злоумышленники могут извлекать данные, включая траекторию его полета и любые сделанные изображения или видео. Они также могут контролировать полет беспилотника, тем самым создавая угрозу для безопасности близлежащих самолетов и персонала, сообщает Федеральное авиационное управление (Arampatzis, 2019).

ГОНКА ВООРУЖЕНИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Глобальные военные расходы на автономные системы вооружения и ИИ, строго говоря, согласно прогнозам, достигнут 16 и 18 миллиардов долларов соответственно, к 2025 году (Sander and Meldon, 2014; Research and Markets, 2018). Соединенные Штаты, Китай и Россия наращивают гонку вооружений в системах на основе ИИ. США лидируют, и прежде всего потому, что они были одним из первых двигателей этого процесса и активно поддерживали исследования в области гражданского применения ИИ (SIPRI, 2019). Еще два субъекта, быстро развивающихся в этой области, – это Южная Корея и Европейский Союз (Haner &Garcia, 2019).

США

США инвестировали 1 миллиард долларов в “Стратегические вычисления” в 1983 году, прежде чем любая другая страна начала работать над возможностями ИИ для военных, и с тех пор постоянно опережали своих конкурентов (Boulanin and Verbruggen, 2017). К 2010 году Соединенные Штаты инвестировали 4 миллиарда долларов в исследования автономных систем вооружения, а еще 18 миллиардов долларов были направлены на развитие автономии до 2020 года (Boulanin and Verbruggen, 2017). Помимо своего раннего выхода на поле битвы, главным преимуществом Соединенных Штатов до сих пор было финансирование; их военный бюджет затмевает совокупные военные расходы Китая, России, Южной Кореи и всех 28 государств – членов ЕС вместе взятых (SIPRI, 2019).

Наиболее важно то, что с учетом большой подвижности исследований в частном и государственном секторах в Соединенных Штатах у них больше всего компаний по ИИ в мире; больше всего публикаций, связанных с ИИ для одной страны; больше всего заявок на патенты и принятых патентов на ИИ. Что оказалось решающим для лидерства США в данной сфере и будет продолжать играть ключевую роль, так это то, что Соединенные Штаты имеют самый большой кадровый резерв талантливых исследователей ИИ, включая тех, кто входит в первые десять процентов в своей отрасли; – это больше, чем у любой другой страны в мире (Gagne et al., 2019).

КИТАЙ

Безусловно, растущим конкурентом США с точки зрения развития автономных систем вооружения и искусственного интеллекта является Китай. Китайский “План развития ИИ следующего поколения” четко демонстрирует его намерения использовать ИИ на поле боя совместно с автономными системами вооружения (China State Council, 2017; Kania, 2017). Китай, согласно прогнозам, потратит 4,5 миллиарда долларов на беспилотные технологии к 2021 году (SIPRI, 2019; Statista, 2019). Китайские компании протестировали технологию роя более чем на 1000 синхронизированных дронов (Kania, 2017). Китай публично заявил о своем намерении стать мировым лидером в области развития ИИ к 2030 году (China State Council, 2017).

В любопытном сопоставлении пользовательского и военного миров Соединенные Штаты все чаще выражают озабоченность по поводу уязвимостей, обнаруженных в приложениях для пользовательских дронов, сделанных в Китае, которые предполагают, что приложение не только собирает информацию с

телефонов, но также способно обновлять ее без проверки изменений со стороны Google, до передачи потребителям. Сотни тысяч клиентов по всему миру используют это приложение для пилотирования своих самолетов с несущим винтом и камерой. Директор Национального центра контрразведки и безопасности Уильям Р. Эванина предупредил, что все американцы “должны быть обеспокоены тем, что их изображения, биометрические данные, данные о местоположении и другие данные, хранящиеся в китайских приложениях, будут переданы китайскому государственному аппарату безопасности.” (Mozur et. al. 2020)

РОССИЯ

Лидерство России в гонке смертоносных автономных систем вооружения является результатом относительно недавних мощных государственных инвестиций и поддержки. В соответствии с российскими программами “Создание перспективной военной робототехники до 2025 года” и “Концепция применения робототехнических комплексов военного назначения на период до 2030 года” Россия планирует располагать автономными системами охраны своих оружейных шахт и все активнее добавлять автономное вооружение в свой арсенал (Bendett, 2017; Moscow Times, 2014). Несмотря на то, что некоторые могут утверждать, что интерес России запоздал, очевидно, что военно-политическое руководство России уделяет все большее внимание боевому потенциалу беспилотных летательных аппаратов (БПЛА) и беспилотных боевых летательных аппаратов (ББЛА).

Денис Федутинов, московский специалист по беспилотным летательным системам, объяснил, почему их роль в современном конфликте недооценивается: “Российские военные, а также политическое руководство страны, успешно проспавшие беспилотную революцию, вдруг осознали в конце 2000-х годов важность и значимость этих систем для себя.” В результате было реализовано несколько масштабных программ по решению этих задач. Однако, как отметил Федутинов, прогресс в текущих условиях не является последовательным, и без фундаментальных технологий невозможно перейти от простых систем к сложным (McDermott, 2020). “Если зарубежные компании, создающие БПЛА, выступают в качестве системных интеграторов, используя наиболее подходящие решения для подсистем, то в нашей стране на старте этих масштабных работ такой подход был просто невозможен из-за отсутствия не только готовых технических решений по многим направлениям, но и отсутствия научно-технических наработок для них” (McDermott, 2020).

ЮЖНАЯ КОРЕЯ

Позиция Южной Кореи в гонке автономных систем вооружения непропорционально сильна, поскольку она является мировым лидером в области автономного охранного оружия (Ipsos, 2018). При соотношении 631 робота на каждые 10 000 рабочих-людей Южная Корея имеет самую высокую концентрацию роботов в мире (Peng, 2018). Южная Корея обладает удивительно мощным потенциалом в области разработки вооружений, ежегодно тратя на оборону 41 миллиард долларов, несмотря на то, что находится под американским зонтом безопасности (SIPRI, 2019).

Развитие знаний об ИИ является основным направлением в Южной Корее, где имеется около 70 000 патентов на ИИ, более 50 000 публикаций по теме ИИ и более 2000 экспертов по ИИ (Body and Hueless, 2018; COSTS, 2019a, 2019c; Shoham et al., 2018). Будучи крупным игроком на мировой арене, Южная Корея стремится сохранить конкурентоспособность во всем мире, открыв к 2020 году шесть новых школ, ориентированных на ИИ (Peng, 2018). Это не случайность – президент Мун Чжэ Ин сделал технологию искусственного интеллекта ключевым достижением в рамках своего первого срока. В октябре 2019 года он запустил национальную стратегию ИИ, закрепив место Южной Кореи в небольшой элитной группе стран, концентрирующих огромные военные, промышленные и образовательные усилия на достижениях в этой области (Choi, 2020).

ЕВРОПЕЙСКИЙ СОЮЗ

ЕС также имеет потенциал стать мировым лидером в области развития автономных систем вооружения (World Bank, 2019). Объявив ИИ одним из главных стратегических приоритетов, ряд государств-членов предпринимают шаги по продвижению стремлений континента к лидерству в этой области. Канцлер Германии Ангела Меркель и президент Франции Эммануэль Макрон подчеркнули необходимость того, чтобы Европа стала ведущим мировым игроком на рынке ИИ, и новая Европейская комиссия сделала ИИ главным приоритетом на ближайшие пять лет. В настоящее время ЕС сосредоточен на промышленном ИИ и робототехнике. Обладая вторым по величине совокупным оборонным бюджетом в мире, составляющим 281 миллиард долларов, и прогнозируемыми расходами на закупку беспилотных летательных аппаратов в размере не менее 8 миллиардов долларов к 2021 году, ЕС обладает потенциалом для разработки оборудования автономных систем вооружения мирового класса (SIPRI, 2019; Statista, 2019). Франция, Германия, Италия и Великобритания активно занимаются системами вооружения на основе ИИ (включая беспилотные летательные аппараты, активную оборону и т. д.). Одна из областей, в которой ЕС продвигается вперед, – это этический и ориентированный на человека ИИ, или развитие технологий, согласующихся с демократическими принципами. В октябре этого года Европейский парламент принял три доклада с обзором того, как ЕС может наилучшим образом регулировать ИИ. Тем не менее, некоторые утверждают, что заявленные цели ЕС по использованию своей мощной регулятивной и рыночной власти – так называемый “Эффект Брюсселя” – в конечном итоге продемонстрируют конкурентное преимущество под знаменем “Проверенного ИИ” и то, какую роль это сыграет с точки зрения военного применения ИИ (Brattberg et.al., 2020).

СДЕРЖИВАЯ ГОНКУ

За последние 5 лет природа войны трансформируется на наших глазах за счет использования ИИ. Это изменение происходит без надлежащей подотчетности или общественного контроля, поскольку несколько стран продолжают вкладывать огромные средства в повышение автономности своих систем вооружения в сочетании с передовым искусственным интеллектом. Учитывая бурные темпы развития, при которых страны пытаются превзойти друг друга в разработке данных систем, в следующем десятилетии начнется массовая вооруженная гонка на местах. Как гражданское общество, так и Организация Объединенных Наций уже предпринимают усилия по смягчению гонки вооружений или, по крайней мере, ее наиболее разрушительных аспектов на основе ИИ.

ИССЛЕДОВАТЕЛИ ИИ / ОБЩЕСТВЕННЫЕ УСИЛИЯ

Исследователи ИИ готовы сыграть определенную роль в смягчении последствий применения оружия на основе ИИ, поддерживая международные усилия по мониторингу текущих разработок в области ИИ и оказывая поддержку соглашениям по контролю над вооружениями. Подобно исследователям в области ядерной физики и биологии, сообщество ИИ может развивать международные усилия по мониторингу, чтобы помочь сдерживать давление и надзор за мерами контроля над вооружениями ИИ. Исследователи ИИ и робототехники также могут помочь предупредить нормативные и политические вмешательства, которые способны помешать их исследованиям и лишить общество потенциальных преимуществ ИИ. Главные военные державы также разделяют общую заинтересованность в ограничении способности стран-изгоев и террористических групп приобретать и использовать военные технологии ИИ. Благодаря совместным усилиям, в том числе дипломатии на треке 2.0, исследователи ИИ могут и должны помочь сократить распространение наиболее опасного оружия на основе ИИ, а также снизить шансы на развитие конфликтов и на воздействие этого оружия на благо человечества.

МЕЖДУНАРОДНЫЕ УСИЛИЯ, ООН И ПАРАЛЛЕЛИ С КИБЕРБЕЗОПАСНОСТЬЮ И ЯДЕРНЫМ ОРУЖИЕМ

Международный характер ИИ, а также сложности, которые представляют собой технологии с точки зрения атрибуции, рисуют параллели с глобальными усилиями по смягчению кибератак и национальных войн в киберсфере. Кибербезопасность стоит на повестке дня ООН по крайней мере с 1998 года, и группа правительственных экспертов добилась определенного прогресса в разработках в области информации и телекоммуникаций. Однако, их усилия зашли в тупик в 2017 году, когда регулирование киберпространства было приостановлено и оказалось в подвешенном состоянии, включая нормы международного

права и то, как они должны применяться в кибервойне.

Государства вновь обратились к ООН, чтобы создать некий рычаг контроля для решения проблемы цифрового управления. В декабре 2018 года Генеральная Ассамблея учредила два процесса: вслед за принятием российского проекта резолюции в Первом комитете была создана Рабочая группа открытого состава, в которую вошли все члены ООН, а также было одобрено предложение США о создании еще одной ГПЭ, состоящей из 25 членов.

Рекомендации по укреплению доверия и мерам сотрудничества в киберпространстве могут быть применены к сфере ИИ, например, предложение государствам создать консультативные учреждения на добровольной основе, укреплять механизмы реагирования на инциденты в области безопасности и чрезвычайных ситуаций или установить "Регулярный институциональный диалог с широким участием под эгидой ООН".

Группа правительственных экспертов ООН (ГПЭ ООН) проводит свои заседания под эгидой Конвенции о конкретных видах обычного оружия (КНО) в целях управления гонкой вооружений на основе ИИ. 125 стран подписали КНО, и с 2014 года было проведено восемь расширенных совещаний по смертоносным автономным системам вооружения. Прогресс на пути к любому многостороннему решению достигается медленно, в то время как технический прогресс намного опережает усилия международной дипломатии. В рамках последней ГПЭ в 2019 году было разработано одиннадцать руководящих принципов, однако, из-за COVID-19 совещание 2020 года не состоялось, странам осталась лишь возможность прокомментировать эти руководящие принципы. Хотя этот процесс все еще находится в зачаточном состоянии, данная группа может влиять на процесс достижения консенсуса и укрепления доверия.

Полностью автономное оружие приводит к серьезным проблемам, связанным с соблюдением норм международного гуманитарного права с точки зрения основополагающих принципов соразмерности и подотчетности. Например, критерий соразмерности требует определения того, превысит ли гражданский ущерб, ожидаемый от участия в боевых действиях, предполагаемое военное преимущество. Подобные определения пропорциональности основаны на высококачественных расчетах и суждениях человека, сделанных в быстро меняющихся условиях, и основаны на правовых и моральных соображениях и нормах, а также на личном опыте. От автономных систем вооружения не приходится ожидать таких сложных, тонких и высокоуровневых суждений. Подобные ожидания также являются трудной задачей и с точки зрения подотчетности. В то время как отдельные лица должны нести юридическую ответственность за военные преступления в соответствии с международным правом и Женевскими конвенциями, будут ли эти же законы применяться к действиям автономного робота или его оператора (операторов)? (Doherty, 2020).

Действительно, применение военного ИИ породило озабоченность по всем четырем основным факторам, обосновывающим прошлые международные усилия по контролю за распространением или развертыванием оружейных технологий: этика, законность, стабильность или безопасность. Помимо этических и международно-правовых (юридических) проблем, отмеченных в связи с роботами-убийцами, существуют опасения по поводу того, как автономное оружие сможет изменить баланс сил между государствами и разрушит ли стабильность, достигнутую благодаря сдерживанию применения ядерного оружия (Geist & Lohn, 2018; Lieber & Press, 2017). Scharre и другие высказывают озабоченность касательно последствий развертывания автономных систем вооружения в части безопасности и уязвимости, которые они создают в отношении оперативных и потенциально масштабных аварий вследствие эскалации (Maas, 2019).

Маттиас Маас из Копенгагенского университета приводит подробную и красноречивую аналогию между нашей текущей потребностью в контроле над автономными системами вооружения и историей нераспространения ядерного оружия, отмечая, что обе системы вооружений предлагают "Ассимметричные" стратегические преимущества, обе имеют двойные технологии и назначение, что превращает полный запрет технологии в спорный вопрос. Хотя Маас согласен с важностью глобальных норм, включая международное право и инструменты, он разделяет мою озабоченность по поводу того, что такие усилия частично стимулируются и полностью поддерживаются эпистемологическими сообществами экспертов. Маас предполагает, что для тех, кто опасается, что исследовательское сообщество ИИ слишком фрагментировано, чтобы быть эффективным в рамках этих усилий, договор по ПРО может обеспечить своего рода план шагов, необходимых с точки зрения мобилизации, интеллектуальных инноваций и институционализации норм (Maas, 2019).

По мере того как государства стремятся все активнее развивать автономные военные системы ИИ, присущая им уязвимость к неожиданным взаимодействиям или операционным авариям (Scharre, 2016a) поднимает риск непреднамеренной эскалации до уровня "внезапной войны" между автономными военными системами, аналогичной внезапным сбоям алгоритмов, уже наблюдаемым в финансовом секторе (Scharre, 2016b, 2018b). Таким образом, поскольку военный ИИ вновь затрагивает эти четыре основополагающие проблемы, вопрос о надлежащем регулировании представляется актуальным. Он также видится своевременным, поскольку "идея контроля над вооружениями для ИИ остается в зачаточном состоянии" (Payne, 2018a) и, как обычное, так и формальное международное право по-прежнему находятся в постоянном изменении. Сегодня представляется разумным рассмотреть вопрос о том, как можно сдерживать или управлять опасной милитаризацией ИИ или динамикой гонки вооружений. Насколько жизнеспособен международный контроль вооружений для военного ИИ?

ЧТО НАМ НЕОБХОДИМО ДЕЛАТЬ?

Поскольку государства стремительно продвигаются вперед в своем развитии и использовании оружия и вооруженных систем с поддержкой ИИ, имеющиеся опасности этих технологий и соответствующие риски аварий делают очевидной необходимость согласованных усилий по их регулированию. Международные усилия по контролю за распространением, разработкой и использованием этих технологий находятся в зачаточном состоянии, но, как таковая, существует острая необходимость в разработке стратегии эффективных рамок того, что необходимо, исходя из исторических уроков, извлеченных в ходе аналогичных кампаний, национальных и международных, для контроля над такими прошлыми и текущими угрозами, как ядерное, химическое/биологическое и кибернетическое оружие. Эти вопросы должны быть в центре внимания активных исследовательских усилий как внутри страны, так и на международном уровне. Однако, помимо этой необходимости в дальнейшем исследовании, я хотел бы предложить базовый перечень шагов по разработке подобной стратегии на будущее:

1. Участие академического сообщества в переговорах на треке 2.0 для понимания рисков и опасностей использования систем оружия на основе ИИ.

Привлечение исследователей ИИ к данному процессу не только поможет наилучшим образом выстроить дискуссию, с большей ясностью касаемо пределов и опасностей ИИ, но они в свою очередь извлекут уроки из политического процесса и поймут требования государств, что в результате поможет формировать технологии таким образом, чтобы интересы государств при создании инструментов на основе ИИ были удовлетворены. Вдобавок к этому, привлечение беспристрастных ученых обеспечит большее доверие к самому процессу. Академическое сообщество также может помочь в определении технических средств отслеживания и проверки происхождения различных видов оружия на основе ИИ.

2. Работа с механизмами ООН для разработки норм и мер укрепления доверия.

Мы должны извлечь уроки из путаницы в ООН, возникшей в ходе создания норм и мер укрепления доверия в киберпространстве и придерживаться куда более тонкого подхода, с меньшим количеством дополнительных соглашений, чем в киберпространстве. Возможно, этого можно добиться, защищая в первую очередь гражданскую критическую инфраструктуру, такую как авиация, энергетика и окружающая среда. Будучи лидерами гонки, США должны занять лидирующую позицию в работе с механизмами ООН для создания норм и мер укрепления доверия, а также в направлении привлечения других стран, союзников и недостаточно представленных стран (глобальный Юг, обедневшие страны и т. д.), чтобы получить и обладать правом первого голоса в этом процессе.

3. Работать совместно с большой пятеркой (США, Россия, Китай, Южная Корея и ЕС), чтобы установить красные линии демаркации, с которыми все согласятся (например, защита критической инфраструктуры).

Проведение двусторонних и многосторонних встреч между разработчиками оружия на основе ИИ в рамках “Большой пятерки” поможет осознать чувствительность различных государств и лучше сформулировать проблему для других стран, участвующих в ГПЭ ООН.

4. Совместно разработать механизмы защиты ИИ, чтобы террористы и преступники не могли использовать ИИ-оружие.

В общих интересах не допустить, чтобы группы изгоев и террористы получили доступ к оружию на основе ИИ и связанным с ним технологиям. Совместная работа над механизмами обеспечения безопасности этих технологий укрепит доверие между развивающимися странами и обеспечит более эффективные решения в области защиты разрозненных видов оружия на основе ИИ. Механизмы контроля за этим оружием также могли бы быть эффективны.

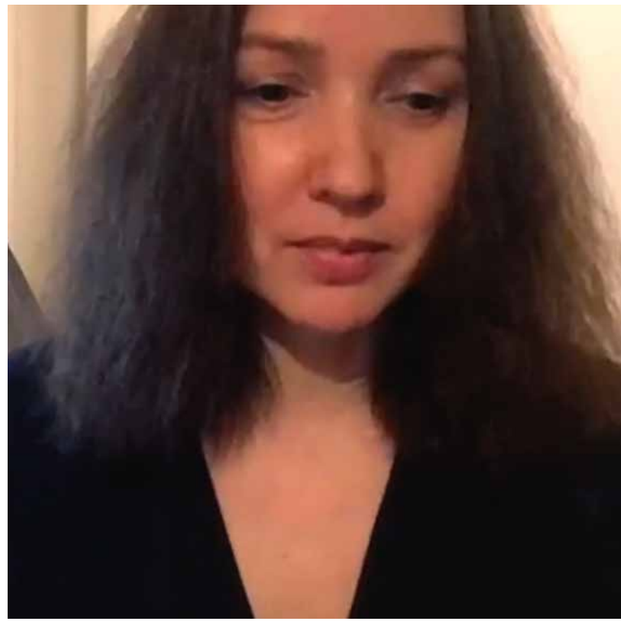
5. Создать основу применения оружия на основе ИИ в соответствии с международным гуманитарным правом.

Нам необходимо учредить процесс разрешения конфликтов о применении оружия на основе ИИ, исходя из норм международного гуманитарного права. Нам нужно прояснить руководящие принципы применения этого оружия, процесс установления вины (атрибуции) и надлежащий соразмерный ответ на инциденты, включая контратаки, санкции или судебное преследование причастных лиц государства. Без строгости выполнения вышеупомянутых задач МГП останется бессильным для подобных систем оружия.

В конечном счете, реальная “Гонка вооружений” в технологиях, основанных на ИИ, и основные приобретаемые выгоды будут связаны с экономическим доминированием. Таким образом, самые талантливые программисты и разработчики в области ИИ – Билл Гейтс – будут переходить в промышленность для работы по созданию пользовательских и бизнес-приложений ИИ. В ответ на растущие глобальные вызовы, такие как изменение климата и рынка товаров и услуг, таланты всегда будут испытывать магнитное притяжение выбора между военной и экономической природой технологий ИИ. Противоречия и конфликты могут привести к переходу кадров из промышленности в вооруженные силы, поскольку государства нанимают лучших специалистов для военных целей, лишая промышленность этих талантов. Одной из целей международных усилий по регулированию должно стать более глубокое понимание этого баланса: приоритеты для отдельных государств и власти, с учетом взаимно гарантированных возможностей уничтожения автономных систем вооружения. Учитывая общую заинтересованность государств в собственном экономическом и политическом развитии и безопасности, должно становиться все более очевидным – нам нужна поддержка международных норм, механизмов и правил; а чрезмерное инвестирование в военное применение технологий ИИ контрпродуктивно.

Энекен Тикк
Исполнительный директор, Институт киберполитики, Эстония

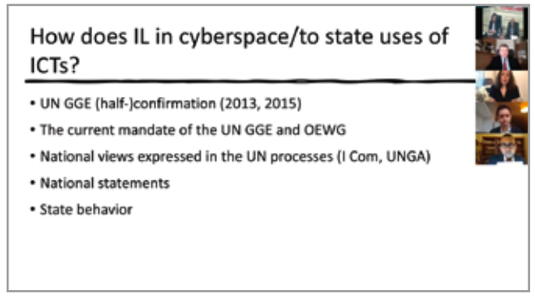
К ВОПРОСУ О ПРИМЕНЕНИИ МЕЖДУНАРОДНОГО ПРАВА В КИБЕРПРОСТРАНСТВЕ

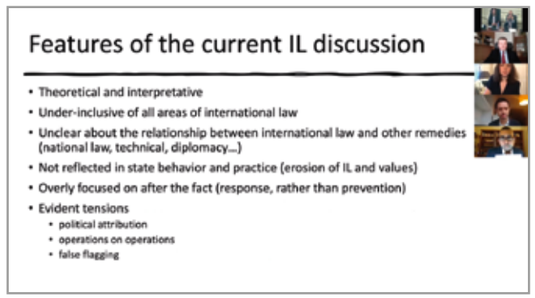


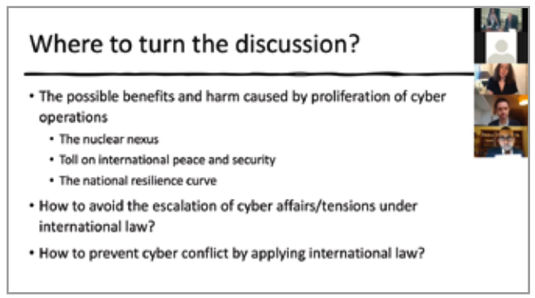
Вопрос о том, как применять международное право в киберпространстве, обсуждается в нескольких процессах. На данный момент у нас есть несколько итогов: подтверждения ГПЭ ООН (2013, 2015); текущий мандат ГПЭ ООН и РГОС ООН; национальные мнения, отраженные в процессах ООН (I комитет, ГА ООН), национальные позиции по международному праву и поведение государств.

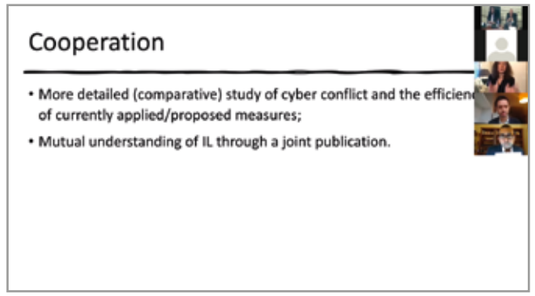
- Текущие дискуссии носят теоретический и интерпретационный характер.
- Наблюдается недостаточный охват всех областей международного права.
- Существует неясность в отношении взаимосвязи международного права и других средств правовой защиты (национальное право, технические, дипломатические меры).
- Позиции не в полной мере отражаются в поведении и практике государства (размывание международного права и соответствующих ценностей).
- Реализация происходит постфактум (реакция, а не предупреждение).
- Сохраняется очевидная напряженность вокруг политической атрибуции, операций в ответных операциях, вопроса о ложных указаниях.

Мы должны развернуть дискуссию в сторону возможных преимуществ и ущерба, обусловленных распространением кибероперациий (ядерное взаимодействие, потери для международного мира и безопасности, кривая









национальной устойчивости). Нам также необходимо конкретно рассмотреть вопрос о том, как избежать эскалации киберотношений и напряженности в соответствии с международным правом.

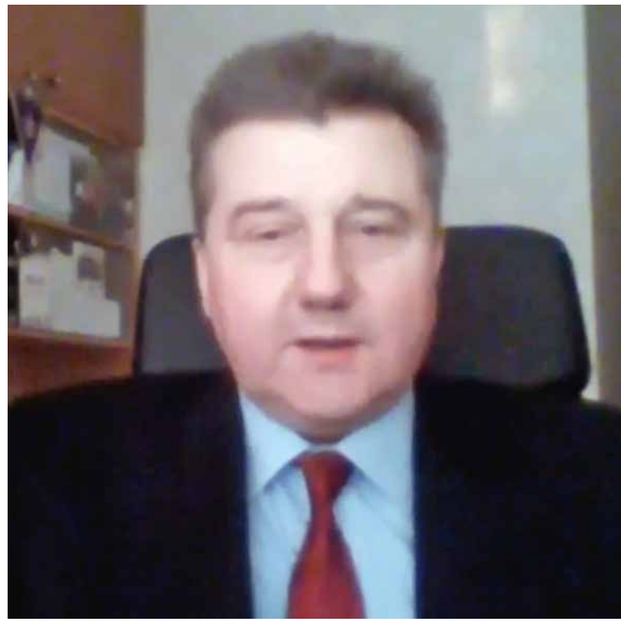
Как предотвратить киберконфликт, применяя нормы международного права?

Кроме того, крайне важно добавить к обсуждению право дружественных отношений и мирного разрешения международных споров.

Нам нужно меньше сосредотачиваться на пороговых значениях и больше на том, как их избежать. Нам нужно извлечь уроки собственно международного диалога (ГПЭ ООН, РГОС, а также переговоры по ядерной безопасности, в рамках Арктического совета). Кроме того, важно, чтобы мы были способны выявлять и признавать (потенциальные) споры и проводить различие между международными и немеждународными проблемами.

А.В. Морозов
Д.ю.н., профессор, заведующий кафедрой информационного права, информатики и математики ВГУЮ (РПА Минюста России)

РОССИЙСКИЙ ПОДХОД К ПРАВОВОМУ ОБЕСПЕЧЕНИЮ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Согласно доктрине информационной безопасности Российской Федерации 2016 года целью обеспечения информационной безопасности в области стратегической стабильности и равноправного партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

В настоящее время отношения между государствами в информационном пространстве урегулированы довольно слабо. Споры вызывают само понятие «информационное пространство». Согласно Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы информационное пространство – совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры. Главным вопросом тут является определение границ внутри такого пространства. Сложность маршрутизации данных в Интернете и рост популярности облачных технологий затрудняют подобное определение.

Доктрина информационной безопасности Российской Федерации 2016 года определяет информационную инфраструктуру Российской Федерации как совокупность объектов информатизации, информационных систем, сайтов в сети “Интернет” и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Согласно ГОСТу Р 51275-2006. «Защита информации» объектом информатизации является совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

То есть, программа, например, сайт, находящаяся в ведении Российской Федерации, в тоже время может быть физически размещена за ее пределами, на аппаратных средствах, которые Российской Федерации не принадлежат, либо принадлежат, но доступ к таким средствам обеспечивается посредством информационной инфраструктуры другого государства. В случае выхода из строя таких средств и сетей связи информационной безопасности России будет нанесен урон, хотя прямого ущерба самим информационным ресурсам нанесено не будет. Не ясно даже, что в данном случае будет считаться информационной инфраструктурой Российской Федерации, а что – другого государства. И это один из примеров.

Построение системы международной информационной безопасности подразумевает принятие мировым сообществом принципов сетевой нейтральности, уважения информационного (цифрового) суверенитета, равноправия и децентрализованного управления Интернетом.

Информационный (цифровой) суверенитет является ключевым понятием в обеспечении информационной безопасности государства. Выработка определения данного понятия позволит провести границу между государствами в информационном пространстве. К сожалению, в настоящее время в российском законодательстве, как и законодательстве других стран данный термин не определен и рассматривается только в контексте общего суверенитета государства.

Рядом западных стран членов НАТО отстаивается противоположная позиция о, во-первых, достаточности норм международного права применимых к информационному пространству, во-вторых, о приравнивании данного пространства к полю боя, в-третьих в отказе странам иметь информационный суверенитет, то есть, постулируется отсутствие границ в информационном пространстве.

Более того, странами НАТО продвигается тезис о необходимости вооруженного ответа на компьютерные атаки, несмотря на то, что источник данной атаки трудно установим, особенно в короткие сроки. Так как, согласно статье 5 Североатлантического договора 1949 года все члены блока имеют право на коллективную самооборону при нападении на одного из них, попытка увязать компьютерные атаки с вооруженным нападением позволит отвечать предполагаемой стране-источнику атаки военной силой.

Российская Федерация предлагает другой подход в формированию международной информационной безопасности, который основан на предотвращении конфликтов в информационном пространстве.

Для формирования системы неконфликтных межгосударственных отношений в информационном пространстве Российская Федерация на международной арене ведет работу на нескольких уровнях сотрудничества:

1. Двухсторонний уровень (межправительственные соглашения и межведомственные договоры);
2. Региональный уровень (СНГ, ШОС, БРИКС, ОДКБ, АСЕАН и т.д.);
3. Мировой уровень (ООН, МСЭ и т.д.).

На двухстороннем уровне основой международной информационной безопасности является заключение межправительственных договоров о сотрудничестве в области международной информационной безопасности. Данные договоры включают в себя такие направления сотрудничества, как:

- создание системы мониторинга и совместного реагирования на возникающие в этой области угрозы;
- противодействие угрозам использования информационно-коммуникационных технологий в террористических и преступных целях;
- содействие обеспечению безопасного, стабильного функционирования и интернационализации управления сетью “Интернет”;
- обеспечение информационной безопасности критической информационной инфраструктуры;
- разработка и осуществление совместных мер доверия, способствующих обеспечению международной информационной безопасности;
- совершенствование международной правовой базы и практических механизмов сотрудничества в обеспечении международной информационной безопасности;
- обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других форумов в области информационной безопасности.

Указанные направления сотрудничества в том или ином виде предлагаются Россией также в региональном и общемировом формате.

Заключение подобных договоров позволяет Российской Федерации налаживать связи в международном пространстве, основанные на принципах равноправия и уважения информационного (цифрового) суверенитета.

На мировом уровне для обеспечения мирного информационного пространства необходимо, чтобы была решена ключевая задача – создание универсальных, согласованных всеми государствами нормативных правовых норм и правил ответственного поведения в информационном пространстве.

Можно провести аналогию с международными правилами судоходства, принимаемыми всеми государствами для обеспечения безопасного движения морских судов.

Как основоположник дискуссии в ООН по международной информационной безопасности, Россия выдвинула проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который внесен в Первый комитет ГА ООН, Москва предложила 25 правил поведения государств. Принципиально важные положения среди них:

- использовать ИКТ исключительно в мирных целях;
- нацелить международные усилия на предотвращение конфликтов в этой сфере;
- соблюдать в ней принципы Устава ООН, включая суверенное равенство государств, неприменение силы или угрозы силой, невмешательство во внутренние дела государств;
- избегать голословных обвинений в злонамеренном использовании ИКТ, подкреплять любые обвинения доказательствами;
- не использовать ИКТ для вмешательства во внутренние дела других государств;
- не использовать посредников для компьютерных атак;
- предотвращать распространение вредоносных ИКТ-инструментов и скрытых вредоносных функций. Это первые шаги в обеспечении международной информационной безопасности.

Подводя итог сказанному, можно сделать следующие выводы:

1. Вопрос о проведении границ в информационном пространстве назрел и требует обсуждения и решения на международном уровне.
2. Информационный (цифровой) суверенитет является ключевым понятием при определении данных границ.
3. Необходима, как минимум, научная проработка данного понятия.
4. Требуется организовать подготовку юридических кадров высшей квалификации (магистров и аспирантов) в сфере международной информационной безопасности.

Г.Г. Шинкарецкая[1]
Старший научный сотрудник ИГП РАН

ОПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ ГОСУДАРСТВ В ИКТ-СРЕДЕ ПРИ ПРИМЕНЕНИИ РЕКОМЕНДАТЕЛЬНЫХ НОРМ

В международном праве до сих пор нет ни одного универсального договора, посвященного урегулированию отношений по поводу использования ИКТ. На этом фоне деятельность физических и юридических лиц, занятых в этой сфере, регулируется внутренним правом того государства, национальность которого имеют эти лица. Поскольку гражданское право разных государств может быть очень разным, трансграничное взаимодействие лиц разной национальности становится затруднительным и специалисты по международному частному праву говорят о необходимости унификации национального законодательства[2]. В процессе согласования норм государства стремятся заключить договор, который бы закрепил за ними твердые обязательства. Такие обязательства создают необходимые в международных отношениях транспарентность и предсказуемость.

В истории международных отношений подобная ситуация создается обычно в тех случаях, когда речь идет о новых сферах регулирования[3]. После Второй мировой войны такая ситуация существовала в области прав человека, в 1960-е годы – в сфере эксплуатации ресурсов глубоководного дна Мирового океана, в настоящее время очень сходная ситуация возникла в отношении космической деятельности.

Полезным в таких случаях оказывается наличие централизованного органа, в котором осуществляется согласование позиций государств, как Третья Конференция ООН по морскому праву или Комитет ООН по космосу.

В сфере ИКТ сформировать такой единый централизованный орган не удается[4]. Очевидно, до сих пор еще живы идеи знаменитой Декларации независимости киберпространства Дж.П. Барлоу 1996 года[5]. И в настоящее время многие комментаторы указывают на то, что действующими лицами в киберпространстве являются не государства, а частные лица и компании. Например, Л. Белли приводит данные целевой группы по разработке Интернета (IETF), которая является наиболее значимым органом по стандартизации киберпространства, что 80,8% акторов были связаны с организациями частного сектора; 6,4% – с академическим сообществом; 12,4% не указали свою принадлежность; и менее 1% заявили, что они связаны с межправительственными организациями[6], из чего делается вывод о непричастности государств к деятельности, и тем самым – к регулированию Интернета. Тем не менее, существует ряд объединений, создающих правовые рамки поведения государств в ИКТ-среде.

1. Организация Объединенных Наций

Начиная с 1998 года Генеральная Ассамблея ООН на каждой своей сессии рассматривает вопросы ИКТ. В преамбуле каждой резолюции Генеральной Ассамблеи содержатся отсылки к ее прежним резолюциям каждого прошедшего года. Сначала это были общие проблемы управления Интернетом и регулирования гражданских отношений онлайн. В настоящее время Генеральная Ассамблея принимает на каждой сессии, как правило, две резолюции:

- одна из них по докладу Первого комитета[7] – об обеспечении международной безопасности и борьбе с киберпреступностью[8];
- вторая резолюция, по докладу Второго комитета – об использовании ИКТ для обеспечения устойчивого развития[9].

В резолюциях обычно суммируются позиции государств и даются некоторые рекомендации. Поэтому резолюции – это документы общего характера, выражающие общие позиции всех членов ООН. В настоящее время в эту организацию входят 193 государства, и их позиции могут быть прямо противоположными. В этих условиях установить универсальное регулирование почти невозможно, но оно совершенно необходимо, учитывая существующую и постоянно возрастающую скорость распространения цифровизации всех сфер государственного управления и переноса многих отношений и областей деятельности в Интернет. Современное положение еще усугубляется тем, что информационные технологии приобрели характер серьезного оружия, которое может использоваться в агрессивных целях[10].

Попыткой найти выход из тупика, сформировать хотя бы общие подходы к общей проблеме, стало создание экспертных групп в рамках ООН и других международных организаций. Группы составляются, как правило, из представителей государств, являющихся высоко квалифицированными специалистами в области ИКТ. К сожалению, эти группы только приходят к общим выводам о том, что существующие и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьезных проблем XXI века[11]. В силу сложной взаимосвязанности телекоммуникационных сетей и Интернета любое устройство ИКТ может служить источником или объектом все более изощренных злонамеренных действий как в отношении целых государств, так и в отношении отдельных прав человека[12].

На основе трудов экспертных групп Генеральная Ассамблея приняла ряд резолюций. Кратко остановимся на их характеристике. При формальном анализе Устава ООН мы не находим там слов «резолюция» или «декларация», которыми озаглавлены многие документы, принимаемые Генеральной Ассамблеей. В ст.18 используется только одно слово – «решения», слова «резолюция» и «декларация» были введены Регламентом Генеральной Ассамблеи.

В любом случае решения Генеральной Ассамблеи – важный элемент современных международных отношений. Ни в Уставе ООН, ни в других его документах о юридической силе этих решений ничего не говорится. Не упомянуты они и в ст. 38 Статута Международного Суда[13], на которую принято ссылаться при

1 Шинкарецкая Галина Георгиевна – доктор юридических наук, главный научный сотрудник Института государства и права РАН. gshink@yandex.ru

2 Hollis D.B. Why States need an International Law for Information Operations // Lewis and Clark Law Review. - 2007. - Vol. 11. - № 4. - P. 1023–1061.

3 Бачило И.Л. Предпосылки укрепления правового регулирования инновационных процессов в публичном управлении на основе информационных технологий // Труды Института государства и права РАН. - 2009. - № 5/2009. - С.10.

4 Жарова А.К. Проблема анонимности субъектов в сети Интернет // Труды Института государства и права РАН. - 2009. - № 5/2009. - С.135–158.

5 A Declaration of the Independence of Cyberspace by John Perry Barlow. https://www.eff.org/cyberspace-independence (дата обращения 26.12..2020)

6 Belli L. A heterostakeholder cooperation for sustainable internet policymaking // Internet Policy Review, 2015. N 4(2).P.38

7 Комитеты Генеральной Ассамблеи ООН – вспомогательные органы, которые учреждаются ею для осуществления своих функций. Первый комитет рассматривает вопросы разоружения и международной безопасности; Второй комитет – экономические и финансовые вопросы.

8 См.: Палаева Л.В., Хафизов А.М., Гилязетдинова А.М., Вахитова А.Р., Давыдова К.Н., Сиротина Е.Р. Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них // Фундаментальные исследования. - 2017. - № 10 (3). - С. 507–511.

9 См.: Понятийный аппарат в информационном праве: коллективная монография / под ред. И.Л. Бачило, Т.А. Поляковой, В.Б. Наумова. М.: ИГП РАН, - 2017. - С. 8–9.

10 Шинкарецкая Г.Г. Международно-правовые проблемы регулирования враждебного воздействия на компьютерные системы // Государство и право 2013, № 9. С.123.

11 См.: например, Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Документ ООН A/65/201. 30 июля 2010.

12 Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. - 2019. - Т. 14. - № 3. - С.122–146.

13 Статья 38: 1. Суд, который обязан решать переданные ему споры на основании международного права, применяет: а) международные конвенции, как общие, так и специальные, устанавливающие правила, определенно признанные спорящими государ-

определении круга источников международного права[14].

Резолюции и декларации Генеральной Ассамблеи, согласно ст. 18 Устава, обязательны, когда они касаются внутренних и административных вопросов ООН, таких как бюджетные вопросы, выборы непостоянных членов в Совет Безопасности, выборы членов Экономического и Социального Совета, Совета по опеке, прием новых членов в Организацию, приостановление прав и привилегий членов ООН, исключение из Организации ее членов и некоторых других вопросов.

Некоторые авторы считают, что резолюция ГА ООН может стать обязательной в тех случаях, когда она повторяет, разъясняет или по существу воплощает ранее существовавшую норму международного права[15]. С нашей точки зрения, это немного неестественная конструкция. Если до принятия резолюции существовала норма международного права, она могла войти в любой документ – в политическое заявление, в коммюнике государственных деятелей, в дипломатическую ноту – это не меняет ее характера как нормы, признанной в качестве таковой в первоначально юридическом документе или в международно признанном обычае. В любом случае эта норма не изменяет своей сути и остается частью первоначального документа. Войдя в текст резолюции Генеральной Ассамблеи или иной международной организации, эта норма сохраняет свою юридическую автономность и не распространяет юридическую обязательность на всю резолюцию.

Резолюции – это не нормативные документы, государства не обязаны их выполнять. Однако это и не пустые бумажки, на которые можно не обращать внимание. Аппарат Генерального Секретаря ООН, который готовит документы к каждой сессии Генеральной Ассамблеи, учитывает в них все относящиеся к делу соображения. Кроме того, уже в ходе сессии каждое государство может высказать свои доводы в пользу или против предложенного проекта резолюции. Иногда резолюции, вызывающие большие противоречия, могут быть поставлены на голосование. Все резолюции, принятые по вопросам ИКТ-регулирования, были приняты без голосования.

Такой демократический процесс принятия резолюций придает им моральную силу[16]. Кроме того, в каждой резолюции всегда приводятся веские ссылки на действующие нормы международного права, и если какая-то делегация возражает против резолюции, она приводит юридические контраргументы. Таким образом, резолюции, не являясь юридическим документом, абсорбирует мнения членов ООН. Резолюция – это выразитель общего мнения. На основе этого общего мнения может быть сформулирован текст проекта договора.

Теперь посмотрим, создаются ли условия для формирования норм, регулирующих поведение государств в ИКТ-среде и, в частности, их зоны ответственности.

Результаты работы групп правительственных экспертов подводились в резолюциях Генеральной Ассамблеи. В Резолюции, принятой в декабре 2019 года[17], говорится, что в докладах Группы правительственных экспертов 2013 и 2015 годов содержится вывод о том, что международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет существенно важное значение для поддержания мира и стабильности. То есть, по мнению Генеральной Ассамблеи, международные отношения в ИКТ-среде будут развиваться нормально, если они будут регулироваться международным правом, базовые положения которого зафиксированы в Уставе ООН. Более того, международное право, по мнению Генеральной Ассамблеи, приведет к созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды.

Кроме учета мнения Группы экспертов Генеральная Ассамблея решила запросить

ствами; b) международный обычай как доказательство всеобщей практики, признанной в качестве правовой нормы; c) общие принципы права, признанные цивилизованными нациями; d) с оговоркой, указанной в статье 59, судебные решения и доктрины наиболее квалифицированных специалистов по публичному праву различных наций в качестве вспомогательного средства для определения правовых норм.

14 Лукашук И.И. Международное право. Общая часть. 2-е издание. М. 2004. С.18.

15 Например: Hall S. International Law. Hong Kong, 2006. P.60.

16 Wheatly S. The Democratic Legitimacy of International Law. Oregon, 2010, p.176.

17 Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности Резолюция, принятая Генеральной Ассамблеей 12 декабря 2019 года [по докладу Первого комитета (A/74/363)]. Документ ООН 74/28.

и мнения самих государств. В предыдущей Резолюции, которая была принята в 2018 году[18], содержалось поручение Генеральному Секретарю ООН запросить у государств-членов информацию о трудностях, с которыми они сталкиваются в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях, и представить Генеральной Ассамблее доклад, подготовленный на основе этой информации. Такой доклад был подготовлен[19]. Он содержит на 100 страницах ответы 62 государств.

Представленная государствами информация охватывает проблемы как на национальном, так и на международном уровне, а также меры, принимаемые для их решения на обоих уровнях, в том числе в рамках существующих специальных механизмов. Государства-члены представили информацию о технических и технологических проблемах и поделились своим опытом решения этих проблем. Они также подчеркнули важность международного сотрудничества в рамках противодействия использованию информационно-коммуникационных технологий в преступных целях.

Их ответы можно обобщить следующим образом.

1. Одна из самых серьезных проблем – сфера охвата международных документов. За исключением Конвенции Совета Европы о киберпреступности, другие международные соглашения по этому вопросу пока не заключены. В Конвенции 63 участника, более половины – неевропейские страны. К этой конвенции присоединяются государства, далекие от Европы, например, Аргентина. Это новое явление в международном праве договоров: государства принимают на себя обязательства по региональному соглашению, к которому они формально не относятся.
2. Доказательства относительно использования ИКТ для преступных целей нередко оказываются недоступными, поскольку находятся в иной юрисдикции, а также принадлежат частным компаниям.
3. Не налажен надлежащий обмен между государствами соответствующим опытом, не действует в достаточной мере общепризнанный принцип сотрудничества.
4. Не установлена ответственность частного сектора. Частный сектор играет важнейшую роль в связи с проблемами, которые создает киберпреступность. К сфере ответственности компаний относятся такие аспекты, как контроль и управление факторами уязвимостями данных, возникающими на платформах и в устройствах, и использование социальных сетей в преступных целях. Не ограничиваясь добровольным сотрудничеством частного сектора, необходимо провести анализ потребности в правилах, подлежащих обязательному соблюдению.
5. В отслеживании киберпреступлений есть и технические препятствия, как, например, появление новых устройств, недорогих и потому доступных лицам разных наклонностей.
6. Источником риска могут стать инициируемые государством проекты, направленные на создание механизмов дешифровки информации, полученной с устройств и/или из приложений, а также механизмов обхода компьютерной защиты. Оценки требуют и предлагаемые различными судебными органами инструменты для взлома и извлечения информации или мониторинга соответствующих действий.
7. Необходима организация специального дополнительного обучения следственных и судебных кадров и обеспечение их специальным оборудованием.
8. Необходимы меры унификации как материального, так и процессуального права государств.

Позиции и мнения государств, отображенные в Докладе Генерального секретаря ООН, получили отклик в Резолюции Генеральной Ассамблеи[20].

18 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года [по докладу Первого комитета (A/73/505)] . Документ ООН A/RES/73/27

19 Противодействие использованию информационно-коммуникационных технологий в преступных целях. Доклад Генерального секретаря ООН. Документ ООН A/74/130. 30 июля 2019.

20 Резолюция, принятая Генеральной Ассамблеей 21 декабря 2020 года [по докладу Второго комитета (A/75/454, пункт 11)] 75/202. Документ ООН A/RES/75/202.

В этой резолюции содержатся рекомендации относительно развития международного сотрудничества в борьбе с киберпреступностью в плане использования более разнообразных форм правовой помощи. В ней говорится также о полезности использования многосторонних договоров, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Совета Европы о киберпреступности, в качестве основы для международного правового сотрудничества в дополнение к своим двусторонним и внутренним договоренностям. Отмечена также необходимость в сотрудничестве и взаимодействии между такими организациями, как УНП ООН, Международный союз электросвязи и Интерпол, для осуществления совместной работы в целях решения проблем, связанных с использованием преступниками сетей информационно-коммуникационных технологий для совершения преступлений. В Резолюции обращено внимание на то, что важной мерой была бы разработка механизма предоставления международными корпорациями информации и доказательств государствам-членам, а также оказания корпорациями помощи в расследовании преступлений, совершенных в принадлежащих им сетях.

2. Организация экономического сотрудничества и развития (ОЭСР)

Вторая организация, уделяющая значительное внимание регулированию отношений между государствами в ИКТ-сфере – это Организация экономического сотрудничества и развития (ОЭСР), которую часто называют сердцем глобализации[21]. Ее участниками являются 27 стран с самой мощной экономикой[22]. Данная организация может принимать решения, относящиеся к ее членам, однако в отношениях с государствами – не участниками ОЭСР ее члены обязаны применять ее правила. Понятно, что правила, принимаемые этой организацией, поневоле выполняются многими государствами. Правда, учтем, что Организация принимает рекомендации, а не обязательные постановления.

ОЭСР стала проявлять интерес к ИКТ довольно давно. Еще в 1980 году ею были разработаны «Основные направления» или «Руководящие указания» о защите частной жизни и трансграничном перемещении персональных данных[23]. Этот документ, как и многие последующие, по содержанию были очень похожи на те, что принимались в рамках Европейского Союза. Тем самым документы, имевшие региональное значение, воспринимались практически всеми государствами мира.

Декларация о трансграничном переходе данных[24] принята для некоторого уточнения статуса распространяемых документов: она была уже не европейским, а универсальным документом, но как бы приспособлена для имплементации ее в правовую систему всех государств. Декларация была фактически заявлением о намерениях вести определенную политику: на основе принципа свободного перемещения информации.

С распространением в сфере ИКТ новых видов деятельности ОЭСР откликается на это принятием новых документов. Упомянем Указания о мерах, необходимых для защиты прав потребителей в электронной торговле и о защите потребителей от мошеннических и обманных коммерческих практик[25]; а также Указания по обеспечению безопасности информационных систем[26]. Содержание нескольких документов были обобщены в Рекомендациях Совета ОЭСР о принципах построения политики в Интернете[27]. Это фактически были советы государствам относительно объема компетенции в управлении Интернетом.

21 Boulle L. The Law of Globalization/ An Introduction. Wolters Kluwer, p.295.

22 См. официальный сайт ОЭСР: OECD <http://www.oecd.org/>. (дата обращения 01.01.2021)

23 OECD Council. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1980). <http://www.oecd.org/>. (дата обращения 01.01.2021)

24 OECD, Declaration on Transborder Data Flows (Paris: OECD, 1985) http://www.oecd.org/>. (дата обращения 01.01.2021)

25 OECD Council, Guidelines for Consumer Protection in the Context of Electronic Commerce (Paris: OECD, 2000) http://www.oecd.org/>. (дата обращения 01.01.2021); OECD Council, Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (Paris: OECD, 2003) http://www.oecd.org/>. (дата обращения 01.01.2021).

26 OECD Council, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Paris: OECD, 2002). http://www.oecd.org/> (дата обращения 01.01.2021).

27 OECD Council Recommendation of the on Principles for Internet Policy Making. . 14 December 2014.). http://www.oecd.org/> (дата обращения 01.01.2021).

ОЭСР как всемирная, фактически универсальная организация оказывала содействие и ООН в деле организации управления Интернетом[28]. На основании рекомендаций ОЭСР была принята Декларация Всемирного саммита на высшем уровне[29] и фактически разработки ОЭСР учитываются в ходе организации деятельности в Интернете специализированных учреждений ООН (Международный Союз Электросвязи (МСЭ) и Всемирная организация интеллектуальной собственности (ВОИС)[30].

Примечательно, что в Декларации принципов, принятых в Женеве, сказано: «Политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств. Государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня»[31]. Таким образом, развитие идей управления Интернетом ведет к укреплению роли государства в этом процессе.

3. Документы, разрабатываемые неправительственными организациями.

Нельзя не признать, что неправительственные организации играют в ИКТ-сфере ключевую роль. В глобальном информационном обществе действует значительное число негосударственных акторов — физических и юридических лиц. Они нередко образуют объединения для институализации своей деятельности.

Прежде всего, следует назвать Рабочую группу проектирования Интернета; Общество Интернета; Консорциум всемирной паутины (англ. World Wide Web Consortium, W3C); Корпорацию по присвоению имен и адресов в Интернете (англ. Internet Corporation for Assigned Names and Numbers, ICANN).

Следует назвать также некоторые международные неправительственные организации, содействующие развитию международного частного права в сети Интернет.

Международная торговая палата – это «всемирная бизнес-организация»[32]. Ее цель – содействие развитию торговых отношений между юридическими лицами разных стран. Документы, принимаемые ею, не являются юридическими. Они применяются добровольно и благодаря своей универсальности содействуют формированию международных юридических принципов. Важное место среди них занимают списки терминов, которые обычно обозначают как «инкотермс». Это обобщенные Международной торговой палатой общепринятые обозначения типовых ситуаций, используемые обычно в торговых контрактах[33].

Типовые контракты – это еще один значительный вклад Торгово-промышленной палаты в облегчение мировой торговли[34]. Было создано несколько типов таких контрактов: о передаче технологии, о строительстве «под ключ» и другие.

Центры международного арбитражного разбирательства. Наиболее известны и популярны – Постоянная палата третейского суда, Международный арбитраж Международной торговой палаты, Лондонский арбитражный суд, арбитраж Стокгольмской торговой палаты, Американская арбитражная ассоциация, Венский Центр международного арбитража, Сингапурский Центр международного арбитража, Комиссия международной экономики и торговли Китая. Эти международные торговые арбитражи публикуют правила арбитражного процесса, а также арбитражные решения, и тем самым обеспечивают определение состава источников права и доступ к ним в области международного коммерческого арбитража, и становятся частью глобального правового развития.

28 OECD INPUT TO THE UNITED NATIONS WORKING GROUP ON INTERNET GOVERNANCE (WGIG). DSTI/ICCP(2005)4/FINAL. http://www.oecd.org/> (дата обращения 26.12..2020)

29 Декларация принципов ВСИС, пункты 48–50 (WSIS-03/GENEVA/DOC/0004).

30 См.: официальный сайт Секретариата ООН: https://publicadministration.un.org/en/ (дата обращения 01.01.2021).

31 Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. Построение информационного общества — глобальная задача в новом тысячелетии. Женева, 2003. Режим доступа: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf (дата обращения 01.01.2021).

32 International Chamber of Commerce Home Page, http://www.iccwbo.org (дата обращения 15.01.1021)

33 См.: International Chamber of Commerce, Policy and Business Practices, Commission on Commercial Law and Practice, http://www.iccwbo.org/policy/law/id3l5/index.html

34 International Chamber of Commerce, Commission on Commercial Law and Practice, ICC Model Contracts and Clauses, http://www.iccwbo. org/policy/law/id272/index.html

Ассоциации международной торговли исчисляются тысячами в рынках разных типов. Ассоциации выпускают руководящие указания для юристов, а также модельные документы. Эти указания и модельные документы активно используются практиками. Принципы и основные положения, содержащиеся в этих документах, становятся элементами возникающих обычно-правовых норм, ведущих к определенным формам гармонизированных норм права.

4. Заключение

Казалось бы, новая область регулирования – правоотношения в ИКТ-среде – требует новых подходов. На заре Интернета была популярной идея полной независимости ИКТ от государств. Однако с течением времени выяснилось, что право, действующее в Интернете – это нормы права государств, национальность которых имеют физические и юридические лица, осуществляющие деятельность онлайн. Упорное нежелание государств идти на заключение международных договоров в этой сфере может быть продиктовано политическими или коммерческими соображениями. Государства как будто уступают место частно-правовому регулированию. На первое место выходит международное частное право. В настоящей статье мы не касались реального выяснения масштабов его действия. Мы старались показать, что имеет место также активный процесс публично-правового регулирования, но оно складывается скорее как международное мягкое право, и формулируется в рекомендательных документах, принимаемых как межгосударственными, так и негосударственными международными организациями.

Рекомендательные документы обобщают позиции разных государств и как будто выводят общий знаменатель, на основании которого государства принимают свое законодательство. Этот процесс выступает как своеобразный метод формулирования *opinion juris*, ведущий к возникновению международного обычая.

П.У. Кузнецов
Заведующий кафедрой информационного права Уральского государственного юридического университета, д.ю.н., профессор

ОТДЕЛЬНЫЕ МЕТОДОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кризисные тенденции (предисловие)

В наше время много озвучивается и пишется о том, что повестку дня определяет глобальный системный кризис. Научно-технический прогресс и связанные с ним проблемы международной информационной безопасности стали как бы драйвером общемирового кризиса, в том числе и кризиса международного права.

Так ли это с точки зрения динамики развития мировой цивилизации в целом? Ответ, как всегда, неоднозначный, если мерить такое движение веками, тем более тысячелетиями. Ведь международному праву всего-то чуть более 200 лет, если его началом считать Вестфальский мир.

Но если измерять современные кризисные явления более коротким отрезком времени (40–60 лет), то тогда, конечно, с этим утверждением можно согласиться. Ведь общепринято считать 1970–1980-е гг. были временем общемирового покоя и устойчивости, если не считать локальные военные конфликты. Именно в этот период наблюдался расцвет научно-технических открытий и их реализации в практической жизни: кибернетика и космонавтика определяли радости жизни и строились фантастические проекты.

Но после этого наступили времена Его Величества Интернет, в связи с его рождением все испытывали восторг, но и вскоре цивилизационные радости стали поутихать, а нынче вовсе померкли. И тогда грянул Кризис во всей его «красе», кризис традиций и традиционных ценностей, в т.ч. традиционных регуляторов. «Старые и ветхие меха» уже не могли сдержать бурный процесс «брожения» новейших модернистских проектов, опять же связанных с результатами научно-технического прогресса (или регресса!) в области создания, как сегодня говорится «прорывных» информационных технологий. А впереди еще «радости» жизни создания искусственного интеллекта и реалии виртуальной реальности…

Правовые средства обеспечения международной информационной безопасности

О том, в чем проявляется смысл проблем правового обеспечения международной информационной безопасности, нет необходимости повторяться. Об этом уж неоднократно и обстоятельно демонстрировал профессор А.А. Стрельцов в своих докладах на протяжении последних лет.

Не буду отмечать строго политические причины проблемы МИБ. Не в наших силах их анализировать, да и не наш это предмет исследований.

А вот что касается теоретических и методологических инструментов путей решения названных проблем, то о них стоит рассуждать и пытаться осмыслить – находятся в русле попыток исследований юристов и не только в области международного информационного права.

Существующие современные концепции обеспечения международной информационной безопасности предполагают возможное использование технологических подходов к решению проблем в этой области. Однако, все же нельзя забывать о том, что технологии – это продукт человеческой деятельности

и с их помощью можно только дополнить процесс нормативного правового обеспечения безопасности, но он не будет эффективным, поскольку только с помощью норм права (нормативных правил ответственного поведения) можно устанавливать качественный правопорядок и предупреждать негативные явления в киберпространстве.

Наверное, это может иметь место и такие средства, как известно, используются и порой бывают эффективными. Но до определенных пределов, в т.ч. до пределов процедур разбирательств по инцидентам, где уже требуются правовые инструменты.

Да и сложившиеся принципы международного права (суверенного равенства, доверия и сотрудничества, невмешательства во внутренние дела, уважения прав и свобод и др.) и правила ответственного поведения невозможно заменить средствами технического и технологического контроля и воздействия. Другое дело, когда их применяют в комплексе с правовыми. В этом заключается определенный смысл. В традиционных областях применения международного права (например, ограничения гонки вооружений) они успешно применяются. Думается, что в киберсфере они могут быть еще более эффективными.

Например, при разумном сочетании правовых и технологических средств можно использовать такое правовое средство, как ОБЯЗЫВАНИЕ (не надо путать их с обязанностями), которое используют в публичной сфере права, когда на субъект права возлагается определенное бремя выполнения конкретных действий, без выполнения которых не могут продолжаться или возникать конкретные общественные отношения. Их невыполнение становится юридическим фактом возникновения ответственности.

Фиксирование таких обязываний в юридически значимых документах (международных договорах), дополненных техническими регламентами контроля за выполнением обязательных действий ключевых субъектов международных информационных отношений может стать эффективным средством правопорядка в киберпространстве. Таких субъектов в нем немало, в т.ч. системно определяющих мировой информационный климат. Названное правовое средство в комплексе с технологическими инструментами можно использовать в правилах ответственного поведения в качестве предупреждающего злонамеренные действия субъектов распространения информации, несущей запрещенный или нежелательный контент.

Кратко о проблемах суверенитета в области обеспечения международной информационной безопасности.

Проблема эта, как известно, сверхактуальная и сверхсложная для исследователей и практиков. Представляется, что эту проблему надо попытаться рассматривать не в статике, а в динамике, т.е. в развитии этой конституционной ценности любого государства.

Самыми существенными признаками сущности суверенитета – это верховенство, независимость и самостоятельность реализации государственной власти, полнота осуществления законодательной, исполнительной и судебной её функции на всей территории и независимость в международном общении.

Но ведь суверенитет можно рассматривать не только в жестких пределах государственной границы, но за их пределами, когда речь идет о продолжении распространения влияния и воздействия ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ в рамках определенных международных договоров региональных международных союзов – СНГ, ОДКБ и даже БРИКС.

Участники названных союзов могут создавать ЗОНЫ совместного телекоммуникационного пространства, т.е. совместного СУВЕРЕНИТЕТА.

Это можно определить и на принципиальном уровне (на уровне принципов) и на уровне процедур и регламентов, в т.ч. процедур взаимодействия и контроля.

Иначе говоря, речь идет о РАСПРЕДЕЛЕННОМ или МНОГОУРОВНЕВОМ СУВЕРЕНИТЕТЕ.

К вопросу о понятии «ИКТ-среда»

Уже не один десяток лет пытаемся расщепить и распознать этот краеугольный камень. В разных фундаментальных и прикладных источниках науки делаются попытки ему толкования.

Как его рассматривать – как пространство, объект или как совокупность условий? Чаще его сравнивают или сопоставляют с информационной сферой как пространственно-временной областью человеческой деятельности, как её часть.

Прежде всего, это, конечно, многоуровневый концепт. Его надо рассматривать и на макроуровне (например, международном, региональном или даже национальном). Его надо представлять и на микроуровне, как среда деятельности коллективов людей либо деятельности отдельного человека.

Причем, названная среда является совокупностью объектов и условий социального, информационного и технологического характера, а потому обычно ИКТ-среду (или IT-среду) рассматривают как совокупность таких компонентов и условий реализации информационных потребностей.

Поэтому ИКТ-среда – это окружающие человека информационно-технологические условия его обитания в информационной сфере его деятельности.

Главным образом, в состав таких условий входят сама информация, включая контент и её разновидность в форме сообщений, а также обеспечивающие их получение и использование технологии, включая средства доступа и передачи.

Что касается наименования информационной среды, особенно названия «ИКТ-среда», то используемая аббревиатура ИКТ в известном смысле это общепризнанное сокращение, как и все вообще аббревиатуры.

Думается, что на прикладном уровне использования наименования можно всегда договориться и включить его в текст какого-либо стандарта как технического правила, использовав аббревиатуру ИКТ (информационно-коммуникативные технологии) либо ИТ (информационные технологии), а на международном уровне утвердить наименование такой среды – АЙ-ти среда либо киберсреда. Но только в самом крайнем случае можно использовать наименование «диджитал» (цифровая среда), поскольку грядут квантовые вычисления и слово «цифровой» зависнет, как зависает компьютер.

Спорным остается вопрос о сущности и пределах ИКТ-среды, а также использовании этой сущности в практике международных отношений.

Причем самым неочевидным решением этой проблемы является экстерриториальность сети Интернет как компонент и инструмент ИКТ-среды.

Главное, думается, заключается в определении его в качестве объекта международного права, а не только как технологического средства, находящегося по сути в пределах деятельности одного оператора – США.

А нужно, чтобы этот объект был выведен из юрисдикции одной страны и реально стал объектом совместной международной деятельности.

При этом разместить основные технические и технологические комплексы, обеспечивающие функционирование сети Интернет на территориях, подконтрольных ООН и/или государств, входящих в состав Совета Безопасности ООН. В условиях существующего кризиса доверия это может быть весьма сдерживающим фактором в развязывании информационных конфликтов.

В соответствии с таким же подходом можно определить пределы и границы ответственного поведения по аналогии с правилами Открытого моря, режимом территориальных вод и внутреннего моря.

На уровне ООН разработать и принять Конвенции об Открытом информационном пространстве, Территориальном информационном пространстве и Внутреннем (суверенном) информационном пространстве.

Луиджи Мартино
Профессор, координатор Центра исследований кибербезопасности и международных отношений, университет Флоренции, Италия

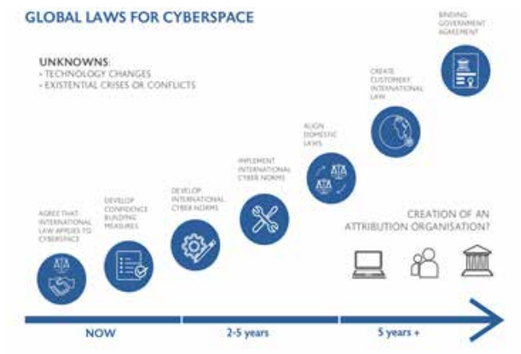
КИБЕРПРОСТРАНСТВО И МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ: ЛАНДШАФТ ДИПЛОМАТИЧЕСКИХ ИНИЦИАТИВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НА ИКТ-АРЕНЕ И ОБОСНОВАНИЕ СУЩЕСТВУЮЩИХ ТЕОРИЙ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

Я хотел бы поблагодарить Национальную ассоциацию международной информационной безопасности за приглашение и за ваши усилия по организации этой конференции, посвященной столь острой теме, как дипломатические и нормативно-правовые проблемы, связанные с киберпространством.

Сегодня я хотел бы остановиться на конкретной теме кибердипломатии в киберпространстве, осветив сильные и слабые стороны текущего состояния дел, включая данный анализ в рамках теорий международных отношений.

Во-первых, нужно определить, где мы находимся, чтобы ответить на главный вопрос, который уже рассматривался сегодня на пленарном заседании: является ли киберпространство бесконтрольным пространством?

Текущее положение таково, что мы достигли соглашения о том, что международное право применимо к киберпространству, и разработали меры доверия, но есть ряд проблем, связанных с разработкой, реализацией и внедрением международных обязательных кибернорм и созданием международной организации по атрибуции:



Эту ситуацию следует анализировать с осознанием того неопровержимого факта, что поле битвы стало виртуальным, особенно если учесть способность кибероружия наносить реальный физический ущерб. Более того, реальные действующие лица в сфере ИКТ не являются традиционными участниками международных отношений.

Киберарена охватывает целый ряд заинтересованных сторон, которые являются уже не только государствами, но и негосударственными субъектами, транснациональными компаниями, террористами, частными лицами: все эти заинтересованные стороны противостоят друг другу на киберарене без нормативно-правовой базы.

Даже если мы находимся перед объединением (кибер) поля боя, (кибер) оружия и (мульти) акторов, киберарена хаотична и, следовательно, опасна ввиду отсутствия общих “правил игры” – крайне необходимых элементов борьбы с насилием и предотвращения военной и политической эскалации.

В этом смысле международные инициативы (в процессе реализации) создали почву для политических и дипломатических действий. Несмотря на то, что это всего лишь “добровольные” инициативы, они способствовали установлению минимальных рамок для международного взаимодействия с участием таких ведущих игроков, как Китай, Россия и Соединенные Штаты на уровне ООН; Россия и Соединенные Штаты на уровне ОБСЕ (меры доверия).

На мой взгляд, когда мы говорим о киберпространстве, стоит рассматривать эту область, пространство или измерение как дополнительную арену международной системы, но при этом мы должны учитывать препятствия, лежащие в основе международного сотрудничества.

Согласно классической и современной теориям международных отношений, государства соглашаются взаимодействовать, если на основании проведенной калькуляции затрат/преимуществ сотрудничество более выгодно. В свете этого, возможно ли международное сотрудничество в киберпространстве? Это еще один все еще открытый вопрос, и я полагаю, данная конференция внесет свой вклад в поиск соответствующего ответа для его решения. В частности, на мой взгляд, для окончательной выработки подходящей основы сотрудничества, мы должны начать рассматривать тех субъектов, которые должны быть вовлечены в механизмы взаимодействия, а также основные элементы международного сотрудничества. Это следующие элементы: доверие, прозрачность, надежность и защищенные каналы связи. Все эти вопросы являются частью существующих дипломатических инициатив на международном, региональном и двустороннем уровнях, и ОБСЕ представляет собой передовую практику в данном направлении.

Однако, я полагаю, что ключевые препятствия, лежащие в основе существующих дипломатических инициатив в сфере киберотношений / ИКТ, – следующие:

1) Отсутствие взаимного доверия между государствами вследствие идеологических и геополитических факторов;
2) Секьюритизация действующих механизмов кибердипломатии.

Для анализа и решения этих вопросов, я думаю, мы должны пересмотреть существующие подходы, реализуемые до сих пор. В практическом плане мы должны рассматривать и анализировать киберпространство через призму международного сообщества, а не в качестве международной системы, с тем, чтобы привлечь соответствующих игроков к взаимодействию.

Международное сообщество означает, что мы должны привлечь: государственные и негосударственные субъекты, частные и гражданские заинтересованные стороны, для того чтобы укрепить доверие, избежать секьюритизации и балканизации, а также усовершенствовать нормотворческий процесс.

Существующие международные и региональные форумы по-прежнему ограничиваются рассмотрением ИКТ-арены в устаревшей динамике международных отношений, с исключительной ролью государств, по-прежнему рассматриваемых в качестве единственных участников международной системы.

Является ли это по-прежнему актуальным решением? На мой взгляд, такой подход не только не полезен, но и опасен, поскольку возникает главный риск – спровоцировать гонку вооружений и поляризацию политических позиций.

В этом контексте подход Международного сообщества позволяет задействовать не только государства, но и другие релевантные заинтересованные стороны, что может быть охарактеризовано названием данной конференции: “Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности”.

На мой взгляд, такой подход должен основываться на беспроигрышном решении для всех участников партнерства, с использованием, к примеру, метода “снизу-вверх” на треке 2.0, но при этом – с надежной и твердой нормативно-правовой базой, имеющей обязательную силу.

Сегодня у нас есть несколько интересных тематических исследований, которые можно расценивать как передовую практику, поскольку эти инициативы основаны на подходе “снизу-вверх”, например, Парижский призыв к доверию и безопасности в киберпространстве, который содержит 9 принципов:

1) Защита физических лиц и инфраструктуры;
2) Защита Интернета;
3) Защита избирательных процессов;
4) Защита интеллектуальной собственности;
5) Нераспространение;
6) Безопасность жизненного цикла;

7) Кибергигиена;
8) Никаких частных взломов;
9) Международные нормы.

Все эти принципы должны представлять собой ландшафт сегодняшней повестки дня в сфере кибердипломатии в целях обеспечения безопасности информационного пространства, и, безусловно, эта конференция должна сыграть ключевую роль на пути к достижению этой цели.

А.Л. Козик
Региональный советник по правовым вопросам в странах Восточной Европы и Центральной Азии Международного Комитета Красного Креста

ЗАЩИТА ГРАЖДАНСКОЙ ИНФРАСТРУКТУРЫ И МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО

Уважаемые со-председательствующие,
Участники конференции,
Дамы и Господа!

С большой благодарностью мы в Международном Комитете Красного Креста приняли приглашение к участию в конференции. Считаем, что этот престижный форум вносит важный вклад в развитие тематики кибербезопасности. Я лично искренне рад принять в нем участие.

Как известно, МККК работает в ситуации вооруженных конфликтов. Моими коллегами во всем мире движет, по большому счету, только один тезис. Мы верим, что каким бы не был вооруженный конфликт, Комитет и воюющие стороны могут приложить усилия для того, чтобы спасти жизни гражданских лиц. Так родилось международное гуманитарное право (МГП). Оно не судит, оно не оценивает. Оно действует в пределах уже существующего вооруженного конфликта. Ему безразлично кто начал конфликт и почему. Оно подчинено только одной задаче – сократить количество жертв, предотвратить излишние страдания.

Мне особенно приятно говорить об этом в России. Стране, внесшей огромный вклад в развитие МГП. Благодаря России в Санкт-Петербургской декларации 1868 года закреплен основополагающий принцип – для победы в войне достаточно выводить из строя как можно больше комбатантов. Делать их смерть неизбежной или причинять излишние страдания – противно принципам человеколюбия и не дает военного преимущества. Благодаря выдающемуся российскому ученому юристу Федору Федоровичу Мартенсу на Гаагских конференциях мира принята оговорка, которую весь мир знает как оговорку Мартенса – независимо от действующих предписаний жертвы войны всегда находятся под защитой принципов человеколюбия и гуманности. Благодаря Советскому Союзу в Женевских конвенциях 1949 года появилась известная ст. 3 общая для всех конвенций, а четвертая конвенция – о защите гражданского населения – приняла нынешний, очень прогрессивный на момент принятия, вид. Когда в 1996 году Международный суд ООН применял оговорку Мартенса к вопросу легальности применения ядерного оружия Российский судья, как и весь состав суда, проголосовал за то, что независимо от вопроса принципиальной законности применения ядерного оружия применение его всегда должно подчиняться требованиям международного гуманитарного права (пункт D заключения).

МГП для Международного Комитета Красного Креста – не пустой звук, не просто отрасль права. Это часто единственная защита для жертв войны и для персонала самого Красного Креста. Сотрудники МККК не носят оружия, не используют бронежилеты при этом работая часто там, куда другие акторы не могут получить доступ. Каждый день мы видим тысячи жертв войны участь которых зависит от того – применяется ли сторонами МГП или нет.

И поэтому вопрос о применимости МГП к кибернападениям является для нас принципиальным. Мы можем только приветствовать желание государств развивать нормы поведения в киберпространстве, дискутировать об интерпретации уже существующих норм. Но для нас является принципиально важным,

чтобы на всех форумах, однозначно и определенно звучал тезис о применимости МГП. МГП применяется только в ходе вооруженного конфликта. МГП не решает вопроса о законности применения силы государствами друг к другу – этим занимается совершенно другая отрасль права – право международной безопасности. МГП заботит, главным образом, что или кто является объектом нападения – нападения должны строго ограничиваться военными объектами.

Я думаю, в этом зале нет никого, кто бы возражал, что, например, госпитали и медицинские учреждения не должны становиться объектом нападения – будь то кинетическими средствами или посредством кибернападений.

Я помню момент искренней радости когда Группа правительственных экспертов ООН по информационной безопасности (GGE) в 2013 году провозгласила консенсусом принципиальную применимость международного права к кибероперациям. Я имел честь разделить эту радость работая в группе эксперта GGE от Беларуси и был свидетелем вклада России и лично Андрея Владимировича Крутских в этот триумф. В 2015 году благодаря GGE появляются нормы ответственного поведения государств. Эта инициатива идет много дальше требований МГП резервируя за государствами право на защиту своей критической инфраструктуры (норма g) и постулируя запрет на такие нападения (норма f). И здесь снова вклад российской делегации трудно переоценить.

Мандат МККК включает статус хранителя МГП. В 2019 году мы сформулировали институциональную позицию по вопросу применения международного гуманитарного права к кибероперациям в ходе вооруженного конфликта. В виде документа она доступна на нашем сайте и переведена на все основные языки. Использование в названии документа фразы «в ходе вооруженного конфликта» умышленно подчеркивает, что МГП применяется только в ходе уже существующего вооруженного конфликта. Мы приветствуем дискуссию государств по сложным аспектам интерпретации конкретных норм МГП, но отправной точкой такой дискуссии является принципиальная применимость МГП.

Если вернуться к нормам ответственного поведения (в частности нормам g и f), то, принимая во внимание что они охватывают и ситуации вооруженных конфликтов, можно привести несколько примеров их взаимодействия с существующими нормами МГП. Ограничусь тремя.

Во-первых, МГП налагает абсолютный запрет на нападения против гражданских объектов. Критическая гражданская инфраструктура – такая, например, как электрические сети питающие жилые зоны, в терминах МГП являются гражданским объектом. По мнению МККК запрет на нападения на гражданские объекты распространяются и на кибероперации спроектированные таким образом, чтобы вывести их из строя без физического уничтожения.

Во-вторых, МГП предоставляет особую защиту медицинским учреждениям и медицинскому персоналу. В соответствии с МГП стороны в вооруженном конфликте обязаны в любое время уважать и защищать медицинские учреждения. Это означает, что в дополнение к требованию воздерживаться от создания препятствий к их функционированию, государства должны предпринимать все возможные меры для организации их работы и предотвращать ущерб в отношении них, включая причинённый путем кибероперациий.

В-третьих, некоторые типы критической инфраструктуры, квалифицируемые как необходимые для выживания гражданского населения, такие, например, как установки обеспечивающие питьевую воду, в соответствии с МГП, также подлежат особой защите. Они защищены против любых кибероперациий, включая те, которые приостанавливают их функционирование.

Завершая свое выступление, я хочу еще раз подчеркнуть, что МГП применяется исключительно в ходе вооруженного конфликта и посвящено исключительно вопросу защиты жертв войны. Это неоднократно подтверждено государствами. Вопрос поддержки Россией позиции МККК по применимости МГП к кибероперациям в ходе вооруженного конфликта был затронут и в ходе встречи Министра иностранных дел С.В. Лаврова и Президента МККК П. Маурера. Верим в продуктивный диалог и искренне благодарим за приглашение выступить на этой конференции.

Благодарю за внимание.

А.А. Тедеев
заместитель декана Высшей школы государственного аудита (факультет) Московского государственного университета имени М.В. Ломоносова, доктор юридических наук, профессор

ЦИФРОВОЕ ГОСУДАРСТВО, ГОСУДАРСТВЕННОЕ СТРОИТЕЛЬСТВО И ИНФОРМАЦИОННЫЙ (ЦИФРОВОЙ) СУВЕРЕНИТЕТ

В одной из наших ранних работ по проблемам цифровизации государственного строительства, управления и контроля (цифрового развития системы государственного аудита), мы подчеркивали, что в каждой конкретной исторической ситуации, на каждом этапе социально-экономического развития наиболее распространенной в демократических государствах является наиболее удобная и надежная форма выявления воли большинства населения. Поэтому конкретные формы демократии со временем под влиянием самых различных факторов могут меняться. В современных государствах, формами демократии, как совокупность сложившихся в государственный механизм способов и инфраструктурных инструментов выявления, выражения и реализации суммы воли и согласованных интересов различных слоев соответствующего общества.

Специалистами отмечается, что в настоящее время в современном мире, очевидно, начинается процесс цифровой трансформации государства и правовых систем. Представляется обоснованным безусловно согласиться с тезисами о нарастающей цифровизации права (Т.Я. Хабриева), необходимости разработки и введения Цифровой Конституции (С.М. Шахрай), а затем, в недалеком будущем – кодификации информационного законодательства (И.Л. Бачило, Т.А. Полякова, В.Д. Зорькин и др.). Неслучайно, процессы научно-технического развития, информационной революции «запускают» прогрессию всемерного развития и актуальности получают разработки в области цифрового права (информационного права как права киберпространства).

Отметим, что в мире этот процесс, естественно, проходит не равномерно. Государства с развитой системой публичного управления, сильной судебной и в целом правовой системой, обладают политической, правовой, социальной и экономической инфраструктурой для максимально быстрого и эффективного реагирования на ускоряющиеся факторы социальной нестабильности. При этом, в условиях постоянного повышение степени напряжения социальных отношений, обострения всех вертикальных и горизонтальных связей в обществе особое значение приобретает качество публичного управления. В условиях перехода от информационного общества к обществу цифровому указанное качество становится важнейшим фактором обеспечения государственного суверенитета.

Указанные процессы наиболее быстро проявляются в части трансформации систем публичного администрирования (в области исполнительной власти). Отмечается, что во многом указанная тенденция вызвана тем обстоятельством, что именно перед исполнительной властью в первую очередь встает необходимость адекватного, а в потенциале и прогностического реагирования на современные вызовы. Последние события мировой повестки, в том числе пандемия коронавирусной инфекции наглядно показала механизм такого реагирования. Представительная и тем более судебная власть всегда традиционно характеризуется известной степенью традиционализма. Но маховик изменений раскручивается и в этих областях.

При этом в ряде работ мы подчеркивали, что в случае дальнейшего ускорения научно-технической революции в индустриально развитых демократических странах возможен будет безболезненный переход от представительной демократии к исключительно прямой (непосредственной) демократии.

Однако, как известно, «в будущее пустят не всех». Возможно утверждать, что в цифровую эпоху, для государств, отстающих в своем цифровом развитии, в качестве и скорости цифровой трансформации системы публичного (государственного и муниципального) управления, трансформации национальной правовой системы существенно повышаются риски постепенной утраты, а затем и разрушения структурных элементов государственного суверенитета.

В частности, первое, – отсутствие собственной цифровой технологической и программной инфраструктуры системы цифрового государства как правило, ведет к утрате самостоятельности и независимости государственной власти. Второе, – верховенство государственной власти на всей территории государства возможно только при сохранении единства информационного пространства страны. В-третьих, цифровые разрывы (разрывы «между отдельными лицами, домашними хозяйствами, предприятиями или географическими регионами, которые находятся на разных уровнях социально-экономического развития, которые связаны с их возможностями для доступа к информационным технологиям, а также использованию Интернета (Organisation for Economic Cooperation and Development, 2001) становятся все более ощутимой угрозой обеспечения территориальной целостности государства. Таким образом, феномен цифрового неравенства из важной, но «не смертельной» социальной проблемы в условиях цифровой реальности стремительно обретает общегосударственное значение, становится важнейшим фактором национальной безопасности.

КРУГЛЫЙ СТОЛ № 2
МЕЖДУНАРОДНОЕ ПРАВО И МЕРЫ ДОВЕРИЯ В ИКТ-СРЕДЕ: ПРОБЛЕМЫ ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ В ИКТ-СРЕДЕ

Модератор:

Марков Алексей Сергеевич, доктор технических наук,
президент АО «НПО «Эшелон», Эксперт НАМИБ

А.С. Марков
Доктор технических наук, президент
АО «НПО «Эшелон», Эксперт НАМИБ

ПРОБЛЕМЫ АТРИБУЦИИ И РЕГУЛИРОВАНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Важнейшим направлением международной информационной безопасности является исследование возможности, условий и путей правового и специального регулирования международной информационной безопасности, которое во многом связано с проблематикой атрибуции компьютерных атак (cyber-attack attribution) [1-6].

Определение атрибуции компьютерных атак находится на этапе становления, ее еще нет в терминологических глоссариях подкомитетов и сообществ по защите информации, как-то: IEC, ISO, NIST, ГОСТ, ISACA и пр. Однако в литературе атрибуцию кибератак трактуют как комплекс процедур по выявлению источника атаки с целью возложения ответственности [2, 7-11]. Условно атрибуцию кибератак можно разделить на:

- техническую (криминалистическую), выполняющую функцию определения;
- политическую (правовую, дипломатическую), выполняющую предписывающую функцию (табл.1).

Напомним барьеры, которые обусловили сложность разрешения проблемы атрибуции кибератак, а именно: политический, правовой, организационно-технический и технический уровни.

На политическом уровне атрибуция кибератак представляет собой пока скорее инструмент информационного противоборства. К примеру, когда Россия, инициировала в ООН Свод международных правил, норм и принципов ответственного поведения государств в среде ИКТ (одобренные около 40 странами) [2-7], это вызвало демонстративное неприятие со стороны западных коллег по международной безопасности.

Правовой уровень международных отношений по оценкам ряда ученых представляет собой также пока «серую зону» античного международного права, сформированного изначально в конкретном физическом мире [4, 12]. Например, в киберпространстве нет общей трактовки военного агрессора (например, по Клаузевицу – осуществляющего физическое насилие к людям [13]), отсюда нет четкого понимания какие допустимы контрмеры защитного, сдерживающего или наступательного характера. Как уже упоминалось, неясно как провести демаркацию и делимитацию в виртуальном пространстве.

Организационно-технические барьеры состоят в том, что в настоящее время нет никаких международных организационных стандартов по взаимному мониторингу и контролю действий и деанонимизации в Интернет [15].

Технические проблемы изначально присущи Интернет, организация которого не ориентирована на запрет анонимности [3, 7, 14].

Таблица 1. Сравнение характеристик технической и политической атрибуций

Тип	Функция	Достоверность	Базовые методы
Техническая (криминалистическая)	Определения (детективная)	Высокая	Мониторинг контроль ресурсов и процессов
Политическая (нормативная, дипломатическая)	Предписывающая	Низкая	Соблюдение норм анализ мотивации

Таблица 2. Источники отчетов по атрибуции

Организация	Страна	Тип организации	Пример Интернет-источника
Cisco (Talos)	США	Публичная компания	https://blog.talosintelligence.com/2018/02/group-123-goes-wild.html
CrowdStrike Holdings	США	Публичная компания	www.crowdstrike.com/blog/meet-the-adversaries/
FireEye (Mandiant)	США	Публичная компания	www.fireeye.com/current-threats/apt-groups.html
MITRE	США	Некоммерческая организация	
NSA	США	Федеральная служба	www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/
Secureworks (Dell)	США	Публичная компания	www.secureworks.com/research/threat-profiles
Лаборатория Касперского	Россия	Акционерное общество	www.securelist.com/all/?category=908

Структурная сложность программных средств является объективной причиной для уязвимости сетевых подсистем [15], в том числе компрометации подсистем аутентификации и аудита.

Можно назвать исследовательскую базу тематики путем представления наиболее активных в рассматриваемой области компаний и организаций, которые публично представили обзоры по атрибуции (табл. 2). В связи с тем, что сотни стран имеют подразделения по кибербезопасности, а в 99% кибероперации приходится на 10 стран [7], можно предположить, что ряд стран скрывают свои исследования. Это значит, что большинство представленной аналитики может иметь односторонний политический подтекст.

В международном сообществе делаются попытки повысить достоверность атрибуции путем моделирования отдельных ее аспектов. Наиболее известными являются два подхода:

- моделирование процесса принятия решения [8-11],
- моделирование техник, применяемых исполнителями компьютерных атак [15, 16].

К первому подходу в первую очередь относят так называемую Q-модель процесса атрибуции [10]. Модель носит концептуальный характер, имеет характер аналитического «мозгового» цикла (гипотеза-обсуждение-действие). Визуально процесс сбора и анализа данных представляется тремя кольцами, а вывод (вердикт) иллюстрируется хвостом буквы Q (рис. 1).

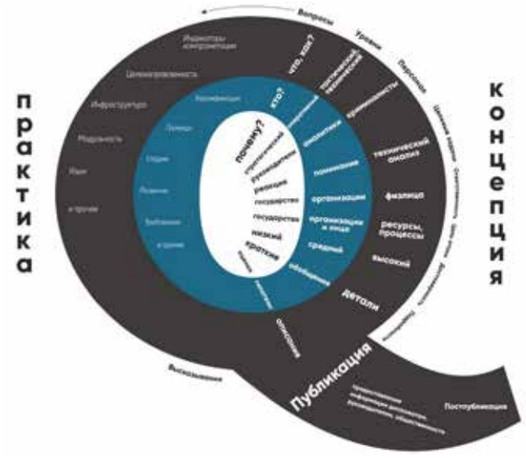


Рис. 1. Q-модель атрибуции кибератак

Таблица 3. Набор методических приемов хакерских групп, систематизированных MITRE

Способы, методические приемы атаки	Число способов
Начальный доступ	9
Выполнение кода	10
Обеспечение присутствия	18
Повышение привилегий	12
Обход механизмов безопасности	34
Получение удостоверяющих данных	14
Разведка ресурсов	24
Горизонтальные действия	9
Сбор данных	16
Управление	16
Вывод данных (эксфильтрация)	9
Воздействие	13

Ко второму подходу в первую очередь относят систематику тактик и техник хакерских групп (ATT&CK), которая поддерживается международной некоммерческой организацией MITRE (табл. 3). Несмотря на статус международной, надо понимать, что MITRE является проектом США, то есть не содержит данных, связанных с кибероперациями США, их союзников и партнеров.

В данной работе автором предлагается дополнить известные модели путем использования многофакторного анализа. Такой анализ включает классификацию атрибутов, а именно:

- особенности программных ресурсов;
- особенности сетевой активности;
- методические особенности атаки;
- данные о субъектах атаки;
- иная информация, полученная без использования собственно компьютерных сетей, например, техническая и агентурная разведка, аналитика по косвенным причинам, разного рода провокации и т.д.

Например, к атрибутам программных ресурсов можно отнести:

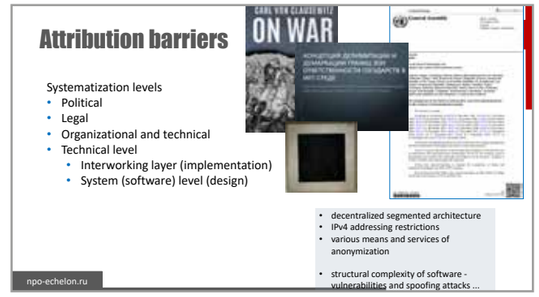
- наборы уязвимостей, повторно используемых злоумышленниками;
- наличие уязвимостей нулевого дня;
- наследование вредоносного кода;
- артефакты в программном коде;
- особенности приемов и стиля программирования;
- стилистика комментариев.

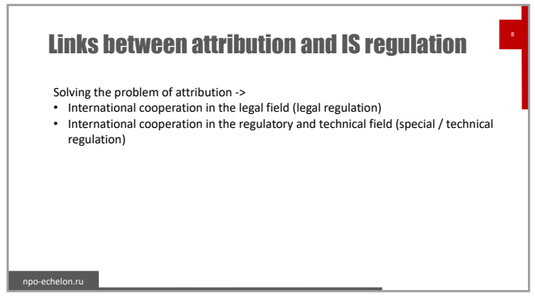
Пример атрибуции кибератак с использованием предложенной классификации представлена в таблице 4.

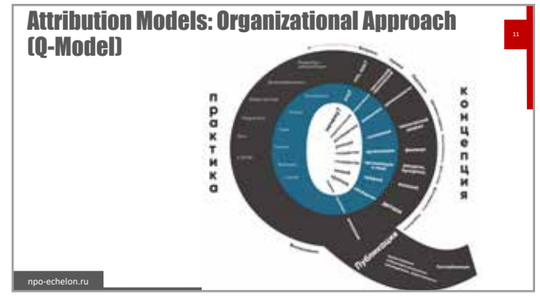
Несмотря на сложность атрибуции и присущие этому процессу барьеры, очевидно,

Таблица 4. Пример классификации и атрибуции кибератак

Название	Уязвимость	Программы	Цели	Источник	Тактические приемы	Группа
Атака на посетителей форумов, посвященных исламскому джихаду	Уязвимость в Firefox 17 (TOR Browser)	Неизвестный эксплойт	В список целей не включены IP-адреса Иордании, Турции и Египта, но включены пользователи определенного провайдера спутникового Интернета в Афганистане.	Серверы Equation Group	Атаке подвергались только авторизованные пользователи, которые зашли с определенных IP-адресов.	Equation Group (США)
Атака на правительст-венные организации с использо-ва-нием уязвимости CVE-2017-11882	Уязвимость в Microsoft Office CVE-2017-11882	Backdoor, написанный на PowerShell-POWRUNER	Правительствен-ные организации в странах Ближнего Востока.	н/д	Массовые рассылки сообщений с использованием скомпро-метиро-ванных учетных записей. Социальная инженерия.	APT 34 (Иран)







что в условиях международного сотрудничества следует стремиться к договоренностям, а в итоге к регулированию процесса международной безопасности и стабильности в киберпространстве. Можно предложить для обсуждения, например, ряд возможных решений в данной области.

Дипломатические направления по повышению эффективности атрибуции:

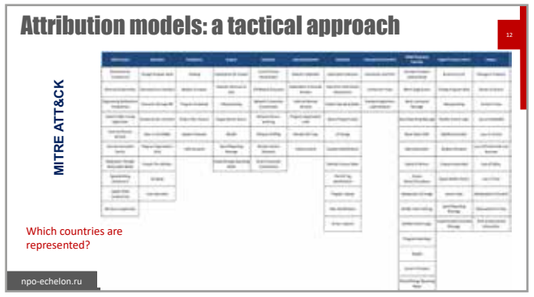
- выполнение соглашений группы правительственных экспертов ООН;
- осуществление взаимодействия между группами CERT различных стран;
- организация экспертного сообщества исследователей для совместной выработки решений на основе различных интересов и подходов;
- осуществление взаимодействия на политическом и техническом уровнях для расследования инцидентов;
- создание консультационных механизмов для повышения доверия;
- усиление защиты критически важной инфраструктуры;
- международное взаимодействие по обмену информацией об инцидентах, их характерных признаках и степени их угроз;
- соглашение о запрете кибератак на элементы информационной инфраструктуры.

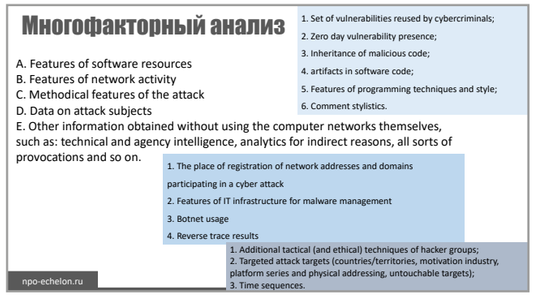
Организационно-технические направления по повышению эффективности атрибуции:

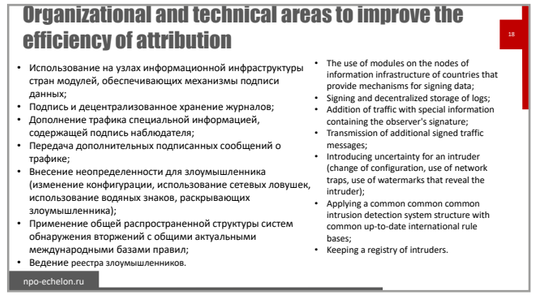
- использование на узлах информационной инфраструктуры стран модулей, обеспечивающих механизмы подписи данных;
- подпись и децентрализованное хранение журналов;
- дополнение трафика специальной информацией, содержащей подпись наблюдателя;
- передача дополнительных подписанных сообщений о трафике;
- внесение неопределенности для злоумышленника (изменение конфигурации, использование сетевых ловушек, использование водяных знаков, раскрывающих злоумышленника);
- применение общей распространенной структуры систем обнаружения вторжений с общими актуальными международными базами правил;
- ведение реестра злоумышленников.

Литература

1. Бойко С.М. Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Международная жизнь. 2018. № 11. С. 23-35.
2. Международная информационная безопасность: теория и практика / Крутских А.В., Бирюков А.В., Бойко







С.М., Волкова С.Г., Зиновьева Е.С., Зинченко А.В., Матюхин Д.В., Смирнов А.И. Учебник для вузов: в 3-х томах / Под общ. ред. А.В. Крутских. – М.: МГИМО, 2021. - Том 1 (2-е изд., доп.) – 384 с.

3. Россия и глобальные вызовы в области информационной безопасности. XII Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» Гармиш-Партенкирхен, Германия 16–19 апреля 2018 года // Международная жизнь, 2018. Спецвыпуск. 146 с. URL: https://interaffairs.ru/virtualread/garmish2018/publication.pdf.
4. Стрельцов А.А. Суверенитет и юрисдикция в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. 2017. № 2. С. 87-106.
5. Стрельцов А.А., Смирнов А.И. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям // Международная жизнь. 2017. № 11. С. 71-81.
6. Information Security Threats during Crisis and Conflicts of the XXI Century. By eds.: A.V.Zagorskii, N.P.Romashkina. Moscow: IMEMO, 2016, 133 p. DOI: DOI: 10.20542/978-5-9535-0461-4.
7. Шерстюк В.П., Крутских А.В., Плохой О.А. и др. Сборник докладов участников Тринадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (22–25 апреля 2019 г., Гармиш-Партенкирхен, Германия). НАМИБ, 2020, 220 с.
8. Grotto A. Deconstructing Cyber Attribution: A Proposed Framework and Lexicon. Computer Science, IEEE Security & Privacy, 2020, V. 18, No 1. DOI:10.1109/MSEC.2019.2938134.
9. Lin H. Attribution of malicious cyber incidents: From soup to nuts, Economics, Hoover Working Group on National Security, Technology, and Law, 2016, Aegis Series Paper No 1607, 56 p.
10. Rid T., Buchanan B. (2015): Attributing Cyber Attacks. The Journal of Strategic Studies, 2015 Vol. 38, Nos. 1–2, 4–37, DOI: 10.1080/01402390.2014.977382.
11. Wheeler D.A., Larsen G.N., Techniques for Cyber Attack Attribution. IDA Paper, P-3792, 2003, 84 p.
12. Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2014. № 11. С. 20-34.
13. Гареев М.А., Турко Н.И. Война: современное толкование теории и реалии практики // Вестник Академии военных наук. 2017. № 1 (58). с. 4-10.
14. Смирнов А.И. Атрибуция кибератаки: на пути к кибер модус ви верди? // XII Конвент Российской ассоциации международных исследований «Мир регионов vs регионы мира, 2019 (22 октября 2019, Москва).
15. Марков А.С., Шеремет И.А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник академии военных наук. - 2019. - № 2 (67). - С. 82-90.
16. Репп П.В. Методология моделирования кибер-атак как основа проектирования системы диагностики информационной безопасности // Информационно-измерительные и управляющие системы. 2018. Т. 16. № 9. С. 51-58.

П.Л. Пилюгин
Старший научный сотрудник,
ИПИБ МГУ имени М.В. Ломоносова

ЗОНА ОТВЕТСТВЕННОСТИ ГОСУДАРСТВ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Физическая граница в киберпространстве

Делимитация пространства и соответственно его демаркация связаны с физическими объектами: земля, вода, воздух, космос и пр. Именно с такими объектами связано международное право, включая морское, воздушное и т.д.

Для ИТКС также можно попытаться привязать эти задачи к физическим устройствам (серверам, линиям связи и пр.), попадающим под правовое или техническое регулирование. Т.е. если контролировать весь информационный поток в устройствах совершающих информационный обмен между людьми, находящимися на территории различных государств, то это и будет основа для установления границы в киберпространстве и определения режима границы.

Примером такой границы является firewall в масштабах страны – «Great Wall» в КНР. И это действительно реальная граница, не смотря на замечания, что она не абсолютна, ведь абсолютно непреодолимых границ и в реальном мире сегодня нет. Однако существование такой границы обусловлено двумя важными обстоятельствами:

1. Стоимость реализации (оборудование, программное обеспечение) и эксплуатации средств контроля межгосударственных информационных потоков.
2. Существенное ограничение всех межгосударственных информационных потоков (запрещены все неразрешенные типы потоков и виды информации, например, может блокироваться шифрованный трафик).

Если стоимостные затраты можно распределить во времени и пространстве (ранее, например, предлагалась концепция «распределенной границы», распределяющая эти функции между провайдерами), то ограничение информационных потоков вступает в противоречие с принципом свободного (или почти свободного) информационного обмена.

Действительно, если разрешить все незапрещенные потоки, то придется контролировать все информационные обмены, что сопряжено с рядом неразрешимых проблем, так как если контейнерный анализ (по меткам или атрибутам) возможен, то эффективный контекстный анализ (перлюстрация, цензура и пр.) потребует ресурсов сравнимых с ресурсами всей существующей сети.

Рассмотрим подробнее возможность контроля при соблюдении принципа свободного информационного обмена.

Принцип свободного информационного обмена и контроль

При сохранении свободного или почти свободного информационного обмена, как показала практика, точечные запреты оказываются не эффективными. Примером тому является недавняя борьба Роскомнадзора и мессенджера «телеграмм». Суть проблемы в том, что попытка заблокировать ресурс свелась к блокировке адресов Интернет, а ресурс и IP адреса, им используемые, это разные сущности, которые не обязательно постоянно связанны.

Например, подавляющее большинство (можно сказать почти все!) пользователей сети Интернет при каждом (!) подключении к сети получают временный (!) адрес – временный идентификатор, а аутентификация пользователей, как правило, не производится, если не предусмотрена оплата услуг подключения к сети (но и в этом случае информация доступна только провайдеру взимающему плату).

Есть и другие примеры блокировки сайтов, которые либо меняли имена/адреса, либо просто уходили в «невидимый Интернет», например, в I2P или TOR. А такие наложенные на Интернет анонимные сети создают еще оду прослойку (надстройку) анонимизации (шифрование, обфускация) между устройствами и ресурсами и их почти невозможно заблокировать. Почти относится к событиям 2010 года в КНР, когда была проведена удачная блокировка сети TOR, но для этого потребовались ресурсы упоминавшейся firewall – и учитывая то, что сеть TOR не полностью децентрализована. Впрочем, если вообще заблокировать весь трафик то и «невидимый Интернет» тоже будет блокирован.

Вообще относительная неэффективность систем контроля объективна по причине отставания средств контроля от неконтролируемого развития технологий. Используемые сегодня механизмы контроля (если не рассматривать почти полную изоляцию) были эффективны 10–20 лет назад. При этом информационные технологии развивались не для обхода контроля, а в стремлении удовлетворения рынка услуг, а это потребовало удешевления, наращивания мощностей и что важно динамичности в оказании услуг, в том числе и динамичности адресного пространства.

Ответом на этот вызов может быть создание таких же динамичных средств контроля, что может потребовать значительных единовременных затрат, а постепенная их модернизация может опять не успеть за развитием технологий. Хотя двигаться в этом направлении надо. Вообще здесь возникает абсурдная идея ограничения развития IT-технологий (по аналогии с нераспространением ядерного оружия), но угрозы этого развития в отличии от выгод не так очевидны.

Таким образом, если мы не стремимся к изоляции, то определение зон ответственности государств в киберпространстве связано, прежде всего, с определением источника (авторства или хотя бы территориальной принадлежности физического устройства – источника атаки) при атрибуции инцидентов. Это позволит реализовать апостериорные механизмы контроля информационных потоков, технически не ограничивая принципов свободного информационного обмена. И в случае возникновения инцидентов эти механизмы должны помочь **доказательно восстановить картину** происшедшего, **связать его с деятельностью определенных субъектов** (или зоной ответственности государства) и тем самым реализовать принцип неотвратимости наказания в соответствии с национальным или международным правом.

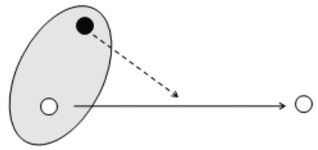
Предлагаемый подход требует реализации двух процедур: **атрибуции инцидента** и **доказательного восстановления картины** происшествия.

Разработка соответствующих технологий и средств реализации этих процедур ограничивается не только стоимостными ограничениями. Вообще представляется важным принципиальная возможность их реализации.

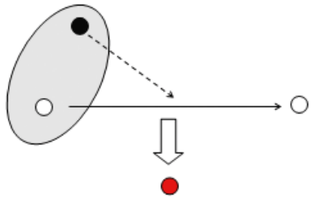
Реализация процедур атрибуции инцидента и доказательного восстановления картины происшествия как задачи технического регулирования

Любое информационное взаимодействие предполагает информационный поток от одного хранилища информации (информационного объекта) к другому:

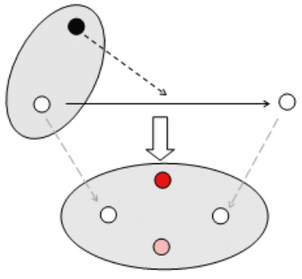
Но сам по себе такой поток не возникает – он должен инициироваться некой активной сущностью – субъектом (владельцем/оператором того или иного субъекта):



На самом деле это в упрощенном виде формальная субъектно-объектная модель обеспечения безопасности, в которой средством (механизмом) обеспечения безопасности выступает субъект (монитор) контролирующий информационные потоки.



Этот монитор не только собирает информацию о взаимодействующих субъектах, но и содержит свою управляющую информацию для фильтрации и хранения этой информации или для активации различных действий вплоть до запрещения потока.



Зачем здесь эти схемы? Они позволяют наглядно представить любое информационное взаимодействие (или цепочку таких взаимодействий).

Что представляют собой эти субъекты и объекты?

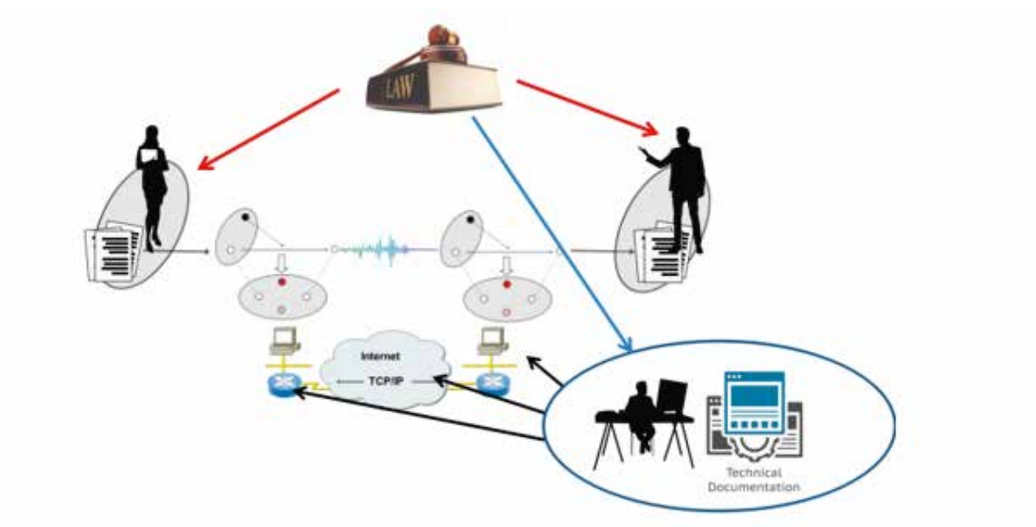
Например, если речь идет о документах и их распространении, то субъектами являются люди, монитором – контролирующий орган, а правила которым они подчиняются можно отнести к области права.

А если в качестве субъектов рассматриваются программы и устройства, то информационные объекты представляют файлы, пакеты информации, состояния компьютерной памяти, и здесь управляющая информация является областью технического регулирования.

Эти области различны, но информационное взаимодействие в среде ИТКС невозможно организовать без одной из них.

Конечно, нужно учитывать различия компьютерных инцидентов и инцидентов в информационном пространстве, так как хотя и то и другое связано с ИТКС, но акторами являются разные сущности. В первом случае использую технические и программные средства (трояны, сниферы, вирусы и пр.) происходит воздействие на физический мир, то во втором случае важно само содержание информации безотносительно среды ее распространения (документ, сайт, блог, новостной канал и пр.).

Более того и для компьютерных взаимодействий эти объекты и субъекты не однотипны. Например, запись файла данных с одного диска на другой или пересылку E-mail с компьютера на компьютер можно представить как цепочки информационных взаимодействий более мелких объектов (записей, кадров, пакетов, датаграмм и т.д.) каждое из которых требует своего технического регулирования.



Какие задачи атрибуция компьютерных инцидентов и доказательного восстановление событий в киберпространстве поможет решить техническое регулирование

Определение устройства источника компьютерного инцидента предполагается по его аппаратному адресу или по его сетевому адресу. Хотя каждое устройство имеет свой аппаратный адрес, но он используется только в локальной сети (или в новой версии протокола IPv6), да там его легко подделать.

Интерес представляет именно сетевой адрес, который, как отмечалось выше, не привязан постоянно к устройству, но во время соединения с сетью эта связь имеет место. Можно ли связать такой адрес устройства (или группу адресов для локальной сети) с конкретной страной? В принципе да, так как адреса распределены администрацией адресного пространства (IANA), региональными (RIR) или локальными (LIR) регистратурами Интернета различным организациям или физическим лицам (а они попадают под юрисдикцию государства). К сожалению, такое распределение не имеет международного правового статуса.

Такое распределение позволило бы условно «раскрасить» все информационные потоки глобальной сети в цвета флага того или иного государства. Однако, аутентификация IP адреса отправителя не только не предусмотрена, но и не требуется для маршрутизации потоков информации. Поэтому возможна подделка этого адреса или его подмена транзитными узлами.

Наглядным аналогом является система каршеринга – т.е у каждого автомобиля есть идентификационный номер, но за рулем может оказаться любой человек.

Поэтому для того, чтобы рассматривать такой адрес как атрибут инцидента он должен быть зафиксирован соответствующими средствами. А чтобы связать его с конкретным устройством должна быть зафиксирована эта связь во время инцидента (а в случае подмены на каком либо прокси также надо фиксировать и связь между проксируемыми адресами в это время). И если фиксация адреса может

Physical boundary in cyberspace

The delimitation of space and, accordingly, its demarcation are related to physical objects: earth, water, air, space, etc.

For ICT, you can also **try to link these tasks to physical devices** (servers, communication lines, etc.) that fall under legal or technical regulation.

If you regulate the entire information flow in devices that make information exchange between people located on the territory of different States, **this will be the basis for establishing a border in cyberspace** and determining the border regime.

Physical boundary in cyberspace

The existence of such a border which regulates the entire information flow between the state and the outside world is due to important circumstances:

1. **Technical difficulties** of "border control»;

2. **The cost of implementation** (equipment, software) and means of control operation for interstate information flows.

3. **Significant restriction** of all interstate information flows (all unauthorized types of flows and types of information are prohibited, for example, encrypted traffic may be blocked).

The principle of free information exchange and control

If we do not seek isolation, then the definition of state responsibility zones in cyberspace is primarily related to **determining the source** (territorial affiliation of the physical source device) **when attributing incidents**.

In the event of an incident, mechanisms for determining the source should help to establish an **evidence-based picture of what happened**, link it to the activities of certain entities (the state's area of responsibility), and, thus, implement the principle of the inevitability of punishment in accordance with national or international law.

This requires the implementation of two procedures: **attribution of the incident and evidence-based recovery of the incident picture**.

Attribution of an incident and evidence-based recovery of an incident event

This is a simplified form of the formal subject-object model of security, in which the means (mechanism) of security is **the subject (monitor) that controls information flows** M1:

проводиться на объекте атаки, то фиксировать связь с устройством-источником возможно только в начале цепочки связи – в сети провайдера. А в случае подмены связь между адресами может фиксироваться только транзитным сервером.

Представляется, что возможность выдвинуть и контролировать организационные и технические требования такой фиксации – и это область ответственности государства при разрешении организациям соответствующего вида деятельности в его правовом пространстве.

Кто и как осуществляет техническое регулирование

Для разных объектов может применяться разное регулирование, которое осуществляется разными организациями специализирующимся в соответствующих областях.

ISO – Международная организация по стандартизации – основная организация по разработке международных стандартов, она была учреждена в 1947 году на основе соглашения между представителями 25-ти индустриально развитых стран о создании организации, обладающей полномочиями координировать на международном уровне разработку различных промышленных стандартов и осуществлять процедуру принятия их в качестве международных стандартов [2]. Членами ISO являются национальные организации по стандартизации 164 стран [3] .

Международная электротехническая комиссия (англ. International Electrotechnical Commission (**IEC**)) – деятельность МЭК/IEC связана со стандартизацией физических характеристик электротехнического и электронного оборудования. Основное внимание IEC уделяет таким вопросам, как, например, электроизмерения, тестирование, утилизация, безопасность электротехнического и электронного оборудования. Членами IEC являются национальные организации (комитеты) стандартизации технологий в соответствующих отраслях, представляющие интересы своих стран в деле международной стандартизации.

Attribution of an incident and evidence-based recovery of an incident event

Why are these schemes here?

They allow you to visualize any information interaction (or a chain of such interactions).

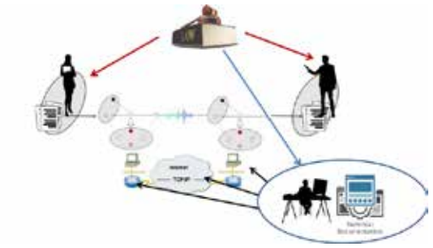
What are these subjects and objects?

If we are talking about documents and their distribution, then the subjects are people, the monitor is a controlling body, and the rules to which they are subject belong **to the field of law**.

If programs and devices are considered as subjects, then information objects represent files, information packets, and computer memory states, and here control information is **a technical regulation**.

Technical regulation

These areas are different, but information interaction in the ICT environment **cannot be organized without one of them.**



Who and how performs technical regulation

National and international standards:

- ISO - international organization for standardization.
- International electrotechnical Commission (IEC).
- International telecommunication Union (ITU).
- European Telecommunications Standards Institute (ETSI).
- IANA (Internet Assigned Numbers Authority).
- IETF (Internet Engineering Task Force).
- World Wide Web Consortium (W3C) .
- .....

Narrowing the scope of technical regulation

The demand for **universal deanonymization and universal control will be too radical** and may require significant technical resources.

You can **limit such requirements to the area of critical information infrastructures (CII)** where the importance of attributing an incident is not in doubt. It is necessary to formulate technical requirements for operators and technical means of CII that allow recording the attributes of an incident.

It is important to ensure the reliability and credibility of the evidence base.

Technical regulation of CII safety in accordance with ISO 15408

The international standard ISO / IEC 15408 is in fact a meta-tool that defines a system of concepts in terms of which an assessment should be made. It describes a relatively complete catalog of security requirements (functional and trust), but does not provide specific sets of requirements and criteria for TICS. **These requirements and criteria are included in the security profiles and security tasks.**

It is the officially accepted security profiles that form the regulatory framework in the field of information security (IS) based on the "General criteria" and used in practice.

A profile describing a particular area of the security system (for example, a profile for CII) can be created using the document structure developed in ISO 15408.

Technical regulation of CII safety in accordance with ISO 15408

The composition of the security profiles:

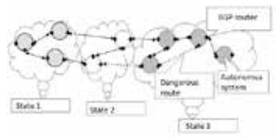
1. General security assumptions
2. Common security threats
3. General security goals
4. General security goals for the environment
5. General functional requirements.
   including **FAU Class: security Audit**
   FIA class: Identification and authentication
6. General trust requirements
7. Specific requirements for security services
8. active audit Systems
9. security Analysis
10. specific requirements for combinations

Areas of state responsibility in cyberspace

Since we are talking about **technical regulation in the network**, a logical assumption would be to assign the responsibility to the administration centers of providers, transit networks (servers) and attacked networks.

These administrative centers in the global network are the **Autonomous system administration centers.**

State responsibility zones can be considered as a **set of Autonomous systems (together with their pool of IP addresses) belonging to legal entities registered in a particular country.**

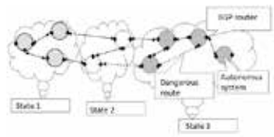


Areas of state responsibility in cyberspace

All the above arguments allowed us to formulate in a discussion with colleagues the definition of a digital border, which is submitted for your discussion:

"The border of the zone of responsibility is the spatial limit of the state's sovereignty, which is determined by the possibility of exerting power over persons engaged in information activities and ensuring the use of ICT within the zone, including by determining the applicable technical regulations"

Streltsov A A



Международный союз электросвязи (англ. International Telecommunication Union (**ITU**)) – международная межправительственная организация в области стандартизации электросвязи. Организация объединяет более 500 правительственных и неправительственных организаций. В её состав входят телефонные, телекоммуникационные и почтовые министерства, ведомства и агентства разных стран, а также организации-поставщики оборудования для обеспечения телекоммуникационного сервиса.

European Telecommunications Standards Institute (рус. Европейский институт по стандартизации в области телекоммуникаций, сокр. **ETSI**) – независимая, некоммерческая организация по стандартизации в телекоммуникационной промышленности (изготовители оборудования и операторы сетей) в Европе. ETSI официально ответственен за стандартизацию информационных и телекоммуникационных технологий в пределах Европы. В ETSI входят более 800 членов из 64 стран мира, включая производителей оборудования, операторов связи, администрации, сервисных провайдеров, исследователей и пользователей – фактически, все ключевые игроки в мире информационных технологий.

Европейский комитет по стандартизации (фр. Comité Européen de Normalisation, **CEN**) – международная некоммерческая организация, основной целью которой является содействие развитию торговли товарами и услугами путём разработки европейских стандартов (евронорм, EN). Организация создана в 1961 году. Одним из главных принципов работы CEN является обязательное использование международных стандартов ISO (IEC) как основы для разработки евронорм либо дополнение тех результатов, которые достигнуты в ISO.

«Корпорация по управлению доменными именами и IP-адресами» (Internet Corporation for Assigned Names and Numbers), сокращённо **ICANN** (читается айкэн[1]) – международная некоммерческая организация, созданная 18 сентября 1998 года при участии правительства США для регулирования вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования Интернета. С 1 октября 2016 года – независимая международная организация.

IANA (от англ. Internet Assigned Numbers Authority – «Администрация адресного пространства Интернет») – функция управления пространствами IP-адресов, доменов верхнего уровня, а также регистрирующая типы данных MIME и параметры прочих протоколов Интернета. Исполняется компанией Public Technical Identifiers, которая находится под контролем ICANN. IANA отвечает за распределение всех зарезервированных имён и номеров, которые используются в протоколах, определённых в RFC. 1 октября 2016 года координирующая роль в исполнении функций IANA перешла в руки международного Интернет-сообщества.

ISOC (Internet Society, Общество Интернета) – ассоциация экспертов, отвечающая за разработку стандартов Интернет-технологий; IAB (Internet Architecture Board, Совет по архитектуре Интернета) – группа в составе ISOC, непосредственно отвечающая за развитие архитектуры Интернет, разработку и сопровождение стандартов протоколов и сервисов Интернет в виде RFC (Reference For Comments); два основных подразделения IAB:

IETF (Internet Engineering Task Force, Рабочая группа инженеров Интернета), решающая текущие задачи в области стандартизации и развития Интернет-технологий.

IRTF (Internet Research Task Force, Исследовательская группа Интернета), решающая проблемные задачи по развитию Интернет-технологий.

Совет по архитектуре Интернета (англ. Internet Architecture Board, англ. **IAB**) – группа технических советников ISOC, которая осуществляет:

Консорциум Всемирной паутины (англ. World Wide Web Consortium, **W3C**) – организация, разрабатывающая и внедряющая технологические стандарты для Всемирной паутины. По состоянию на 29 мая 2019 года Консорциум насчитывает 444 члена.

Сужение области технического регулирования (область ИТКС связанная с критическими информационными инфраструктурами) для атрибуция компьютерных инцидентов

Можно предположить, что такое требование всеобщей деанонимизации и всеобщего контроля будет слишком радикальным и может потребовать значительных технических ресурсов. Можно ограничить такие требования областью критических информационных инфраструктур (КИИ), где важность атрибуции инцидента не вызывает сомнений.

Вместе с тем само понятие критических информационных инфраструктур (КИИ) может иметь разное наполнение в зависимости от их национальной принадлежности. Так, например, в США, Евросоюзе, КНР и РФ существует свое национальное законодательство определяющее это понятие. Для принятия международных мер необходимо общее универсальное определение КИИ, которое будет принято всем мировым сообществом.

На основе этого определения можно сформулировать технические требования к операторам и техническим средствам КИИ, позволяющим осуществлять фиксацию атрибутов инцидента.

Важно при этом обеспечить достоверность и доверие к доказательной базе. Например, для использования фиксируемой информации в качестве доказательной базы можно использовать технологии блокчейна, что позволит исключить возможность манипуляции и подделки фиксируемой информации. Причем сама информация может быть недоступна без разрешения соответствующего национального органа контролирующего национальные КИИ. Технически это можно реализовать, например, используя методы шифрования информации, а ключи для доступа сохранять у операторов КИИ. Другим вариантом может быть самостоятельное хранение информации операторами, предоставляя в распределенный блокчейн только аутентификационные коды хранимой информации.

Техническое регулирование безопасности КИИ в соответствии с ISO15408

Существуют различные документы в отношении атрибуции и расследования инцидентов. Однако хотя все они построены в соответствии с идеологией «общих критериев», но специфика критических инфраструктур в них не рассматривается.

Международной организацией по стандартизации (ISO) были созданы стандарты в области оценки безопасности информационных технологий – “Общие критерии” (ОК).

Кстати, ГОСТ Р ИСО/МЭК 15408, содержащий полный аутентичный текст международного стандарта, принят постановлением Госстандарта России от 4.04.2002 года № 133-ст с датой введения в действие 1 января 2004 года.

Международный стандарт ISO/IEC 15408 является по сути метасредством, задающим систему понятий, в терминах которых должна производиться оценка. Он описывает относительно полный каталог требований безопасности (функциональных и доверия), но не предоставляющих конкретных наборов требований и критериев для ИКТ. **Эти требования и критерии фигурируют в профилях защиты (ПЗ) и заданиях по безопасности (ЗБ).** Предполагается, что профили защиты, в отличие от заданий по безопасности, носят относительно универсальный характер: они характеризуют определенный класс ИКТ или его зависимость от специфики и условий применения.

Именно официально принятые **профили защиты образуют** построенную на основе “Общих критериев” (ОК) и используемую на практике **нормативную базу** в области информационной безопасности (ИБ).

Описывающий ту или иную область системы безопасности профиль (например, профиль КИИ) можно создать с помощью, разработанной в ISO 15408 структуры документа. В стандарте определена также последовательность действий для самостоятельного создания профилей.

Состав профилей защиты (и заданий по безопасности), которые должны учитывать особенности КИИ, включает:

1. **Общие предположения безопасности** – являются частью описания среды, в которой функционирует объект оценки.
2. **Общие угрозы безопасности** – так как современные сервисы безопасности функционируют в распределенной среде, поэтому необходимо учитывать наличие как локальных, так и сетевых угроз.
3. **Общие цели безопасности для объекта оценки** должны быть такими, чтобы их достижение позволяло противостоять угрозам безопасности и реализовать предписания политики безопасности.
4. **Общие цели безопасности для среды** дополняют цели безопасности объекта оценки.
5. **Общие функциональные требования.** Для различных сервисов безопасности общими являются функциональные классы требований, связанные с идентификацией и аутентификацией, управлением доступом, протоколированием и аудитом, а также обеспечением высокой доступности.

В связи с задачей атрибуции инцидентов отдельно выделим:

Класс FAU: Аудит безопасности

Класс FCS: Криптографическая поддержка

Класс FDP: Защита данных пользователя

Класс FIA: Идентификация и аутентификация

Класс FMT: Управление безопасностью

Класс FPR: Приватность

Класс FPT: Защита функций безопасности

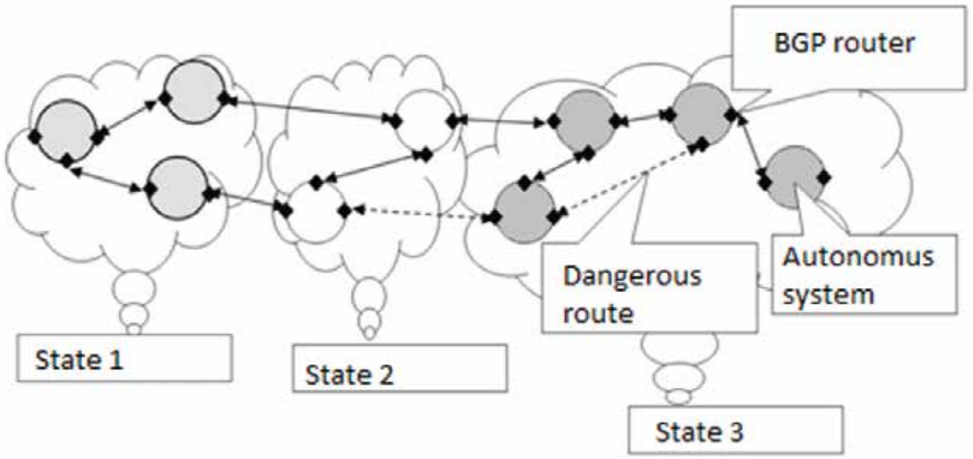
Класс FTA: Доступ к объекту оценки

Класс FTP: Доверенный маршрут/канал

6. **Общие требования доверия безопасности** по сравнению с функциональными, представляются более проработанными, поскольку для них определены удобные на практике оценочные уровни доверия (ОУД).
7. **Специфические требования к сервисам безопасности** – основное внимание посвящено специфическим функциональным требованиям, как наиболее важным для обеспечения безопасности. Управление доступом. МЭ. Аудит. Анонимность. Сертификаты. Анализ защищенности.
8. **Системы активного аудита**
9. **Анализ защищенности** – сравнительно новый, но весьма популярный сервис безопасности, помогающий реализовать профилактический подход к обеспечению защиты информационных систем.
10. **Специфические требования к комбинациям** и приложениям сервисов безопасности.

Зоны ответственности государств в киберпространстве

Таким образом, можно предположить, что ввод через нормативные технические документы (принимаемые международным сообществом) организационных и технических



требований и возможность контролировать их характеризует зону ответственности государства.

Что может представлять в этом случае зона ответственности государства и что можно технически регулировать в ней? Так как вопрос стоит о регулировании администрирования (и как результат маршрутизации) в сети, логичным предположением было бы отнести к зоне ответственности именно центры администрирования провайдеров, транзитных сетей (серверов), атакуемых сетей. Такими центрами администрирования в глобальной сети являются центры администрирования автономных систем. А автономная система, определяемая как обособленная совокупность сетей со своим адресным пространством и под единым управлением, имеет свой уникальный идентификационный номер. И именно по этим номерам строится маршрутизация в глобальной сети. При этом сама автономная система регистрируется (RIR, LIR) как организация – юридическое лицо и поэтому всегда попадает под юрисдикцию государства.

Тогда зоны ответственности государств можно рассматривать как совокупности автономных систем (вместе с их пулом IP адресов) принадлежащих юридическим лицам зарегистрированным в той или иной стране. Границей в этом случае могут стать пограничные маршрутизаторы (граничные шлюзы – известные как Border Gateway).

А это кроме, описанных выше, задач технического регулирования предполагает техническое регулирование граничных сетевых узлов и маршрутизации (создание режима цифровой границы) и необходимость решения ряда правовых проблем, когда, например, организация зарегистрированная в одной стране осуществляет транснациональную деятельность и управляет сетевыми ресурсами на территории другой.

Все приведенные мной выше рассуждения позволили в обсуждениях с коллегами сформулировать определение цифровой границы (приводимая ниже формулировка принадлежит проф. А.А. Стрельцову):

«Граница зоны ответственности, это пространственный предел суверенитета государства, который определяется возможностью оказания властного воздействия на лиц, осуществляющих информационную деятельности и обеспечивающих применение ИКТ внутри зоны, в том числе с посредством определения применяемого технического регламента».

А.К. Жарова
Институт государства и права РАН;
Кафедра правовой безопасности топливно-энергетического комплекса российского Государственного университета нефти и газа им. И.М. Губкина, Москва, Россия

В.М. Елин
Кафедра комплексной безопасности критически важных объектов российского Государственного университета нефти и газа им. И. М. Губкина, Москва, Россия

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ[1]

В сферу обеспечения информационной безопасности экономически развитых государств включены объекты критической информационной инфраструктуры (КИИ). Каждое государство обеспечивает безопасность КИИ организационно-правовыми методами и в данной области невозможно определить единый подход к решению данного вопроса. Максимально жесткий подход демонстрирует США, отраженный в совокупности документов стратегического планирования США[2], содержащие оруэлловские принципы обеспечения безопасности: принцип I – защита американского народа, Америки и американского образа жизни; принцип II – обеспечение процветания Америки; принцип III – сохранение мира методом принуждения; принцип IV – продвижение американского влияния.

В Евросоюзе требование обеспечения безопасности КИИ распространяется на энергетическую и транспортную отрасли. На основании межотраслевых критериев (число жертв, экономические последствия и негативное воздействие на население) Директивой № 2008/114/ЕС Совета Европейского Союза “О европейских критических инфраструктурах и мерах по их защите” допускается отнесение к критической информационной инфраструктуре ряда дополнительных сфер. Методологией идентификации активов и услуг критически важной информационной инфраструктуры, утвержденной Агентством Европейского Союза по кибербезопасности (ENISA) определены следующие информационные инфраструктуры, которые могут быть отнесены к КИИ:

1 Работа выполнена в рамках Проекта РФФИ 20-011-00077 «Правовое регулирование цифрового профиля человека в сети «Интернет»

2 The 2011 U.S. Department of Defense Strategy for Operating in Cyberspace; US Department of Defense Cyber Strategy. 2015; national Cybersecurity Strategy of the United States of America (September 2018)

Таблица1. Характеристика уровня развития обеспечения безопасности КИИ в зарубежных странах

№	Характеристика мероприятий	Характеристика государств
Уровень 1	Отсутствие мероприятий, связанных с защитой критических информационных инфраструктур	Государства, которые определили в качестве критических секторов только транспорт и энергетику
Уровень 2	Идентификация сектора ИКТ как одного из важнейших секторов, требующих внимания	Государства, которые признали сектор информационных и коммуникационных технологий одним из важнейших секторов для поддержания жизненно важных социальных функций
Уровень 3	Разработка общей методологической основы	Государства, у которых есть подробный методологический подход к идентификации деятельности и услуг с конкретными шагами и обязанностями
Уровень 4	Разработка определения КИИ и установление конкретных критериев для идентификации активов КИИ	Государства-члены, которые наиболее продвинулись в области защиты КИИ и приняли особые меры для идентификации и защиты

- промышленные системы управления, включая системы SCADA (диспетчерский контроль и сбор данных) для электростанций, транспортных систем, нефтеперерабатывающих и химических заводов и производственных предприятий;
- инфраструктуры Интернета в т.ч. Интернет-соединения, Inter-X, в т.ч. устойчивость экосистемы подключения к Интернету, разработка безопасного софта;
- интеллектуальные сети (smart grid), под которыми понимается модернизированные электрические сети, зависящие от двусторонней цифровой связи между поставщиком и потребителем, обеспечивающей поддержку интеллектуальных систем измерения и мониторинга;
- финансовые и межбанковские технологии;
- технологии электронного здравоохранения (eHealth);
- транспортный сектор.

Директива № 2008/114/ЕС Совета Европейского Союза «О европейских критических инфраструктурах и мерах по их защите» определяет КИИ как активы, систему или ее часть, расположенные в государствах-членах ЕС, функционирование которых необходимо для решения наиболее важных социальных задач, обеспечения здоровья, безопасности, защиты, экономического или социального благополучия населения; нарушение или уничтожение таких инфраструктур способно вызвать значительные последствия для государства-члена ЕС в виде неспособности исполнения указанных функций[3].

В настоящее время для стран Евросоюза определено несколько уровней обеспечения безопасности критической информационной инфраструктуры[4] (таблица 1).

На этом фоне Российская Федерация предлагает собственный подход к обеспечению безопасности критической информационной инфраструктуры, основными направлениями в котором выступают как безопасность информации ограниченного доступа – ограничение доступа к информации устанавливается федеральными законами[5], так и безопасность КИИ РФ[6] в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

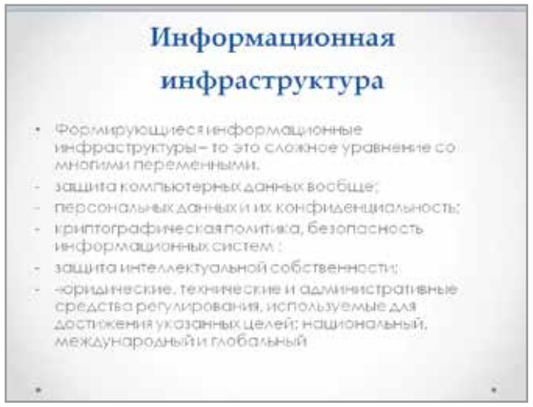
Российский подход к обеспечению правового режима информации ограниченного доступа включает ее целевое назначение; характеристику объекта правового регулирования; правовое положение субъектов правового режима; комплекс способов правового регулирования и средств юридического воздействия.

3 Council Directive no. 2008/114/EC On the Identification and Designation of European Critical Infrastructures and the Assessment of the need to Improve their Protection (Brussel, 8.XII.2008) (Text with EEA relevance) // СПС «Консультант плюс»

4 Methodologies for the identification of Critical Information Infrastructure assets and services// https://www.eN№isa.europa.eu/publicatiO№s/methodologies-for-the-ideN№tificatiO№-of-ciis

5 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» и др.

6 Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «Консультант плюс».



Исключение информации из перечня объектов гражданских отношений, т.е. в отношении нее не может появиться собственник, только обладатель, она не имеет стоимости, осложняет обеспечение режима информации ограниченного доступа. Сделки в отношении информационных объектов запрещены.

Подход, связанный с безопасностью КИИ предполагает:

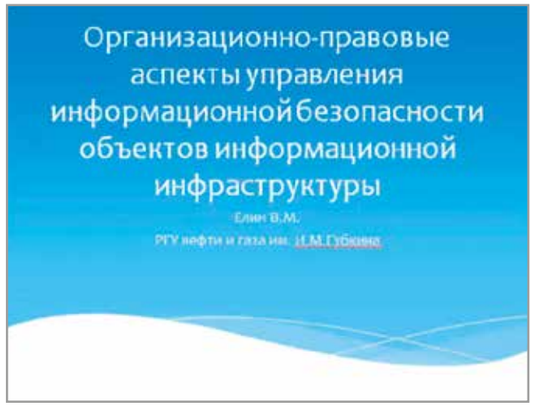
- взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- восстановление функционирования значимого объекта критической информационной инфраструктуры;
- недопущение воздействия на технические средства обработки информации.

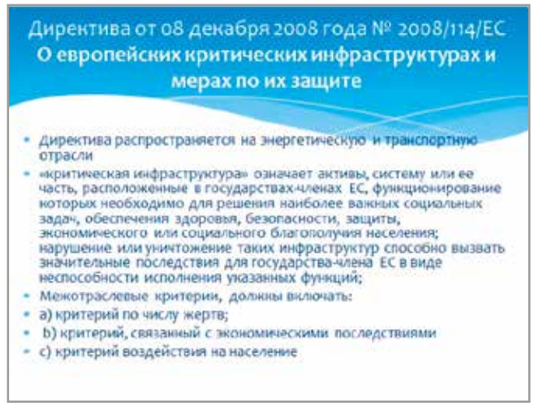
При этом непрерывность и комплексность обеспечения безопасности определены одним из основных принципов обеспечения безопасности КИИ. Дополнительно следует отметить, что политика государства в области информационной безопасности акцентирует внимание на важность контроля за вводимыми в гражданский оборот информационными технологиями и приоритетного использования национальных информационных технологий.

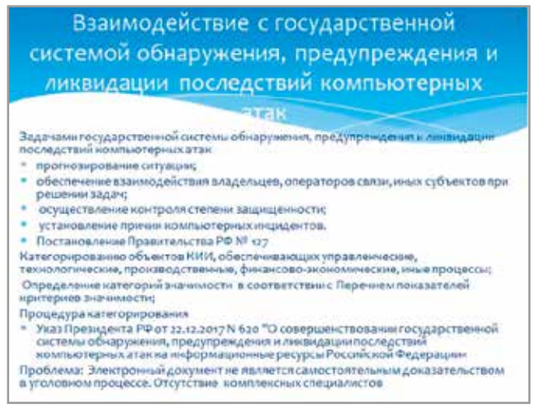
Первый шаг в реализации этой политики связан с разработкой системы национальных стандартов и определения перечня сферы экономических отношений, в которых будет осуществляться контроль и надзор за используемыми информационными технологиями. Для информационных технологий, используемых субъектами в сферах, отличных от КИИ, правовое регулирование пока меняется достаточно медленно.

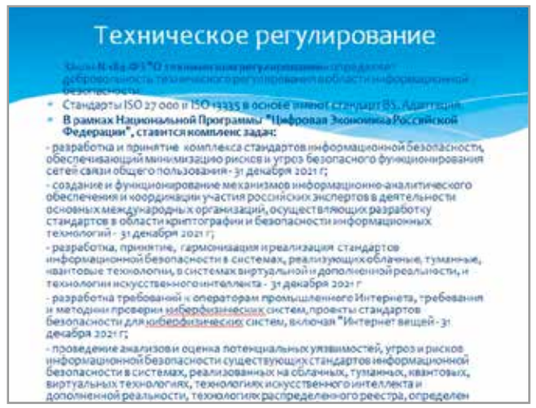
Следует иметь в виду, что Федеральный закон № 184-ФЗ «О техническом регулировании» определяет добровольность технического регулирования в области информационной безопасности. Учитывая изложенное, в рамках Национальной Программы “Цифровая Экономика Российской Федерации”, ставится комплекс задач:

- разработка и принятие комплекса стандартов информационной безопасности, обеспечивающий минимизацию рисков и угроз безопасного функционирования сетей связи общего пользо-









вания – 31 декабря 2021 г. Необходимо учитывать, что стандарты ISO 27 000 и ISO 13335, являющиеся основными стандартами обеспечения информационной безопасности основаны на стандарте «British standards» (BS).

- создание и функционирование механизмов информационно-аналитического обеспечения и координации участия российских экспертов в деятельности основных международных организаций, осуществляющих разработку стандартов в области криптографии и безопасности информационных технологий – 31 декабря 2021 г;
- разработка, принятие, гармонизация и реализация стандартов информационной безопасности в системах, реализующих облачные, туманные, квантовые технологии, в системах виртуальной и дополненной реальности, и технологии искусственного интеллекта – 31 декабря 2021 г
- разработка требований к операторам промышленного Интернета, требования и методики проверки киберфизических систем, проекты стандартов безопасности для киберфизических систем, включая «Интернет вещей» – 31 декабря 2021 г;
- проведение анализов и оценка потенциальных уязвимостей, угроз и рисков информационной безопасности, существующих стандартов информационной безопасности в системах, реализованных на облачных, туманных, квантовых, виртуальных технологиях, технологиях искусственного интеллекта и дополненной реальности, технологиях распределенного реестра, определен перечень необходимых стандартов, ресурсное обеспечение – 31 декабря 2021 г.

Заключение

Проблема обеспечения информационной безопасности объектов КИИ требует комплексного подхода с необходимостью разработки и принятия российских норм правового и технического регулирования.

Для обеспечения безопасности российских пользователей информационных технологий необходимо включить в национальную систему сертификации информационных технологий стандарты продуктов или услуг в области информационной безопасности, в том числе безопасности аппаратного и программного обеспечения.

А.Я. Капустин

Доктор юридических наук, профессор, президент Российской ассоциации международного права, и.о. заведующего отделом зарубежного конституционного, административного, уголовного законодательства международного права Института законодательства и сравнительного правоведения при Правительстве Российской Федерации

МЕЖДУНАРОДНО-ПРАВОВАЯ КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ СУВЕРЕНИТЕТА ГОСУДАРСТВА В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Суверенитет государства – научная категория, имеющая междисциплинарный характер. В свое время еще И.Д. Левин указывал, что «понятие суверенитета является преважнейшим, кардинальным понятием государственного и международного права»[1]. Разумеется, понятие суверенитета широко используется не только в юридической, науке, но и в смежных отраслях гуманитарного знания и обществоведения. Несмотря на такое широкое научное признание в ходе развития человеческой цивилизации, само явление, обозначаемое данной категорией, постоянно сталкивается с новыми вызовами в различных сферах общественных отношений.

Подобные метаморфозы, видимо, далеко не случайны, суверенитет как важнейшее свойство государственной власти, означающее ее верховенство, независимость и самостоятельность, заключает в себе основополагающую идею государства[2]. Государство как политико-правовой феномен, реализует свою сущность внутри страны, его назначение состоит в управлении процессами реализации стоящих перед человеческим обществом исторически значимых задач его существования и развития. Государство – это организация, обладающая верховной политической властью на определенной территории[3]. Исторически сложилось так, что государство существует не в вакууме, а в сообществе себе подобных государств, с которыми оно вступает в отношения и постоянно взаимодействует. Соответственно, без государства и его качественной характеристики – суверенитета, невозможно представить себе существование систем национального права, равно как и международного права, которое регулирует отношения между государствами.

Воззрения на суверенитет как политико-правовую доктрину и явление государственной жизни стали складываться в XVI веке, основоположником учения о суверенитете признается Жан Боден, который систематизировал представления об обязательном признаке государственной власти, идеалом которой он признавал монархию. За истекшие четыре столетия учение о государстве как политико-правовом институте неоднократно менялось, сообразно переменам его правовых форм и видов. Не оставалась без внимания и доктрина суверенитета государства, подвергаясь различным воздействиям и трансформациям, повлиявшим на понимание его природы, источников и форм.

В настоящее время под государственным суверенитетом понимается верховенство государства в пределах границ своей территории и его независимость на международной арене[4]. Сам государственный суверенитет часто признается свойством государственной власти[5] , которой присущи такие качества как верховенство, публичность и единство. Верховенство государственной власти состоит в том, что в пределах территории данного государства не может быть власти, стоящей выше нее. Ее публичность означает ее связь с интересами всего общества. Единство государственной власти выражается в том, что она имеет единый социальный источник, для выполнения своего функционального назначения она имеет единые цели, задачи и направления деятельности. Независимость государственной власти вовне, то есть за пределами границ государства, означает самостоятельность государства, способность свободного и независимого существования и развития среди других народов и государств[6] . Обе стороны суверенитета государства (внутренняя – верховенство и внешняя – независимость от других государств) взаимосвязаны и взаимообусловлены, но не следует забывать, что исторически становлению самостоятельных государств предшествовало утверждение высшей государственной власти внутри определенной территории.

В XXI веке в мире продолжаются процессы глобализации в различных сферах жизни общества (политической, экономической, финансовой, информационной и др.), в условиях которых, как это неоднократно бывало и в прошлом[7], наблюдаются попытки девальвации понятия государства и его суверенитета. В западной международно-правовой литературе высказываются различные идеи, концепции об исчерпании в современном мире возможностей государственного суверенитета, что «по мере глобализации и приватизации идея суверенного государства становится все менее похожей на реальный мир, включающий такие факты, как крупномасштабное перемещение людей и капитала, идей и информации за рамками контроля даже мощных в военном отношении государств»[8]. Созвучно этому и скандально известное[9] предложение американского юриста Л. Хенкина о том, что надо прекратить использовать слово “S”, так как «суверенитет государств в международных отношениях – это, по сути, ошибка, незаконнорожденное детище».

Обращает на себя внимание, что в подобных утверждениях речь идет о расщеплении единого понятия государственного суверенитета и попытке исключить его из употребления в международной сфере. Если отвлечься от того, что подобные теории «исключения» внешнего суверенитета государства, основанные на описании отдельных фрагментарных явлений международных отношений, носят характер легковесных интеллектуальных упражнений, то следует признать их весьма ограниченное применение и рассматривать как традиционный скепсис исследователей в отношении международного права и роли государств в его развитии. Однако, нельзя не заметить, что подобные взгляды появляются в период не только глобализации, но совпадают по времени с попытками установления монополярного мира, модель которого действительно плохо сочетается с международным правом и тем более с признанием суверенитета других государств. Неудивительно, что под предлогом формального характера общепризнанных норм международного права предлагается отбросить принцип суверенного равенства государств, представляющий один из важнейших элементов системы международно-правовой защиты суверенитета. Между тем, очевидно, что общепризнанные принципы и нормы международного права, в том числе принципы Устава ООН, не просто являются важнейшей частью современного международного права, они, кроме того, стали неотъемлемой частью самой системы современных международных отношений. Попытки дезавуировать или исключить их из действующего международного права ведут к дезорган-

1 См.: Левин И.Д. Суверенитет. М., 1948, с. 3.

2 См.: Грачев Н.И. Происхождение суверенитета. М., 2009, с. 40.

3 См.: Лазарев В.В., Липень С.В. Теория государства и права. М., 2015, с. 69.

4 См.: Черниченко С.В. Контуры международного права. М., 2014, 228;

5 См.: Моисеев А.А. Суверенитет государства в современном мире. Международно-правовые аспекты. М., 2006, с.27.

6 См.: Грачев Н. И. Указ. соч., с.48- 72.

7 Как отмечает Н.И. Грачев «в настоящее время происходят процессы, характерные для преддверия Нового времени, только с обратным знаком». См.: Грачев Н.И. Указ. Соч., с. 10. Левин И.Д. также отмечает, что многие зарубежные юристы в то время приходили «к отрицанию суверенитета как понятия «устаревшего»», предлагая его заменить «понятием внутренней компетенции государства, демаркируемой международным правом». См. Левин И.Д. Указ. Соч., с. 111.

8 См.:Kennedy D. The Mystery of Global Governance//Ohio Northern University law review. 2008, v. 34, p. 830.

9 См.: Henkin L. “That “S” word: Sovereignty, and Globalization, and Human Rights, et cetera//Fordham law review. 1999, vol.68, p,2.

зации и хаосу всей системы международных отношений. Трудно не согласиться с мнением судьи Международного суда в отставке, австралийским ученым, профессором Дж. Крауфордом, который утверждает, что «несмотря на неоднократные предположения об устаревании или смерти суверенитета как идеи, его нормативная основа сохраняется»[10]. Следовательно, здравомыслящие специалисты различных национальных школ международного права, не отрицая некоторых дискуссионных моментов в подходах к понятию государственного суверенитета, ясно дают понять, что лучшего средства для защиты национальных интересов в современных международных отношениях у государств нет.

Размывание концепции суверенитета государства отмечается также в связи с широким распространением в мире информационно-коммуникационных технологий (ИКТ) и с появление так называемого «виртуального пространства», которое наиболее радикальными сторонниками объявляется пространством, свободным от суверенитета государства. Сама по себе постановка вопросов зон, свободных от суверенитета не кажется какой-то чересчур радикальной или юридически некорректной. Как известно, в международном праве есть понятие «международных территорий», статус которых определяется международными договорами или обычными нормами международного права. В указанных территориях государства могут осуществлять либо юрисдикцию, либо отдельные суверенные права. К таким территориям международно-правовая доктрина относит открытое море, воздушное пространство над открытым морем, Антарктиду, космос и небесные тела.

Концепция суверенитета государств в международном праве получила подкрепление в целом ряде международно-правовых актов и судебной практике. В доктрине международного права признается, что территориальное верховенство государства является важнейшим элементом его суверенитета[11]. Тезис о том, что суверенитет означает высшую и полную власть над определенной территорией и над населяющим ее народом, исключающую любую другую власть, четко и недвусмысленно подтверждается в международной судебной практике. Так, судья Международного суда ООН М. Альварес в особом мнении по делу «О проливе Корфу» подтвердил, что под суверенитетом «мы понимаем всю совокупность прав и атрибутов, которыми государство обладает на своей территории, исключая все другие государства, а также в его отношениях с другими государствами[12].

Исследователи указывают на то, что территориальное измерение суверенитета объясняется тем, что его возникновение как политической и правовой концепции совпало с возникновением государства как политической единицы после распределения территорий и политического и правового признания такого территориального разделения Вестфальским договором[13]. Подобное понимание природы и причин появления государственного суверенитета поддержал судья М. Гувер в арбитражном разбирательстве дела о государственной принадлежности острова Пальмас, который заявил, что «территориальный суверенитет служит для разделения между государствами пространства, на котором осуществляется человеческая деятельность»[14].

Вместе с тем, признавая неразрывную связь суверенитета, государственной власти и территории, следует указать на один интересный парадокс, который в этой коммуникации проявляется, определяя пределы самого суверенитета. Высший абсолютный характер государственной власти, проявляемый в суверенитете, благодаря понятию территории, как сферы действия суверенитета, делает ничем не ограниченную, высшую власть локализованной на определенной территории, в пределах которой она проявляет свои качества, определяющие природу суверенитета[15]. Локализация суверенитета в пределах определенной территории, делает территорию не только объектом, но и своего рода «вместилищем» суверенитета[16].

Подобное понимание территориальных пределов суверенитета позволяет уточнить, что если внутренний суверенитет по своей сути есть суверенитет над территорией и проживающим на ней населением, является полным и исключительным, то внешний суверенитет означает «независимость, неподчиненность другому государству или какой-либо организации внутри страны во внешних делах»[17]. Объективные условия побуждают государства вступать в отношения с другими государствами на основе международных соглашений или иных договоренностей. Международные договоры государств устанавливают определенные рамки поведения их участников. Данный факт приводит некоторых исследователей к выводу о том, что это влечет за собой признание возможности ограничения суверенитета международным правом[18]. Так, в зарубежной литературе высказывается мнение, что «внешний суверенитет означает власть над внешними факторами, но, поскольку все суверенитеты равны и имеют равную претензию на внешний суверенитет, осуществление суверенной власти за пределами государственной территории одним из них будет посягать на суверенитет других. Таким образом, внешние проявления суверенитета скоординированы и управляемы через согласие. Согласие является суверенным актом добровольного согласия (молчаливого согласия)[19].

Однако добровольность согласия не означает ограничения суверенитета государства, поскольку у государства сохраняется право выйти из того или иного соглашения или международной организации. Согласие государства на обязательность норм международного договора не носит необратимого характера. Соответственно, следует признать более реалистичной точку зрения о том, что «участие государства в многостороннем общении и международных организациях путем реализации любого объема и качества своих неотъемлемых прав является не ограничением, а реализацией суверенитета»[20]. Сегодня к этому можно добавить уточнение, что реализация внешних полномочий государственными органами должна осуществляться на основе национальной конституции.

Вопрос возможности осуществления государственного суверенитета в киберпространстве в принципе должен решаться на основе общих подходов, выработанных наукой в отношении понятия и природы суверенитета. Можно согласиться с тем, что развитие информационно-коммуникационных технологий на современном этапе выступает фактором, воздействующим на функционирование права, государства и других общественных институтов. Более дискуссионным выглядит утверждение о том, что в «результате расширения коммуникационных границ снижается значимость пространственно-временных и национальных границ»[21]. Особенно трудно согласиться с ослаблением актуальности национальных границ, поскольку государства крайне негативно реагируют на любые попытки какого-либо их нарушения, особенно это заметно в международных кризисных или конфликтных ситуациях, что естественно не тождественно недооценки роли информационно-коммуникационных границ в межгосударственном общении.

Еще более наивным выглядит «ниспровержение» суверенитета, ввиду того, что «будучи альтернативным пространственным измерением, киберпространство является фактором разрушения Вестфальской системы, в том числе и трансформации ее стержня – института суверенитета»[22]. Подобные утверждения не более чем формирование мифологических представлений о современной межгосу-

10 См.: Crawford J. Sovereignty as a legal value// Crawford J., Koskenniemi M. The Cambridge companion to international law. Cambridge, 2012, p.129.

11 См.: Моисеев А.А.Указ. соч., с. 18; Броунли Я. Международное право. В 2-х книгах. Книга 1, М., 1977, с. 173-201; Эдуардо Хименес де Аречага. Современное международное право. М., 1983, с.205-209.

12 См.: Corfu Channel Case (UK v. Albania) (Separate Opinion of Judge Alvarez) [1949] ICJ Rep 43.

13 См.: Моисеев А.А. Указ.соч., с. 12-13; Tsagourias N. The legal status of cyberspace//Tsagourias N., Buchan R. Research handbook on International law and Cyberspace. Cheltenham, 2015, p.17.

14 См.: Island of Palmas Case (or Miangas) (United States v. Netherlands) [1928] Reports of International Arbitral Awards, p. 839.

15 Как отмечал И.Д. Левин: «Власть, не терпящая сопротивления действием со стороны какой-либо силы, находящейся на этой территории (полновластие), или вмешательства извне (независимость), составляет внутренний суверенитет». См.: Левин И.Д. Указ.соч., с. 103.

16 См.: Tsagourias N., p.17.

17 См.: Левин И.Д. Указ. соч., с. 104.

18 См.: Василенко В.А. Проблемы теории международного права. Киев, 1989, с. 23.

19 См.: Tsagourias N., Op/ cit., p.17-18.

20 См.: Моисеев А.А. Указ.соч., с.

21 Терентьева Л.В. Концепция суверенитета государств в условиях глобализационных и коммуникационно-информационных процессов// Право. Журнал Высшей школы экономики. 2017. N 1 СКП «КонсультантПлюс.

22 См.: Шарифов М.Ш. Суверенная власть в киберпространстве и в сетевом пространстве // Современное право. 2009. № 6. С. 41.

дарственной системе, которая естественно, адаптируется к реалиям киберпространства, но не до такой разрушительной степени. Государство по-прежнему укрепляет свой суверенитет, примером чего может быть проведенное в 2020 г. в России обновление Основного закона, которое в значительной степени способствовало утверждению верховенства Конституции РФ, укреплению суверенитета российского государства.

Для того, чтобы определить хотя бы контуры ответа на вопрос о значении государственного суверенитета для киберпространства, надо хотя бы в общих чертах понять, что представляет собой это «альтернативное пространственное измерение». В социологической литературе даются следующие характеристики киберпространства. По мнению Д.Е. Добринской «киберпространство, или по-другому цифровая среда, — это пространство функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей»[23]. Специалистами по ИКТ киберпространство определяется как «глобальная сфера внутри информационной среды, отличный и уникальный характер которой оформлен использованием электронного и электромагнитного спектра для создания, сохранения, изменения, обмена и использования информации через независимые и взаимосвязанные сети, использующие информационно-коммуникационные технологии»[24].

Из этого сложного для понимания непрофессионалами нагромождения слов можно заключить, что данная метафорическая конструкция, означает набор компьютерных технологий, позволяющий производить все возможные действия с информацией и поддерживать межличностные коммуникации. Те же ИКТ специалисты позволяют выстроить конструкцию, которая дает возможность составить представление о правовом статусе киберпространства. В частности, отмечается, что «киберпространство состоит из трех слоев: физического слоя, который состоит из компьютеров, интегральных микросхем (ИС, интегральных схем, интегрированных цепей), кабелей, телекоммуникационной инфраструктуры и тому подобное; второй слой предполагает программные продукты; и, наконец, третий слой включает пакет данных и электронику»[25]. На основе этого делается вывод, что «ядро киберпространства может образовывать виртуальное пространство, которое тем не менее поддерживается физическими объектами, такими как компьютеры, которые соединяют неприводимую часть киберпространства и физический мир»[26].

Поскольку ИКТ предназначены для пользования людьми, которые располагаются на определенной территории, государство может осуществлять юрисдикцию как в отношении информационно-коммуникационной инфраструктурой, так и в отношении пользователей – граждан или иных лиц, расположенных и проживающих на данной территории (принцип реальной, тесной и фактической связи гражданина с государством – признанный международно-правовой критерий установления юрисдикции)[27].

В литературе отмечается, что «государство может осуществлять юрисдикцию над информацией, распространяемой через киберпространство в пункте доставки, а также в пункте получения или когда информация пересекает через провода и линии, подпадающие внутри его юрисдикции»[28]. Разумеется, государство может осуществлять юрисдикцию над вэб-адресами в случае, если они зарегистрированы в нем. Следовательно, государство может осуществлять свою законодательную, административную, предписывающую и исполнительную юрисдикцию в киберпространстве и над кибердеятельностью на своей территории как в отношении граждан, так и иных лиц.

Отсюда следует, что государственный суверенитет распространяется на киберпространство посредством осуществления государством юрисдикции в пределах его территории. Но это затрагивает внутренний аспект суверенитета государства. Как убедительно было доказано, государство вправе установить правовое регулирование соответствующих вопросов в своих национальных интересах, что легитимно с точки зрения современного международного права.

В отношении внешнего аспекта суверенитета следует заметить, что противоправное применение киберпространства в противоречие с императивными принципами и нормами международного права, включая принципы Устава ООН, позволяет государству, которое подверглось кибератакам, применить необходимые меры обеспечения национальной безопасности и обеспечения своего суверенитета. Но подробное рассмотрение этого вопроса заслуживает отдельного исследования.

23 См.: Добринская Д.Е. Киберпространство: территория современной жизни//Вестник Москвоского университета. Серия 18. Социология и политология. 2018.Т.24. № 1., с.52-70.

24 См.: Kuehl T.Daniel. From cyberspace to cyberpower: defining the problem// Kramer D. Franllin, Star H.Stuart, Wentz K,Larry. Cyberpower and National Security. W., 2009, p.28.

25 См.: Tobansky L. Basic concepts of cyber warfare//Military and Strategic Affairs. 2011, vol. 75, p. 77-78.

26 См.: Bryant R. What kind of space is cyberspace? Minerva. An Internet Journal of Philosophy. 2001, V. 5, p. 138.

27 См.: Nottenbohm Case (Lichtenstein v. Guatemala) [1955] ICJ Rep 4 23. В отношении распространения юрисдикции на неграждан государства соответствующее положение содержится в упоминавшемся выше деле «Лотос», рассмотренном Постоянной палатой международного правосудия, в особом мнении судьи Мора.

28 См.: Kanuck S. Sovereign discourse on cyber conflict under international law// Tax Law review, 2010, v. 88 (7), p. 1573-1575.I

В.А. Горжалцан
Первый заместитель директора.
Координационный центр доменов .RU/.РФ

ВИЗУАЛИЗАЦИЯ ГЕОЛОКАЦИИ И ТОПОЛОГИИ АВТОНОМНЫХ СИСТЕМ И ПРОЦЕССОВ В ИКТ-СРЕДЕ

В ноябре 2020 года Глобальная комиссия по стабильности киберпространства (GCSC) провела виртуальные сессии на пятнадцатом ежегодном заседании Форума по управлению Интернетом (IGF). Также опубликован Заключительный отчет. Некоторые выводы из которого я бы хотел привести далее для того, чтобы рассмотреть основы стабильности системы Ядра Интернета и задачи, которые предстоит решать для ее укрепления.

Но прежде, на мой взгляд, следует отметить на каком этапе развития международной стабильности находится глобальный мир. Признательный вывод Комиссии на слайде 2.

Мы подошли к концу двадцатипятилетнего периода стратегической стабильности и относительного мира между крупными державами. Конфликты между государствами приобрели новые формы, и киберативность играет ведущую роль в этой новой нестабильной среде. За последнее десятилетие количество и изощренность кибератак со стороны государственных и негосударственных субъектов увеличились, что угрожает стабильности киберпространства. Проще говоря, люди и организации могут больше не быть уверены в своей способности безопасно и надежно использовать киберпространство или быть уверенными в доступности и целостности услуг и информации.

В Отчете Комиссия дала определения СТАБИЛЬНОСТИ КИБЕРПРОСТРАНСТВА и ПУБЛИЧНОМУ ЯДРУ КИБЕРПРОСТРАНСТВА.

Определение Стабильности мы видим на слайде 3.

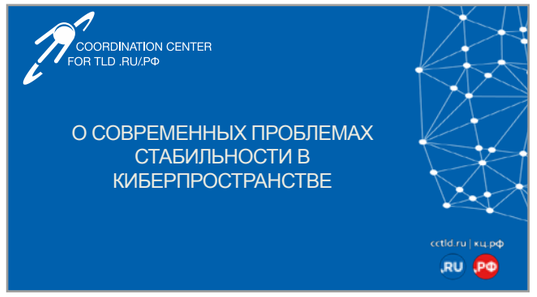
Стабильность киберпространства определяется как ситуация, когда все пользователи вполне уверены в том, что они могут пользоваться возможностями киберпространства безопасным и надежным образом, что доступность и целостность данных и сервисов в киберпространстве в общем и целом гарантирована, что управление переменами происходит сравнительно мирно и что возникающие противоречия регулируются без их эскалации.

Как видим, несмотря на драматическое заключение комиссии об окончании 25 летнего периода стабильности, она все же предлагает определение Стабильности с некими гарантированными нормами (приведенными далее) в постоянно меняющемся технологическом ландшафте киберпространства и, в частности, в публичном ядре. А что такое публичное ядро?

Комиссия определяет фразу «публичное ядро Интернета», чтобы включить такие критические элементы инфраструктуры Интернета, как маршрутизация и пересылка пакетов, системы имен и нумерации, криптографические механизмы безопасности и идентификации, средства передачи, программное обеспечение и дата-центры.

Как видим это определение, включает элементы критической инфраструктуры. И далее в Отчете комиссии раскрываются и конкретизируются отдельные элементы Критической инфраструктуры. Элементы маршрутизации и пересылки пакетов на слайде 5.

Элементы маршрутизации и пересылки пакетов включают в себя, помимо прочего, (1) оборудование, средства, информацию, протоколы и системы, которые облегчают передачу пакетных сообщений от их источников к их получателям; (2) точки обмена трафиком (физические сайты, на которых создается



пропускная способность Интернета); (3) одноранговые и базовые маршрутизаторы основных сетей, которые передают эту полосу пропускания пользователям; (4) системы, необходимые для обеспечения аутентичности маршрутизации и защиты сети от злонамеренного поведения; (5) проектирование, производство и цепочка поставок оборудования, используемого для вышеуказанных целей; и (6) целостность самих протоколов маршрутизации и процессов их разработки, стандартизации и обслуживания.

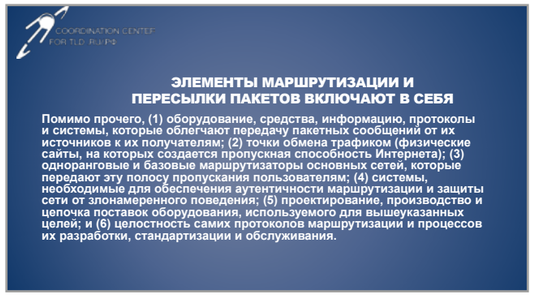
Далее конкретизируются Системы именования и нумерации – это системы DNS и другие на слайде 6.

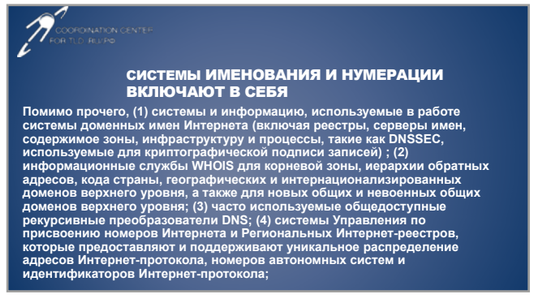
Системы именования и нумерации включают в себя, помимо прочего, (1) системы и информацию, используемые в работе системы доменных имен Интернета (включая реестры, серверы имен, содержимое зоны, инфраструктуру и процессы, такие как DNSSEC, используемые для криптографической подписи записей); (2) информационные службы WHOIS для корневой зоны, иерархии обратных адресов, кода страны, географических и интернационализированных доменов верхнего уровня, а также для новых общих и невоенных общих доменов верхнего уровня; (3) часто используемые общедоступные рекурсивные преобразователи DNS; (4) системы Управления по присвоению номеров Интернета и Региональных Интернет-реестров, которые предоставляют и поддерживают уникальное распределение адресов Интернет-протокола, номеров автономных систем и идентификаторов Интернет-протокола.

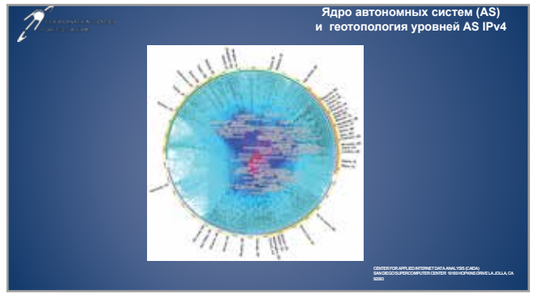
Не буду конкретизировать остальные элементы публичного ядра из-за ограниченного времени. Мы рассмотрим только элементы маршрутизации и пересылки пакетов и, в частности, более подробно рассмотреть ядро автономных систем (AS), которое по терминологии Комиссии называется – Элементы маршрутизации, пересылки пакетов и системы нумерации. Сделаем это с помощью существующих средств визуализации, например, инструментов Центра прикладного анализа данных в Интернете (CAIDA). Этот Центр проводит сетевые исследования и создает исследовательскую инфраструктуру для поддержки, сбора, курирования и распространения данных среди научно-исследовательского сообщества. CAIDA базируется в суперкомпьютерном центре Сан-Диего, расположенном в Калифорнийском университета в Сан-Диего (Center for Applied Internet Data Analysis (CAIDA) San Diego Supercomputer Center 10100 Hopkins Drive La Jolla, CA 92093).

Этот инструмент позволяет сделать макроскопический снимок образцов топологии Интернета IPv4, снятых в течение года. На слайде 7.

Снимок иллюстрирует как обширный географический охват, так и взаимосвязь узлов, участвующих в глобальной системе марш-







рутизации Интернета. Снимок отображает географическое расположение автономных систем Интернета (AS) – мы видим номера и названия автономных систем, количество клиентов и взаимосвязей. Каждая AS примерно соответствует интернет-провайдеру (ISP). Положение каждого узла AS отображается в полярных координатах (радиус, угол) на окружности, рассчитанных по специальной формуле. Давайте вспомним как в плоскости отображаются в полярных координатах географические объекты.

Москва – примерно 37° восточной долготы, а Владивосток примерно – 130° восточной долготы.

У автономных систем на внешнем краю круга нет клиентов, а у автономных систем в центре наибольшее количество клиентов (красным цветом). Угловая координата указывает на географическую долготу AS. Трафик, исходящий идет от AS в одну сторону, а финансовые потоки за транзит – в обратную.

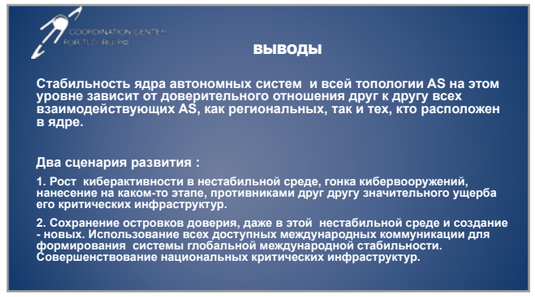
Для этой визуализации использовали набор данных топологии интернета за февраль 2017 года. AS ранжируются не по исходящей линии, а по их транзитному значению. Ядро этой топологии (отмечается красным цветом), набор автономных систем с самыми большими конусами клиентов (это закрытый клуб провайдеров). Это в основном американские автономные системы. Это так называемые сети 1-го уровня – Tier1 на слайде 9.

Мы видим здесь IXP-точки обмена трафиком, объединенные по геолокационному направлению. Pop 1, 2 и 3 точки объединения маршрутизаторов по геолокационному направлению.

Наиболее распространенное и общепринятое определение сети уровня 1 – это сеть, которая может подключиться к любой другой сети в Интернете без покупки IP-транзита или оплаты пиринга. Согласно этому определению, сеть уровня 1 должна быть сетью без транзита (без покупки транзита), которая бесплатно взаимодействует с любой другой сетью уровня 1 и может достигать всех основных сетей в Интернете.

В этой сети обычно порядка 2-х десятков AS (таких как AT&T, Orange, Verizon, Deutsche Telekom Global и др.). Это закрытый клуб. Они никому не платят за транзит. Все сети платят им. Напомню, что данные модели условные и сильно упрощены.

Как видим доминирование AS в ядре, это, казалось бы, в чем-то очевидное преимущество-AS этого клуба. Но это благополучие возникает потому, что финансовые потоки идут из региональных AS. Поэтому здесь важно доверительное отношения друг к другу всех взаимодействующих AS. **Эта доверительность обеспечивает стабильность всей системы. У этой стабильности есть очень серьезный аргумент-ДОВЕРИЕ ради бизнеса.**



Таким образом, мы видим естественный физический островок Стабильности, несмотря на декларацию об окончании периода стратегической стабильности.

Конечно, рассматривая схема значительно упрощает действительную ситуацию, но она позволяет рассмотреть и понять процессы, происходящие в ядре AS.

Выводы

Стабильность ядра автономных систем и всей топологии AS на этом уровне зависит от доверительного отношения друг к другу всех взаимодействующих AS, как региональных, так и тех, кто расположен в центре ядра.

Итак, что будет происходить дальше – после окончания «периода относительной стабильности» (Заключительный отчет Глобальной комиссии по стабильности киберпространства (GCSC). Глобальная комиссия не дает ответ на этот вопрос. Какие сценарии пост- стабильного периода возможны:

Мне видится два сценария:

1. Рост кибератаки в нестабильной среде, гонка кибервооружений, нанесение на каком-то этапе, противниками друг другу значительного ущерба его критических инфраструктур.
2. Сохранение островков доверия, даже в нестабильной среде и создание – новых. Использование всех доступных международных коммуникаций **для формирования системы глобальной международной стабильности.** Совершенствование национальных критических инфраструктур.

Второй вариант мне представляется более оптимистичным и надеюсь, что стороны будут следовать по данному сценарию.

М.В. Анисимов
старший менеджер, Международная компания по распределению доменных имен и адресов, США

ICANN КАК НАБЛЮДАТЕЛЬ ТЕКУЩЕЙ ДИСКУССИИ В ГОСУДАРСТВЕННЫХ И МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЯХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Интернет – это общий ресурс, который принадлежит всему человечеству. Для того чтобы он работал и развивался стабильно, необходимы усилия всех заинтересованных сторон, государства, бизнеса, академического и гражданского сообщества.

Корпорация ICANN совместно с другими техническими организациями и партнерами по всему миру работает над поддержкой некоторых наиболее чувствительных частей инфраструктуры интернета. В частности, ICANN занимается обеспечением стабильности и безопасности работы системы доменных имен, что особенно важно для обеспечения функциональной совместимости глобальной сети. И в течение тех 20 лет, во время которых ICANN выполняла эту функцию, в ней не было сбоев.

ICANN участвует в разработке политик с использованием мультистейкхолдерного подхода, то есть с учетом мнений всех заинтересованных сторон. Важно отметить, что ICANN – это техническая организация, и мы не занимаемся вопросами, которые лежат вне технической сферы. Однако именно техническая экспертиза позволяет нам лучше понимать, как различные регуляторные практики могут повлиять на работу инфраструктуры Интернета.

В ICANN действует департамент по работе с правительствами и межправительственными организациями. Это своего рода think tank – исследовательско-аналитический отдел, который занимается анализом различных регуляторных практик во всем мире. Его специалисты занимаются исследованием того, как регулирование интернета в области информационной безопасности может сказаться на стабильности, безопасности и функциональной совместимости Интернета, а также на выполнение корпорацией ICANN своей функции.

В 2019 году была принята стратегия корпорации ICANN на 21-25 годы, и впервые туда была включена оценка того, как регуляторная практика может повлиять на работу международной системы технических идентификаторов. В результате ICANN готовит обзоры регуляторных практик в разных странах и регионах мира.

В начале 2021 года был подготовлен большой отчет, в котором приведены основные российские инициативы в области регулирования Интернета, а также те инициативы, которые были представлены Российской Федерацией в ООН. Отчет доступен публично на сайте корпорации ICANN, он опубликован на английском и русском языках. Важно отметить, что этот отчет не содержит оценок этим инициативам, только описание. Отчет предназначен для информирование широкого круга специалистов в сообществе ICANN по всему миру.

Ашраф Патель
исследователь в сфере цифровой экономики, Институт глобального диалога, ЮАР

По техническим причинам Ашраф Патель не смог выступить на Форуме, но предоставил текст своего выступления на английском языке для публикации в сборнике.

КАКИМ СТАНЕТ УПРАВЛЕНИЕ ИНТЕРНЕТОМ В БУДУЩЕМ? СООБРАЖЕНИЯ, ВЫСКАЗАННЫЕ НА ЧЕТЫРНАДЦАТОМ МЕЖДУНАРОДНОМ ФОРУМЕ ПО ВОПРОСАМ УПРАВЛЕНИЯ ИНТЕРНЕТОМ В БЕРЛИНЕ, И БОЛЬШЕ

Ежегодная конференция «Форум по вопросам управления Интернетом», поддерживаемая ООН, состоялась 25–29 ноября 2019 в Берлине. На фоне сложной ситуации для мультилатерализма, когда глобалисты столкнулись с ростом экономического национализма, обсуждение проблем цифровой экономики вновь стало предметом споров на Форуме по вопросам управления Интернетом (далее – ФУИ). Тема «Один мир. Одна сеть. Одно видение.» была особенно уместной и актуальной.

Генеральный секретарь Организации Объединенных Наций Антонио Гутерриш также ссылается на Организацию Объединенных Наций как на соответствующую платформу, в рамках которой все соответствующие субъекты могут встречаться для решения таких глобальных проблем. Это может свидетельствовать о том, каким образом может быть определена будущая роль и функции ФУИ. В своем вступительном заявлении канцлер Германии Ангела Меркель подчеркнула преимущества Интернета и стратегическую значимость физической инфраструктуры, которая обеспечивает поток данных и информации, соединяя континенты и регионы. Ее размышления были сосредоточены на вопросе цифрового суверенитета, а также на рисках протекционистских подходов и проблемах крупных технологий. Говоря о технологических достижениях, она напоминает нам, что, хотя что-то технически осуществимо и возможно в сети, это не означает, что это является желательным с этической точки зрения.

Меркель считает, что процесс глобальной цифровой политики быстро меняется. Описывая это изменение как «реорганизацию управления Интернетом», она повторила слова Гутерриша об ООН как о базе для переориентации глобальной политики Интернета. Например, общий регламент защиты персональных данных ЕС рассматривается как основная модель регулирования для большей части мира, которая оказалась между американской моделью «свободного рынка» таких ИТ-гигантов, как Google, Amazon и Facebook и монетизацией данных, и китайской моделью управления, которая привела к выходу Alibaba, Tencents и других на мировой уровень на фоне торговых войн между США и Китаем. Многое будет зависеть от того, как в предстоящие годы будет продолжаться обсуждение будущей роли ФУИ. Некоторые из новых институциональных новшеств ФУИ связаны с переходом к так называемому ФУИ плюс с такими вспомогательными механизмами, как инкубатор политики, подчеркивающий, что саморегулирование как способ управления политикой в любом контексте не является жизнеспособным.

Генеральный секретарь Международного союза электросвязи (МСЭ) Хоулин Чжао выступал за более прочную политическую основу, созданную в рамках международных норм и системы Организации Объединенных Наций, такую, как предложенная МСЭ, которая представляется более устойчивой, инклюзив-

ной и демократической моделью, которые могут обеспечить Интернет для общественного блага и двигаться в направлении достижения таких ценностей Организации Объединенных Наций, как Декларация прав человека ООН и Цели устойчивого развития ООН (ЦУР).

Интернет, как обширная социально-экономическая экосистема и сила для «общественного блага», стал объектом пристального внимания на ФУИ 2019, особенно на фоне доминирования ИТ-гигантов, нарушений конфиденциальности, монетизации в рекламе, неправильного использования данных во время выборов, рост числа экстремистов, злоупотребляющих социальными сетями, и отсутствие глобального доступа для всех. Эти многочисленные мнения были характерны для онлайн-дебатов в Берлине. Например, Тайм Бернер Ли, один из основателей веб-сайтов, запустил новый **«Контракт для Интернета»,** план из девяти пунктов по обеспечению того, как Интернет мог бы служить общественному благу и не был бы захвачен узкими, местными корпоративными и государственными интересами. Частная жизнь – это постоянная проблема, особенно когда мы обсуждаем передовые технологии. Очевидный конфликт между безопасностью и конфиденциальностью осложняется подходами к защите данных. Но как далеко должно зайти регулирование?

Продвижение модели ФУИ в национальных контекстах в Африке рассматривалась на открытом форуме Комиссии Африканского союза. Африканские страны сталкиваются с многочисленными проблемами в своих усилиях по участию в глобальном управлении Интернетом в контексте Африканской континентальной зоны свободной торговли, в рамках которого обсуждается новая повестка дня в области цифровой торговли и цифровой индустриализации.

Приватизация и продажа домена .org венчурному капиталу в качестве пробного теста.

Доменная система .Org, принадлежащая Обществу Интернета (ISOC), была продана частной акционерной компании Ethos Capital за $ 1 млрд долларов. Международная НПО, борющаяся за цифровые права, выступила против продажи домена .org, ссылаясь на различные проблемы конфиденциальности глобального гражданского общества и трудовых групп, и отсутствие прозрачности по этой мега-сделке, по иронии судьбы заключенной с Обществом Интернета (ISOC) – некоммерческой организацией.

Возможно, этот случай удачно обозначил более глубокие проблемы, разногласия и споры по поводу управления Интернетом в XXI веке.

Возможно ли такое взаимодействие мира и Интернета? Возможно, но сейчас управление Интернетом ориентируется на неспокойную геополитику.

Определение сложного и противоречивого мира управления Интернетом – 14 лет существования ФУИ

Основанный в 2006 году по итогам Всемирной встречи на высшем уровне по вопросам информационного общества Организации Объединенных Наций, Форум по вопросам управления Интернетом (ФУИ) является уникальной организацией, с одной стороны входящей в традиционный межправительственный мир Организации Объединенных Наций, а с другой – в неконституционный, неформальный мир многосторонних отношений. Его процессы направлены на то, чтобы отражать и претворять в жизнь обе культуры, высоко систематизированные дипломатические традиции организаций системы ООН и восходящий дух многосторонних договоренностей. В буквальном смысле ФУИ представляет собой серию глобальных конференций, дополняемых растущим числом подготовительных и межсессионных процессов, а также региональными филиалами в форме национальных и региональных форумов. На более абстрактном уровне ФУИ обеспечивает базирующееся в ООН пространство для глобального обсуждения правил и положений, технологий и практики, формирующих Интернет. Поскольку ФУИ уделяет пристальное внимание диалогу и не располагает потенциалом для принятия решений, он институционализирует непоследовательное пространство, охватывающее группы заинтересованных сторон и регионы, но не имеет связи с миром регулирования, управления и развития технологий.

Первый ФУИ был организован в 2006 году в Афинах. С тех пор он ежегодно проводится в различных местах. Он проходил в Рио-де-Жанейро в 2007 году, в Хайдарабаде в 2008 году, в Шарм-эль-Шейхе в 2009 году, в Вильнюсе в 2010 году, в Найроби в 2011 году и в Баку в 2012 году. В 2013 году ФУИ состоялся на Бали.

Основные темы ФУИ на сегодняшний день:

2006 и 2007 – Интернет в целях развития

2008 – Интернет для всех

2009 – Управление Интернетом и создание возможностей для всех

2010 – Развитие будущего вместе

2011 – Интернет как катализатор перемен: доступ, развитие, свободы и инновации

2012 – «Управление Интернетом в интересах устойчивого человеческого, экономического и социального развития».

В 2013 года ФУИ решительно поддержал две темы: «Наведение мостов» и «Укрепление многостороннего сотрудничества в интересах роста, развития и прав человека».

Помимо сквозных тем, основное внимание в нем уделяется некоторым темам, которые обсуждались во всех ФУИ:

- Права человека/свобода слова
- Безопасность, киберпреступления, спам
- Защита и конфиденциальность данных
- Права потребителей, сетевая нейтральность
- Права и развитие интеллектуальной собственности (вопросы, связанные с цифровым разрывом)
- Открытые стандарты
- Наращивание потенциала
- Вопросы, связанные с процессами и принципами
- Электронная торговля и электронное управление

Структура ФУИ в системе Организации Объединенных Наций и за ее пределами.

Секретариат ФУИ базируется в Организации Объединенных Наций. Основная функция ФУИ заключается в координации и содействии работе Консультативной группы широкого состава. Консультативная группа была впервые создана Генеральным секретарем ООН Кофи Аннаном в 2006 году. Основная функция Консультативной группы заключается в принятии решений по вопросам и темам, которые должны рассматриваться в рамках каждого ФУИ. В состав Консультативной группы входят представители всех заинтересованных сторон и всех регионов.

Форум организует и проводит пленарные заседания, рабочие совещания, открытые форумы и форумы по образцовому опыту.

Динамичные коалиции: концепция динамичных коалиций была задумана в рамках первого ФУИ в Афинах. Они носят неофициальный и тематический характер. В их состав входят представители различных заинтересованных групп. В настоящее время существует десять активных динамичных коалиций, например, Динамичная коалиция по вопросам доступности и инвалидности, права и принципов Интернета, а также безопасности детей в Интернете и т.д.

В научной области терминология, основанная на участии многих заинтересованных сторон, получила развитие в рамках теории заинтересованных сторон. Заинтересованными сторонами в определении Фримена (1984, 46) являются любые группы или отдельные лица, которые могут влиять на достижение целей организации. В своей основополагающей работе он утверждал, что не только владельцы и акционеры, но и гораздо более широкий круг социальных субъектов важны для корпораций. Общая критика подхода Фримена заключалась в том, что, концентрируясь на корпорации, теория заинтересованных сторон косвенно предполагала, что менеджеры являются «мастером их взаимодействия с заинтересованными сторонами». На практике в ФУИ это означает, что крупные «большие технологические корпорации», такие как Google, Facebook и т.д., имеют асимметричную власть в дебатах и дискурсах и успешно смогли обеспечить в основном нормативно-правовую базу вокруг политики Интернета.

Начиная с начала 1990-х годов, всемирные конференции Организации Объединенных Наций постепенно открывали свои двери для участия негосударственных субъектов и тем самым расширяли разнообразие голосов, которые хотели, чтобы их мнения были отражены в заключительном документе (Гшталь, 2005: 410). Всемирная встреча на высшем уровне по вопросам информационного общества сделала еще один шаг вперед, открыто предложив «неправительственным организациям, гражданскому обществу и частному сектору внести свой вклад в межправительственный процесс подготовки к Встрече на высшем уровне и самой Встречи на высшем уровне

и принять в нем активное участие» (ООН, 2001 год). Впервые Организация Объединенных Наций призвала к активному участию негосударственных субъектов в деятельности, которая по-прежнему официально является межправительственным учреждением.

Создание ФУИ является частью общей тенденции к институционализации глобальной сферы. Начиная с 80-х годов за рамками системы Организации Объединенных Наций возникло все больше разнообразных частных или государственно-частных механизмов управления (Эббот и Снидал, 2009 год). В литературе, посвященной транснациональному регулированию, это явление в основном объясняется растущими проблемами координации или коллективных действий. Согласно этой точке зрения, государственные и частные субъекты участвуют в институциональном строительстве в целях устранения неопределенности и решения проблем, связанных с растущей сложностью, фрагментацией и взаимозависимостью, характеризующими транснациональную вселенную (см., например, Хейл и Хелд 2012; Леви-Фор 2011; Блэк 2008). Эта концепция глобализации подразумевает функциональную перспективу, которая приписывает изменения в транснациональных структурах управления проблемам, требующим решения, с тем чтобы «потребность в новых институтах просто стала их объяснением» (Бартли, 2007: 298; Дэвис, 2012).

ФУИ возникло в контексте, который вполне соответствует ситуации, описанной Барри. Он был основан в условиях фундаментального конфликта почти всех важных элементов управления Интернетом, его тематики, основных норм, структуры власти, источников легитимности и принципов. В рамках эндогенного подхода к ФУИ особое внимание уделяется конкретному контексту, конкретным рационализациям в работе и объединению субъектов, которые в той или иной степени были вовлечены в то, что я называю «коллективным авторством» институциональных изменений. В ФУИ соответствующая структура была сформирована на Всемирной встрече на высшем уровне по вопросам информационного общества ООН, а на совместной основе участвовали правительства и заинтересованные группы.

Большое число правительств, большинство из которых являются членами группы 77, утверждали, что они не имеют эффективного влияния на развитие Интернета, хотя оно все больше затрагивает то, что они считают их суверенными правами. Как отметила Бразилия, «Интернет превратился в глобальное общественное благо, и его управление должно стать одним из ключевых вопросов повестки дня информационного общества. Развивающиеся страны должны иметь полный доступ ко всем директивным органам и процессам, касающимся структуры и функционирования киберпространства, и принимать в них участие». Страны Группы 77 оценили существующую институциональную архитектуру с точки зрения обеспечения справедливого представительства и однозначно сочли ее неудовлетворительной (см., Цихэн Ху, 2005 год: 186). Они также считали себя в невыгодном положении по сравнению со странами ОЭСР, в частности с США, которые выполняют особую надзорную роль в отношении важнейших Интернет-ресурсов, регулируемых Корпорацией по управлению доменными именами и IP-адресами (ICANN). В то же время страны Группы 77 поставили под сомнение понимание и масштабы управления Интернетом, лежащие в основе нынешнего механизма.

Страны Группы 77 решительно поддерживают акцент на наращивании потенциала, но не согласны с идеей ограничения обсуждения целями «Информационных и коммуникационных технологий для развития» (ICT4D). Бразилия предложила Форуму рассмотреть вопрос о том, что, по ее мнению, является «корнем проблемы» в управлении Интернетом, а именно «отсутствие соответствующего международного договора по вопросам государственной политики в отношении Интернета», и принять соответствующие меры. Она предусматривала, что ФУИ станет форумом для обсуждения «готовности международного сообщества в целом – и я вновь подчеркиваю это в целом – создать необходимые международно-правовые рамки для решения связанных с Интернетом вопросов государственной политики». Первое совещание в Афинах должно начаться с переговоров по рамочному договору, однако последующие переговоры могут также быть направлены на разработку «конкретных протоколов» по таким вопросам, как кибербезопасность, спам или конфиденциальность. Таким образом, страны Группы 77 также отметили актуальность диалога по вопросам политики с участием многих заинтересованных сторон в качестве практических достижений. Тем не менее для них это правовой договор, который будет считаться успешным, в отличие от числа людей, имеющих доступ к Интернету, предложенного частным и техническим секторами.

Политические области создают «политические продукты» (Бурдье, 1991: 172), которые могут принимать форму законов, правил, мировоззрений и повествований, социальных проблем, а иногда и новых организаций, таких как ФУИ. Вместе взятые, организационные области являются идентифицируемыми социальными областями с различной степенью автономии в отношении окружающей их среды. Они образуют социальные порядки или «структурные строительные блоки современной политической/организационной жизни в экономике, гражданском обществе и государстве» (Флигштейн и Макадам 2012: 3). В области управления Интернетом термин «экосистема» в настоящее время используется для того, чтобы подчеркнуть ее характер как признанной области институциональной жизни. В этой статье концепция областей является отправной точкой для разработки эндогенного подхода к истокам ФУИ.

СЕМИНАР–КРУГЛЫЙ СТОЛ № 3

ПРОБЛЕМЫ РАЗРЕШЕНИЯ МЕЖДУНАРОДНЫХ СПОРОВ, ОБУСЛОВЛЕННЫХ ИНЦИДЕНТАМИ В ИКТ-СРЕДЕ, МИРНЫМИ СРЕДСТВАМИ

Модератор:

Мирошников Б.Н., Член Президиума НАМИБ

Б.Н. Мирошников

Член Президиума НАМИБ

Характеристика криминогенной ситуации в ИКТ-среде. Ухудшение по всем показателям – количество преступлений и инцидентов, рост ущерба и убытков. Пандемия лишь усугубила ситуацию. Формат мероприятия – новый для нас, постараемся, чтобы он сильно не сказался на качестве дискуссии.

Характеристика юридически-правовой ситуации в международной ИКТ-среде: рост недоверия и взаимных упреков и обвинений, отсутствие общепринятых документов.

Сложности в ИКТ-среде при определении качества – происходящих в ней событий – что есть инцидент и что есть преступление. Трудности атрибуции источников происходящих событий, юридической квалификации.

Цифровое неравенство не только не преодолено, но и усугубляется. Это основа неравенства участия государств в разрешении международных споров.

На этом фоне поиск механизмов разрешения споров и конфликтов продолжается. Надо найти общий язык и общий знаменатель в оценках событий в ИКТ-среде.

Россия прикладывает большие усилия для достижения международного единого понимания проблем урегулирования инцидентов в ИКТ-среде мирными средствами. Большая работа проводится внутри страны для формирования инструментов участия России в различных международных форматах – от государственных до частного бизнеса.

Нам не нужны информационные войны, ни как самостоятельный вид боевых действий, ни как составляющая современных гибридных войск.

Участники круглого стола – опытный и высококвалифицированный состав специалистов, есть и новые молодые ученые и аналитики.

Есть уверенность, что запланированная дискуссия поможет раскрыть хотя бы часть существующих проблем, сформулировать какие-то предложения по мирному урегулированию международных споров в ИКТ-среде.

С.А. Комов

Эксперт Минобороны России

О ПОДХОДЕ МИНОБОРОНЫ РОССИИ К АТРИБУЦИИ ГОСУДАРСТВ, ВИНОВНЫХ В НАРУШЕНИИ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ[1]

Обсуждаемая на конференции проблема атрибуции государств, виновных в нарушении норм ответственного поведения в информационной сфере, с политико-правовой точки зрения далеко не нова.

Последние двадцать лет страны Запада усиленно формируют атрибутивные механизмы, предназначенные для «назначения виновных в нарушении установленных норм поведения» в сферах контроля над химическими, биологическими, ядерными и обычными вооружениями.

Сейчас идет активная работа по формированию таких механизмов в космическом пространстве, в сферах использования ударных беспилотных летательных аппаратов, искусственного интеллекта, а также в информационном пространстве.

Что можно сказать об итогах формирования всех этих механизмов? Где-то их создание продвинулось достаточно далеко, где-то процесс находится в зачаточном состоянии. Наиболее показателен опыт формирования атрибутивного механизма ОЗХО, который на наших глазах привел к росту недоверия, усилению международной напряженности, накоплению конфликтного потенциала в международных отношениях, принятию неадекватных мер реагирования на якобы выявленные нарушения.

Напомню, что недостоверные данные о применении химического оружия Сирией уже дважды стали предлогом для нанесения западной коалицией авиаударов по объектам в городах Хан-Шейхун (2017 г.) и Дума (2018 г.).

Говоря об атрибуции в информационной сфере, начать необходимо с факторов, влияющих на ее результативность.

В частности, первопричиной сложности идентификации источников вредоносной деятельности в этой сфере являются весьма специфические **технологические факторы**.

Не мне вам рассказывать, что функционирование всемирной Сети основано на принципах децентрализации и распределенного использования данных. Существующий протокол не создавался для решения задач идентификации и аутентификации таких источников. Не существует препятствий для осуществления подмены их истинных адресов. Кроме того, для того, чтобы «замести следы» искушенные злоумышленники, как правило, используют средства для поддержания анонимности и прокси-серверы. Последних может быть использовано последовательно сколь угодно много в течение краткого промежутка времени, за которое данные пересекают множество государственных границ и континентов.

Имеются и другие сложности технического характера. Например, проблема хранения огромных объемов данных, необходимых для последующего проведения процессуальных действий по идентификации правонарушителей.

Наряду с технологическими важную роль в результативности атрибуции играют **правовые факторы.** Этой теме на конференции уделено очень много внимания. Поэтому не буду подробно на них останавливаться. Просто поставлю три вопроса.

1. Имеет ли сейчас мировое сообщество надежную и исчерпывающую

1 Статья подготовлена коллективом авторов в составе: генерал-лейтенант Дылевский И.Н., генерал-майор Базылев С.И., полковник Запивахин О.В., полковник в отставке Комов С.А., полковник Песчаненко К.О., полковник Юниченко С.П.

правовую основу для оперативного и беспристрастного проведения «атрибуции», кроме 11 **рекомендательных** норм ответственного поведения государств в информационной сфере в мирное время, а также **декларации** о применимости в ней Устава ООН и международного гуманитарного права?

2. Имеется ли какая-либо апробированная общепризнанная надежная и практичная процессуальная основа расследования инцидентов в информационной сфере?
3. Можно ли на существующих «правовой» и технологической основах выдвигать **обоснованные обвинения** суверенным государствам, и, тем более, **налагать на них наказания** в нарушение Устава ООН?

Для нас ответ на все три вопроса очевиден – нет нельзя!

В Вашингтоне и Евросоюзе считают иначе. С 2014 года по настоящее время США издали более 10 обвинительных актов о «злонамеренной кибердеятельности» в отношении Китая, Ирана, России и Северной Кореи. До сих пор непонятно какие конкретно нормы ответственного поведения государств в информационной сфере были ими нарушены. Как нет и убедительных доказательств этих нарушений. Однако Евросоюз с готовностью берет на вооружение американский подход и в мае 2019 года приступает к созданию своего собственного атрибутивного механизма по расследованию компьютерных инцидентов, который планируется использовать для предъявления коллективных обвинений нарушителям норм ответственного поведения в информационной сфере от имени всех членов ЕС.

Так как Россия, Китай, Иран и Северная Корея не были приглашены к диалогу в рамках этой работы, для нас очевидно, в отношении кого эти обвинения будут звучать.

По нашей оценке, пока у названных моделей механизма атрибуции отсутствует стройная централизованной система сбора доказательств виновности в нарушении «норм ответственного поведения» и каких-либо контрольных механизмов верификации соблюдения этих норм государствами, гарантирующих их объективность и непредвзятость. К тому же они не основаны на всеобъемлющем международном консенсусе. Большинство стран мира просто не спросили: «Согласны ли они с создаваемым механизмом атрибуции»?

Обвинения, исходящие от Вашингтона и его союзников имеют сугубо политическую мотивацию. Налагаемые рестрикции на юридических и физических лиц зарубежных государств являются вмешательством во внутренние дела других государств. Предъявляемые обвинения суверенным державам и наложение на них каких-либо наказаний является нарушением исключительных прерогатив Совета Безопасности ООН.

Используемый коллективным Западом подход к «атрибуции» ведет к разрушению существующей системы международного права, росту напряженности международной обстановки, поляризации человечества на два враждебных лагеря.

По нашему мнению, действенной альтернативой создаваемому сейчас «атрибутивному механизму» является продвижение российских международных инициатив в области международной информационной безопасности.

В частности, Минобороны России уже много лет предлагает заключать двусторонние договоры о предотвращении опасной военной деятельности в информационном пространстве. Убеждены, что наличие таких обязывающих договоров между странами, находящимися в военно-политической конфронтации друг с другом, позволит повысить уровень доверия, купировать существующую военную напряженность, способствовать предотвращению возможности возникновения военных конфликтов в результате недопонимания сути явлений и событий, происходящих в информационной сфере.

На многостороннем уровне основные усилия целесообразно сосредоточить на создании альтернативного механизма разрешения инцидентов и конфликтов в информационной сфере, опираясь на полномочия Совета Безопасности ООН и положения Устава ООН о мирном разрешении международных споров, облеченные в форму универсального обязывающего договора. Но это тема отдельного обсуждения.

В заключение очередной раз предлагаем нашим западным коллегам отказаться от реинкарнации идеологии времен «холодной войны» и приступить к совместному формированию универсального механизма международной информационной безопасности, основанного на взаимном доверии и сотрудничестве.

Джеймс А. Льюис
Старший Вице-Президент и директор, Стратегическая технологическая программа, Центр стратегических и международных исследований, Вашингтон, США

КИБЕРКОНФЛИКТЫ И ТРЕБОВАНИЯ К СОГЛАШЕНИЮ

I. Конфликт нарастает, а сферы договоренностей сокращаются

- Могут ли нормы и меры укрепления доверия помочь оппонентам найти точки соприкосновения и договориться о снижении риска?
- Требуется ли общее восприятие рисков для эффективного соглашения?
- Каким должен быть ответ, если нормы и МД игнорируются?

II. Традиционные подходы не работают

- Один высокопоставленный американский дипломат просил меня задать такой вопрос: какова польза от наличия критической линии связи, если одна сторона всегда отрицает свою вину?
- Киберпотенциал требует секретности и внезапности; это работает вопреки сдерживанию.
- Текущий период похож на 1930-е или 1950-е годы, предшествовавшие соглашениям о контроле над вооружениями.
- Такие понятия, как стабильность, сдерживание, эскалация, должны быть пересмотрены путем сопоставления с реальной государственной практикой.

III. Оценка эффективности кибер-МД

- Забудьте о горячих линиях или других традиционных механизмах.

Вероятность эскалации из-за киберинцидента равна нулю.

Прозрачность минимальной ценности в скрытой среде.

Не существует никаких значимых ограничений, кроме негласного порога силы.

- Есть ли смысл в глобальных мерах доверия?

Озабоченности небольших государств отличаются от тех, с которыми сталкиваются кибердержавы.

- Можем ли мы определить “точки разногласий”, где соглашение может быть полезным?

Существующее международное право не запрещает применение силы (ст. 51).

- Будет ли призыв воздерживаться от отрицательного поведения укреплять доверие?

Нужны ли для этого общие стандарты проверки?

IV. Реакция США эволюционирует

- Укрепление рамок ответственного поведения государств в 2015 году.
- Упорное сражение, защита на опережение – все это, вероятно, продолжится.

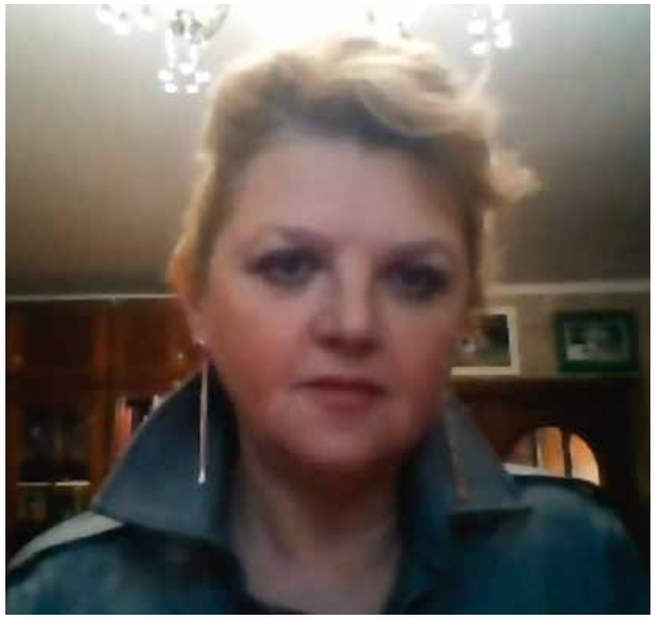
Дискуссия в США о целесообразности сдерживания:

- К сдерживанию призывают, но не соблюдают.
- Создание коалиции для введения последствий.
- Определить пропорциональные ответы в соответствии с американской интерпретацией международного права.

V. Что нужно изменить?

- Обостренное восприятие риска, разделяемое всеми участниками.
- Возросший интерес к соглашению между кибердержавами.
- Ясность в отношении собственных ожиданий и ожиданий партнеров.
- Общее понимание международного права.
- Повышение доверия к США за счет реагирования и противодействия вредоносным кибератакам.
- Переговорный процесс между крупными державами за пределами ООН.

Н.П. Ромашкина
Руководитель подразделения проблем информационной безопасности ЦМБ ИМЭМО РАН, профессор, член-корреспондент АВН РФ, кандидат политических наук



СТРАТЕГИЧЕСКИЕ СУЩЕСТВУЮЩИЕ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Становление новой системы международной безопасности в XXI веке характеризуется ускоренным ростом угроз миру на планете, исходящим из цифрового пространства и связанным с вредоносным применением информационно-коммуникационных технологий (ИКТ).

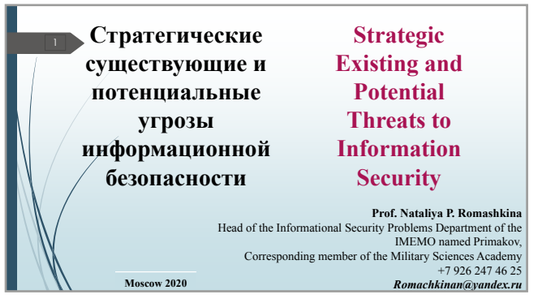
Остановимся на наиболее опасных существующих и потенциальных информационных угрозах (ИКТ-угрозах, кибернетических угрозах), которые носят глобальный, стратегический характер. Их можно разделить на три большие группы:

- применение ИКТ-оружия в военно-политических целях для осуществления враждебных действий и актов агрессии;
- деструктивное ИКТ-воздействие на элементы критически важных объектов государственной инфраструктуры;
- вмешательство во внутренние дела суверенного государства, снижение общественной стабильности, разжигание межэтнической и межнациональной розни посредством ИКТ.

В современных условиях, когда международные отношения по-прежнему строятся на принципах взаимного вооруженного сдерживания и все более привержены политике с позиции силы, информационные угрозы добавляют неопределенности и могут способствовать эскалации конфликтов, что снижает уровень стратегической стабильности. Использование ИКТ в качестве важного инструмента разрешения межгосударственных споров и противоречий становится все более значимой проблемой в процессе обеспечения международной безопасности. Таким образом, использование ИКТ превращается в один из важнейших элементов военно-политического потенциала государств, дополняющий, а иногда и заменяющий традиционные политико-дипломатические средства и вооружения. В условиях параллельно развивающихся процессов разрушения режима контроля над вооружениями и роста противоречий в отношениях «великих держав» значение военной мощи, цифровых технологий военного и двойного назначения как одного из ключевых факторов соперничества и противоборства сохраняется и даже увеличивается.

Наличие этих факторов требует поиска дополнительных механизмов международного управления. Однако, несмотря на то, что Россия еще с конца прошлого века выступает за создание международных инструментов контроля над ИКТ-вооружениями под эгидой ООН, они до сих пор отсутствуют. При этом вероятность осуществления указанных ИКТ-угроз возрастает с каждым годом.

Так, в настоящее время для большинства стран мира стратегическое значение имеет защищенность ИКТ-систем, которые стали важным фактором обеспечения суверенитета, обороноспособности и безопасности государства. При этом речь сегодня идет об угрозе ускоренного развития (гонки) информационных вооружений. По некоторым оценкам, уже более 30 государств обладают наступательным кибернетическим оружием (кибероружием). ИКТ, таким образом, могут спровоцировать развязывание межгосударственного военного конфликта, в первую очередь, из-за



возможности несоразмерного использования методов реагирования на ИКТ-угрозы и атаки: пострадавшая сторона может применить в ответ реальное оружие.

Кроме того, конфликт может возникнуть по ошибке, так как в настоящее время отсутствует универсальная методология идентификации нарушителей, не выработаны критерии отнесения кибератак к вооруженному нападению, не сформированы универсальные принципы расследования инцидентов. Эта угрозы усиливается с учетом решения НАТО о применении Статьи 5 Устава Альянса в ответ на кибернападения. Напомню, что Статья 5 предполагает возможность применения всех имеющихся сил и средств НАТО в том числе, и ядерного оружия (ЯО), в ответ на нападение на одного из членов Альянса. Большую опасность также представляют широко применяемые возможности по подрыву политической, экономической и социальной систем, по психологическому воздействию на население для дестабилизации государства и общества с применением ИКТ.

Таким образом, ситуация в области стратегической стабильности может оцениваться как кризисная. В условиях существующих дестабилизирующих факторов, отсутствия переговоров по ограничению и сокращению ЯО, а также ускоренного развития вредоносных ИКТ существующих механизмов международного управления в этой области не достаточно.

В контексте обеспечения стратегической стабильности особого внимания требует безопасность ракетно-ядерных вооружений. Все ядерные державы модернизируют их, стремясь внедрять новые компьютерные технологии. Все больше компонентов военной ядерной инфраструктуры – от боеголовок и средств их доставки до систем управления и наведения, систем связи, командования и контроля над ядерными силами – зависят от сложного программного обеспечения, что делает их потенциальными мишенями для ИКТ-атак.

Таким образом, защита стратегических вооружений, систем предупреждения о ракетном нападении (СПРН), противовоздушной (ПВО) и противоракетной обороны (ПРО), связи, командования и контроля над ЯО от вредоносных ИКТ являются актуальными глобальными проблемами современности. При этом в дополнение или вместо принципа сдерживания за счет неминуемого ответного удара, растет интерес к сдерживанию путем блокирования использования наступательных средств («блокирование пуска»," left of launch") с помощью ИКТ.

Одной из важнейших существующих угроз стратегического характера является развитие новейших противоспутниковых средств на основе ИКТ, позволяющих уничтожать спутники при помощи размещенных на земле противоспутниковых систем, а также влиять на работу не только искусственных спутников Земли

мирного, но также двойного и военного назначения, включая элементы СПРН. Такие средства могут повлиять на эффективность работы спутников в рамках систем Ведения боевых действий в едином информационном пространстве, которые активно совершенствуются в развитых в военном отношении государствах. Это одна из самых серьезных угроз стратегической стабильности на современном этапе. Напомню, что в июне 2018 года впервые была озвучена информация о кибервмешательстве в работу американского спутника военного назначения, когда, по утверждению компании Symantec, внедрение «закладки» в ПО СУ позволило изменить орбиту спутника и перехватить чувствительные данные.

Снижение уровня стратегической стабильности, в первую очередь, обусловлено влиянием вредоносных ИКТ на рост вероятности:

- ошибочного санкционированного пуска БР, а также предотвращения (блокирования) пуска;
- получения ложной информации от СПРН о запуске БР со стороны противника из-за растущей изощренности ИКТ-атак;
- повреждения или разрушения каналов коммуникаций, создания помех в системе управления, командования и контроля ВС;
- снижения уверенности военных, принимающих решения, в работоспособности систем и восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения.

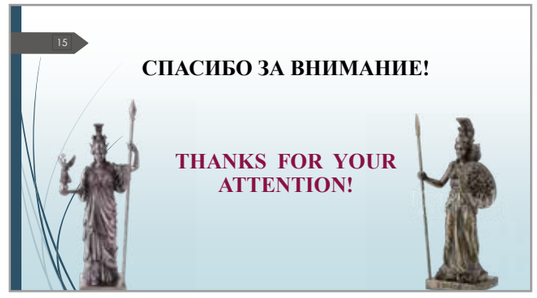
В таких условиях, когда обеспечение безопасной ИКТ-среды стало частью системы глобальной международной безопасности, целесообразно ставить вопрос о необходимости разработки российской Стратегии информационной безопасности. Это обосновано, в частности, тем, что стратегические документы, на юридической основе определяющие направления и перспективы развития государства (а ИКТ являются одной из важнейших характеристик развития), играют особую роль на современном этапе и создают правовой фундамент инновационного развития, определяя основы государственной политики.

Важнейшими характеристиками стратегии в отличие от всех других видов документов, в частности, являются:

1) целевой подход к разработке, основанный на определении важнейшей цели и задач по ее достижению, приоритетность которых определяет содержание и сущностные результаты действий по развитию соответствующей сферы;
2) системный подход к реализации, предусматривающий решение указанных задач и, соответственно, максимальный охват всех основных направлений, которые должны быть задействованы в реализации стратегических установок государственной политики в соответствующей области;
3) комплекс конкретных согласованных и взаимосвязанных мероприятий, средств и ресурсов, обеспечивающих достижение результатов, предусмотренных указанными задачами в рамках каждого из приоритетных направлений;
4) действия по единому поэтапному плану с четко обозначенными целевыми индикаторами и показателями на каждом из этапов, а также разработанной системой финансирования основных мероприятий;
5) мониторинг за ходом реализации стратегии и применение системы мер юридического контроля за достижением конечных и промежуточных результатов.

Таким образом, стратегия разрабатывается на основе глубокого научного прогнозирования, планирования и программирования на нескольких уровнях: федеральном, субъектов Российской Федерации и муниципальных образований. Очевидно, что Стратегия как система формально-определенных положений, закрепляющих стратегическую цель, задачи и направления деятельности органов государственной власти по ее достижению, средства и ресурсы, которые должны быть на это затрачены, существенно отличается от Доктрины (в России действует Доктрина информационной безопасности), которая по сути представляет собой философскую, политическую либо правовую теорию, концепцию, учение, систему воззрений, руководящий теоретический или политический принцип.

Стратегия информационной безопасности России сможет стать фундаментом развития информационной сферы в стране, обеспечивающим организационные, законодательные и экономические условия, а также гарантии безопасного эволюционного процесса. Документ призван сформулировать цель и задачи развития, обеспечить защиту от угроз и рисков в информационном пространстве. Стратегия описывает комплексный системный подход к реализации указанных цели и задач, согласованные и взаимосвязанные действия и мероприятия на базе целевых индикаторов и показателей на каждом этапе реализации. Важной частью стратегии, как правило, является также четко прописанная система мониторинга и мер юридического контроля за достижением конечных и промежуточных результатов. Такой документ может сыграть важную роль в создании концепции сдерживания агрессивных действий в условиях новой эры стратегического ИКТ-противоборства, заложить фундамент режима контроля над ИКТ-вооружениями, позволяющего избежать информационной войны с глобальными разрушительными последствиями.



Кроме того, для обеспечения более безопасного и стабильного мира в условиях всеобъемлющего влияния цифрового пространства целесообразны международные действия с участием России:

1) разработка и внедрение новых ИКТ России, совершенствование соответствующих специальных гражданских и военных структур для обеспечения глобального баланса сил и средств;
2) включение вопросов обеспечения информационной безопасности в обсуждения и переговоры по ядерным вооружениям и стратегической стабильности на двусторонней (РФ-США) и многосторонней основе с участием России;
3) разработка на международном военно-политическом уровне конкретных мер по укреплению доверия, в частности, обмен данными об информационных угрозах, практическое межгосударственное сотрудничество и др. на многосторонней основе, в первую очередь, между РФ и США с целью выхода на подписание документа о безопасности военной деятельности в информационном пространстве;
4) активизация работы в государствах – обладателях ЯО по более эффективной подготовке персонала и защите программно-аппаратных средств военной инфраструктуры от различных ИКТ-нападений (в частности: унификация; территориальное распределение; дублирование обработки данных; создание «воздушной прослойки», т.е. отсутствие пересечения внутренних сетей критически важных объектов с глобальной информационной сетью; узкая специализация программного обеспечения и др.) для обеспечения как национальной, так и международной безопасности;
5) для более эффективного решения последней задачи целесообразно активизировать усилия по созданию исследовательской программы по ИКТ-стабильности военной сферы экспертами из ядерных держав;
6) выработка и фиксация общего для РФ и США понимания опасности ИКТ-угроз для международной безопасности и стабильности, дальнейшая деятельность по привлечению к этому процессу всех ядерных держав;
7) выработка общих подходов к оценке вероятности непреднамеренных и преднамеренных ИКТ-атак на СЯС;
8) четкая фиксация всеми ядерными державами вероятного ответа в случае обнаружения ИКТ-атак на СЯС в целях обеспечения сдерживания в применении ИКТ-вооружений.

Эти меры могут заложить основу для создания политики сдерживания в цифровой среде так, как это было сделано в период биполярности в отношении ядерных вооружений, стать фундаментом для более широких двусторонних и многосторонних соглашений о контроле над вооружениями в так называемом информационно-ядерном пространстве в будущем. При этом работа по оценке ИКТ-угроз находится на одном из первых этапов, и логично полагать, что деятельность экспертного сообщества сегодня может быть исключительно полезной для структур, принимающих государственные решения.

Параллельно целесообразно работать над созданием режима контроля над ИКТ-вооружениями, который мог бы включать:

- запрет на ИКТ-атаки на конкретные объекты, в первую очередь, в военной сфере (заявления, обязательства, соглашения, договоры);
- ограничение и/или отказ от наступательных ИКТ-возможностей;
- меры контроля за распространением ИКТ-вооружений;
- международные нормы в отношении средств и методов предотвращения и устранения киберконфликтов;
- разработку конвенции о запрещении вредоносного использования ИКТ в сфере ЯО.

Более подробно ознакомиться с указанными проблемами Вы можете с помощью новой монографии нашего подразделения Проблем информационной безопасности ЦМБ ИМЭМО РАН им. Е.М. Примакова «Международная безопасность, стратегическая стабильность и информационные технологии».

Спасибо за внимание!

А.А. Вураско
Руководитель отдела анализа цифровых угроз компании ИНФОСЕКЬЮРИТИ

ВЛИЯНИЕ РАЗВИТИЯ КОНЦЕПЦИИ CAAS (CYBERCRIME AS A SERVICE) НА ЛАНДШАФТ УГРОЗ В ОБЛАСТИ ИКТ

В последние 20–25 лет развитие киберпреступности происходит сразу по нескольким направлениям.

Первое направление – это изменение мотивации киберпреступников. Если на рубеже XX–XXI веков основным движителем хакеров было желание продемонстрировать свои умения или прикоснуться к каким-либо знаниям, недоступным для большинства людей (в качестве примера можно привести шотландского хакера Гэри Маккиннона, совершившего взлом серверов Пентагона и NASA с целью получения доказательств сотрудничества правительства США с инопланетянами), то начиная с 2005–2006 года основным мотивом киберпреступников стало желание извлечения материальной выгоды.

Изменение мотивации привело к завершению «эпохи хакеров» и положило начало эпохе организованной преступности в IT-сфере. Представители «традиционного» криминального бизнеса быстро оценили все прелести информационных технологий и ринулись покорять новую для себя область, вкладывая значительные деньги в развитие киберпреступности.

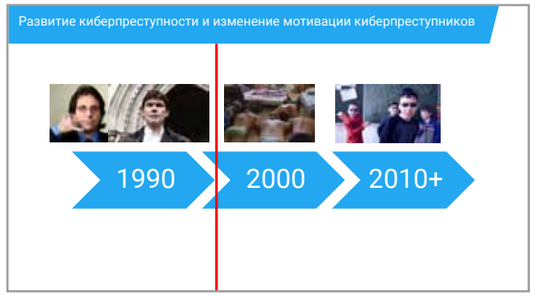
Успех подобной интеграции традиционной и «цифровой» преступности был связан еще и с тем, что она происходила на фоне стремительной цифровизации нашего общества, развития электронной коммерции и безналичных платежей. Все это привело к размытию границы между двумя категориями преступлений: преступлений в сфере информационных и телекоммуникационных технологий, то есть составов преступлений, не мыслимых в отрыве от ИКТ; и преступлений, совершаемых с использованием информационных и телекоммуникационных технологий – традиционных видов преступной деятельности, в рамках которых ИКТ выступают в качестве прикладного инструмента.

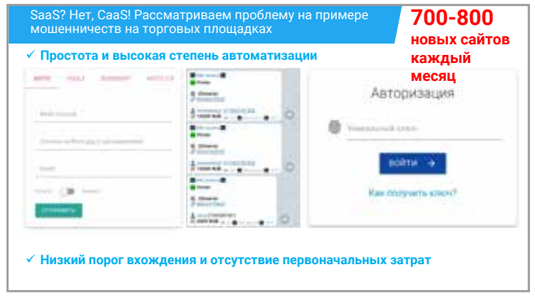
Такие традиционные виды преступлений, как кражи, мошенничества или вымогательства стали совершаться с использованием вредоносных компьютерных программ или благодаря неправомерному доступу к компьютерной информации жертвы. При этом стоит отметить широкое использование социальной инженерии, завязанное на электронные коммуникации.

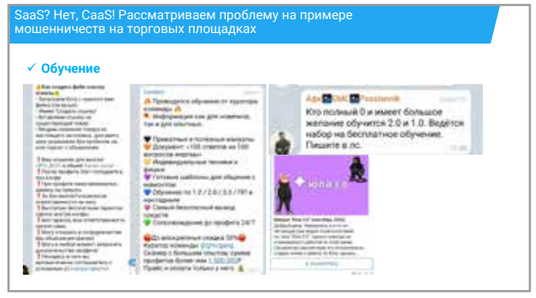
Второе направление развития – это переход от преступников-одиночек к распределенным и зачастую трансграничным преступным сообществам. И это логично, ведь каждое преступление в IT-сфере, сопряженное с хищением денежных средств, – это сложный и многоэтапный процесс, требующий привлечения значительного количества специалистов, обладающих самой разной квалификацией: начиная от тех, кто будет непосредственно проводить атаку или создавать и поддерживать вредоносное программное обеспечение, и заканчивая теми, кто обеспечит вывод и обналичивание похищенных денег.

Так мы получили целую плеяду криминальных сообществ, пик деятельности которых пришелся на 2010 годы. Однако, эволюция киберкриминала не стоит на месте, и дальнейшим витком развития киберпреступности стало широкое распространение концепции CaaS – Cybercrime as a Service или «Киберпреступление как услуга».

Суть данной концепции предельно проста. Злоумышленники создают готовые инструменты и сопутствующую инфраструктуру,







которые позволяют неподготовленным людям с легкостью, буквально в два клика совершать технически сложные преступления, после чего предоставляют эти инструменты всем желающим на условии аренды, подписки или комиссии от суммы похищенных с их помощью денежных средств.

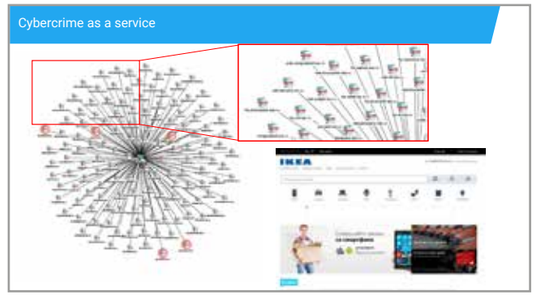
Сама по себе концепция CaaS зародилась примерно в середине 2010 годов и была обкатана на вредоносных программах, предназначенных для хищения денег с банковских счетов физических лиц. Любой желающий мог арендовать готовую бот-сеть, состоящую из тысяч зараженных компьютеров или смартфонов, и использовать все ее возможности для собственного обогащения. В состав подписки входил доступ в командный центр бот-сети, обладающий простым и понятным веб-интерфейсом, сервис вывода похищенных денег, а также, в ряде случаев, круглосуточная техническая поддержка. Таким образом, организаторы преступного бизнеса напрямую не занимались хищением денег, сосредоточившись на поддержании функционирования сервиса, а арендаторам не нужно было вникать в технические детали работы схемы.

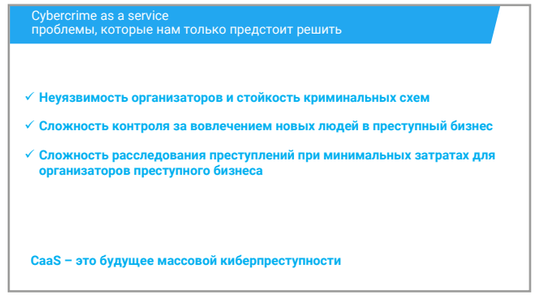
Концепция CaaS привела к революции в киберпреступном мире, значительно снизив планку требований к квалификации киберпреступника, в результате которой в эту отрасль за легкими деньгами ринулось огромное количество неподготовленных людей.

Очень скоро стало понятно, что даже далекий от IT человек при наличии у него автоматизированных инструментов с интуитивно понятным интерфейсом может совершать технически сложные преступления. Отличным примером этого является целая череда достаточно мощных DDoS-атак, совершенных в прошлом десятилетии школьниками, имевшими в своем распоряжении лишь вредоносную программу под названием Low Orbit Ion Cannon. Для детей все выглядело как игра: предварительно обсудив план в соцсетях, они вводили в соответствующее поле программы адрес атакуемого ресурса, в установленное время нажимали на кнопку и ресурс «падал», не выдерживая нагрузки.

Концепция CaaS уверенно вошла в третье десятилетие XXI века. Помимо вредоносных программ стало появляться много примеров «бизнеса под ключ», реализуемых в рамках CaaS. Самым ярким примером последнего года, пожалуй, является схема, связанная с мошенничествами на электронных торговых площадках, именуемая своими создателями и адептами «Охотой на Мамонта».

Сама по себе суть «Охоты на мамонта» предельно проста и заключается в обмане пользователей сайтов бесплатных объявлений с использованием методов социальной инженерии, в результате чего жертву вынуждают ввести данные своей банковской карты на фишинговом сайте, закамуфлированном либо





под саму торговую площадку, либо под ресурс одной из популярных служб доставки. Данная криминальная схема буквально расцвела на фоне пандемии и самоизоляции.

При этом на протяжение всего года схема непрерывно эволюционировала и совершенствовалась: существенно расширилась ее география; выросло количество охватываемых площадок: от сайтов типа Авито и Юлы злоумышленники перешли к сайтам, посвященным продаже автомобилей, а также аренде недвижимости; значительно увеличилась автоматизация процесса создания фишинговых страниц; улучшились методы сокрытия ресурсов от систем противодействия фишингу. На протяжение всего 2020 года в сети ежемесячно появлялось примерно 700-800 новых фишиновых сайтов, созданных в рамках «Охоты на мамонта».

В соответствии с концепцией CaaS всех участников можно поделить на 2 категории:

Организаторы – люди занимающиеся организационно-техническими аспектами работы и не вовлеченные напрямую в процесс хищения денег. Однако, именно они и являются основными выгодоприобретателями, так как алгоритмы «Охоты на мамонта» подразумевают автоматическое списание комиссии в пользу организаторов с каждой похищенной при помощи этой схемы суммы денег.

«Воркеры» – участники, непосредственно осуществляющие мошеннические действия на торговых площадках и иных охватываемых схемой сайтах.

Понятно, что финансовое благополучие организаторов напрямую зависит от количества и успешности работы «воркеров», поэтому они активно рекламируют данную схему на различных сетевых площадках, позиционируя ее в качестве средства легкого заработка.

Схема имеет предельно низкий порог вхождения. Желающему опробовать свои силы в качестве сетевого мошенника не требуется буквально ничего. Достаточно вступить в соответствующую группу в Telegram или отправить сообщение боту. В распоряжении участников-«воркеров» имеются обучающие материалы, шаблоны общения с жертвами, инструменты, позволяющие в два клика создать фишинговую страницу под конкретную жертву и обеспечить быстрый и безопасный вывод денежных средств.

Все эти факторы привели к новому и крайне опасному явлению – массовому вовлечению в этот преступный бизнес несовершеннолетних.

Анализ тематических Telegram-каналов показывает, что до 80 процентов участников сообществ, посвященных «Охоте на мамонта» составляют несовершеннолетние. При этом масштабы их вовлечения в преступный бизнес поражают. Некоторые сообщества насчитывают десятки тысяч участников. Большая часть состоящих в них людей не считают подобный «бизнес» чем-то противозаконным, а скорее воспринимают это как некую игру, которая позволяет не только заработать денег, но и почувствовать себя умнее жертвы, которая может быть намного старше их. Естественно, ни у кого из них не возникает мысли о том, что они становятся соучастниками многоэпизодного преступления, совершаемого группой лиц по предварительному сговору.

Несмотря на то, что в рамках каждого эпизода сумма хищения как правило невелика, их массовость позволяет организаторам криминальных схем получать стабильно высокий доход.

Подводя итог, хочется обозначить проблемы, с которыми мы уже столкнулись и с которыми нам еще предстоит сталкиваться.

Концепция CaaS позволяет формировать стойкие и масштабные распределенные преступные сообщества, объединяющие единой

целью тысячи людей, в том числе находящихся на территории разных стран.

Несмотря на то, что прибыльность схемы зависит от количества и эффективности работы рядовых низовых участников («воркеров»), сами по себе «воркеры» по сути являются «пушечным мясом»: в случае задержания правоохранительными органами «воркеры» не смогут выдать никого из организаторов преступного бизнеса или нарушить стабильность функционирования криминальной схемы. А на место одних мошенников сразу же придут другие желающие подзаработать.

Второй проблемой является сложность контроля за вовлечением людей в подобного рода криминальные структуры. Все общение между участниками в значительной степени обезличено, они используют методы сетевой конспирации и активно обучают им друг друга.

И третья проблема – заключается в том, что при всей простоте совершения подобных преступлений, их расследование является крайне сложным и долгим процессом, требующим проведения компьютерных исследований и экспертиз, а также привлечения высококвалифицированных специалистов.

На сегодняшний день можно уверенно сказать, что CaaS является настоящим и будущим компьютерной преступности – концепция уже показала свою состоятельность и продолжает активно развиваться. И нам, в свою очередь, необходимо сосредоточиться на выработке путей решения данной проблемы и недопущения усугубления ситуации в будущем.

Филипп Бомард
профессор университета, директор лаборатории SDR3C (безопасность, оборона, разведка, криминология, киберугрозы, кризисы). Национальная консерватория искусств и ремесел, Париж.

По техническим причинам Филипп Бомард не смог выступить на Форуме, но предоставил текст своего выступления на французском языке для публикации в сборнике.

РЕКВИЕМ ПО АБСКОНАМ: ПОРОЧНЫЕ ПОСЛЕДСТВИЯ КРАЙНЕГО ИСПОЛЬЗОВАНИЯ ПРИНЦИПА ПРЕДОСТОРОЖНОСТИ

С октября 2019 г. человечество столкнулось с крупнейшим пандемическим событием в своей новейшей истории. Проявило ли человечество мудрую предусмотрительность и надлежащую стратегию? Должно ли оно праздновать свою победу над пандемией Sars2-CoV-2, действительно ли оно извлекло уроки из своих прошлых неудач?

“Принцип предосторожности” гласит, что “при отсутствии определенности, с учетом современных научно-технических знаний, принятие эффективных и соразмерных мер по предотвращению риска серьезного и необратимого ущерба окружающей среде при экономически приемлемых затратах не должно задерживаться” (статья 200-1).

Речь идет о законодательном механизме, призванном обеспечить разумный баланс – то, что англосаксы назвали бы справедливым *компромиссом* – между нынешним и будущими поколениями; придать статус закона; свести воедино принцип сдержанности (предосторожности), принцип превентивных действий, принцип участия (транспарентности граждан) и принцип, который в тексте самого закона странным образом называется “загрязнитель платит”.

Применительно к химии, промышленности, телекоммуникациям и транспорту принцип предосторожности очень похож на корректирующую меру, направленную на то, чтобы избежать ошибок прошлого. Применительно к здравоохранению этот принцип был подвергнут жестокому воздействию во время пандемии атипичной пневмонии VOC 2 из-за COVID-19.

Мы рассмотрим, как мы не смогли стратегически справиться с пандемией Sars2-CoV-2; потенциальные причины этой неудачи; стратегическую слепоту эпидемиологических моделей; коллективную истерию предпечатной подготовки, кратчайший путь к карьере и публикации, практикуемый в настоящее время *JAMA, Nature, Science, Cell,* а также в малоизвестных китайских публикациях.

Это история одной из величайших современных неудач в истории человечества; истории мирового кризиса, который не был преодолен; история управляемого с такой некомпетентностью, что уже нельзя говорить о неудаче, а можно говорить о заумном *реквиеме,* где поют смерть того, чего никогда не было, чтобы избежать конца, который не наступит; заменив его самым могущественным, самым слепым и самым смертоносным из стратегических пустот.

Когда разум поглощается моделями, задуманными как религия, политическое принятие решений берет на себя наряд культа. И суеверное обучение изобилует. Реальность такова, что не существует единой модели, которая могла бы описать, понять, объяснить и предсказать пандемическую ситуацию. Когда обучение или логическое рассуждение убедительно, но не соответствует какой-либо осязаемой или доказуемой ре-

альности, мы говорим о “суеверном обучении”, или как писали Левитт и Март (1988): “Суеверное обучение происходит тогда, когда субъективный опыт обучения убедителен, но связь между действиями и результатами плохо прописана”.

В случае с COVID-19 первые сообщения, которым удалось избежать бдительности китайского контроля, указывают на очень высокий уровень смертности: почти 10% в бассейне Ухань и почти 3,5% во всех других китайских регионах. Всемирная организация здравоохранения объявила о 3,4%. В статье, опубликованной в феврале 2020 г. в *журнале Американской медицинской ассоциации,* указано 2,2%.

Это ужасные цифры. Это те числа, которые заставят вас мгновенно запереть всю планету… Если бы эти цифры были верны, мы находились бы в ситуации, очень похожей на ситуацию H1N1 (*так называемый свиной грипп*), которая привела к тому, что большинство европейских правительств сильно переоценили эпидемию; применили принцип предосторожности; и создали чрезмерно большие стратегические резервы.

Главной причиной глобального снижения смертности от инфекций является успех первоначальной стратегии в период с марта по май 2020 г. Все без исключения политики слишком остро реагировали, потому что были зажаты своими мнениями (Россия, Китай, Ливан, Венгрия и т.д.), приближались к национальным выборам (США) или сталкивались с протестными движениями (Франция, Россия, Германия, Италия, Гонконг и т.д.).

Затем обнаружилось, что Sars2-CoV-2 находился в обращении не менее трех месяцев до его открытия в январе 2020 г.; что это увеличивало начальное заражение еще больше и можно предполагать, что некоторые районы мира, находящиеся в частых экономических контактах с материковым Китаем и бассейном Ухань, могли “извлечь выгоду” из раннего заражения.

Управление кризисом пандемии Sars2-CoV-2 является безпрецедентным провалом в истории человеческих организаций; провалом суждения, провалом оценки и, безусловно, провалом принципа предосторожности. Несомненно, для первого эпизода пандемии Sars2-CoV-2 “*Нам повезло*”.

В 2005 году мы опубликовали вместе с У.Х. Старбаком в издании “*Long Range Planning*” статью под названием: “*Учиться на неудачах? Почему этого может не случиться*” (Baumard and Starbuck, 2005). Цель состояла в том, чтобы дать ответ на исследование коллеги и друга Сима Ситкина (1992), который установил очень элегантную и рациональную теорию, предполагающую, что принятие и осознание небольших потерь позволяет предвидеть и справляться с большими неудачами.

Наш крестовый поход против суеверной теории привел к довольно мрачному открытию: организации и их лидеры не учатся ни на больших неудачах, ни на маленьких. Мы используем ту же “основу”, что и наш обзор 2005 года в этой статье, чтобы попытаться понять и объяснить, как принцип предосторожности привел к провалу большинства обществ в 2020 году; были ли извлечены уроки из предыдущих неудач в борьбе с пандемией? Почему в конкретном случае пандемического феномена так трудно извлечь уроки из наших неудач? Каковы основные препятствия для стратегического обучения, адаптированного к пандемическим явлениям?

Идея о том, что отдельные организации учатся, родилась вместе с Сайертом и Мартом (1963). Согласно им, организационное обучение включает в себя изменение целей и прогнозов для отражения текущего опыта и восприятия, адаптацию правил принятия решений к обстоятельствам, изменение целей для того, чтобы сделать их реалистичными, и рассмотрение того, где предыдущие исследования увенчались успехом. Их утверждение о том, что организации учатся в первую очередь, сталкиваясь с проблемами, а не с успехами, особенно актуально (Cyert and March, 1963).

В случае пандемии COVID-19 сразу же возникло очень удивительное явление: прямой диалог между ВОЗ и Председателем КНР о соответствующем стратегическом обучении для управления глобальной пандемией; и это, ровно через 15 дней после официального объявления об “обнаружении” этой болезни в Ухане.

“КПК ограничил 57 миллионов жителей Хубэя в своих домах”. В то время наблюдатели в области прав человека выражали свою озабоченность. Как сказал один эксперт газете “*Нью-Йорк Таймс*”, “это закрытие почти наверняка приведет к нарушениям прав человека и будет явно неконституционным в Соединенных Штатах Америки”. Тем не менее, 29 января Генеральный директор ВОЗ Тедрос Адханом заявил, что он “очень впечатлен и воодушевлен подробными знаниями Президента [Си Цзиньпина] об эпидемии”, а на следующий день он поблагодарил Китай за то, что тот “установил новый стандарт в ответ на эпидемию”. Тем не менее, всего через шесть дней тупиковая ситуация – “беспрецедентная в истории здравоохранения” – не дала никаких результатов” (Senger, 2020).

Однако международная истерия COVID-19 началась примерно 23 января, когда “просочившиеся” видео в Ухане начали наводнять международные социальные сети, включая Facebook, Twitter и YouTube – все, по-видимому, заблокированные в Китае, показывая ужасы Уханьской вспышки и серьезность ее блокировки. Вирусные видеоролики утверждали, что жители стихийно рушатся на улицах в сценах, похожих на те, что в фильме “*Зомбиленд*” и сериале “*Ходячие мертвецы*”. На одном видео показано, как спецназ поймал человека с сеткой для бабочек за то, что тот снял маску[1]. Но в ретроспективе это кризисное кино несколько комично; в печально известном видео человек “самопроизвольно рушится”, протягивает руки, чтобы наверстать упущенное (Senger, 2020).

“В вирусном твиттере 25 января эпидемиолог с небольшим опытом в области инфекционных болезней написал: “Слава Богу, новый коронавирус – это 3,8! Каково значение R0 для воспроизводства? Это плохо для термоядерной пандемии”. Это был первый из серии сомнительных твитов, широко разрекламированных до сих пор неизвестным Эриком Файгл-Дингом, что побудило одного из видных коллег по Гарварду осудить его как “шарлатана” (Senger, 2020).

Одним из способов замедлить процесс обучения противника является, как показывают исследования, повышение “жесткости угрозы” (Staw, Sandelands and Sutton, 1981). Жесткость реагирования на угрозу может быть повышена за счет использования различных рычагов. Чем больше воспринимается угроза, приводящая к непримиримым потерям, тем более разрозненной и неполной является информация об угрозе, тем больше она усиливает стресс и тревогу; и тем более “жесткой” будет реакция, основанная на хорошо усвоенных ответных репертуарах или на первом доступном доминирующем ответе (Staw *et al., op. cit., pp. 502-503*).

Несмотря на отсутствие эпидемиологических данных, многочисленные организованные утечки данных из материкового Китая сообщают о показателях размножения в диапазоне от 3,3 до 3,7; однако именно через Национальный исследовательский центр Лос-Аламоса и три его наиболее авторитетных отдела (*Центр нелинейных исследований CNLS; Информационная научная группа CCS3 и Теоретическая биология биофизики T-6*) 11 февраля 2020 г. в Соединенных Штатах распространяется самая страшная угроза.

Исследование Национального центра Лос-Аламоса основано на мета-анализе, то есть делает выводы на основе перекрестных ссылочных исследований, уже опубликованных в период с 23 января 2020 г. по 20 февраля 2020 г.; в основном из китайских источников в Ухане.

Это предварительная печать: исследовательский документ, принятый “в предварительной печати”, в ожидании подтверждения его авторами научной достоверности; иными словами, носитель, надежность и подлинность которого не имеет себе равных ни в одном таблоиде, под видом научного издания, и на котором громко и ясно висит флаг Лос-Аламоса.

Исследования в области стратегического обучения безжалостны в отношении роли, которую играет человеческое познание в его успехе. Его практически не существует. Люди не только делают *ошибочные* выводы из разрозненных данных; точность или достоверность исходных данных плохо коррелирует, если вообще коррелирует, в формулировке обучения (Starbuck and Hedberg, 2001; Mezias and Starbuck, 2003). Другими словами, люди всегда будут стремиться укрепить поведение, которое делает их успешными, отбросив в сторону поведение, которое, по их мнению, может сделать их неудачниками, не придавая никакого значения достоверности исходных данных (Starbuck and Hedberg, 2001).

1 https://twitter.com/1nfodaily/status/1232719653983617026.

Никто не ставил под сомнение строительство “за одну неделю”, о котором объявила китайская пропаганда, совершенно новой больницы в Ухане, которая на самом деле представляла собой видеосюжет о строительстве квартир более чем в 900 километрах от города Ухань.

А потом – успех! Начиная с февраля, КПК сообщал об экспоненциальном снижении числа случаев коронавируса вплоть до 19 марта, когда он объявил, что его блокировка полностью ликвидировала внутренние случаи. В своем докладе от 24 февраля ВОЗ рапсодировала триумф Китая. “Строгое и бескомпромиссное применение Китаем нефармацевтических мер по сдерживанию передачи вируса COVID-19 в различных условиях дает жизненно важные уроки для глобального реагирования” (Senger, 2020).

Сообщение результатов оказывает парадоксальное воздействие на стратегическое обучение. В то время как в управленческой литературе проповедуется 360-градусное отчуждение, микроменеджмент и ключевые показатели эффективности, Клугер и ДеНиси (1996), напротив, показали, что такая обратная связь снижает эффективность реагирования в трети случаев.

Внезапно все официальные китайские сообщения фокусируются на понятии скорости репликации, с чрезвычайной готовностью – для Китая, который не привык делиться с внешним миром данными в области здравоохранения, – поделиться высокоточными эпидемиологическими данными. Еще до того, как мировое научное сообщество смогло провести серьезные исследования с реальными испытуемыми группами населения, ожидание результатов “в диапазоне от 3,5 до 6” для коэффициента репликации и “в диапазоне от 3,4 до 10%” для коэффициента смертности было определено в качестве критерия кризисного чтения, а авторитарная модель сдерживания пропагандировалась в качестве архетипичного и действенного ответа на эту глобальную пандемию.

“26 февраля канадец Брюс Эйлвард из ВОЗ, который затем прервал интервью в прямом эфире[2], когда его попросили признать Тайвань, прямо сказал: “Скопируйте ответ Китая на COVID-19”. В апреле канадский парламент вызвал Эйлварда на слушания, но ВОЗ запретила ему давать показания” (Senger, 2020).

Случай стратегического ответа Запада на Sars2-CoV-2 и глобальную пандемию COVID-19 интересен по нескольким причинам. Это, прежде всего, “проклятие победителя”. Проклятие победителя – это тенденция к тому, что выигравшая заявка на аукционе намного превышает внутреннюю стоимость лота. Конечно, его вредоносный противник должен перебить ставку соперника, чтобы его обязательство стало дорогостоящим и уменьшило его конкурентоспособность. Разрыв между реальной и внутренней ценностью может быть обусловлен неполной информацией о хорошем (здесь реальная ситуация с пандемией), об эмоциях (здесь страх перед болезнью, более опасной и заразной, чем лихорадка Эбола, по крайней мере, как было объявлено в феврале 2020 г.).

Эта странная стратегия как раз и является выводом статьи Талера (1988), впервые определяющей это “проклятие победителя”. Он пишет: “Возможность неоптимального поведения других участников аукциона ставит вопрос, редко затрагиваемый в экономической теории, а именно: что делать, когда понимаешь, что твои конкуренты совершают ошибки” (Thaler, 1988, p. 200).

Лучшим решением, продолжает Талер, является обмен информацией с конкурентами в кратчайшие сроки, чтобы они, в свою очередь, сократили свои позиции. “Если они поверят вашему анализу, игра может быть выгодной для участников торгов” (Thaler, *там же*). Вывод: “Исследование оптимальной стратегии для игр, в которых противники не вполне рациональны, заслуживает большего внимания со стороны экономистов” (Thaler, *там же*). В пандемическом кризисе COVID-19 все глобальные игроки, за исключением Китая, перевесили предвзятые эпидемиологические данные, все они были загнаны в неудержимый механизм жесткого реагирования на угрозу терроризированного населения, разрушенной экономики и “проклятия победителя”.

Когда Госдепартамент предоставил выборку из 250 000 аккаунтов, которые, как считается, причастны к дезинформации о коронавирусе, “Твиттер” отказался принимать меры. Эта деятельность затрагивает страны, которые практически не имеют права голоса в управлении социальными сетями; недавнее исследование показало, что тысячи неоригинальных аккаунтов продолжают способствовать дружбе между сербами и китайцами после того, как “Твиттер” удалил тысячи других аккаунтов. Бывший сотрудник Facebook написал: “У меня на руках кровь”, потому что компания систематически исключала злонамеренную политическую деятельность, несмотря на ее непропорциональное влияние” (Senger, 2020).

В целом, исследования, посвященные урокам, извлеченным из успеха, показывают, что многие организации улучшают свою работу, но организации могут переучитывать поведение, которое, по их мнению, способствует успеху, и становятся нереалистичными в отношении того успеха, который последует за ними. В результате уроки успеха постепенно превращаются в смирительные рубашки, которые мешают организациям адаптироваться к социальным и технологическим изменениям. Успех пандемического антикризисного управления в Китае в точности соответствует этой логике.

9 марта Италия, первая крупная европейская страна последовавшая рекомендациям ВОЗ и ставшая первой за пределами Китая закрывшейся страной. Премьер-министр Италии Джузеппе Конте давно выступает за более тесные связи с Китаем. Китайские эксперты прибыли в Италию 12 марта и через два дня посоветовали ужесточить закрытие: “На улицах все еще слишком много людей и деятельности, чтобы улучшать”. 19 марта они повторили, что Италия не была “достаточно строгой” в своей политике закрытия: “Нам нужно, чтобы каждый гражданин был вовлечен в процесс COVID-19 и следовал этой политике” (Senger, 2020).

Сайерт и Март (1963 год) подчеркнули центральную роль правил принятия решений в создании рутинных рамок в организациях. Рутина – это краеугольный камень институциональной теории. Гораздо более мощного контроля можно добиться с помощью простых поведенческих процедур, чем с помощью стратегического сдерживания. Восприятие неудачи побуждает организации брать на вооружение новые методы работы. Северная Италия с помощью китайской пропаганды становится архетипом этого провала.

С самого начала пандемии именно в Италии научные мнения повышали тон, указывая на необходимость учитывать, что вирусное явление – это аэрозоль, и что лучшей стратегией было бы усиление иммунной защиты individual, проветривание и вентиляция, поддержание динамического социального дистанцирования, но избегание массивного заключения, которое, помимо экономического разрушения, ослабляет иммунитет, истощает психологию, снижает иммунитет и создает вспышки.

“Италия была одновременно обстреляна китайской дезинформацией”. С 11 по 23 марта около 46% твитов с хэштегом #forzaCinaeItalia (Go China, Go Italy) и 37% с хэштегом #grazieCina (Спасибо Китаю) пришли от роботов (Senger, 2020). Это было сделано без учета усиления повествования об успехе; успех, согласие которого получено для “аудитории-призрака” (Lippmann 1922, 1925), чье выражение сводится к инвазивности в социальных сетях. Любой научный разговор о реальной природе Sars2-CoV-2, смертности от инфекции, об аэрозольной или проекционной диффузии был потушен.

ВОЗ полностью построена на едином повествовании об успехе ограничений.

Длительные периоды непрерывного успеха способствуют структурной и стратегической инерции, экстремальной ориентации процесса, невнимательности и замкнутости (Baumard and Starbuck, 2005). Обучение устраняет виды деятельности, которые кажутся иностранными, в результате чего организации становятся более простыми, менее осведомленными о событиях, происходящих вне их непосредственной сферы деятельности, и менее способными к разнообразным действиям. Например, сосредоточение внимания на навыках, необходимых для поддержания конкурентного преимущества, изначально способствует успеху, но затем имеет тенденцию делать организацию более специализированной и жесткой (Miller, 1993 and 1994). Специализация дискурса, процедур и рутины нормализует поведение; устанавливает стандарты поведения; создает нормы восприятия; позволяет обвинять и указывать пальцем на инакомыслие, которое осмеливается бросить вызов общей норме.

2 Интервью, прерванное экспертом ВОЗ при упоминании Тайваня, доступно по адресу: https://twitter.com/DailyCaller/status/1250198856735875072.

В конце мая 2020 г. Китай начал новую глобальную коммуникационную кампанию, призывающую людей носить маску как символ уважения; повествование, которое принимают все западные СМИ, включая доктора Энтони Фаучи, использующего его дословно[3]. Отныне неношение маски связано с отсутствием гражданской позиции, недостатком человечности, а роботы пропаганды распространяли сфабрикованные свидетельства людей, которые “убивали” своих соседей или бабушек и дедушек, отказывающихся носить маску. Механизмы усиливающей ловушки существуют: постепенная потеря свободы выбора, неопределенность процесса, повторяющийся характер решения, вынужденные инвестиции в публичное пространство (Brockner and Rubin, 1985).

Те же самые процессы, которые организации используют для извлечения уроков из своих успехов, ставят под угрозу их долгосрочную устойчивость. Чтобы повторить свои успехи, организации создают поведенческие программы и буферы, а также сосредоточивают свои усилия на сборе информации и коммуникации, чтобы сделать их эффективными. Поскольку они опасаются, что их успехи не будут продолжаться в изменившихся условиях, организации пытаются заблокировать изменения (Baumard and Starbuck, 2005).

“В марте государственные СМИ Китая начали описывать стратегию “иммунитета стада” – позволяющую распространять коронавирус среди молодых и здоровых – как нарушение “прав человека”... В январе Пекин пригрозил разорвать все коммерческие связи со Швецией, чтобы наказать шведского издателя Гуй Конью, который с тех пор находится в Китае, за присуждение ему литературной премии. Швеция не отступила и отказалась следовать китайской модели локаута, выбрав стратегию иммунитета стада. В результате Швеция стала главной мишенью китайского лагеря, представляя его как слабую перед лицом угрозы COVID” (Senger, 2020).

Организационная среда создает жесткость, требуя от организаций рационализации, прогнозирования и надежности. Однако организации имеют ограниченные возможности для блокирования экологических изменений, и сбор информации, который, по их мнению, является эффективным, может помешать им воспринимать критические изменения. Когда они воспринимают критические изменения, обязательства по существующим программам и выполнение их прогнозов могут помешать им быстро и эффективно реагировать (Starbuck, Greve and Hedberg, 1978).

Однако приверженность суеверному обучению затруднена, особенно в сочетании с простыми прямыми наблюдениями, которые могут быть сделаны с помощью умеренного опыта. Именно здесь стратегии “отчуждения” вступают в игру с самого начала пандемии, “растущий страх, подпитываемый драматическими прогнозами инфекции и смерти, мотивирующими неотложные действия и, следовательно, растворяющими подходами” (Rowe *et al. 2020, p. 13*). Идет ли речь о нормативном давлении, геолокализации, наказании в уголовном порядке или в СМИ, стыде нецивилизованного жеста, доносе соседей: механизмы усиления вездесущие, чтобы ни один актор не отступил от доминирующей логики.

Сайерт и Март (1963 год) утверждали, что организации с гораздо большей вероятностью изменят свое поведение в ответ на неудачи, чем на успехи. Фактические или ожидаемые сбои, говорят они, могут привести к тому, что организация изменит свои цели или ожидания результатов. Критерий успеха должен быть достижим; напротив, это может подтолкнуть участников к эскалации приверженности, т.е. слепой приверженности недостижимой цели (Staw and Ross, 1978).

Проблема первоначальной китайской коммуникации в том, что она была слишком карикатурной. Официальное число смертей, объявленное КПК в ознаменование победы над пандемией, составило 2 535 смертей в городе Ухань (8,9 млн. жителей); или 28,48 смертей на 100 000 жителей, что соответствует смертности в Южной Африке или Аргентине, но намного ниже, чем во Франции (46,79 на 100 000 жителей), Соединенных Штатах (61,09), Бразилии (65,53) или Испании (65,63)[4]. В эпицентре пандемии, с трехмесячной задержкой вмешательства из-за местной цензуры, такое представление математически невозможно; то, что проницательные наблюдатели вскоре заметили, когда обнаружили бесконечные очереди перед городскими моргами, которые трудно скрыть[5]. Только в один из этих моргов было доставлено 5000 урн для похорон; все это, конечно же, было восхитительно задокументировано, с фотографией приема урн, сделанной в морге[6]. Китайская Народная Республика, находящаяся под эмбарго и заключенная в тюрьму, – это не совсем то место, где кто-либо может обратиться в морг, не будучи допрошен полицией.

Китай должен был потерпеть неудачу, но не смог в умеренной степени создать то, что Ситкин (1992) называет более сильной приверженностью повествованию о преодолении неудачи. Как заметили Хьюст и Михайлова (2002, p. 587), “люди не могут свободно и открыто делиться своими знаниями об ошибках, которые они совершили”; и чем скорее неудача будет свободно обсуждаться как неудавшийся “эксперимент”, тем скорее основные убеждения организации укрепятся (Baumard and Starbuck, 2005). Это механизм самопроизвольного раскаяния загрязнителя; но это также и средство захвата политического определения успеха (Anheier, 1999). К концу марта 2020 г. Китай навязал миру три ключевых понятия: уровень воспроизводства, уровень смертности от инфекций и критерий успеха, навязанный всем остальным странам: менее 5000 смертей для города с населением менее 10 миллионов человек.

В планах нерешенных сражений девятая из 36 лунок называется “Наблюдение за огнем с другой стороны”. Когда исход битвы скомпрометирован или не решен, эта китайская военная уловка рекомендует подождать или вызвать максимальный переворот в лагере противника, чтобы дождаться нужного момента, или создать поражение собственной рукой.

Глобальное управление этим пандемическим кризисом, несомненно, является неудачей, особенно для Запада. Она начинается с небольшого провала, местного случая цензуры со стороны Уханьского политического бюро, которое отчаянно пытается скрыть местную эпидемию, которая может дорого стоить главам его муниципалитетов. Но, как мы показали в 2005 году, небольшие неудачи, как правило, укрепляют фундаментальные убеждения, и фундаментальные убеждения используют эти небольшие неудачи в качестве повествовательных историй, которые укрепляют основополагающее убеждение (Baumard and Starbuck, 2005).

Организационное обучение, которое казалось настолько доброкачественным и желательным, когда Сайерт и Март впервые указали на него, может быть опасным или неэффективным (Baumard and Starbuck, 2005). Обучение, которое следует за первоначальным успехом, может быть ядовитым для других организаций, которые на основе неопределенных или фальсифицированных успехов определяют ложные правила и критерии успеха. Обучение, которое должно было последовать за первоначальным провалом, никогда не произойдет, или когда оно произойдет, как это произошло в Европе, Австралии или Новой Зеландии, были извлечены неправильные уроки.

В этот кризисный период мы сталкиваемся с пустым стратегическим регистром. По принципу предосторожности все западные и большинство восточных стран бросились в стратегическую слепоту, продолжая изгибать воображаемые кривые; в то время как Sars2-CoV-2, очень реальный, более генетически сложный, чем предыдущие коронавирусы, но также, во многом, менее страшный, распространился по всему миру. Архетипичная замороженная реакция, распространенная Китаем одновременно с открытием пандемии, привела к экономическому разрушению свободного мира и оказалась неадекватной стратегией реагирования на пандемический кризис COVID-19.

3 Пример развития этого повествования в основных средствах массовой информации см. Хиллари Люн (Гонконг), «Почему в Азии поощряется ношение маски для лица, а в США - нет», журнал «Тайм», 12 марта 2020 г. https://time.com/5799964/coronavirus-face-mask-asia-us/.

4 Данные Джона Хопкинса от 23 сентября 2020 года: https://coronavirus.jhu.edu/data/mortality.

5 Алекс Линдер, «Урны в Ухане намного превышают число погибших, что вызывает больше вопросов о подсчетах в Китае. За последние два дня в один морг было доставлено 5000 урн, что вдвое превышает зарегистрированное число погибших от коронавируса в городе», Шанхайст, 27 марта 2020 г. http://shanghaiist.com/2020/03/27/urns-in-wuhan-far-exceed-death-toll-raising-more-questions-about-chinas-tally/.

6 Источник: Кайсин, 27 марта 2020 года. Мы рекомендуем использовать VPN, прежде чем обращаться к этому источнику: http://photos.caixin.com/2020-03-26/101534542.html.

Принцип предосторожности, родившийся в 1995 году, который вошел в популярную культуру и сразу же покинул ее, только что продемонстрировал пандемию Sars2-CoV-2, что она порождает явления жесткости к угрозе (Staw, 1981); толкает акторов в регистры прошлого, не пригодные к новым ситуациям (Starbuck, 1983); и делает лиц, принимающих решения, восприимчивыми к тому, чтобы стать объектом кампаний влияния или дезинформации.

Отсутствие стратегического обучения во время пандемии Sars2-CoV-2 иллюстрирует такой стратегический вакуумный механизм; он воспринимается не как возможность выздоровления или стратегического обращения вспять, а как пострадавший, парализующий и ослепляющий вакуум. Способы управления стали заменителями стратегического мышления. А сама стратегия превратилась в самонаводящуюся тактическую реакцию. Можно подумать, что нам не хватает стратегов, но на самом деле именно сами стратеги создали ситуацию.

Мы не были свидетелями выражения мира предосторожности, заботящегося о будущих поколениях, как Мишель Барнье намеревался в своем “принципе предосторожности” в 1995 году… Мы создали мир постоянного удивления, постоянного разъединения между постоянным стратегическим вакуумом и прирученной тактической ерундой.

Идеологии развиваются и процветают в таком мире. Тактические возвраты приносят плоды. Глобальные дезинформационные кампании вступают в силу немедленно. Страх распространяется как неконтролируемые лесные пожары. Все должно стать тем, что Клаузевиц уже представлял себе как “нерегулярную войну в глобальном масштабе”. Развитие глобальной информационной инфраструктуры обеспечивает эластичность между этими тремя в остальном несовместимыми областями. Когда тактика спотыкается – потому что спотыкается – мгновенные “когнитивные корректировки”, которые некоторые назвали бы информационной войной и другими измышлениями согласия, немедленно заполняют пустоту. Когда глобальные идеологии терпят неудачу, есть тактика, чтобы заверить всех в том, что мир без цели работает.

“Психология стаи” спонтанных восстаний может быть как поглощена, так и искусственно сгенерирована. Стратегии дестабилизации и психологические операции, сопровождавшие эпизод пандемии Sars2-CoV-2, демонстрируют, как этот оскорбительный вакуум, эта системная стратегия депортации создала благодатную почву для глобальной “нерегулярной войны”, как предвидел Клаузевиц, с той разницей, что эти войны сегодня столь же когнитивны, сколь и физически репрессивны.

Для того чтобы выйти на новый путь, нам необходимо бороться с этими тремя механизмами одновременно. Для того чтобы положить конец тактике, мы должны энергично воссоздать преобразующую ценность человеческой деятельности в науке, образовании, экономике, финансах и, в конечном счете, в обществе в целом.

Этот абсолютный кризис COVID-19 покажет, чего стоит обществу и цивилизации потерять стратегическое обучение. Уступая предварительным условиям, утрачивая фундаментальное стремление к свободе, которая определяет как республики, так и демократии, современный мир вступил в дурацкую игру, в которой он поставил свою свободную волю, свою изобретательность и свою надежду против обещания лучших эпидемиологических кривых, страха в своем желудке.

СЕМИНАР–КРУГЛЫЙ СТОЛ № 4
ПРОБЛЕМЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ЦЕЛЯХ БЕЗОПАСНОСТИ БИЗНЕСА В ИКТ-СРЕДЕ

Модератор:
Григорьев Дмитрий Игоревич, Директор департамента защиты информации и IT-инфраструктуры ПАО «Норильский Никель»

Д.И. Григорьев
Директор департамента защиты информации и IT-инфраструктуры ПАО «Норильский Никель»

О НЕКОТОРЫХ АКТУАЛЬНЫХ ПРОБЛЕМАХ КРУПНОГО ПРОМЫШЛЕННОГО БИЗНЕСА В КОНТЕКСТЕ МИБ

Развитие технологий, в том числе цифровых, создало условия для появления новых вызовов и угроз и потребовало принятия мер противодействия на всех уровнях. Сфера использования информационно-коммуникационных технологий наиболее ярко демонстрирует взаимосвязь и взаимозависимость корпоративной и национальной безопасности.

В целях противодействия посягательствам на информационные активы ПАО «ГМК «Норильский никель», в структуре Компании создан Центр оперативного реагирования (Security Operational Center) на компьютерные инциденты. Центр аккумулирует компетенции в сфере борьбы с киберпреступлениями и разрабатывает технологические решения по обеспечению безопасности информационной инфраструктуры «Норникеля».

Современная ИТ-платформа ПАО «ГМК «Норильский никель» позволяет внедрять передовые технологии и открывает возможности цифровизации производства. «Норникель» реализует пилотные проекты по внедрению перспективных цифровых решений и систем. Сформирована «Цифровая лаборатория «Норникеля», на базе которой было апробировано более 10 решений, среди них: системы имитационного моделирования, оптического распознавания, работы с большими данными и Интернета вещей. Ведется запуск разработанных решений в промышленную эксплуатацию.

В силу исторически сложившихся условий сегодня ИТ-инфраструктура промышленных холдингов построена в основном на решениях/продуктах/услугах ограниченного числа вендоров, зарегистрированных в юрисдикции США, Израиля и еще нескольких стран Западного блока. В такой ситуации промышленный бизнес вынужден учитывать риски, связанные с геополитическим противостоянием держав и возможными, политически мотивированными санкциями (эмбарго

и пр. ограничениями) на поставку продукции этих вендоров. Существует вполне реальная угроза для бизнеса стать заложником политических баталий геополитических противников. На наш взгляд, стоит подумать о введении **особого международно-правового режима** для продукции/услуг вендоров, обеспечивающих значимую долю критических ИТ-инфраструктур с целью снизить указанные риски, а также повысить надежность и устойчивость глобальной ИТ-инфраструктуры в целом. Ярким негативным примером использования доминирующего положения в ИТ-секторе в политических целях является отключение от финансовой системы S.W.I.F.T. Ирана и КНДР.

В настоящее время мы видим устойчивую тенденцию со стороны крупных ИТ-вендоров по переводу ИТ-сервисов в «облака». Для крупных государственно значимых промышленных холдингов это влечет серьезные проблемы, так как их ИТ-ресурсы должны быть защищены в соответствии с суверенными требованиями своих государств, которые не обеспечиваются в «облачных решениях». Эта сложная проблема требует комплексного: международно-правового, организационного и технического рассмотрения с участием всех заинтересованных сторон. Предлагаю подумать на эту тему, в том числе с привлечением ресурса академических и международных научных структур, таких как МИКИБ.

Еще одна проблема связана с темой социальных сетей. Сегодня социальные сети становятся мощным инструментом мобилизации и управления массами. В руках недобросовестных конкурентов они могут стать опасным орудием шантажа через дестабилизацию социальной обстановки, провокации недовольства в регионах доминирующего присутствия промышленных холдингов. Эта непростая тема требует взвешенного подхода, необходим точный баланс между соблюдением прав и свобод граждан при обеспечении интересов бизнеса. Считаю полезным организовать регулярный международный обмен «лучшими практиками» по этой теме.

Надеюсь на плодотворную дискуссию на нашей секции желаю успеха всем выступающим.

Чжу Ликсин, Чжан Руолин
Профессор, Хуан Джаотанг Университет, Институт Суджень, КНР

ПРАВОВЫЕ ОСНОВЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

1. Вопросы безопасности КИИ имеют международное значение

Критическая информационная инфраструктура (КИИ) является базовым звеном Интернета, а ее безопасная и непрерывная работа является основой сетевой безопасности. В последние годы преступления против КИИ становятся все более распространенными, это стало тенденцией в части проведения транснациональных атак. Например, системы аэропортов во многих городах, включая Вену и Нью-Йорк, финансовые системы в таких странах, как Бангладеш и Украина, медицинские и здравоохранительные системы в Японии и Австралии, энергетические системы в Германии и Турции – информационные системы критических инфраструктур во всех этих странах подверглись нападениям.

Мы обратили внимание на атаку, проведенную в начале апреля 2018 года у побережья Африки, когда был перерезан подводный сетевой кабель системы «Побережье Африки к Европе», что нарушило доступ к территориям Сьерра-Леоне и национальной сети Мавритании – она была “оффлайн” в течение двух полных дней. Атаки на энергосистемы становятся все более частыми. Отключение электроэнергии в Венесуэле нетрудно связать с отключением электроэнергии в Иране посредством Stuxnet и сбоями в украинской энергосистеме. От Ирана до Украины и Венесуэлы - кибератаки на критически важную информационную инфраструктуру стран стали заметной формой киберпреступности, кибератак и обороны.

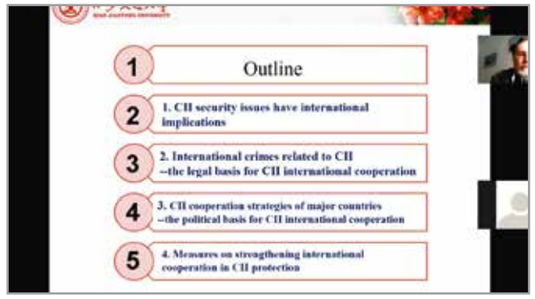
2. Международные преступления против КИИ – правовая основа для международного сотрудничества в сфере КИИ

Что касается тех вопросов, которые серьезно влияют на сетевую безопасность, то мы надеемся выработать нормативные решения и идеи с точки зрения существующего международного права. Современные исследования показывают, что международные преступления, связанные с КИИ, можно разделить на “совершаемые в военное время” и “совершаемые в мирное время”. “Военное время” включает в себя преступления, связанные с нарушением мира, военные преступления и преступления против человечности. “Мирное время” составляют террористические акты и компьютерные преступления.

В настоящее время, несмотря на возможность регулирования некоторых видов поведения, нарушающих международный мир и порядок, отмечается недостаток конкретных мер по поддержанию международного сетевого порядка и защите КИИ. Тем не менее, международное сообщество достигло консенсуса в отношении того, что борьба с преступностью является правовой основой международного сотрудничества в целях защиты КИИ.

3. Стратегии сотрудничества крупнейших стран по защите КИИ – политическая основа международного сотрудничества в сфере КИИ

Ввиду взаимосвязи и глобализации сети проблема сетевой безопасности стала общим вызовом, с которым сталкиваются все страны мира, и его ядром является защита КИИ. Международные организации и ключевые страны уделяют большое внимание выстраиванию



КИИ и стратегиям по ее защите, законодательству и организационной системе. Изучая намерения США, России и Китая в области стратегического сотрудничества, мы обнаруживаем, что крупные державы имеют схожие стратегические намерения в отношении защиты КИИ, и все они признают важность защиты КИИ посредством международного взаимодействия.

4. Меры укрепления международного сотрудничества по защите КИИ

Для стран существует два основных направления в решении проблем кибербезопасности на правовом уровне: первое – использовать традиционное законодательство и изучать преступления “постфактум” в качестве основного средства эффективной борьбы с различными незаконными и преступными актами в киберпространстве; второе – разработать эффективную систему надзора за процессами с помощью отдельного законодательства. Традиционные правовые методы закреплены в уголовном и уголовно-процессуальном законодательствах различных стран, во главе с Будапештской конвенцией о киберпреступности 2001 года. Однако, проблемы, которые могут быть решены традиционными судебными процессами в отношении киберпреступности, – это лишь верхушка айсберга. Как отметил Натан Александр Сейлз: “Сетевая безопасность слишком важна и слишком сложна, чтобы полностью регулироваться уголовным правом и правом вооруженных конфликтов”.

Мы могли бы укрепить международное сотрудничество в области защиты КИИ тремя путями. Во-первых, укреплять международное сотрудничество в области судебной системы. Международное взаимодействие при борьбе с преступлениями против КИИ или совместная защита КИИ главным образом опираются на внутреннюю юрисдикцию каждой страны. Следовательно, усиление защиты критически важной инфраструктуры требует расширения обмена между судебными структурами и сотрудничества между странами и регионами. Во-вторых, укрепление международного сотрудничества в части управления уязвимостями сетей. Уязвимости, обнаруживаемые в Интернете, являются одной из ключевых причин большинства сетевых атак. С развитием Интернета вещей потенциальное влияние посягательств на незащищенные элементы КИИ возрастает. Итак, важно укреплять международное сотрудничество в сфере управления уязвимостью сетей. В-третьих, необходимо создать объединенное Координационное агентство по международному сотрудничеству. Уже сегодня действует большое количество международных организаций по сотрудничеству, гарантирующих сетевую безопасность, но необходимо учредить специальную международную организацию, которая бы гарантировала безопасность критической информационной инфраструктуры.

А.Н. Петухов
Начальник отдела безопасности КИИ МТУСИ

МЕХАНИЗМЫ И ОСОБЕННОСТИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

Безопасность в индустриях, изобилующих критическими информационными инфраструктурами (КИИ), является доминирующим фактором и не ограничивается внутригосударственной локализацией. Сегодня основная проблематика обеспечения безопасности неуклонно перемещается из области создания высокоэффективных программно-технических средств, криптостойких алгоритмов и интеллектуально насыщенных эвристических методов в область разработки и поддержания правил, условий и ограничений, т.е. в область управления.

Будем воспринимать управление как целенаправленное формирование решений и выполняющее эти решения воздействие на управляемый объект. Эта дефиниция вполне применима для случая управления информационной безопасностью, если соответствующим образом раскрыть используемые в ней понятия, а именно:

- субъект управления;
- управляемый объект и состояния управляемого объекта;
- цель управления и целевое состояние управляемого объекта;
- механизмы формирования решений и инструменты воздействия на управляемый объект.

Уместность обсуждения этих вопросов связана с тем, что в части создания и развития безопасной информационно-технологической операционной и коммуникационной среды и инфраструктуры субъектом управления безопасностью являются:

- государственные и межправительственные организации, влияющие на состояние правовой системы и развитие технологий;
- международные профессиональные объединения, связанные со сферой информационных технологий, телекоммуникаций и информационной безопасности;

- крупные транснациональные компании, работающие в сфере информационных технологий и определяющих состояние информационной безопасности в сообществе пользователей.

Кроме того, вопросам управления безопасностью посвящено большинство международных стандартов серии ISO 27000.

Целью управления информационной безопасностью является защищенность, которая в традиционном понимании возникает и существует как приемлемая реакция на возможное воздействие, нарушающее нормальное функционирование защищаемого объекта. В любом случае управление безопасностью имеет в качестве цели некоторое состояние свойств, факторов и характеристик (критериев) безопасности объекта, которое полагается удовлетворительным (безопасным). Это может быть:

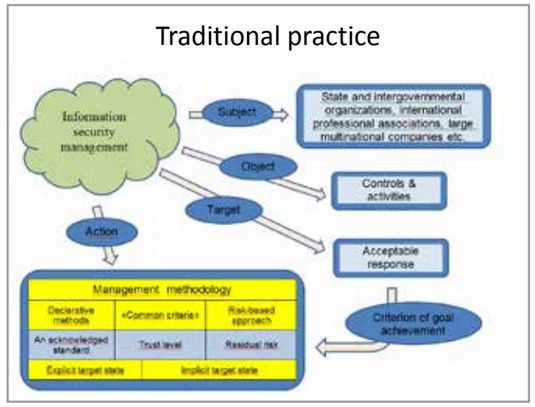
- соответствие принятому нормативу;
- соотнесение с установленным уровнем остаточного риска;
- достижение некоторого уровня доверия к средствам безопасности объекта.

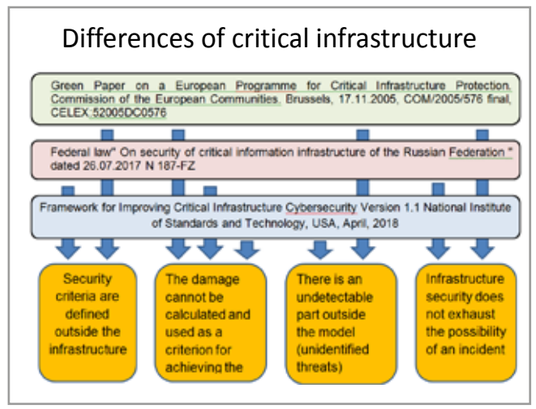
Главное – в составе модели управления всегда есть способ, позволяющий **отличить целевое (безопасное) состояние** объекта от всех остальных (т.н. рекурсивность управления).

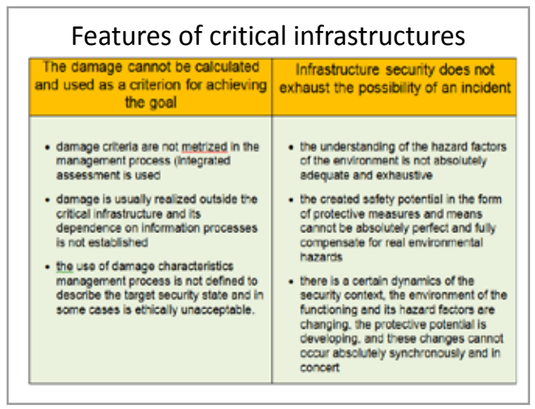
Объектами управления являются активности и контроли. Активностями выступают ограничения, накладываемые на отношения

Mechanisms and features of security management for critical information infrastructures

Andrey Petukhov
Moscow Technical University of Communications and Informatics







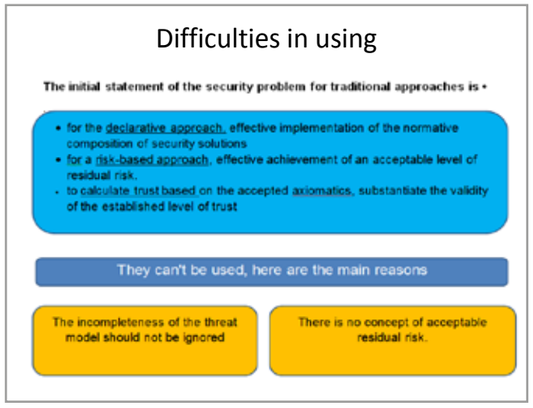
субъектов и объектов информационной деятельности. Контроли поддерживают наблюдение за объектом для оценки и прогнозирования защищенности объекта (пребывания в целевом состоянии).

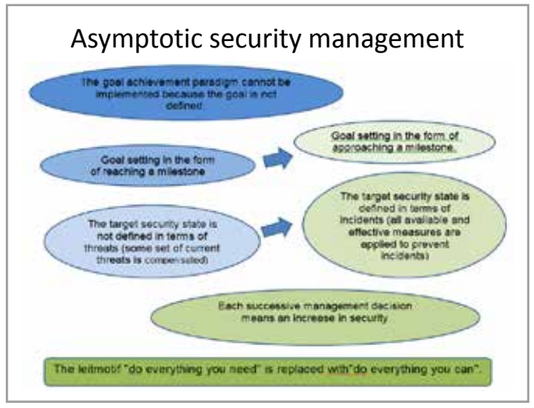
Замысел и облик активностей и контролей составляет содержание политик безопасности, а их реализация – функций безопасности. Руководствуясь предположениями о формах и интенсивностях агрессивности среды и дефектах защищенности объекта, конфигурируется арсенал активностей так, чтобы обеспечить достижение целевого состояния. Контроли служат для удержания объекта в целевом состоянии при изменении предположений об угрозах и уязвимостях.

В случае информационной безопасности представление о целевом состоянии объекта может устанавливаться как в явном (эксплицитном) статическом виде, так и определяться в процессе управления (имплицитный вид). В соответствии с этим определяется характер **управляющего воздействия.**

Эксплицитная форма содержит заранее сформулированные в явном виде условия (требования), выполнение которых соответствует достижению объектом управления целевого состояния. Цели формируются за пределами управляемого объекта (нормативы и руководства регулятора, ведомственные установки, общеметодические решения и т.п.). Это внешние аксиоматические положения, и формально предполагается, что они полностью описывают целевое состояние объекта управления (**декларативная методология**), управляющее воздействие состоит в реализации и удержании этих положений.

Имплицитная форма нашла свое наиболее развитое воплощение в **рискоориентированном подходе,** предполагающем идентификацию, спецификацию и метризацию возможностей возникновения инцидентов. Управляющее воздействие состоит в том, чтобы реализовать меры, снижающие факторы стоимости рисков: интенсивность возникновения инцидента и размер негативных последствий. Целевое состояние характеризуется величиной остаточного риска, означающего достижение некоторого уровня





защищенности, а приемлемость этого уровня соответствует допустимому остаточному риску.

Еще одна распространенная методология управления безопасностью, изложенная в документах **Общих критериев** («исчисление доверия») использует смешанную эксплицитно-имплицитную форму, реализуя управляющее воздействие в виде формирования на базе принятой аксиоматики (цели, угрозы, политики, предположения) заданных требований (функциональных и доверия), полному выполнению которых соответствует целевое состояние.

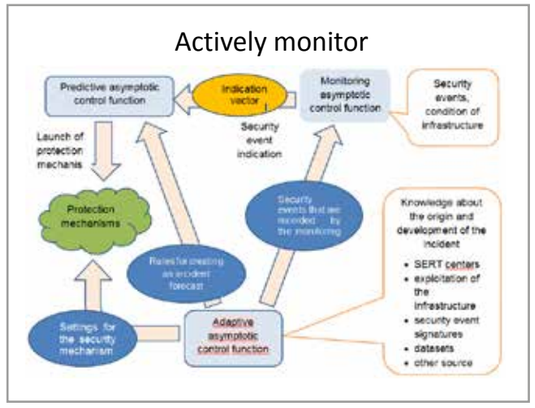
Несмотря на то что эти методологии управления достаточно развиты и имеют обширный опыт применение, попытки непосредственно использовать их в контексте КИИ выявили некоторые особенности. Эти особенности рельефно проявляются уже в базовых документах, определяющих понятие КИИ:

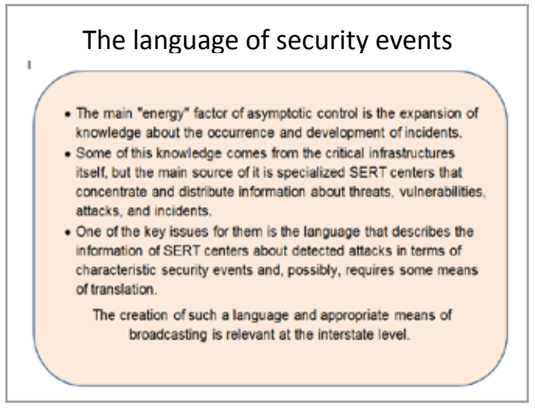
- Green Paper on a European Programme for Critical Infrastructure Protection. Commission of the European Communities. Brussels, 17.11.2005, COM/2005/576 final, CELEX:52005DC0576
- Federal law" On security of critical information infrastructure of the Russian Federation" dated 26.07.2017 N 187-FZ
- Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology, USA, April, 2018

Все доступные источники определяют КИИ в составе критического объекта. Эти определения содержат два общих аспекта: перечисление индустрий, где используются эти инфраструктуры, и неприемлемость (недопустимость, неизмеримость, несоотносимость и т.п.) ущерба, который возникает при нарушении функционирования самого критического объекта. Действительно, трудно себе представить какие-либо измерения, арифметические действия или сравнение цифр там, где речь идет о жизнях и здоровье людей или необратимых экологических катастрофах.

Первый аспект (перечисление индустрий) указывает на то, что информационная инфраструктура является критической не в силу каких-то своих особенных собственных свойств, а в связи с участием в определенной деятельности объекта, на котором она эксплуатируется. И во многих нормативно-методических источниках в качестве задач безопасности указываются обеспечение не традиционных критериев конфиденциальности и целостности, а допустимого функционирования критического объекта в условиях проявления киберопасности. Следовательно, **критерии безопасности** для КИИ определяются допустимостью функционирования критического объекта, **находятся за пределами** собственно КИИ и выражаются в состояниях КИИ, обеспечивающих это допустимое функционирование. Соответственно, состояния КИИ, не обеспечивающие допустимое функционирование критического объекта, являются инцидентами безопасности КИИ.

Второй общий аспект дефиниций, состоящий в тезисе о неисчислимости ущерба, неявно свидетельствует о том, что какие бы усилия ни были предприняты в отношении КИИ, ущерб от нарушения безопасности критического объекта будет все равно оставаться неприемлемым. Такой ущерб не ограничивается разрушением или компрометацией информационных активов КИИ, и даже внутренних процессов самого критического объекта, множество «реципиентов» ущерба может быть гораздо шире. Это приводит к выводу о невозможности использовать ущерб в качестве объекта управления, потому что:





- критерии ущерба в процессе управления не метризуются (используется интегральная оценка его «неприемлемости»);
- ущерб реализуется, как правило, за пределами КИИ и зависимость его от информационных процессов не устанавливается;
- использование характеристик ущерба в процессе управления для описания целевого состояния безопасности КИИ не определено и в ряде случаев этически недопустимо.

Попытки спроецировать это отношение на управление безопасностью приводят к выводу о том, что неприемлемость возможного ущерба соответствует недопустимости остаточного риска и, как следствие, невозможности использования понятия остаточного риска для описания целевого состояния безопасности КИИ. Это прямое следствие невозможности целенаправленного и исчислимого воздействия на величину возможного ущерба в процессе управления безопасностью КИИ. И даже, если бы удалось осознать величину остаточного риска (сколь бы незначительным он не оказался), невозможно отнестись к нему как к некоторому **допустимому** уровню, представляя «несоотносимость» возможного ущерба.

Постоянным мотивирующим фактором деятельности по обеспечению безопасности в критической инфраструктуре является осознание принципиальной возможности инцидента независимо от реальной защищенности критической инфраструктуры. Это соответствует ненулевой оценке субъективной вероятности инцидента – меры экспертной уверенности в том, что данное событие состоится в действительности. Величина этой оценки играет вторичную роль, важно, что она всегда присутствует (отлична от нуля), по причинам, вытекающим из оценки контекста безопасности:

- представление о факторах опасности среды функционирования КИИ не является абсолютно адекватным и исчерпывающим (номенклатура, характеристики);
- созданный в рамках КИИ потенциал безопасности в виде защитных мер и средств не может быть абсолютно совершенным и полностью компенсировать реальные факторы опасности среды;
- существует определенная динамика контекста безопасности, изменяется среда функционирования КИИ и ее факторы опасности, развивается КИИ и ее защитный потенциал, эти изменения не могут происходить абсолютно синхронно и согласованно.

Все известные методологии моделирования угроз явно или неявно исповедуют догмат, утверждающий достаточную полноту модели. Тем не менее, положительных результатов создания корректного механизма для формального доказательства исчерпывающей полноты используемой модели угроз пока неизвестно, скорее, в общем случае, можно утверждать обратное. В этих условиях подобно целевому состоянию безопасности КИИ роль модели угроз несколько деформируется, фактически допуская, что включенные в модель угрозы (идентифицированные угрозы)

составляют лишь часть реально существующих угроз, наряду с которой есть неопределяемая часть за пределами модели (неидентифицированные угрозы).

В случае КИИ при сделанных предположениях становится невозможным определить достижение целевого состояния. Целевое состояние либо не существует, либо недостижимо, и совершенно определенно утрачивает свойство рекурсивности. Задачу безопасности КИИ решила бы некоторая гипотетическая «абсолютная защита», но такой не существует, и между ней и реальной защитой есть разница. Проблема в том, что существующие методологии управления безопасностью не призваны воздействовать на эту разницу, сокращая ее.

Первоначальной постановкой задачи безопасности для традиционных подходов является:

- для декларативного подхода эффективное внедрение нормативного состава решений безопасности;
- для риск-ориентированного подхода эффективное достижение приемлемого уровня остаточного риска;
- для исчисления доверия на основании принятой аксиоматики обоснование правомерности установленного уровня доверия.

Высказанные ранее суждения приводят к выводу о том, что ни один из этих подходов в полной мере **не подходит** для обеспечения безопасности критических объектов потому, что решение этой задачи не может ограничивать себя нормативными номенклатурами решений, аксиоматически приняв постулат полноты модели опасности, и удовлетвориться понятием приемлемого остаточного риска.

Сделанный вывод о неопределенности целевого состояния безопасности КИИ и о неполноте модели угроз вовсе не лишает процессы управления смысла. Если невозможна реализация парадигмы достижения цели ввиду неопределенности последней, то ее следует заменить парадигмой приближения к цели. Целеполагание в виде достижения рубежа заменяется целеполаганием в виде направления движения к рубежу. Таким образом, вводится в рассмотрение понятие асимптотического управления безопасностью КИИ, для которого каждое последовательное решение означает рост уровня безопасности КИИ (асимптотическое приближение к «абсолютной защите»).

При такой постановке в качестве цели управления безопасностью КИИ рассматривается уже не заданный уровень защищенности, который достигается путем конфигурирования системы защитных мер («сделать все, что нужно»). Целью обеспечения безопасности КИИ становится исчерпание текущего потенциала защиты независимо от содержания и направленности агрессивных проявлений («сделать все, что можно»).

В этой парадигме целевое состояние безопасности определяется не в терминах угроз, когда утверждается, что некоторый набор актуальных угроз скомпенсирован, оно определяется непосредственно в терминах инцидентов, когда для предотвращения инцидентов применены все доступные и эффективные меры (разумеется, в пределах ресурсных и функциональных ограничений). Уровень защищенности определяется знаниями об инциденте и мерах его предотвращения, с расширением таких знаний, уровень защищенности растет.

При выполнении конкретной транзакции обработки (передачи) информации может проявиться неидентифицированная угроза в виде возникновения некоторого события, развитие которого может привести к инциденту. Поэтому привлекает внимание **активный мониторинг** событий как средство индикации неидентифицированных угроз и организация реагирования на такие события. В каждый момент дискретного времени определяются случившиеся события из множества событий, коррелированных с инцидентом (события безопасности). Это собственно **функция мониторинга** асимптотического управления.

Источников событий безопасности может быть несколько. Во-первых, это сигнатуры событий, определенно свидетельствующих об инциденте или возможности инцидента. Эти описания относятся к конкретной КИИ и формируются совместно с описаниями инцидентов для данной КИИ. Кроме того, сигнатуры могут носить общий характер и привлекаться из практики и данных SERT-центров.

Во-вторых, это обучающие и тестовые корпуса данных («датасеты»), характеризующие состояние КИИ в стационарном и безопасном состоянии и в условиях проведения атаки заданного типа. На базе их совместного анализа выявляются характерные отличия в фиксируемых событиях безопасности.

После собственно мониторинга выполняется прогноз инцидента (**прогностическая функция** асимптотического управления). Поскольку для КИИ не важно различать потенциальный, развивающийся и свершившийся инциденты, то можно говорить просто об оценке степени опасности по каждому из видов инцидентов (направлений опасности). Результаты прогноза (оценки степени опасности) являются исходными данными для запуска и выполнения механизмов защиты (аргументами функций безопасности). Механизмы защиты полагаются всегда активными и совершенными.

На каждом шагу адаптации могут приниматься и реализовываться решения по внесению «улучшающих изменений» в следующие элементы (**адаптивная функция** асимптотического управления), коррекции подвергаются:

- состав, описание и параметры событий безопасности, которые фиксируются функцией мониторинга (индикация событий) для того, чтобы передать вектор индикации событий прогностической функции;
- состав и параметры правил формирования прогноза инцидента (оценки степени опасности);
- параметры настроек используемых механизмов защиты.

Предлагаемая модель управления **не является альтернативой** традиционных решений, она рассматривается как их развитие и дополнение. Более того, ее применение вызывает необходимость решения ряда теоретических и методических **проблем,** например:

- Как обосновать полноту множества учитываемых инцидентов, которые в условиях асимптотического управления играют роль угроз?
- Что может быть алгоритмической основой прогнозирования инцидентов на основании вектора индикации событий, включая процедуры обучения и тестирования?
- Что является свидетельством необходимости внесения корректировок и определяет их содержание?
- Как обеспечить устойчивость сходимости вносимых изменений и что свидетельствует об эргодичности процесса адаптации?
- и многие другие.

Среди видимых проблем есть направление, которое выходит за пределы конкретных КИИ и носит **интернациональный характер.** Основным «энергетическим» фактором асимптотического управления является расширение знаний о возникновении и развитии инцидентов. Частично эти знания возникают в процессе работы самой КИИ, но основным источником их служат специализированные SERT-центры, концентрирующие и распространяющие сведения об угрозах, уязвимостях, атаках и инцидентах. Одним из ключевых вопросов для них является язык, описывающий сведения SERT-центров об обнаруженных атаках в терминах характерных событий безопасности и, возможно, требующий каких-то средств трансляции. Создание такого языка и соответствующих средств трансляции представляется актуальным на межгосударственном уровне.

Такахиро Сасаки
Приглашенный профессор, Токайский университет
Научно-исследовательский институт стратегического развития мира и международных отношений

БУДУЩАЯ КИБЕРВОЙНА И ТРАНСНАЦИОНАЛЬНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С КИБЕРУГРОЗАМИ

ВВЕДЕНИЕ

За последние годы киберугрозы стали более комплексными. В частности, в будущем предполагается, что Искусственный интеллект (ИИ) будет использоваться для проведения кибератак и осуществления киберзащиты.

Таким образом, сначала в данной статье будет дана оценка того, как ИИ может быть использован в будущих сражениях в киберпространстве. Отдельно взятой стране трудно противостоять подобным комплексным киберугрозам. Затем будут предложены пути сотрудничества в различных странах.

1. ОЦЕНКИ БУДУЩЕЙ КИБЕРВОЙНЫ

1.1. Киберзащита с использованием искусственного интеллекта

В будущем, киберзащита с использованием ИИ сформирует интеллектуальную платформу, способную к обнаружению и защите от изощренных кибератак, а также к автоматическому отслеживанию информации, связанной с кибератаками, получаемой из громадных объемов открытых данных.

В дополнение, высокоточный мониторинг атак, способный обнаруживать, классифицировать, прогнозировать и визуализировать отклонения, будет совершенствоваться, а автономные функции обучения, такие как дополнительное обучение, онлайн-извлечение характеристик, автоматический сбор данных и автоматическая маркировка, будут развиваться и повышать защитные свойства.

Преимущества машинного обучения включают в себя возможность получения знаний из больших объемов многомерных данных наблюдений, а также возможность обнаружения, классификации и прогнозирования отклонений в ответ на атаки путем дополнительного анализа данных наблюдений. Безусловно, ИИ способен функционировать 24/7/365, и все, что может быть зафиксировано с помощью машинного обучения, может быть автоматизировано, что значительно снижает нагрузку на администраторов.

1.2. Кибератаки с применением искусственного интеллекта

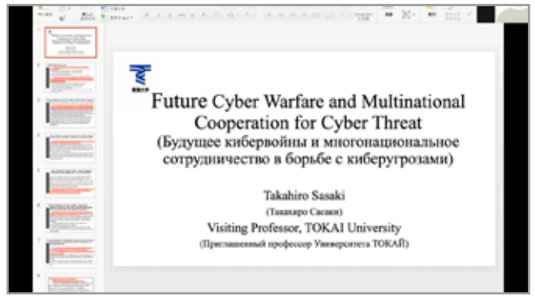
ИИ может помочь точно определить и идентифицировать цели. Множество источников могут идентифицировать людей, которые особенно уязвимы для атак.

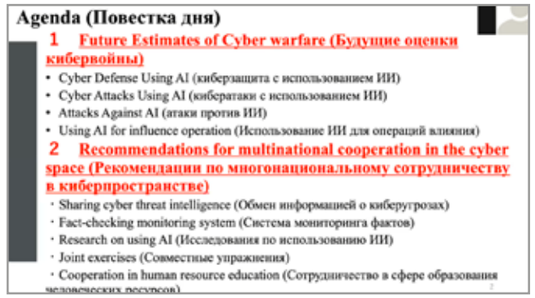
ИИ также может использовать машинное обучение для разрушения спам-фильтров на предприятии. Алгоритмы машинного обучения используются для имитации поведения пользователей в сети с тем, чтобы избежать обнаружения аномального поведения. До сих пор не установлен надежный способ узнать, каким образом злоумышленник проникнет в корпоративную сеть и атакует ее, следовательно, сложно разработать признаки раннего предупреждения.

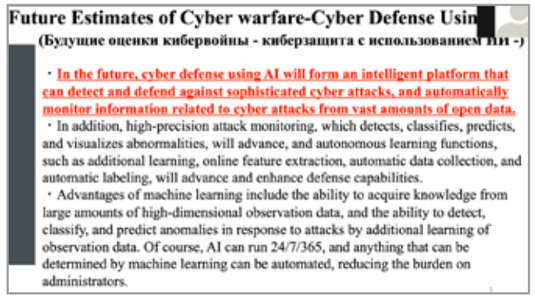
Кроме того, ИИ может сделать существующие кибератаки, такие как кража идентификаторов, DDoS-атаки и взлом паролей, более мощными и эффективными, сделать сложные атаки быстрее и эффективнее, чем атаки хакеров, и помочь киберпреступникам модифицировать свои атаки.

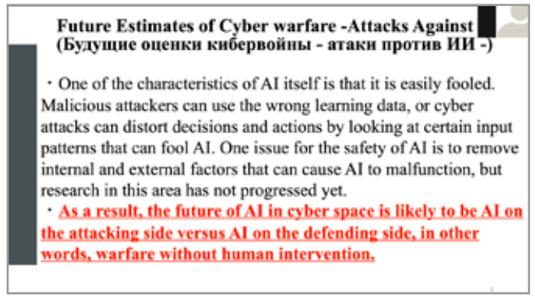
1.3. Атаки против ИИ

Одна из особенностей самого ИИ заключается в том, что его легко обмануть. Злоумышленники могут использовать некорректные обучающие данные, кибератаки могут искажать решения и действия, анализируя определенные входные паттерны, которые способны обмануть ИИ. Одной из проблем безопасности ИИ является устранение внутренних и внешних факторов, способных привести к сбоям в работе ИИ, но исследования в этой области пока не продвинулись.









В результате будущее ИИ в киберпространстве, скорее всего, будет следующим: ИИ на атакующей стороне против ИИ на обороняющейся стороне, другими словами, война без вмешательства человека.

1.4. Использование ИИ в операциях влияния

Технологические преимущества ИИ обуславливают возможности для его будущего применения в операциях влияния с использованием “дезинформации”. В отношении проведения операций влияния, таких как вмешательство в выборы, машинное обучение может применяться для сбора, анализа и прицельного использования всех доступных данных, включая расу, этническую принадлежность, идеологию, демографию и географические условия. Также предполагается, что злоумышленники смогут делать это автономно, без участия человека.

Для распространения информации используются поддельные аккаунты, созданные ИИ, и аккаунты, украденные в результате кибератак, и, таким образом, поддельная информация может распространяться очень быстро.

2. РЕКОМЕНДАЦИИ ПО ТРАНСНАЦИОНАЛЬНОМУ СОТРУДНИЧЕСТВУ В КИБЕРПРОСТРАНСТВЕ

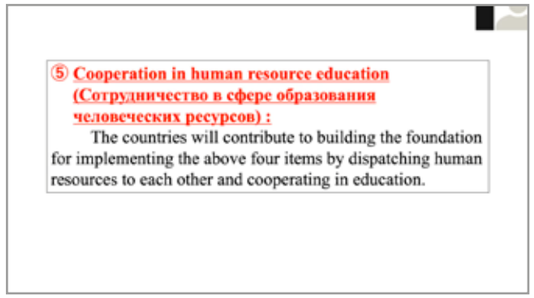
Как мы убедились, в будущем отдельно взятой страны будет трудно противостоять растущей угрозе использования ИИ в киберпространстве. Следовательно, транснациональное сотрудничество в области безопасности и международные структуры имеют жизненно важное значение.

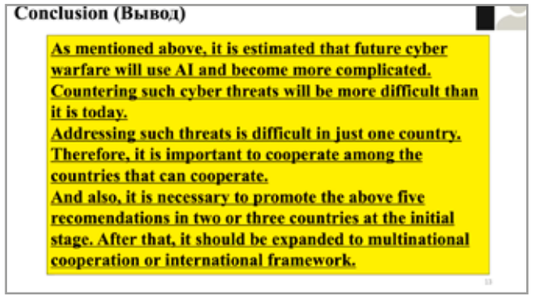
Поскольку каждая страна имеет разный уровень взаимоотношений в контексте безопасности, трудно сказать, какого рода сотрудничество в целом странам следует развивать.

Однако, для того, чтобы противостоять киберугрозам, необходимо будет шаг за шагом углублять сотрудничество, по крайней мере, в следующих областях:

2.1. Обмен разведданными об угрозах

В том, что касается обмена разведданными об угрозах, некоторые страны имеют основу для обмена информацией об угрозах, в то время как другие этого не делают. В связи с этим установить отношения сотрудничества довольно сложно. Однако, необходимо разработать новую основу для эффективного обме-





на информацией, а также обеспечить обмен разведывательными данными о киберугрозах между странами для противодействия таким угрозам.

2.2. Система мониторинга проверки фактов

В последние годы дезинформация с применением киберпространства стала серьезной проблемой. Для того, чтобы противостоять этой угрозе, мы полагаем, что в рамках сотрудничества между странами должна быть создана система проверки фактов (в том числе ее правовые основы).

2.3. Исследования по применению ИИ

Как я говорил ранее, предполагается, что в будущем ИИ будет использоваться в киберпространстве. Для роста возможностей к взаимодействию и взаимного повышения уровня каждой страны необходимо развивать исследования в странах, способных сотрудничать в этой области.

2.4. Совместные учения

Совместные учения проводятся в каждой стране, у них есть свои сильные и слабые стороны. Важно также проводить совместные учения, чтобы изучить сильные стороны других стран и значительно повысить их способность реагировать на трудности. Совместные учения, демонстрирующие глубину сотрудничества, помогут сдерживать атакующие страны.

2.5. Сотрудничество в сфере кадров и образования

Страны внесут свой вклад в создание основы для реализации вышеупомянутых четырех пунктов путем обмена кадрами и сотрудничества в области образования.

ЗАКЛЮЧЕНИЕ

Как уже упоминалось выше, предполагается, что в будущем кибервойна будет использовать ИИ и станет более комплексной. Противостоять подобным киберугрозам будет сложнее, чем сегодня.

Бороться с подобными угрозами в отдельно взятой стране трудно. Поэтому так важно сотрудничать тем странам, которые могут это делать.

Кроме того, на начальном этапе необходимо продвигать вышеупомянутые пять рекомендаций в двух-трех странах. После этого они должны быть распространены до уровня транснационального сотрудничества или международных структур.

Андреас Кюн
Старший научный сотрудник программы "Глобальное сотрудничество в киберпространстве", Институт «Восток-Запад», США

БЕЗОПАСНОСТЬ И НАДЕЖНОСТЬ ИКТ В ЦЕПОЧКАХ ПОСТАВОК: УКРЕПЛЕНИЕ ДОВЕРИЯ С ПОМОЩЬЮ НОРМ В КИБЕРПРОСТРАНСТВЕ И СНИЖЕНИЯ РИСКОВ

Пандемия COVID-19 подчеркнула важность не только эффективных цепочек поставок, но и безопасности и устойчивости этих глобальных производственных и распределительных сетей. Для экспертов по кибербезопасности, специализирующихся на рисках третьих сторон в области ИКТ, вопросы целостности и безопасности цепочек поставок в последние несколько лет вызывают все большую озабоченность. В последнее время геополитическая напряженность вокруг новых технологий, в том числе 5G, искусственного интеллекта и полупроводников, а также растущая обеспокоенность проблемами национальной безопасности привели к ограничительным мерам и призывам к переориентации производства, созданию технологических альянсов между государствами-единомышленниками и разделению технологических и экономических миров.

Ряд нормативных усилий направлен на решение этих проблем безопасности, связанных с ИКТ и цепочками поставок, в контексте международной дискуссии о нормах, правилах и принципах ответственного поведения в киберпространстве. Они сосредоточены на (i) обеспечении безопасности и целостности цепочек поставок ИКТ; (ii) предотвращении фальсификации продуктов ИКТ и создании бэкдоров; а также (iii) смягчении последствий вредоносных скрытых функций. Примеры включают:

- Консенсусный доклад Группы правительственных экспертов ООН (ГПЭ ООН) по достижениям в области информатизации и телекоммуникаций за 2015 год, в котором говорится, что:
  - "(i) Государствам следует принимать разумные меры для обеспечения целостности цепочки поставок, с тем чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ…".
- Международный кодекс поведения в области информационной безопасности Шанхайской организации сотрудничества 2015 года, который отмечает, что:
  - "Каждое государство, добровольно подписавшееся под настоящим Кодексом поведения, обязуется: ...(5) стремиться обеспечить безопасность цепочек поставок товаров и услуг в области информационно-коммуникационных технологий; …".
- Итоговый доклад Глобальной комиссии по стабильности киберпространства 2019 года "Продвижение киберстабильности" предлагает "Норму, позволяющую избежать подмены", которая гласит:
  - "Государственные и негосударственные субъекты не должны вмешиваться в разработку и производство продуктов и услуг и не должны допускать такое вмешательство, если это может существенно подорвать стабильность киберпространства."

Другие релевантные примеры включают в себя фундаментальные элементы Группы

семи (G7) 2018 года для управления киберрисками третьих сторон в финансовом секторе, а также положения соглашения о кибербезопасности «Cybersecurity Tech Accord», Парижского призыва к доверию и безопасности в киберпространстве и Хартии доверия, выпущенных в 2018 и 2019 годах.

Эти недавние отраслевые усилия с участием многих заинтересованных сторон, отражающие передовой опыт, имеют решающее значение для внедрения норм безопасности цепочек поставок ИКТ на практике. Частные компании и правительства посредством государственных закупок ИКТ играют центральную роль. Продолжающаяся цифровая трансформация придает задаче внедрения таких норм срочный характер, поскольку безопасность ИКТ и цепочек поставок не ограничивается только отраслью ИКТ, но также имеет последствия для национальной и глобальной экономики. Например, цифровая цепочка поставок облачных услуг затрагивает все отрасли промышленности и государственный сектор. Более того, цифровые и физические цепочки поставок все больше переплетаются друг с другом. В условиях глобальной пандемии сектор здравоохранения оказывается под перекрестным огнем вредоносных кибератак. В начале декабря подразделение IBM по анализу угроз выявило кибератаки, нацеленные на учреждения и организации, участвующие в дистрибуции вакцины COVID-19, в частности в обеспечении морозильных складских помещений для вакцины. Такие кампании наглядно демонстрируют необходимость принятия мер безопасности ИКТ с учетом рисков, основанных на международных стандартах и передовой практике, на всех этапах глобальных цепочек поставок.

На прошлых форумах в Гармише я утверждал, что роль частного сектора в обеспечении кибербезопасности и реализации норм в киберпространстве имеет решающее значение. Безопасность и надежность ИКТ являются важнейшими условиями цифровой трансформации и глобальных цепочек поставок ИКТ. Но, исходя из названия этой сессии “Проблемы международного сотрудничества при обеспечении безопасности бизнеса в ИКТ-среде”, нынешняя геополитическая напряженность делает безопасность и целостность глобальных цепочек поставок ИКТ все более сложной задачей. Государства приняли или рассматривают ограничительные меры в ответ на растущие проблемы безопасности, поскольку они признают стратегический характер ИКТ для безопасности и экономики, а также свою зависимость от иностранных поставщиков ИКТ в отношении критически важных технологий.

В недавнем докладе Института «Восток-Запад» о безопасности цепочек поставок который доступен по ссылке www.eastwest.ngo/technationslism — мы определяем это явление как “технологический национализм” или «технационализм», который мы определяем следующим образом: “Государственная политика или действия, в рамках которых прямо или косвенно отдается предпочтение продуктам и услугам ИКТ, продаваемым компаниями со штаб-квартирами на территории данной страны или государств-союзников, по сравнению с компаниями со штаб-квартирами в государствах, считающихся конкурентами или противниками”.

Примеры ограничительных мер варьируются в широком диапазоне: от требования к компаниям по локализации данных до применения к иностранным компаниям повышенных требований безопасности, основанных на внутренних стандартах, и заканчивая запретом конкретных иностранных продуктов или поставщиков.

Распространено мнение, что «технационализм» – лучший выход для безопасности и национальной экономики. Но непредвиденные последствия подобных мер могут иметь противоположный эффект, снижая кибербезопасность, обеспечивая ложное чувство безопасности и защищенности и приводя к экономическим потерям.

Доклад Института «Восток-Запад» предлагает альтернативный подход к решению проблем безопасности, основанный на оценке рисков, с одновременным получением поддержки от правительств для устранения долгосрочных рисков и повышения конкурентоспособности. Предлагаемый в докладе подход направлен на обеспечение безопасности и надежности ИКТ с помощью обоснованных, объективных и поддающихся количественной оценке мер по укреплению гарантий безопасности, транспарентности и подотчетности.

Основополагающая идея заключается в том, что отдельные меры не обеспечивают достаточной безопасности или надежности, но в сочетании они способны привести нас к более высокому, приемлемому уровню доверия. Доверие будет завоевано благодаря постоянной, непрерывной верификации данных мер. Ключ к построению доверия заключается в том, что мы должны согласиться выполнять общие правила безопасности и требования к ИКТ. Если мы сделаем это и сможем эффективно противостоять нарушителям, тогда возможно достижение доверия и различия во взглядах на суть проблемы станут менее актуальными.

Модель, предлагаемая Институтом «Восток-Запад» (см. Рисунок 1), состоит из пяти компонентов, которые я резюмирую здесь для большей наглядности:

- Первый компонент посвящен тому, что могут предпринять покупатели ИКТ с точки зрения требований к закупкам с учетом риска: сюда входит требование к поставщикам следовать международным стандартам безопасной разработки продуктов и обеспечивать, к примеру, поставку услуг и программного обеспечения в стандартной, безопасной конфигурации.
- Второй и третий компоненты касаются требований на отраслевом уровне к покупателям и поставщикам ИКТ. Покупатели ИКТ, используя свою коллективную покупательскую способность, должны разработать передовую практику, требующую от поставщиков ИКТ предоставления отчетов об управлении рисками цепочки поставок и формирования отраслевых консорциумов для оценки безопасности ИКТ. С другой стороны, поставщики должны настаивать на требованиях к обеспечению гарантий и прозрачности, принимать конкретные технологические схемы оценки и аккредитации и создавать общеотраслевые наблюдательные структуры.
- Четвертый и пятый компоненты касаются более широкой промышленной экосистемы, включая региональные центры транспарентности, которые позволяют проводить независимый анализ и проверку кодов, а также глобальных программ соответствия.

Рисунок 1: Модель безопасности и надежности, разработанная Институтом «Восток-Запад»

Важно осознавать, что безопасность - это общая ответственность поставщиков, операторов и покупателей. Защищенное устройство, выпущенное на рынок в дефективной конфигурации, ставит под угрозу безопасность, защищенность и конфиденциальность своих пользователей. Таким образом, необходимы совместные усилия и координация для обеспечения безопасности и устойчивости на протяжении всего жизненного цикла ИКТ.

Наконец, правительства должны играть свою роль, особенно в тех областях, где промышленность не обладает соответствующими возможностями, например, для разработки нормативных требований к безопасности, основанных на оценке рисков, или осуществления стратегических инвестиций в науку и технологии.

В.И. Иванов
К.и.н., директор филиала в России, Институт «Восток-Запад»

Добрый день, уважаемые коллеги!

Как представитель Института «Восток-Запад» в России я хочу сделать несколько замечаний в качестве послесловия к выступлению Андреаса Кюна. При этом мои комментарии в первую очередь отражают мою личную точку зрения, не обязательно совпадающую с позицией Института.

Прежде всего, должен проинформировать вас, что наши с Андреасом выступления скорее всего будут последними на подобных международных форумах, в роли представителей Института «Восток-Запад». Дело в том, что на днях Совет директоров Института принял решение о кардинальной трансформации всей организации, включая головной офис в Нью-Йорке и отделения в Брюсселе и Москве. В результате Институт «Восток-Запад» в том виде, в котором он был создан ныне покойным Джоном Мрозом в годы холодной войны и успешно проработал 40 лет, в 2021 году перестанет существовать. Для меня и моих коллег, кто работал в Институте на российском направлении, это особенно драматично, поскольку Советский Союз, Россия и российско-американские отношения всегда были одной из опорных тем Института. Мы всегда стремились наладить конструктивный диалог с российскими партнерами, основываясь на принципах политической беспристрастности, открытости для значимых игроков со стороны как Запада, так и России, и в этом качестве являлись важным переговорным каналом на уровне общественной дипломатии. В том числе в середине нулевых мы одни из первых НКО, вместе с такими партнерами, как Институт проблем информационной безопасности МГУ, ввели вопросы информационной безопасности, защиты критической информационной инфраструктуры и их места в системе международного права, в глобальную повестку дня отношений между государством и бизнесом.

В чем причины такого решения о трансформации Института? Опуская детали корпоративной истории, обозначу два существенных, на мой взгляд, глобальных фактора.

Первое – это обострение геополитической конфронтации между великими державами, а также, особенно в годы администрации Трампа, развертывание беспрецедентной внутриполитической борьбы в США со всеми вытекающими для всего мира последствиями. В этих условиях платежеспособный спрос на институты, обеспечивающие беспристрастность международного диалога, заметно снизился, а требования к ресурсообеспеченности таких институтов критически возросли.

Второе – это коронавирусная пандемия. Помимо общего негативного эффекта COVID-19 на социальные и международные связи, всеобщий переход в онлайн резко снизил возможности для использования инструментов доверительного диалога, основанных на личном живом общении.

На этом фоне представленный Андреасом анализ плюсов и минусов «технологического национализма» выглядит весьма символично. Строительство «цифровых крепостей» разрывает естественную ткань международной кооперации, вышибает из нее существенные звенья, такие как наш Институт, игравший заметную роль в производстве такого продукта, как международная стабильность и безопасность.

Однако во всей этой истории есть и поводы для оптимизма. Достигнуты договоренности о слиянии основных программ Института с рядом международных экспертных организаций, придерживающихся схожих принципов, но оказавшихся более стойкими в нынешней токсичной среде. Кроме того, на базе Чарльстонского Колледжа (штат Южная Каролина) создается Институт глобального лидерства имени Джона Эдвина Мроза, призванный транслировать интеллектуальное наследие Института «Восток-Запад» новым поколениям дипломатов, поддерживать исторический архив, базу контактов и координировать взаимодействие бывших сотрудников и друзей Института.

На ближайший год я вижу свою задачу в том, чтобы сохранить в рабочем состоянии и подключить к новому «пост-иствестовскому» универсуму все продуктивные партнерские связи в России, особенно по вопросам информационной безопасности и киберсотрудничества.

Огромное спасибо НАМИБ и ее руководству за работу по интеграции усилий различных российских игроков и проектов государственного, академического и бизнес-характера по снижению международной напряженности и достижению устойчивых договоренностей в этой критической области. Надеюсь продолжить совместную работу в ближайшие годы.

Благодарю за внимание!

Од Жери[1]
Аспирант-исследователь,
Университет Париж-8, Франция

РАСТУЩАЯ НОРМАТИВНОСТЬ ПОЛОЖЕНИЙ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ КРИТИЧЕСКИХ ИНФРАСТРУКТУР И ПОЯВЛЕНИЕМ СПЕЦИАЛЬНОГО ПРАВОВОГО РЕЖИМА

Защита критически важных информационных инфраструктур является одним из наиболее актуальных вопросов обеспечения безопасности и стабильности киберпространства, а также международного мира и безопасности. Генеральная Ассамблея Организации Объединенных Наций (ГА ООН), а также Совет Безопасности ООН приняли ряд положений, связанных с этим вопросом. Все они рекомендуют государствам принять правовые, технические, кадровые и организационные меры для защиты критически важных информационных инфраструктур, на которые опираются наши общества.

Действительно, уже в 2002 году Генеральная Ассамблея Организации Объединенных Наций (ГА ООН) занялась этим вопросом и приняла специальную резолюцию, именуемую “Создание глобальной культуры кибербезопасности”[2]. ГА ООН приняла еще две резолюции по этому вопросу: резолюцию 58/199 “Создание глобальной культуры кибербезопасности и защита критически важных информационных инфраструктур”[3] и резолюцию 64/211 “Создание глобальной культуры кибербезопасности и подведение итогов национальных усилий по защите критически важных информационных инфраструктур”[4]. Многочисленные положения о защите критически важных информационных инфраструктур были также приняты тремя ГПЭ в их соответствующих докладах в 2010[5], 2013[6] и 2015[7] годах, будь то нормы ответственного поведения государств, меры укрепления доверия или меры по оказанию помощи и сотрудничеству.

Но, отталкиваясь от резолюций ГА ООН о создании глобальной культуры кибербезопасности, мы видим, что эти положения имеют очень низкую степень нормативности, то есть они не предписывают принятие определенного поведения как такового. Внимательное изучение положений, принятых позднее, показывает, что они постепенно менялись. Поворотным моментом является принятие нормы 13 (g) в докладе ГПЭ за 2015 год, в которой ГПЭ, а затем и ГА ООН рекомендовали государствам принять во внимание резолюцию 58/199 и другие соответствующие резолюции, включая резолюцию 64/211. При этом ГПЭ преобразовала то, что было просто системой координат, в положения, предписывающие принятие определенного поведения, описанного в упомянутых резолюциях.

Другие элементы могут быть приняты во внимание для анализа того, как положения о создании глобальной культуры кибербезопасности и, в частности, о защите критических информационных инфраструктур сегодня предписывают государствам принимать правовые, технические, кадровые и организационные меры для защиты критических информационных инфраструктур. В результате мы можем утверждать, что сегодня поведение государств в отношении защиты критических информационных инфраструктур действительно регламентируется – хотя и необязательным образом – международными положениями, и мы можем даже задаться вопросом, не сформировала ли ГПЭ 2015 года скромное обязательство защищать критические информационные инфраструктуры.

Даже если эти положения действительно приобретают растущий нормативный характер, мы не можем утверждать, что они являются нормативными с точки зрения права. Тем не менее мы можем утверждать, что находимся на пути к созданию особого режима, который, вероятно, будет способствовать обеспечению безопасности и стабильности киберпространства.

1 Од Жери имеет степень доктора в области международного публичного права. Она является аспирантом-исследователем в Парижском университете 8.

2 ГА ООН, Резолюция 57/239 “Создание глобальной культуры кибербезопасности”, 20 декабря 2002, A/RES/57/239.

3 ГА ООН, Резолюция 58/199 “Создание глобальной культуры кибербезопасности и защиты критически важных информационных инфраструктур”, 23 декабря 2003, A/RES/58/199.

4 ГА ООН, Резолюция 64/211 “Создание глобальной культуры кибербезопасности и подведение итогов национальных усилий по защите критически важных информационных инфраструктур”, 21 декабря 2009, A/RES/64/211.

5 ГА ООН, Доклад Группы правительственных экспертов о достижениях в области информатизации и телекоммуникаций в контексте международной безопасности, 30 июля 2010, A/65/201.

6 ГА ООН, Доклад Группы правительственных экспертов о достижениях в области информатизации и телекоммуникаций в контексте международной безопасности, 24 июня 2013, A/68/98.

7 ГА ООН, Доклад Группы правительственных экспертов о достижениях в области информатизации и телекоммуникаций в контексте международной безопасности, 22 июля 2015, A/70/174.

О.А. Мельникова
Старший советник ДМИБ МИД России

ОБ УЧАСТИИ БИЗНЕСА В ПРОДВИЖЕНИИ РОССИЙСКИХ ПОДХОДОВ В СФЕРЕ МИБ

Уважаемые коллеги!

Прежде всего позвольте поблагодарить организаторов XIV международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» Национальную Ассоциацию международной информационной безопасности за возможность стать его участником и выступить по заявленной теме.

Вопрос о необходимости более активного участия бизнеса в международной дискуссии по вопросам обеспечения безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) назрел уже давно.

ИКТ проникли во все сферы управления и ведения бизнеса. Финансовые операции, логистика, все виды транспорта осуществляются при широком использовании ИКТ. Во многие отрасли начинается внедрение технологий искусственного интеллекта.

Потеря информационных ресурсов или завладение секретной информацией конкурентами, как правило, наносит любому предприятию значительный ущерб и зачастую может привести к его банкротству.

Сфера бизнеса, напрямую связанная с электронным оборотом финансов, товаров, услуг, пожалуй, одна из наиболее привлекательных для злоумышленников. Количество преступлений в данной сфере пока не имеет тенденции к снижению. Целями преступных атак могут выступать не только финансовые гиганты, которые по роду своей деятельности владеют ценными данными и активами, но и организации среднего звена, а также структуры, имеющие весьма скромный оборот денежных средств. Уязвимыми могут быть и такие компании как, например, крупная датская «Moller-Maersk», осуществляющая по всему миру контейнерные перевозки и потерявшая в 2017 г. вследствие атаки вируса-шифровальщика 300 млн. долларов, и австрийский отель «Romantik Seehotel Jaegerwirt», где злоумышленники дистанционно заблокировали входные двери в номера. Для освобождения своих постояльцев руководству отеля пришлось выплатить преступникам €1,5 тыс. в биткойнах.

Ежегодно увеличивается ущерб мировому бизнесу только от кибератак. В 2016 г. он составил $445 млрд., в 2017 г. достиг $1 трлн, в 2018 г. – $1,5 трлн, в 2019 год – более $2,5 трлн, а в 2022 году, по прогнозу Всемирного экономического форума, сумма может вырасти до 8 трлн долларов. По этим цифрам видно, что рост составляет более 50%.

Мировая пандемия коронавируса усугубила ситуацию, поскольку вызвала лавинообразный рост числа пользователей цифровых инструментов, и, как следствие, активизацию кибермошенников и увеличение злонамеренных актов в ИКТ-среде. Существенно возрос экономический ущерб от подобных противоправных акций.

Бизнес-структуры вкладывают колоссальные средства в техническое обеспечение собственной безопасности, но при этом все яснее осознают объективную уязвимость перед злонамеренными действиями в отношении своих активов. Бизнес стал отчетливо понимать, что задача построения защиты, которую нельзя взломать, утопична по своей сути.

Традиционные методы оказания содействия бизнесу, предпринимаемые со стороны государств, применительно к сфере безопасного использования ИКТ не могут быть достаточной степени эффективными. Например, каким бы современным ни было национальное законодательство, оно не гарантирует защиты, поскольку источник злонамеренного воздействия может располагаться на территории другого суверенного государства. При этом общепринятых международных юридических норм для регулирования информационного пространства пока, к сожалению, недостаточно. Более того, подходы России и ряда западных стран в данной сфере противоречивые. Россия отстаивает позицию о неприменимости международного права к ИКТ-среде, в то время как западные страны и их союзники настаивают на применимости к киберпространству действующего международного права.

И пока продолжается переговорный процесс по вопросам МИБ бизнес продолжает терять колоссальные финансовые средства.

При выработке юридических правил, норм и принципов ответственного поведения государств в киберпространстве гарантирована защита для бизнеса, как одного из акторов ИТК-среды. Однако в настоящее время наблюдается определенная стагнация переговорного процесса, а также серьезное противодействие со стороны ряда технологически развитых государств во главе с США в части выработки приемлемых для всего международного сообщества «правил игры» в киберпространстве. Стоит здесь упомянуть и о попытках легализации ряда западных концепций: так называемой коллективной атрибуции и превентивных кибердударов, предпринимаемых в отношении других стран и по надуманным предлогам. Все это не способствует нормализации или эффективности переговоров по МИБ.

Исходя из необходимости заблаговременно озаботиться о будущем переговорного процесса и сохранить в системе ООН профильный универсальный механизм, Россия в начале октября с.г. внесла в Первом комитете 75-й сессии Генеральной Ассамблеи ООН актуализированный проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». По результатам голосования 9 ноября большинством голосов (104 государства) принят российский проект резолюции, соавторами которой стали 27 стран. Таким образом, в 2021 г. будет учреждена новая Рабочая группа открытого состава (РГОС) по вопросам безопасности в сфере использования ИКТ и самих ИКТ на 5-летний срок (2021–2025 гг.).

Одна из важнейших компетенций новой Группа заключается в том, что она уполномочена обсуждать выдвигаемые государствами инициативы в области обеспечения МИБ, а также создавать вспомогательные подгруппы по отдельным аспектам своего мандата. В частности, предусмотрена работа в специализированных подгруппах, включающих, в том числе, участие бизнеса, что придаст дискуссиям тематически более структурированный и динамичный характер.

Мы видим реальную возможность вовлечения бизнеса в переговорный процесс с акцентом на взаимодействия с ним, а также активизацию его технологического, финансового и интеллектуального потенциала. Задача эта и утилитарная, и рациональная. Рассчитываем, что переговоры представителей мирового бизнеса на площадке единственной международной организации ООН повысят степень доверия со стороны бизнеса к государственным институтам.

Разработка и принятие резолюций, договоров, конвенций применительно к сфере бизнеса и с его участием будет реальным шагом в части выработки унифицированных правил и норм для ИКТ-среды.

В условиях экономической стагнации и одновременной цифровизации экономики и многих других сфер жизни, прагматичная, взвешенная позиция предпринимателей и частных компаний, составляющих основу экономического потенциала современных государств, может способствовать выработке понятных базовых правил и норм поведения в киберсреде.

Бизнес объективно станет тем локомотивом, который подтолкнет государства к выработке четких «правил игры» в киберпространстве.

Пока не так много примеров вовлеченности бизнес-сообщества в юридически оформленные взаимоотношения. В 2017 г. свыше тридцати IT-компаний подписали так называемую Цифровую женевскую конвенцию, подразумевающую отказ от участия в кибератаках, вне зависимости от того, кем они организованы (киберпреступниками или правительствами каких-либо стран) и на кого они направлены. Участники соглашения взяли на себя обя-

зательства оказывать помощь любой стране, подвергшейся атаке в виртуальном пространстве.

В числе подписавших конвенцию немало гигантов IT-отрасли – Microsoft, Facebook, Cisco, Nokia, Dell, HP, Symantec, Trend Micro и другие, всего на сегодняшний день 34 компании. В то же время такие крупные и высокотехнологические бренды как Google, Apple, Amazon и Twitter отказались от участия в соглашении.

Хочу напомнить, что еще в 2017 году в ходе данного Форума была представлена, а впоследствии, в 2018 году в ходе XII Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» была принята разработанная российской ГК «Норникель» «Хартия информационной безопасности критических объектов промышленности». Главный ее посыл – обезопасить информационные структуры предприятий, чья деятельность имеет стратегическое значение для национальных экономик, от попыток внешних злонамеренных воздействий.

Важно диверсифицировать процесс подключения бизнеса к переговорному формату, задействовав этот механизм на таких статусных площадках, как БРИКС, ШОС, АСЕАН и др.

Например, страны-участники АСЕАН в последнее время неоднократно высказывали заинтересованность в широком вовлечении бизнес-структур в переговорный процесс по МИБ. Эти тезисы звучали и на традиционной Сингапурской кибернеделе, состоявшейся в октябре с.г., а также в ходе видеоконференции с участием Директора Департамента международной информационной безопасности А.В. Крутских и высших должностных лиц по кибербезопасности стран-участниц АСЕАН.

Осознают важность данных подходов и наши китайские партнеры, которые в таких значимых региональных структурах как ШОС, АРФ начинают продвигать свои концепции цифровой экономики для защиты бизнеса и с его участием.

Вместе с тем, принципиально важно, чтобы участие негосударственных игроков в переговорном процессе не воспринималось как их уравнивание с суверенными государствами и не происходило в ущерб принятию конкретных политических решений.

Считаем, что разработка универсальных подходов и договоренностей, а также согласование путей урегулирования имеющихся проблем в ИКТ-сфере должны быть прерогативой государств, обладающих исключительным суверенитетом в цифровой сфере.

Вместе с тем, защита информационных ресурсов российских компаний является одним из безусловных факторов экономической безопасности страны.

Благодарю за внимание!

Д.Б. Фролов
Директор Департамента информационной безопасности Телерадиосеть России

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ТЕЛЕРАДИОВЕЩАНИЯ В УСЛОВИЯХ ПАНДЕМИИ: МЕЖДУНАРОДНЫЕ АСПЕКТЫ

Сегодняшний доклад, хотелось бы посвятить проблеме: с какими вызовами столкнулись подразделения ИБ РТРС (Российской телевизионной и радиовещательной сети) в условиях пандемии 2020 года.

Для тех, кто еще не знает, что такое РТРС. РТРС – это предприятие России, осуществляющую трансляцию телерадиосигнала, оно составляет основу государственной системы телерадиовещания и относится к стратегическим предприятиям Российской Федерации. В составе РТРС 78 филиалов – от Калининграда до Камчатки. РТРС – это самая большая телерадиосеть в мире, включающая в себя более пяти тысяч объектов вещания и покрывающая более семнадцати миллионов квадратных километров территории. Начиная с 2019 года, практически все население России может смотреть телевидение в современном цифровом качестве.

Но РТРС – это не только цифровое телевидение, а также и новые технологии в телерадиовещании с использованием сети Интернет. Позвольте сделать небольшое лирическое отступление: что является нефтью 21 века? Это данные. Любой сервис (амазон, фейсбук и другие), а начиная с последнего времени – и операционные системы (виндовс, айос, андройд) – собирают и обрабатывают множество данных, которые используются потом в разных сферах жизни.

Поэтому РТРС, как современный телеком-оператор, чьи интересы не ограничиваются только телерадиовещанием, активно испытывает и внедряет новые технологии: интерактивное телевидение (Эйч Би Би Ти Ви), когда телезритель может принимать участие в передачах, например, в голосованиях за лучшую песню, либо получать какую-то целевую, предназначенную специально для него информацию. Разумеется, РТРС поддерживает внедрение технологий 5G. Большое участие РТРС, как значимое для России предприятие, принимает и в цифровой экономике. Но новые технологии – это всегда и новые угрозы информационной безопасности. Особенно с учетом пандемии.

HbbTV

Исследования интерактивного телевидения, говорят нам об уязвимостях, которые позволяют злоумышленнику внедрять вредоносное ПО в интеллектуальный телевизор с поддержкой (Эйч Би Би Ти Ви), что может заставить его выполнять различные действия, такие как изменение отображаемого контента, добыча биткойнов или атаковать другие устройства, подключенные к сети, к которой подключен телевизор. Смарт-телевизоры в 90% поддаются удаленному взлому с помощью мошеннических телевизионных сигналов. Ещё в далёком 2013 году исследователи из Технического университета Дармштадта обнаружили широкое распространение, без согласия сторонних технологий веб-аналитики, сторонние файлы cookie, в контенте (Эйч Би Би Ти Ви) для отслеживания шаблонов просмотра.

Мобильный оператор T-Mobile (Т – мобайл) первым в 2019 году в Европе запустил коммерческое использование связи 5G. С помощью нового стандарта миллиарды устройств смогут получить возможность так называемого коллективного общения, то есть 5G объединит в одну сеть самоуправляемые машины, устройства сферы ЖКХ и другие гаджеты

виртуальной и дополненной реальности, показатели новой сети позволяют в режиме онлайн транслировать видео в разрешении 4K (Ультра ЭЙЧДИ). Во всем мире идет активное развитие сетей пятого поколения, в России внедрение 5G планируется к 2024 году, ввиду того, что будет использоваться отечественное оборудование и программное обеспечение.

Технологии машинного обучения и искусственного интеллекта (ИИ) уже сейчас широко применяются в информационных системах для увеличения производительности труда, повышения продаж и обучения. Их использование в защите от кибератак становится одним из ключевых направлений в информационной безопасности.

На текущий момент количество атак растёт, а ландшафт угроз меняется с молниеносной скоростью. Очевидно, что при таких объёмах вредоносной деятельности злоумышленники активно применяют средства автоматизации кибератак, в том числе используют технологии искусственного интеллекта и машинного обучения для их совершенствования и трансформации, а также для обхода известных средств защиты. Так, например, эффективным прототипом является известный троян Emotet. Основным каналом для его распространения является спам-фишинг, и группировка, стоящая за созданием Emotet, могла без особых затруднений использовать ИИ для усиления атаки, встраиваясь нативно в цепочки разговоров и используя анализ текста на естественном языке.

Другой возможной сферой вредоносного применения искусственного интеллекта является более эффективный подбор паролей или обход двухфакторной аутентификации.

По данным Webroot, около 85% профессионалов по информационной безопасности уверенны в том, что злоумышленники используют технологии машинного обучения и искусственного интеллекта в своих атаках, это существенно меняет уровень рисков и требования к решениям для обеспечения защиты.

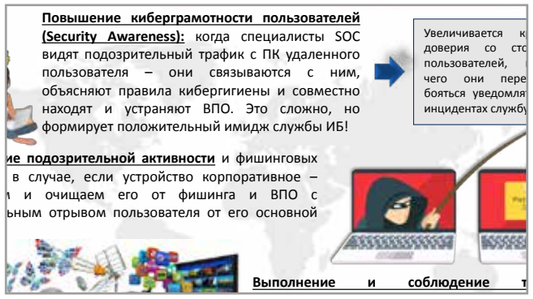
Искусственный интеллект вносит заметный вклад в борьбу с современными информационными угрозами. В частности, в большинстве случаев внедрение технологий ИИ в информационной безопасности организации сокращает время выявления проблем и реагирования на инциденты, а также расходы на управление персоналом. Специалисты по информационной безопасности отмечают рост эффективности детектирования неизвестных угроз, а также скорости анализа и обнаружения вредоносной активности на конечных точках и в приложениях.

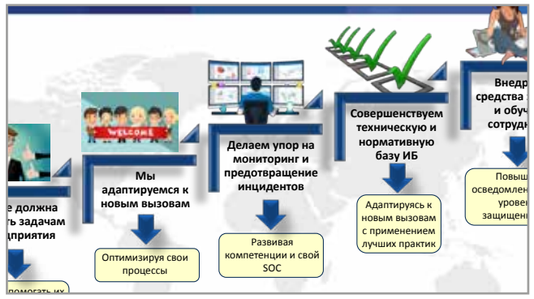
Здесь мы видим основные угрозы, которые характерны для многих предприятий телеком-отрасли. Из специфических угроз можно отметить прерывание ТВ и радиовещания, но хотелось бы обратить внимание на актуальные в связи с пандемией угрозы, которые

характерны и для общемирового масштаба: это кража авторизационных данных (креденшл стаффинг). На «черных рынках» разных регионов (Латинская Америка, СНГ, Европа) появился устойчивый спрос на такие данные и, как следствие – появилось предложение. Данные похищаются преимущественно через фишинговые формы, которые пользователи получают через мошеннические письма, маскирующиеся под письма технической поддержки. Поскольку сами по себе такие формы не являются вредоносными, их не видит большинство средств защиты. Действенные меры – это блокировка таких ресурсов или отправителей, но пока у них не испортится репутация, а до этого пройдет какое-то время, то такие письма очень часто проходят через существующие системы спам-фильтрации. Нередки случаи, когда распространение таких писем идет через «хорошие» почтовые сервера, пользователи которых были взломаны аналогичным способом. Вторая актуальная угроза – это домашние устройства пользователей, через которые они осуществляют удаленный доступ. Неизвестно, что на них находится и зачастую они своевременно не обновляются. Также существуют риски, связанные с использованием одного устройства членами семьи сотрудника.

Кроме того, зафиксирован рост «традиционных» угроз: возросшие нагрузки на канал связи, что в некоторых случаях может привести к прерыванию услуг оператора, а также участившиеся случаи DDoS-атак. В связи ростом числа устройств Интернета вещей – возрастают риски эксплуатации уязвимостей этих устройств, создание из них ботнетов – и, как следствие, использование инфраструктуры оператора в ботнетах. Применительно к РТРС это могут быть зараженные смарт-телевизоры абонентов. Возросло количество программ-вымогателей, поскольку это направление киберпреступности в текущее время активно развивается: на смену одиночкам пришли организованные киберпреступники, которые сдают за определенный процент в аренду свои программы-вымогатели всем желающим. Это – тема отдельного большого доклада и сейчас останавливаться на этом не будем. И, конечно, утечки данных. Поэтому сейчас ценятся абсолютно любые данные: всему найдется применение. Не обязательно утечка пойдет непосредственно из организации: может произойти атака из смежных сетей, либо данные «утекут» через подрядчика. Так как РТРС является объектом КИИ, мы в полной мере озабочены вопросами обеспечения безопасности и бесперебойности работы нашей инфраструктуры

Обеспечение безопасности критической инфраструктуры на территории РФ берёт своё начало в 2012 г. с принятием Федерального закона № 256 «О безопасности объектов топливно-энергетического комплекса», далее в 2014 году





появляется Приказ ФСТЭК России № 31 об обеспечении защиты в АСУ ТП на критически важных объектах. Ещё 3 года назад, когда речь шла о безопасности критически важных объектах, на ум приходили только выше сказанные документы. С 1 января 2018 года вступил в силу 187 ФЗ о безопасности КИИ, вводящий понятие критической инфраструктуры.

Если рассматривать эту проблему в международном аспекте, то основоположником в обеспечении информационной безопасности в области защиты ключевых объектов инфраструктуры берут начало с формирования в США Президентской комиссии по защите критической инфраструктуры в 1996 году. Затем был разработан Национальный план защиты информационных систем США, подписанный президентом в 2000 году.

Основные задачи в области кибербезопасности США заключаются в том, чтобы “предотвратить кибернетические нападения на критическую инфраструктуру, снизить уязвимость нации к таким нападениям и минимизировать ущерб и время восстановления”. Существует международная практика решения задач стандартизации решений информационной безопасности для объектов КИИ. Например, текущая версия стандарта информационной безопасности промышленных систем управления NIST SP “Guide to Industrial Control Systems (ICS) Security”, которая включает в себя лучшие практики и принципы управления рисками для организаций, независимо от их статуса или размера. Данный, документ позволяет собрать требования и рекомендации международных стандартов в одно целое.

Общеевропейские решения по безопасности КИИ.

Что касается европейских решений в области КИИ, то страны Западной Европы были первыми, кто начал заниматься проблематикой идентификации и защиты критической инфраструктуры. В 1999 г. в Великобритании был открыт Координационный центр по безопасности национальной инфраструктуры (National Infrastructure Security Coordination Centre). Так, основным документом в 2005 году, был принят «Зеленая книга о Европейской программе по защите критической инфраструктуры» (EPCIP).

Национальные решения европейских стран по безопасности КИИ.

Помимо Великобритании и другими странами ЕС, такими как: Германия, Франция, Нидерланды, Финляндия, Чехия, Венгрия и др., разработаны и внедрены свои стандарты в обеспечении информационной безопасности критической инфраструктуры.

Для многих, информационная безопасность – это что-то непонятное, поэтому мы стараемся действовать «прозрачно», а именно:

Повышение киберграмотности пользователей (Security Awareness): когда специалисты SOC видят подозрительный трафик с ПК удаленного пользователя – они связываются с ним, объясняют правила кибергигиены и совместно находят и устраняют ВПО. Это сложно, но формирует положительный имидж службы ИБ!

Выявление подозрительной активности и фишинговых писем – в случае, если устройство корпоративное – выявляем и очищаем его от фишинга и ВПО с минимальным отрывом пользователя от его основной работы.

Выполнение и соблюдение требований регуляторов в области обеспечения информационной безопасности.

Но несмотря даже на эти сложности, информационная безопасность должна адаптироваться и помочь бизнесу. Как же происходит эта адаптация? Мы не запрещаем все подряд – а изучаем бизнес-процессы предприятия. Анализируем их – и ищем способы минимизировать риски, ограничивая что-то только там, где это действительно необходимо. Мы адаптируемся к новым вызовам – и оптимизируем свои внутренние процессы. Мы делаем упор на мониторинг и предотвращение инцидентов – еще до того, как они произошли – за счет развития как компетенций сотрудников, так и своего SOC, внедряя процессы трейт хантинга – «охоты на угрозы», когда детально рассматривается подозрительная активность внутри предприятия и используя киберразведку. Помимо этого, постоянно совершенствуем локальную техническую и нормативную базу ИБ, адаптируясь к новым вызовам. И, разумеется, внедряем новые средства защиты и повышаем киберграмотность сотрудников, поскольку основной вектор атаки сейчас все же социальный – направленный на человека. И, конечно, везде стараемся соблюсти баланс между удобством и безопасностью. ИБ должна быть прозрачна для большинства сотрудников предприятия.

Как уже отмечал выше, телекоммуникационные, радиовещательные и медиакомпании в большинстве стран мира являются объектами критической инфраструктуры. Это – важная для государства структура как в сфере информационного воздействия и массовых коммуникаций, так и средств связи и оповещения. Поэтому эти компании в зоне риска: на них будут направлены как политически ангажированные группы, так и отдельные хактивисты, недовольные политикой какой-либо страны или публичными высказываниями конкретного человека, либо желающие несанкционированно донести свою противозаконную или антиконституционную информацию до населения. Поэтому, среди основных и значимых компаний, задействованных в этой отрасли, должен на постоянной основе идти информационный обмен (во благо всех и в интересах каждого), невзирая на политические и иные барьеры. Этого, частично, можно достичь за счет как неформального обмена, так и создания профессионального сообщества пользователей – участников групп реагирования на инциденты (CERT/CSIRT) и центров мониторинга и реагирования на инциденты информационной безопасности (SOC), где уже разработаны основные критерии и стандарты по линии ИБ.

В заключении хотелось бы отметить, что будущее, связанное с построением Общества 5.0 призвано создать новые институты, право, образование, медицину, быт, межчеловеческие отношения, соответствующие наступающей новой технологической реальности. Но цифровая трансформация порождает серьезные социальные и гуманитарные проблемы, прежде всего занятости значительных контингентов рабочей силы и образа жизни в обществе и его культурных ценностей. Поэтому нельзя ограничиваться узкой трактовкой складывающейся ситуации в одних лишь цифровых технократических терминах. Обеспечение цифрового суверенитета становится одним из самых актуальных вызовов. В данном аспекте безопасность КИИ, с точки зрения определения согласованных международных подходов их обеспечения, непростой, но необходимый шаг в этом направлении.

СЕМИНАР–КРУГЛЫЙ СТОЛ № 5

ПРАВОВЫЕ МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИКТ-СРЕДЫ ДЛЯ ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ, ВКЛЮЧАЯ ГУМАНИТАРНОЕ ИЗМЕРЕНИЕ

Модераторы:

Смирнов А. И., Генеральный директор НАМИБ;

Куракин М. Б., заместитель Главного редактора журнала «Международная жизнь» МИД РФ

А.И. Смирнов
Генеральный директор НАМИБ,
профессор МГИМО МИД России

Уважаемые коллеги!

Позвольте мне, как сомодератору данного круглого стола «Правовые механизмы противодействия использованию ИКТ-среды для вмешательства во внутренние дела суверенных государств, включая гуманитарное измерение», выступить первым. Тема моей презентации – «Гуманитарное измерение безопасности глобальной цифровизации как фазового перехода человечества».

Развитие шестого технологического уклада (на Западе известен как Industry IV) с нано, био-, инфо- и когнотехнологиями резко ускорило процессы цифровизации. Некоторые эксперты рассматривают глобальную цифровизацию как фазовый переход человечества, сопоставляя её, например, с переходом от аграрной к индустриальной фазе цивилизации.

Беспрецедентная революция в области ИКТ, произошедшая за последние 30 лет, наряду с прорывом в цифровизации и социализации человечества, породила принципиально новые угрозы для международной безопасности. Проблема инфогенного нарратива угроз нашла свое отражение в целом ряде решений ООН и других международных организаций. Анализ документов НАТО показывает, что их киберполитика становится все более агрессивной в контексте гибридных войн.

Для обеспечения глобального информационного доминирования НАТО используют широкий набор киберинструментария от информационно-технотронных войн (сетецентрические, информационно-алгоритмические, хакерские войны и др.) до гражданских сетевых и поведенческих войн, особенно актуальных в ходе так называемых цветных революций.

В речи при открытии Форума Президент Ассоциации Владислав Шерстюк отметил, что одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере. При этом, наряду с угрозами использования ИКТ в военно-политической сфере, киберпреступностью и терроризмом («цифровой джихад»), в последнее время резко обострилась проблема использования ИКТ-среды для вмешательства во внутренние дела суверенных государств.

Проблема правомерности, или справедливости, обращения к информационному вмешательству во внутренние дела других государств крайне актуальна ввиду того, что применение такого воздействия находится в настоящее время на острие гибридных и высокотехнологичных войн, ведущихся США и их сателлитами против России и её союзников.

С точки зрения международного права государства могут предпринимать меры в ответ на акты информационного вмешательства, достигающие уровня вооруженного нападения, в соответствии со статьей 51 Устава ООН и согласно их неотъемлемому праву на самооборону. При этом государства также могут адекватно отвечать на акты информационного вмешательства, не достигающие уровня вооруженного нападения, но являющиеся составной частью действий, имеющих тенденцию к перерастанию в вооруженное нападение. Имеются в виду случаи, когда самооборона является последним доступным средством из совокупности имеющихся у государства возможностей по отражению нападения, а информационное вмешательство является составной частью уже необратимых действий близкого по времени и неизбежного нападения[1].

1 См. https://www.imemo.ru/files/File/magazines/puty_miru/2019/02/08-Korostelyov.pdf

Таким образом, единственное актуальное договорное ограничение информационного вмешательства состоит в том, что его последствия не должны достигать уровня последствий применения таких средств и способов ведения войны, которые составляют угрозу миру и в этом качестве становятся предметом рассмотрения СБ ООН.

Неопределенность трактовки данного вопроса проистекает из процесса постоянного развития обычного права и возникновения новых норм, регулирующих ведение боевых действий, а также фиктивности международного права, регулирующего угрозы ИКТ-среды. Основным политическим детерминантом формирования характера таких норм видится усиливающаяся асимметричность вооруженного и невоенного противостояния, то есть рост роли «слабых» в военном отношении государств, которые будут стремиться к балансу в международных отношениях, в том числе с использованием ИКТ и методов информационного вмешательства. Существующий в настоящее время раскол мирового сообщества по данному вопросу в ООН не способствует его решению, ибо когда отсутствует сила права, работает право силы.

Особая ответственность за международную информационную безопасность (МИБ) лежит на ключевых игроках в сфере ИКТ. В этой связи очень важное значение имеет обращение президента В.Путина к США с предложением одобрить комплексную программу практических мер по перезагрузке наших отношений в сфере ИКТ[2].

Напомню их суть.

Первое. Восстановить полномасштабный двусторонний регулярный межведомственный диалог по ключевым вопросам обеспечения МИБ на высоком уровне.

Второе. Поддерживать непрерывную и эффективную работу каналов связи между компетентными ведомствами наших стран по линии центров по уменьшению ядерной опасности, групп оперативного реагирования на компьютерные инциденты и должностных лиц высокого уровня, курирующих проблематику МИБ в рамках структур, связанных с вопросами обеспечения национальной, в том числе информационной, безопасности.

Третье. Совместно разработать и заключить двустороннее межправительственное соглашение о предотвращении инцидентов в информационном пространстве по аналогии с действующим советско-американским Соглашением о предотвращении инцидентов в открытом море и воздушном пространстве над ним от 25 мая 1972 года.

Четвёртое. Во взаимоприемлемой форме обменяться гарантиями невмешательства во внутренние дела друг друга, включая избирательные процессы, в том числе с использованием ИКТ и высокотехнологичных методов.

И наконец, последнее. Владимир Путин призвал США дать ход российско-американскому профессиональному экспертному диалогу по вопросам МИБ, не делая его заложником политических разногласий и обратился ко всем странам, включая США, выйти на заключение глобальной договорённости о принятии политического обязательства государствами о ненанесении первыми удара с использованием ИКТ друг против друга.

В ходе участия в итоговой пленарной сессии XVII ежегодного заседания Международного дискуссионного клуба «Валдай» 22 октября 2020 г. Владимир Путин напомнил об инициативе по восстановлению доверия в киберпространстве.

Однако через несколько дней власти США негативно отреагировали на это предложение. Помощник генерального прокурора США по национальной безопасности Джон Демерс назвал нашу инициативу «не более чем лживой риторикой, циничной и дешевой пропагандой». А госсекретарь Майк Помпео безапелляционно заявил, что Россия пренебрежительно относится к общественной безопасности и международной стабильности в киберпространстве.

Одновременно НАТО и ЕС резко усилили информационное воздействие на Россию и её союзников, как составляющую гибридной войны. Наиболее известные по своей русофобской направленности – это центры передового опыта НАТО: Таллинский центр кибероборонны (CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), Рижский центр по стратегическим коммуникациям (NATO Strategic Communications Centre of Excellence), Евро-

2 http://www.kremlin.ru/events/president/news/64086

пейский центр противодействия гибридным угрозам (в Хельсинки ЕС совместно с НАТО) (European Centre of Excellence for Countering Hybrid Threats), Рабочая группа ЕС по стратегическим коммуникациям (EU vs disinfo).

Феноменальный парадокс заключается в том, что данная политика сдерживания России проводится под флагом борьбы якобы с российской дезинформацией.

В этом контексте следует подчеркнуть, что 29 октября 2020 г. НАМИБ был проведен семинар по результатам исследования «Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды». Один из выводов, что ИКТ-среда – юридическая фикция, заключающаяся в том, что ИКТ-среде приписывают свойства традиционной территории государства и распространяют на нее государственный суверенитет.

В ходе видеоконференции с комиссией ПА ОДКБ глава комиссии Госдумы России по расследованию фактов иностранного вмешательства во внутренние дела Василий Пискарев заявил 16 октября 2020 г. о схожести технологий, примененных для организации протестов в прошлом году в Москве, в Гонконге и в 2020 году в городах Белоруссии[3].

Среди этих технологий координация действий через соцсети и мессенджеры, скоординированная информационная поддержка одних и тех же иностранных СМИ, трансформация митингов в шествия, перекрытие дорог, низкий средний возраст протестующих и геймификация протеста, фейковые вбросы, постановочные фото и видеофейки. При этом данные информационные атаки совпадали с активными фазами проведения несогласованных акций.

В поле зрения комиссии Госдумы России находится более 10 активно действующих против России зарубежных центров подготовки на базе нежелательных в России НПО и свыше 40 их выпускников.

Как категорический императив прозвучал 26 ноября 2020 г. на заседании коллегий министерств иностранных дел России и Белоруссии в выступлении Сергея Лаврова призыв к поиску договоренностей: «В нашей повестке дня стоит вопрос международной информационной безопасности. <…> Очевидно, что без универсальных договоренностей мир рискует погрузиться в киберхаос, последствия которого могут оказаться катастрофическими»[4].

Спасибо за внимание!

3 https://tass.ru/politika/9737855

4 https://ria.ru/20201126/kiberkhaos-1586438194.html

М.Б. Алборова
К.и.н., доцент, ведущий эксперт Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России

ПОКОЛЕНИЕ Z В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: ВЫЗОВЫ И РИСКИ ЦИФРОВОГО ОБЩЕСТВА[1]

Аннотация

Статья посвящена анализу влияния информационного общества на формирование нового поколения. Рассматриваются основные факторы, которые способствуют изменению уровня восприятия информации современной молодежью. В этой связи актуализируется проблематика выявления рисков коммуникативно-информационного влияния на общество.

Ключевые слова: информационное общество, научно-техническая революция, глобальное информационное пространство, поколение Z, культура виртуальной реальности.

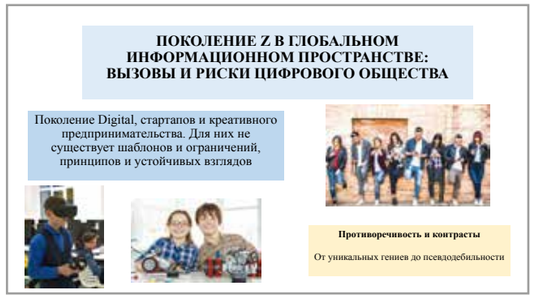
Научно-техническая революция неразрывно связала жизнедеятельность социума с глобальными информационными потоками. С каждым днем все большее число людей становятся пользователями современных информационно-коммуникационных систем, позволяющих получить мгновенный доступ к огромным массивам информации, все стороны общественной деятельности постоянно втягиваются в единую цифровую систему[2]. Человечество попадает в зону информационно-психологического пространства, которое оказывает комплексное влияние на формирование и развитие людей. В этих условиях наибольшее беспокойство вызывают попытки манипуляций сознанием той части общества, которая менее всего расположена к критическому и аналитическому восприятию поступающей из Сети информации. Современное юное поколение уже не мыслит себя без мессенджеров и гаджетов, а зависимость от них становится не только очевидной, но иногда и требующей серьезной медико-психологической помощи.

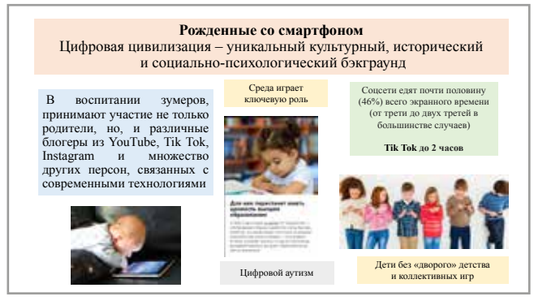
Научное сообщество неоднократно обращалось к вопросу анализа влияния глобальных мессенджеров и социальных сетей на сознание общества. Еще в начале XXI века сформировались основы для «культуры виртуальной реальности» и цифрового мира. Особенности данной культуры заключаются в полном погружении сознания в это новое информационное пространство, где зачастую создается иллюзия подмены реальности. Именно через этот мир изменяются человеческие ценности и социально-экономические и политические реалии. В этих условиях развивается мировоззрение поколения Z и оттого каким контентом будет наполнено информационное пространство во многом зависит формирование ценностных ориентиров и приоритетов молодежи.

На современном этапе выросло целое новое поколение в буквальном смысле с планшетом в руках, их родители часто использовали современные гаджеты в качестве бебиситтеров, постоянное нахождение в руках у молодых людей тех или иных мобильных средств сегодня стало повседневным и естественным явлением. Юное поколение XXI века увеличило свое экранное время с 6–7 часов до 10–12 часов в сутки. А пандемия 2020 посадившая большинство населения по своим

1 Исследование выполнено при финансовой поддержке РФФИ и ЭИСИ в рамках научного проекта № 20-011-31493. The reported study and funded by RFBR and EISR according to the research № 20-011-31493.

2 Бирюков А.В. Международные научно-технологические отношения в цифровую эпоху. М.: Аспект Пресс, 2020. – 224 с.





квартирам и усилила процесс вовлечения юного поколения в социальные сети.

Сегодня все больше пользователей выходят в соцсети с мобильных телефонов: по состоянию на январь 2019 в мире примерно 3,2 мил. человек являются постоянными участниками социальных сетей, эта цифра ежегодно растет, при этом привычка постоянно находиться в онлайн стала абсолютной нормой жизни.

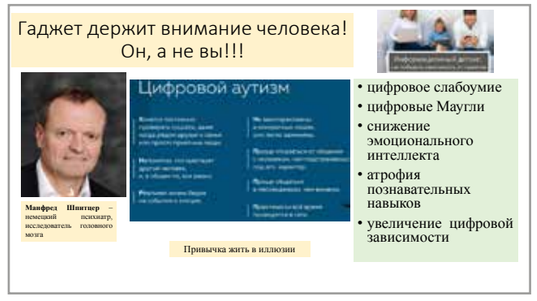
В условиях информационного общества распространение, использование и обработка информации представляет собой значительную часть жизни и деятельности людей[3]. К сожалению, при всех возможностях информационного пространства, позволяющего активно развиваться и много изучать, большинство времени тратится на развлекающий контент. При этом концентрация внимания на образовательном материале постоянно снижается и на момент 2020 года составляет не более чем 8–10 минут. Юное поколение Z явные визуалы, для них зрительный контент – это основа восприятия материала.

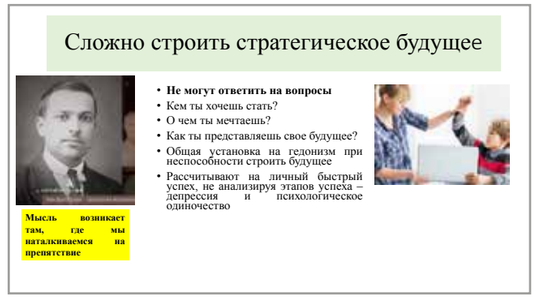
По меткому выражению Андрея Курпатова, «мы живем в уникальный период перехода от цивилизации Гуттенберга к цивилизации Цукенберга», именно в рамках цифровой цивилизации мы переходим от мира текстов и представлений к миру зрительных образов. Это приводит к активному развитию клипового мышления современной молодежи. Им крайне трудно воспринимать материал, если у него нет яркой и двигающейся картинки. При этом лидерами, ориентирующими в жизненном пространстве основную часть молодежи, становятся инфлюенсеры и блогеры, на мнение которых ориентируется большинство.

Интересно отметить, что точка зрения инфлюенсеров стала настолько значима, что это отразилось и на политических мнениях и даже ценах на акции. Именно они стали агентами влияния, руками своей огромной армии подписчиков. Они влияют на выборы, на мнение электората, на цены финансовых активов и так далее. Цивилизация постиндустрии построена на мнениях и знаниях, на прохождении информации, когда финансовые рынки, как и рынки услуг зависят от мнения человека, блогеры стали играть уникальную роль диктатора этих мнений.

Сегодня капиталом инфлюенсеров становятся фанаты и подписчики, объединённые в социальные сообщества. Компании стали эффективно использовать этот ресурс, ведь качественно подобранный и играющий на интересы компании блогер предоставляет доступ к сознанию огромной целевой аудитории, а это значительно может увеличить спрос, главное, чтобы в социальную группу входили лояльные и вовлеченные люди и тогда вирус-

3 Бирюков А.В. Международные научно-технологические отношения в цифровую эпоху. М.: Аспект Пресс, 2020. – 224 с.





ное распространение информации не заставит себя ждать.

Интересно отметить и позитивный результат социальных сетей. Так, например, постоянная демонстрация в глобальных сетях здорового образа жизни стала одним из факторов увеличения численности молодых людей, ведущих спортивный образ жизни, новое цифровое поколение меньше ходит по ночным клубам, больше сидит дома, у них больше безопасности в этом смысле, они меньше пьют алкоголь и менее склонны к авантюризму, домашний уют для них важнее. При этом они больше подвержены депрессии и суицидам, и в целом менее счастливы. Часто они не готовы жить самостоятельно и требуют сопровождения в жизни. Снизился и порог живого общения со сверстниками как дружеский, так и романтический.

Влияние цифрового мира на здоровье и развитие человека очевидно, множество исследований проведено по этому поводу. Важно отметить, и еще один аспект, специфика работы человеческого мозга ориентирована на столкновение с трудностями и решение их, при этом новый технологичный мир очень часто даёт готовые решения и это приводит к тому, что потребность в сложной работе человеческого мозга снижается. У молодых людей поколения Z часто отсутствует критическое мышление и потребность к глубокому изучению информации.

Развитие глобального информационного пространства привело к тому, что информационная лавина, накрывшая человечество оказывает все более массивное влияние на каждого из нас. 2015 год стал своеобразным рубежом: в мире в течение года было произведено столько же информации, сколько за всю историю существования письменности[4]. Современное информационное пространство ежедневно обрушивает на человека лавину информации, что приводит к постепенному формированию «гипертекстового мышления» – формы параллельной переработки информации вместо последовательной. У юного поколения Z активно развивается пространственное мышление и когнитивные карты, расширяется распределение внимания, все больше проявляется способность к индуктивному мышлению, при этом доверие к чужому мнению беспрецедентно.

Цифровой век многозадачен, это породило новое явление – феномен «мультитаскинга», который все больше изучается экспертами всего мира. К сожалению, даже высокий уровень многозадачности приводит к резкому снижению качества проработки и переработки информации при этом нагрузка на нервную систему увеличивается, а итоговое количество

4 Ларина Елена, Овчинский Владимир. Чёрный шар и глобальная инквизиция Ника Бострома. // Наш современник. 2019. Февраль. – URL: https://reading-hall.ru/publication.php?id=24905 (дата обращения: 15.01.2021)

полноценно законченных задач сокращается. Человек стремится все успеть, при этом мало, что доводится до качественного результата, растёт количество обещанных и незавершенных дел, а вместе с этим и депрессивность и неуспешность в глазах окружающих.

Интересно отметить, что у активных молодых мультитаскеров – людей, которые сидят перед двумя компьютерами, на одном работают, при этом на соседнем экране идет фильм, сбоку следят за бегущей строкой котировок и при этом отвечают на сообщения в социальных сетях, объем серого вещества в зоне мозга, отвечающей за когнитивный и эмоциональный контроль резко снижен. Чаще всего мультитаскеры мало эмоциональны, на это просто нет времени, отсюда и снижение возможности к эмоциональной привязанности и социальной ответственности. Падает и уровень эмоционального интеллекта.

Подводя итоги, хотелось бы отметить, что новое поколение Z несомненно имеет большие возможности для своего развития. Глобальное информационное пространство представляет широкий спектр для прогресса человечества, но вместе с тем несет и значительные риски. Своевременный анализ возможных угроз позволит минимизировать негативные факторы информационного воздействия на человека.

Значительную роль регулятора в этом вопросе может и должно играть государство и гражданское общество, от качественной работы которого зависит создание здоровой социальной среды для современного человека, а также обеспечение решения вопросов безопасности в информационной среде.

Бай Яцзе
Аспирантка МГИМО МИД России

КИБЕРПОЛИТИКА ЗАПАДА ПО ВМЕШАТЕЛЬСТВУ ВО ВНУТРЕННИЕ ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ (НА ПРИМЕРЕ ГОНКОНГА)

С развитием процесса цивилизационного человечества, современные угрозы все время меняются и возрастают, становятся все более разнообразными и гибридными. При этом против гибридных угроз для оказания на противника концентрированного давления используются не только военные силы, а в большей степени – политико-дипломатические, экономические и информационные средства. Среди данных средств все более важную роль играют информационно-коммуникационные технологии (ИКТ).

Революция в области ИКТ породила принципиально новые угрозы для международной безопасности. Проблема инфогенного нарратива угроз нашла свое отражение в целом ряде решений ООН и других международных организаций. Анализ документов НАТО показывает, что киберполитика альянса становится все более агрессивной в контексте гибридной войны.

В концептуальных документах НАТО особая роль отводится наступательному использованию интернет-технологий (Internet offensive use) с проведением нетрадиционных таргетированных операций психологической войны (Unconventional psychological warfare). Речь идет о политике «постправды», фейках, «глубоких фейках» как инструменте цифровой манипуляции в информационном сопровождении боевых операций. В информационно-психологическом арсенале альянса выделяют ментальные, консциентальные войны, когнитивные и контентные войны. Кроме того, для обеспечения глобального информационного доминирования НАТО использует широкий набор киберинструментария от информационно-технотронных войн (сетецентрические, информационно-алгоритмические, хакерские войны и др.) до гражданских сетевых и поведенческих войн, особенно актуальных в ходе так называемых цветных революций.

Среди методов информационно-психологического противоборства в киберполитике НАТО все шире используются методы переформатирования массового сознания, метапрограммирования, медиавирусного заражения («феномен толпы»), когнитивных подмен.

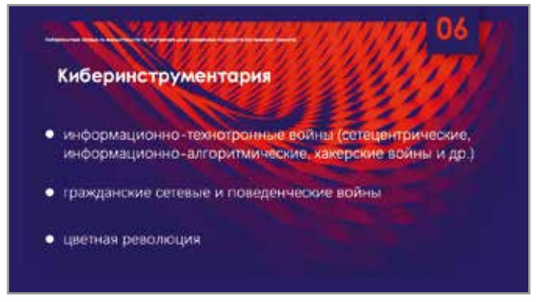
В геополитическом измерении в альянсе активно продвигаются методы воздействия на мировое общественное мнение, создание «образа врага» как угрозы цивилизованному миру, использование «подставных персонажей», манипулирование результатами социологических опросов, контроля информации, информационной блокады, информационных фильтров, безальтернативной подачи контента, контролируемых утечек информации.

Актуальность исследования подчеркнута в Стратегии национальной безопасности России (п. 12 и 21) и в документах стратегического планирования КНР. Позиции России и Китая по МИБ почти полностью совпадают и изложены в совместном заявлении руководителей стран Владимира Путина и Си Цзиньпина от 5 июня 2019 г.

Пример Гонконга

В 2019 году в Гонконге происходила серия демонстраций против законопроекта об экстрадиции. Быстрая эскалация произошла с демонстрации в широкомасштабное насилие.

Помимо частых демонстраций с применением насилия и разрушения различных районов Гонконга, участники беспорядков переносили агрессивное поведение из реальности



в киберпространство, используя «профессиональные технологии». Одни из этих технологий специально предоставленные американской неправительственной организацией (НПО) Civic Hall.

НПО Civic Hall находится в Нью-Йорке (США). Оно разрабатывает технологии информационной войны для демонстрантов и исполнителей «цветных революций» на Ближнем Востоке, в Северной Африке и других местах. Оно предоставляет разработанные технологии или полуфабрикаты для НПО в целевой области для дальнейшей «обработки» или «бесплатного использования». 10 декабря 2019 года эти участники представили НПО Civic Hall «обратную связь от клиентов», опубликованную на официальном сайте Civic Hall. В этом отчёте демонстранты описали 13 технологий и стратегий, использованных за последние шесть месяцев в мятеже в Гонконге.

1. Цифровые риски на приложении

Приложение «Телеграмм» — популярный зашифрованный чат-инструмент. Его использование в Гонконге также резко возросло по мере того, как огромные толпы людей собирались. На самом деле, протестующие группы в Телеграмм должны быть арестованы за “подстрекательство к общественному вмешательству” (“inciting public obstruction”), то есть, управление протестными группами в Телеграмм оказалось рискованным. Поэтому появился зашифрованный чат-бот BigOcean, который может выступать в роли администратора группы Телеграмм, снижая риск ареста реальных администраторов.

2. Fakenews

Fakenews – это информационные фальшивые новости, обычно появляются в социальных сетях и традиционных СМИ с целью введения в заблуждение. Авторы часто используют броские заголовки или полностью сфабрикованные истории для привлечения внимания, расширения распространения и увеличения влияния.

Fakenews были повсюду в протестах в Гонконге. Один из демонстрантов рассказал, что они в социальных сетях дискредитировали полицию Гонконга, чтобы запятнать их имидж. Группы протеста еще провели операцию под названием “кибервирус”. Они распространяют слухи о полиции Гонконга по различным онлайн-каналам, как будто это вирусы. Чтобы повысить “достоверность” слухов, они наклеивают на другую этикетку некоторую информацию, например, распространялись слухи о том, что полиция убивает протестующих и скрывает это, притворяясь самоубийцами, эти слухи подтверждались сфальсифицированными необработанными данными, а затем распространяли ее по разным каналам.

3. Использование ИКТ для вмешательства и управления распространением информации в СМИ

FreedomHKG TV – это аппаратный проект, который предлагает «сломать монополию на медиа» для глушения распространения информации в других СМИ. Его цель – позволить молодым людям захватить телевизоры своих родителей с устройствами Raspberry Pi для того, чтобы они могли получать только контент, пропагандирующий насилие и радикальное поведение.

Помимо использования ложной информации для разжигания ненависти, они также запустили множество связанных онлайн-игр для молодых людей, позволяющих им изучать насильственные методы в смоделированной среде. Все главные герои этих игр являются демонстрантами. Например, видеоигра “Liberate Hong Kong”. Его главный герой – анонимный гонконгец, который борется за то, чтобы остаться на линии фронта протеста, несмотря на то, что был застрелен, арестован и подвергнут нападению со стороны полиции.

Причина, по которой демонстранты беспорядков в Гонконге такие радикальные, жестокие и с разными технологиями. Вмешательство иностранных сил в Гонконг уже давно является “открытой тайной”. Эти раскрытые операции “информационной войны” являются лишь вершиной айсберга, используемого протестующими в ходе беспорядков в Гонконге.

И.В. Сурма
Заведующий кафедрой государственного управления во внешнеполитической деятельности Дипломатической академии МИД России, к.э.н., член-корреспондент РАЕН

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРОБЛЕМА ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ

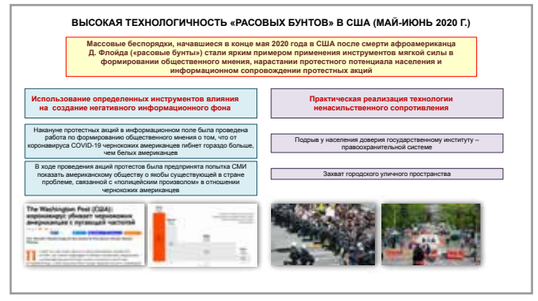
Дестабилизация общественно-политической ситуации в начале нынешнего века в ряде стран, так или иначе представляющих геополитический интерес для стран Запада и в особенности США, характеризуется определенной особенностью, а именно практической реализацией технологий «цветной революции». Приведем несколько примеров, где была использована данная технология с применением инструментов дестабилизации – в Югославии («Бульдозерная революция» – 2000 год), в Грузии («Революция роз» – 2003 год), на Украине (2004 год и «Евромайдан» – 2013–2014 годы), в Ливане («Революция кедров» – 2005 год), в Кыргызстане («Тюльпановая революция» – 2005 и 2010 годы), в Молдавии («Сиреневая революция» – 2009 год), в Египте («Революция лотоса» – 2011 год), в Тунисе («Жасминовая революция, «Финиковая революция»– 2010–2011 годы), в Ливии (2011 год), в Сирии (2014 год), как элементы «арабской весны и зимы», а также последние протесты в Белоруссии (май – август 2020 – ...).

Отметим, что в настоящее время США являются бесспорными лидерами, как в области теоретических исследований в сфере политических и геополитических технологий (Дж. Най, Д. Шарп и др.), так и в реализации технологии «цветной революции» (издается журнал Foreign Affairs для активного обсуждения новых внешнеполитических концепций и инициатив и формирования необходимого мировоззрения у общественной и научной мировой элиты; создаются неправительственные организации, выступающие под видом благотворительных и решающих на практике разведывательные и подрывные задачи в странах геополитического интереса; осуществляется экономическое и политическое давление на законное правительство стран в ходе «цветных революций» и т.п.) [1], [2].

Цель дестабилизации общественно-политической ситуации в государстве – это генерирование протестного потенциала в обществе и создание политической сингулярности, что приводит к инфляции власти в этой стране, её дискредитации и т.д. После прохождения точки политической сингулярности государство должно либо качественно измениться, либо быть уничтожено.

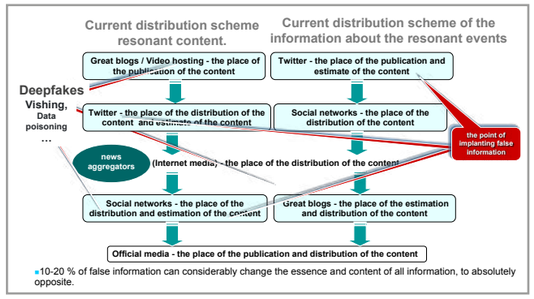
При этом используются кибератаки с высоким уровнем социального инжиниринга и применением комбинированных систем, включающих возможности искусственного интеллекта и различные роботизированные устройства (боты). Задачи, которые преследуются в этом процессе, это: информационная поддержка и непосредственное сопровождение протестных выступлений в той или иной стране; придание своеобразного имиджа протестам и возведение их в ранг «народных»; управление и манипуляция народной массой в ходе протестных акций и склонение действующей власти к принятию требований протестующих, даже если они наносят ущерб национальным интересам государства.

Механизм непосредственного информационного сопровождения протестных выступлений также достаточно хорошо отработан в настоящее время и включает в себя: создание и распространение информации о демонизации власти; активное распространение в медиапространстве выступлений и комментариев официальных представителей иностранных государств и международных организаций, артистов, звезд шоу-бизнеса и мнения «обычных» людей; сбор и рассылка материалов обосновывающих справедливость и необходимость проведения акций, а также участия в них населения; распространение информации о планируемой акции, дате, времени и месте проведения, целях, лозунгах; создание и распространение информации о «сакральной жертве» и формирование жестокого образа правоохранительных органов с одновременным оправданием участников протестных акций и т.п.



Безусловно, всему этому процессу предшествует целенаправленное идеологическое и информационное воздействие, ключевыми задачами которого являются: поощрение внутренних протестов и различного ненасильственного сопротивления с целью снижения активности страны на международной арене; ослабление веры в избирательную систему государства и формирование представления о том, что существующий в стране политический режим не преследует общественные интересы. В конечном итоге, реализуется механизм создания общего негативного информационного поля в государстве с доминированием тяжелой, деструктивной информации. Также формируется негативное общественное мнение и отрицательное отношение к институтам государства на фоне резкой активизации деятельности СМИ в критически важные моменты жизнедеятельности общества и государства в целом.

Примером может служить высокая информационно-коммуникационная технологичность протестов в Москве в июле-августе 2019 года. Причем, при организации этих протестов были использованы новые каналы коммуникаций для вовлечения большого количества людей к протестам и формированию негативного общественного мнения. Протестная активность была переведена из виртуальной плоскости в уличное противостояние, в ходе которого осуществлялась попытка радикализации протеста и практического захвата городского пространства. Подчеркнем, что в ходе протестов активно применялась тактика провокации правоохранительных органов к «жестким» (по мнению протестующих) действиям и задержаниям, а также к разгону «мирного» (по мнению протестующих) митинга. При этом в информационно-коммуникационном поле были предприняты попытки подмены смыслов с целью проведения кампании по формированию негативного образа правоохранительных органов, а именно, переложение ответственности за «жестокое» обращение с протестующими на представителей правоохранительных органов. Также осуществлялись попытки привлечения артистов и представителей шоу-бизнеса на



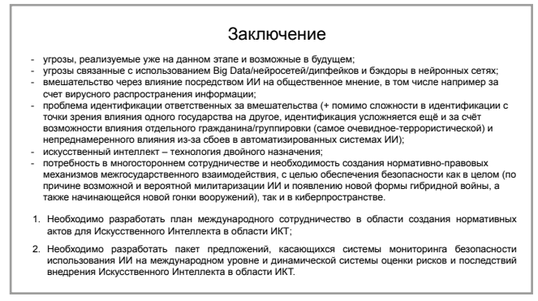
сторону протестующих для поддержания протестного настроения у населения и демонстрация того, что поддерживать действующую власть сегодня не популярно.

Такую же высокую информационно-коммуникационную технологичность эксперты отметили в «расовых бунтах» в США в мае-июне 2020 года. Массовые беспорядки в США, которые начались в конце мая 2020 года после смерти афроамериканца Д. Флойда являются достаточно ярким примером использования инструментов дестабилизации общественно-политической ситуации, включая формирование протестного потенциала населения и дальнейшее информационное сопровождение протестных акций.

Подчеркнем определенный механизм использования инструментов влияния при создании негативного информационного фона. В процессе проведения протестных акций были попытки со стороны СМИ показать американскому обществу о якобы существующей в стране проблеме «полицейского произвола» в отношении чернокожих американцев. Кроме того, накануне протестных акций была проведена работа по формированию общественного мнения о том, что чернокожих американцев от коронавируса COVID-19 гибнет гораздо больше, чем белых американцев. С практической точки зрения реализация технологий ненасильственного сопротивления осуществлялась через подрыв у населения доверия государственному институту и правоохранительной системе в целом, включая традиционный захват уличного пространства. Причем в ходе массовых выступлений в США механизм подрыва правоохранительной системы государства включал несколько этапов, начиная от «возвышения толпы над правопорядком», «ограничения полномочий полиции» и «публичного признания недееспособности правоохранительных органов представителями органов власти» и заканчивая «сложением полномочий и сдачей городского пространства» [1].

Как правило, за успешной реализацией данной технологии будет следовать реформа правоохранительной системы или как минимум изменение кадровой политики и обновление кадров, лояльных той политической элите, которая будет находиться у власти.

Отметим, что в процессе дестабилизации общественно-политической ситуации в стране используются возможности современной трансформации информационно-коммуникационного и медийного пространства в целом, с широким применением виртуальной реальности и фейковых технологий [3] как элементов «гибридного воздействия», а также новых цифровых манипуляций, например, таких как, Deep Fake Technology. Эта технология заключается в использовании искусственного интеллекта для создания и редактирования вполне реалистичных аудио- и видеозаписей различных людей. Для этого применяются возможности различных нейронных сетей, таких как реккурентные (Recurrent Neural Network, RNN), сверточные нейронные сети (Convolutional Neural Network, CNN) и генеративно-состязательные сети (Generative Adversarial Network, GAN), которые являются своего рода алгоритмом, способным создавать новые данные из существующих наборов данных (датасетов). Например, GAN может анализировать тысячи записей голоса конкретного человека, а затем на основе этого анализа создать полностью новый аудиофайл с таким же точно голосом, использующим те же самые речевые шаблоны.



Беспокойство, связанное с данной технологией, вызывает тот факт, что существует возможность ее использования для создания и распространения фейковых аудио- и видеозаписей мировых лидеров, политиков и других публичных персон. Например, Deep Fakes известного политика, который якобы выступает с расистскими лозунгами, может существенно повлиять на результаты выборов или даже спровоцировать акты насилия.

Эти технологии напрямую касаются гигантов мирового ИТ-рынка, которые пытаются по-своему бороться с существенным обилием фейковых аудио- и видео. Например, Twitter удаляет фейковый контент и ищет пути для более качественного его отслеживания, Facebook инвестировал 10 млн долларов на создание организации «DeepFake Detection Challenge», а Google собрала огромный архив DeepFake-видео для анализа.

И тут на помощь может прийти тот же самый искусственный интеллект, который великолепно справляется со сбором, анализом, сортировкой и передачей данных, улучшая скорость и качество реализации внутренних процессов. А технология блокчейн обеспечивает нормальную работу искусственного интеллекта и защищает данные и их последовательность от любых посягательств извне. Поэтому симбиоз искусственного интеллекта и технологии блокчейн является наиболее перспективным направлением.

Сегодня осуществляются исследования практически во всех областях современного искусственного интеллекта, в том числе распознавания изображений, управления знаниями, интеллектуальной визуализации и моделирования, многоагентных систем, речевых и неречевых технологий, интеллектуальных пользовательских интерфейсов и робототехники.

Искусственный интеллект (ИИ), как и все технологии Четвёртой промышленной революции, в реальной жизни реализуется в трех основных направлениях: для развития экономики, общества и укрепления безопасности граждан; для военных целей; для целей криминального характера. Сегодня более 30 стран, включая Россию разработали национальные стратегии развития искусственного интеллекта. В России, например, была создана, так называемая, экосистема развития искусственного интеллекта, неизменным ядром которой выступают Газпромнефть, Сбербанк, группа Mail.ru, Яндекс, Российский фонд прямых инвестиций, МТС и ряд компаний разработчиков.

Еще раз подчеркнем, что для современного этапа характерно очень быстрое развитие технологий искусственных нейронных сетей, имитирующих работу биологических нейронов живых существ. В этом отношении является весьма интересным проект Blue Brain, базирующийся в Швейцарии, в котором исследуется работа ансамблей нейронов. Другой проект, SyNAPSE, финансируемый DARPA и корпорацией IBM, ставит своей задачей создание физической копии человеческого мозга, воплощенной в виде специальных микросхем с искусственными нейронами. Это направление получило название нейроморфной электроники. Аналогичные проекты развивает также и Китай. Тем не менее, в настоящий момент исчерпывающее моделирование человеческого мозга невозможно в силу ограниченных возможностей современных суперкомпьютеров (для этого требуется производительность в десятки и сотни эксафлопс, то есть на 3–4 порядка больше достигнутой ныне). По данным 2020 года самым мощным является суперкомпьютер Summit (IBM, Национальная лаборатория Ок-Риджа, США) [4]. В 2018 году Summit стал первым суперкомпьютером, преодолевшим эксафлопсный барьер. Анализируя геномные данные, он достиг пиковой пропускной способности в 1,88 эксафлопс, что составляет почти 2 миллиарда миллиардов вычислений в секунду. Вторым по мощности является суперкомпьютер Sierra (IBM, Ливерморская национальная лаборатория им. Лоуренса, США), который специально предназначен для оценки эффективности систем ядерного оружия и используется для прогнозных применений в управлении запасами в американской программе испытаний надежности и технического обслуживания ядерного оружия без каких-либо ядерных испытаний. К этим двум суперкомпьютерам приблизились китайские суперкомпьютеры Sunway TaihuLight (NRCPC, Национальный суперкомпьютерный центр в Уси, Китай) и Tianhe-2A (NUDT, Национальный суперкомпьютерный центр в Гуанчжоу, Китай) [4]. Первый из них в дополнение к наукам о жизни и фармацевтическим исследованиям, используется для моделирования Вселенной с десятью триллионами цифровых частиц, а второй, в основном используется в приложениях моделирования, анализа и государственной безопасности. Причем Китай пытается достичь гораздо большего и уже официально заявил о своей цели стать лидером в области искусственного интеллекта к 2030 году.

Следует отметить, что сегодня развитие искусственного интеллекта еще не является предметом какого-либо управления, но технология развивается гораздо быстрее, чем нормативно-правовое поле и дипломатические возможности. Тем не менее, в международном поле договариваться о «правилах игры» уже необходимо сейчас. Но Европа остается относительно инертной, несмотря на расцвет общественных дебатов, при том, что Соединенные Штаты, видимо, склоняются в сторону отмены своих мультилатеральных обязательств. Тем не менее, все большее число новых участников, как государственных, так и негосударственных, заинтересованных в развитии потенциала искусственного интеллекта нуждается в выработке мультикомпонентного управления, где могли бы взаимодействовать правительства, гражданское общество и частные игроки, примерно, как это происходит в Интернете. Подчеркнем, что были выработаны относительно ценные положения для регулирования процессов применения искусственного интеллекта и Big Data

и содержатся в Европейской этической хартии использования искусственного интеллекта в судебной и правоохранительной системах, принятых Европейской Комиссией в декабре 2018 года, в итоговом заключении Конференции высокого уровня Совета Европы по вопросам развития влияния искусственного интеллекта на права человека и верховенство права в феврале 2019 года, а также в отчёте об алгоритмических инструментах оценки рисков в системе уголовного правосудия США, принятом в начале 2019 года Партнерством по искусственному интеллекту, в которое входят более 80 корпоративных разработчиков и пользователей искусственного интеллекта. Кроме того, важнейшие позиции по регулированию искусственного интеллекта закреплены в Принципах ответственного управления надёжным искусственным интеллектом, которые поддержала в мае 2019 года Организация экономического развития и сотрудничества (ОЭСР).

Сегодня можно четко определить проблемные зоны и угрозы, реализуемые уже на данном этапе и те, которые возможны в будущем [5]:

- угрозы, связанные с использованием Big Data/нейросетей/ Deep Fakes и бэкдоры в нейронных сетях;
- вмешательство через влияние посредством искусственного интеллекта на общественное мнение, в том числе, например, за счет вирусного распространения информации;
- проблема идентификации ответственных за вмешательства (помимо сложности в идентификации с точки зрения влияния одного государства на другое, идентификация усложняется ещё и за счёт возможности влияния отдельного гражданина/группировки (самое очевидное-террористической) и непреднамеренного влияния из-за сбоев в автоматизированных системах искусственного интеллекта);
- искусственный интеллект – технология двойного назначения;
- потребность в многостороннем сотрудничестве и необходимость создания нормативно-правовых механизмов межгосударственного взаимодействия, с целью обеспечения безопасности как в целом (по причине возможной и вероятной милитаризации искусственного интеллекта и появлению новой формы гибридной войны, а также начинающейся новой гонки вооружений), так и в киберпространстве.

В заключение отметим важную и ответственную роль и инициативы России на международных площадках по этим вопросам, которая предложила план международного сотрудничества в области создания нормативных актов для искусственного интеллекта в сфере информационно-коммуникационных технологий, а также выступила с инициативой разработки пакета предложений, касающихся системы мониторинга безопасности использования искусственного интеллекта на международном уровне и динамической системы оценки рисков и последствий внедрения искусственного интеллекта в области информационно-коммуникационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Ювачёв М.Ю. Инструменты «мягкой силы» в дестабилизации общественно-политической ситуации в стране. // Сборник материалов круглого стола «Современный миропорядок и его влияние на национальную безопасность Российской Федерации». – М.: ВАГШ ВС РФ, 2020. – с.572-584.

2. Нарочницкая Н. «Аналитические институты» – глаза, уши и мозг Америки // Наш современник. – М., 2004. - № 3. – с.185-194.

3. Сурма И.В. Внешнеполитические вызовы и угрозы цифровому суверенитету государства. // Сборник докладов участников XIII международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». 22-27 апреля 2019 г. Гармиш-Партенкирхен, Германия. – М.: НАМИБ, 2020. – с.136-146.

4. Источник: New-Science.ru https://new-science.ru/12-samyh-bystryh-superkompjuterov-v-mire-v-2020-godu/ (дата доступа 27.11.2020)

5. Сурма И.В. Виртуальное противоборство и кибербезопасность: внешнеполитические вызовы и угрозы. // Сборник материалов круглого стола «Современный миропорядок и его влияние на национальную безопасность Российской Федерации». – М.: ВАГШ ВС РФ, 2020. – с.481-497.

А.Н. Пекшев
директор АНО «Институт конфликтологии»

ПРИНУЖДЕНИЕ К ДОВЕРИЮ: УСПЕЕМ ДО КАТАСТРОФЫ?

Ни для кого ни секрет, что отсутствие доверия в современном мире – это правило, причем, железное. Не доверяя друг другу, политики возводят между собой и народами огромное количество геополитических, экономических, военных стен. Что касается нашей страны, исторический опыт показывает, что импульсы к успешному развитию России получает, только когда находится в конфронтации и конфликте с западными странами. Но ситуация складывается гораздо серьезнее…

Тонкий механизм настройки доверительных отношений в политике в большинстве случаев остается за пределами научной дипломатии: нет единого, однозначного понимания феномена доверия. Например, в английском языке для обозначения понятия «доверие» используется несколько слов: confidence, faith, trust.

Доверие связано с ожиданиями, убеждениями, волеизъявлением или установкой; оно проявляется по отношению к разным объектам – политическим элитам, группам, организациям, социальным институтам; доверие имеет деятельностный характер, именно действия партнера рассматриваются как способы проявления доверия.

Как конфликтолог отмечу, что толкование доверия включает *рискованность* ситуации принятия решения. Не каждый готов взять на себя ответственность за действия партнера: Иисус Христос доверял человеку, а поздний Карл Маркс – нет.

Есть две составляющие доверия – *рациональная* и *эмоциональная*. К рациональной относится уверенность в том, что партнер способен выполнить взятые на себя обязательства с учетом его:

1. предсказуемости;
2. компетентности;
3. результативности.

Эмоциональная – оценка «доброй воли» партнера, анализ общности ценностей и мотивов – доброжелательности, открытости для успешного решения проблем, мотивированности на достижение общей цели, порядочности.

Однако вспомним слова лорда Пальмерстона: «Therefore I say that it is a narrow policy to suppose that this country or that is to be marked out as the eternal ally or the perpetual enemy of England. We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow».

Собственно, эксперты Института конфликтологии на мастер-классах утверждают, что для успешной реализации переговорного процесса лучше сразу принять за аксиому: **«Никакого доверия нет в принципе, оно – величина сугубо статистическая».** А мастерство вызывать **неосознанное доверие** в дипломатической и экспертной сферах – сегодня как никогда актуально и именно этому стоит учиться.

Можно порассуждать и о так называемом «**вынужденном доверии**». В США концепция приоритета безопасности по отношению к ограничениям основных прав человека сохраняется с 2001 года, с момента террористической атаки на Всемирный торговый центр в Нью-Йорке, за 20 лет в стране не произошло никаких серьезных терактов.

Американцам объяснили, что в условиях нарастающих террористических угроз основные полномочия спецслужб по ведению скрытого наблюдения за общением граждан с помощью телекоммуникационных технологий жизненно необходимы, чему подтверждение вынужденное принятие сначала Патриотического акта, а затем Акта о свободе, где заново переосмысливается баланс свободы и безопасности в пользу безопасности.

Руководитель ФСБ РФ Бортников в июне 2020 года отмечал, что в России за 10 лет было предотвращено около 700 терактов. К сожалению, российская статистика не показывает, сколько терактов готовили участники организованных инженерных групп (групп ученых). Про США есть информация из открытых источников, что доля таких групп за 10 лет выросла с 5 до 11%.

Наиболее опасен технологический терроризм, заключающийся в применении ядерного, химического или бактериологического оружия, радиоактивных и высокотоксичных веществ и т. п., а также в угрозе захвата ядерных и иных промышленных объектов.

Специалисты по контртеррористической деятельности из разных стран утверждают, что образованные экстремисты более опасны, доля террористов-выходцев из среднего класса неуклонно возрастает, они, как правило, наносят больший урон.

Один из наиболее опасных видов терроризма – кибертерроризм, это информационная атака на компьютерную информацию, вычислительные системы, аппаратное обеспечение, непосредственно на оператора.

Пожалуй, самое уязвимое звено – это оператор. По оценкам психиатров, примерно 1/6 часть из них может быть с успехом подвержена деструктивному воздействию. Согласно европейским исследованиям, наиболее уязвимы системы «умный дом, умный город, смарт-город, умная дорога, видеонаблюдение с системой распознавания лиц». В 2018 году независимая экспертиза выявила у трех лидеров западного рынка – поставщиков программного обеспечения для умных городов – **от 3 до 7 уязвимостей, позволяющих в некоторых случаях перехватить управление системой,** внести изменения в нейросеть, управляющую городом.

Свежий пример разгильдяйства и коррупции из России: в конце 2020 года произошла утечка персональных данных более 300000 москвичей, которые болели ковидом: ФИО, телефон, адрес регистрации и проживания, особенности течения болезни, сведения о сданных анализах. Также злоумышленники получили доступ к образовательным счетам московских школьников. Абсолютно не соблюдался и более серьезный протокол безопасности: порталы Правительства Москвы почему-то использовали европейские сервера для хранения информации и получения QR-кодов для передвижения в период пандемии по городу, в результате данные сотрудников российских спецслужб стали доступны иностранным «партнерам». И сегодня персональные данные из электронных медицинских карт москвичей можно свободно купить в Даркнете.

И ещё. Я называю это «**искушением 30 млн долларов**» – это примерно такая сумма, на которую можно приобрести профессиональное оборудование, технологии, программное обеспечение, обеспечить безопасность и *стирание (корректировку) этических* норм для членов инженерной команды, которые могут быть привлечены для осуществления террористических атак.

Известно, что в 80-х годах прошлого века в рамках секретных учений ФБР, инженеры-выпускники технологического университета в Бруклине, используя компоненты, находящиеся в свободной продаже, смогли собрать «грязную» атомную бомбу. Прошло почти 40 лет, и военные эксперты отмечают, что идея создания частного ядерного оружия близка к реализации. Создать и «апробировать» химическое, биологическое, бактериологическое оружие стало значительно проще.

Существуют 2 математические модели неизбежной мировой катастрофы, где может погибнуть до 25% населения земли: согласно первой - до 2026 года человечество неизбежно вытащит черный шар в соответствии с «Концепцией чёрных шаров в уязвимом мире» Ника Бострома.

Процитирую, **«чёрный шар – это технология, которая сама по себе, в рамках саморазвития, незаметно, вследствие усилий различных не связанных между собой групп и команд, преследующих свои собственные интересы, способна до основания или в основном разрушить цивилизацию».** Ник Бостром относит к черным шарам, не только машины и физические устройства, а также программные продукты, программно-аппаратные решения, идеологии, психопрактики, организационные методы.

По другой математической модели, процесс пойдет еще быстрее в связи со взрывным развитием технологий AI: до 2025 года велика вероятность катастрофического события, связанного с терактом, организованным инженерной группой (группой ученых), и вызванного им последующего, распространяющегося по миру, веера технологических отказов и аварий.

Теперь об экспертизе в эпоху недоверия. Согласитесь, доверие – самый трудно продаваемый товар в высококонкурентном и враждебном мире, где осторожность и осмотрительность невозможны в принципе. Есть путь – *подождать неизбежной катастрофы* и тогда произойдет своеобразное **принуждение к доверию.**

Лучшие умы, эксперты, прежде всего из России и континентальной Европы, которые предупреждали об опасностях технологического прогресса и ратовали за его ограничение и даже торможение, призывали к доверию между государствами во имя выживания человеческой цивилизации, наконец будут услышаны правящими элитами, но сотни тысяч погибших будет уже невозможно вернуть.

Да, сегодняшний тренд – это социальная апатия, неверие, что можно что-либо изменить в мире, но, вспомните: в нашем недалеком прошлом советским людям было как-то неприлично не думать о стране, о ее будущем, о будущем цивилизации…

Ганди говорил: «**станьте сами проводником тех перемен, которые вы хотите видеть в этом мире**», ведь угрозы цивилизации носят глобальный характер, и, пожалуй, второй выход для экспертов – принять участие в создании и работе эффективных глобальных *наднациональных* институтов противодействия.

Именно в этом направлении стоит двигаться и искать единомышленников в тех структурах, которые, даже вопреки национальным законодательствам, имеют возможности мониторить и ***пресекать*** **научно-исследовательскую деятельность и разработки, угрожающие стабильности человечества в целом.** Имеющий уши да услышит…

Е.С. Зиновьева

Доктор политических наук, заместитель директора центра международной информационной безопасности и научно-технологической политики, профессор кафедры мировых политических процессов МГИМО МИД России

АКТУАЛЬНЫЕ ТЕНДЕНЦИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА ГОСУДАРСТВ

На современном этапе в политической науке появляется новая научная категория – «цифровой суверенитет», обусловленная стремительным развитием информационно-коммуникационных технологий и их проникновением во все сферы жизни общества и государства, а также актуализацией вызовов и угроз международной информационной безопасности террористического, криминального и военно-политического характера. Под цифровым суверенитетом понимается верховенство и независимость государственной власти при формировании и реализации информационной политики. Верховенство реализуется в национальном сегменте, а независимость – в глобальном информационном пространстве. Согласно авторскому подходу к данной проблеме, цифровой суверенитет можно определить как полноту государственной власти и контроль над информационными потоками и информационной инфраструктурой внутри своих границ и независимость государства в своей информационной политике на международной арене.

Проблема обеспечения цифрового суверенитета становится одной из важнейшей в государственной политике современных стран, в том числе Российской Федерации. Необходимость обеспечения суверенитета в цифровом пространстве зафиксировано и в основополагающих документах стратегического планирования России в области информационной безопасности. Согласно официальному подходу Российской Федерации, зафиксированному в первой Доктрине информационной безопасности от 2000 года, «под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Данное определение было дополнено в актуальном тексте Доктрины информационной безопасности Российской Федерации от 2016 года, согласно которой «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 целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Таким образом, оба документа исходят из того, что обеспечение информационной безопасности страны опирается на уважение цифрового суверенитета, то есть независимости страны в информационном пространстве, как внутриполитической, так и внешнеполитической. Показательно, что 1 ноября 2019 года в Российской Федерации были приняты поправки в Закон о связи и информации, получившие в СМИ название «закона о суверенном рунете», которые направлены на обеспечение информационной безопасности страны и независимости.

Актуальные тенденции международного сотрудничества в области информационной безопасности и проблема обеспечения цифрового суверенитета государств

Зиновьева Елена Сергеевна, д.полит.н., заместитель директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России

Цифровой суверенитет

- верховенство и независимость государственной власти при формировании и реализации информационной политики. Верховенство реализуется в национальном сегменте, а независимость – в глобальном информационном пространстве

Информационная безопасность

- Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства
  - Доктрина информационной безопасности РФ 2000 г.
- 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 целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства
  - Доктрина информационной безопасности Российской Федерации 2016 г.

Основные направления внешней политики России в области международного сотрудничества по обеспечению информационной безопасности

- Выработка правил ответственного поведения государств в глобальном информационном пространстве.
- Продвижение проекта концепции конвенции ООН «Об обеспечении международной информационной безопасности».
- Продвижение проекта универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности.
- Продвижение концепции конвенции ООН (или концепции безопасного функционирования и развития сети Интернет).

Различными странами международного сообщества накоплен достаточно большой опыт реализации программ, направленных на обеспечение цифрового суверенитета, а сама эта проблематика стала особенно актуальной после событий «арабской весны», когда стало очевидно, что контроль над информационными потоками является важной составляющей национальной безопасности каждого государства. По мере развития информационных технологий актуализировались внутренние и внешние угрозы информационной безопасности в большинстве стран, и тема обеспечения цифрового суверенитета привлекает к себе все большее внимание и выходит на передний план международной повестки дня, а также становится одним из приоритетов во внутренней политике большинства стран мира. При этом, большая часть программ связана с обеспечением внутреннего суверенитета в цифровом пространстве.

В Китае, первом государстве проводившем политику, направленную на укрепление цифрового суверенитета, в 2010 году в «Белой книге» были зафиксированы положения о необходимости обеспечения цифрового суверенитета, позднее идеи цифрового суверенитета и цифровых границ получили развитие в исследовательских работах китайских ученых. 8 сентября 2020 МИД КНР была представлена Глобальная инициатива по безопасности данных, в которой детализируется понимание Китаем цифрового суверенитета и постулируется, что безопасное развитие современного глобального информационного пространства возможно только с опорой на цифровой суверенитет.

Показательно, в условиях актуализации угроз информационной безопасности в 2016 году в Европейском Союзе была принята директива о защите персональных данных, которая обязует компании Интернет-индустрии хранить персональные данные их пользователей из стран ЕС на территории стран-участниц ЕС. 19 февраля 2020 года принята Цифровая стратегия ЕС, которая также направлена на укрепление «цифровых границ» в Европе с целью обеспечить сувереннитет не на уровне отдельных стран, но на уровне региона в целом.

Проблематика технологического суверенитета (который является синонимом цифрового суверенитета, в силу того, что большая часть современных технологий в той или иной мере опирается на «цифру») обсуждается и США в настоящее время, когда ставится вопрос о реализации китайской компании Huawei сетей 5G на территории США. И сегодня мы можем говорить, что внутренний информационный суверенитет во многих странах мира довольно успешно реализуется.

Следует также отметить, что основные направления внешней политики Российской Федерации в области международной информационной безопасности, которые включают в себя: выработку правил ответственного поведения государств в глобальном информационном пространстве; продвижение проекта концепции конвенции ООН «Об обеспечении международной информационной безопасности»; продвижение проекта универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности; продвижение концепции конвенции ООН (или концепции безопасного функционирования и развития сети Интернет) – также исходят из необходимости закрепления категории «цифрового суверенитета» как основы для формирования глобального режима информационной безопасности.

При этом, внешняя политика России на данном направлении учитывает и актуальные тенденции технологического развития, которые дополнительно актуализируют проблему обеспечения цифрового суверенитета стран. Ускоренная цифровизация всех сфер жизни общества и государства, реализуемая зачастую без учета соображений информационной безопасности, обусловленная пандемией COVID-19, в свою очередь дополнительно актуализировала выбранную тему исследования. По мере растущего проникновения и увеличивающегося использования ИКТ во всех сферах жизни общества и государства возрастает и количество угроз. Так, в период эпидемии коронавируса существенно увеличилось общее количество киберпреступлений во всем мире[1]. Более того, как отметил Генеральный директор ВОЗ Т. Гебреисус, в условиях пандемии COVID-19 аткуализировалась проблема трансграничного распространения недостоверной информации, когда фейковые новости «распространяются легче и быстрее, чем сам вирус», что получило название «инфодемии»[2].

Более того, новые вызовы международной информационной безопасности появляются в связи с развитием перспективных направлений информационно-коммуникационных технологий и научно-технического прогресса в целом, в том числе таких направлений развития, как развитие «больших данных», технологии искусственного интеллекта, блокчейн-технологии, Интернет вещей, технологии робототехники и другие. Эти вызовы дополняют повестку дня двустороннего и многостороннего сотрудничества в сфере международной информационной безопасности.

Россия осознает огромный потенциал информационно-коммуникационных технологий и опасность информационных вызовов и угроз и активно продвигает на международной арене инициативы, направленные на формирование глобального режима информационной безопасности. Российская дипломатия инициативно участвует в международных переговорах в данной области, на практике реализуя официальную позицию, изложенную в Концепции внешней политики России[3], а также в таких документах как Стратегия развития информационного общества[4], Доктрина информационной безопасности[5], в которых ставится задача обеспечить достойное место России как влиятельного центра силы в глобальном информационном обществе.

Значимость проблематики информационной безопасности для политики и дипломатии России находит отражение в целом ряде внешнеполитических инициатив в данной сфере, к числу которых следует отнести проект Концепции конвенции о международной информационной безопасности[6] от 2011 года, а также Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[7], принятые в 2013 году. В 2016 году была принята новая редакция Доктрины информационной безопасности Российской Федерации[8]. В 2011, а затем в 2015 году по инициативе Россий-

1 Киберпреступность и распространение дезинформации во время пандемии COVID – 19 // Департамент глобальных коммуникаций ООН. URL: https://www.un.org/ru/coronavirus/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19

2 Там же.

3 Концепция внешней политики Российской Федерации. Утв. Президентом РФ 30.11.2016.

4 Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утв. Президентом РФ 09.05.2017.

5 Доктрина информационной безопасности Российской Федерации. Утв. Президентом РФ 5.12.2016.

6 Конвенция об обеспечении международной информационной безопасности (концепция). Утв. 22.09.2011.

7 Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утв. Президентом РФ 01.08.2013.

8 Доктрина информационной безопасности Российской Федерации. Утв. Президентом РФ 5.12.2016.

ской Федерации на рассмотрение Генеральной Ассамблеи ООН был предоставлен документ «Правила поведения в области международной информационной безопасности». В 2018 году свод правил поведения в области информационной безопасности был поддержан в качестве резолюции Генеральной Ассамблеи ООН[9]. В 2019 году данная резолюция вновь была принята Генеральной Ассамблеей, при этом в ее поддержку проголосовали рекордное количество стран.

9 Резолюция ГА ООН A/C.1/73/L.27/Rev.1 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 29.10.2018.

И.Ю. Тарасова
Кандидат политических наук,
Комитет Совета Федерации ФС РФ
по экономической политике.
Помощник сенатора Российской
Федерации.

НОВЕЙШИЕ ИКТ КАК ИНСТРУМЕНТ ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ

Стремительное развитие информационно-коммуникативных технологий (ИКТ) сформировало безграничное киберпространство и создало беспрецедентные возможности психологического, политического, социального и иного воздействия на население всей планеты.

В международных отношениях прочное место заняла цифровая дипломатия. С появлением Искуственного Интелекта (ИИ), роботизации, нанотехнологий, технологии блокчейн, Интернета вещей и т.д. технологический прорыв в современной промышленной революции постепенно размывает границы цифровой, физической и биологической сфер. Говоря о ближайшем будущем, нельзя не упомянуть о квантовом компьютере – как любая новая технология, он принесет обществу как существенную выгоду, так и неминуемые угрозы. Он может преобразить банковское дело, создать мощную систему киберзащиты, может на порядок усовершенствовать систему защиты от любого военного нападения, а может стать страшным оружием в руках террористов или мафиозных структур. Так, серьезную угрозу глобальной безопасности, экономике и повседневной жизни представляет использование квантовых компьютеров для взлома кодов. (Даже на начальной стадии применения квантовые компьютеры могут практически мгновенно сломать любой антивирусник и получить доступ, согласно мнению АНБ, примерно к 97% индивидуальных компьютеров, смартфонов и ноутбуков и не менее 65% – корпоративных).

С развитием новейших ИКТ возникают новые стратегические риски и глобальные вызовы для национальной и международной безопасности. С одной стороны, ИКТ являются одним из показателей глобального прогресса и процветания мирового сообщества, и, кстати,

неоднократно выступали на службе развития гражданского общества (ситуация с незаконно задержанным в 2019 г. в Москве журналистом Иваном Голуновым – пример того, как соцсети помогают восстановить справедливость). Но следует учитывать и оборотную сторону ИКТ – нарастание угроз в глобальной цифровой среде, которое может привести и к масштабному вооруженному противостоянию. Киберпространство рассматривается Западом как сфера стратегического противоборства. Медиасфера используется для манипуляции национальным и международным общественным мнением, для надуманных обвинений России в кибератаках, для «наказания» нашей страны международными санкциями, для попытки силовых решений межгосударственных споров и оправдания вмешательств извне во внутренние дела суверенного государства.

Обсуждая «гуманитарный» аспект применения ИКТ, в контексте иностранного вмешательства во внутренние дела государств, необходимо сказать об активном использовании ИКТ в пропаганде экстремистской и террористической деятельности, в организации протестных настроений на территории суверенных государств и в дальнейшем осуществлении революционных переворотов. Информационная обработка населения проводится, в частности, через Интернет-телевидение, мобильные устройства, социальные сети, мессенджеры, новые медиа, блоги и иные меди-

аплощадки в сети. По данным отчета о состоянии цифровой сферы Digital 2020, который каждый год готовят We Are Social и Hootsuite, на начало 2020 года более 4,5 миллиарда людей пользовались Интернетом, а аудитория социальных сетей перевалила за отметку в 3,8 миллиарда. Почти 60% мирового населения уже онлайн, и есть все основания полагать, что к началу 2021 половина всех людей на планете будут пользоваться соцсетями. На этой площадке ИКТ хочу остановиться особо.

Психологически человек воспринимает свою страницу как личное пространство, и доверие пользователя к получаемой информации из соцсети изначально выше, чем к другим источникам (федеральным СМИ, например). При этом соцсети зачастую предоставляют СМИ информацию, на основании которой и создается готовый новостной и аналитический контент. Так, отмечается частое появление роликов с видеохостинга Youtube.com в новостных и аналитических передачах телеканалов. Все больше усиливается политизация сервисов, созданных для межличностного общения, и социальные сети становятся еще и формой политического воздействия и манипуляции общественным сознанием. Как это работает? Есть приемы, схожие со СМИ-технологиями:

- **Обилие информации,** ежедневно публикуемое в Интернет-среде в несистемном виде, мешает полностью осмыслить сообщения;
- **Подача искаженной информации,** Интернет-опросы ангажированной аудитории (вспомним отравление семьи Скрипалей в Солсбери и локальные Интернет-голосования по поводу мнения общественности о виновных в этом происшествии);

Классический пример такой манипуляции в международном масштабе – постановка «химической атаки» в Идлибе, когда под общим давлением международной прессы и сообщений в соцсетях стали возможны дальнейшие обвинения Запада и последующее введение санкций против России.

Еще пример: недавний международный скандал с «отравлением» А. Навального и обвинениями в адрес России. Кстати, в соцсетях «Фонд борьбы с коррупцией» и блоге А.Навального активно используется прием – **одновременная подача противоречивой информации,** когда происходит лишь частичный ее вброс в Интернет-среду, умалчивание ряда фактов, заставляя тем самым пользователей додумывать общую картину в нужном для манипулятора русле.

Фейковые новости – одна из технологий дезинформации, инструмент политической пропаганды и недобросовестной конкурентной борьбы. Так, общеизвестны неоднократные попытки западных (в частности, польских) политических деятелей исказить историю Второй мировой войны. Можно вспомнить сетевые атаки на аккаунты наших дипведомств за рубежом. Например, фейковые аккаунты посольств России в Чехии и Словакии Facebook не тронул, а реальные страницы посольств заблокировал. Запад финансирует в том числе создание поддельных аккаунтов российских политических лидеров и государственных органов (В ФБ-Мария Захарова, в Твиттере-Сергей Лавров; МИД России и т.п.). Авторы размещают там фальшивые новости, компрометирующие нашу страну вбросы. Для борьбы с информационными фейками на сайте МИДа создана страничка, где формируют архив фейк-новостей, однако последний «не успевает» за разоблачением антироссийской пропаганды.

Многие помнят, как обвинения России в убийстве журналиста А. Бабченко в 2018 г., вслед за убийством Дениса Вороненкова и отравлением Скрипалей, вызвали негативную реакцию у части международного сообщества. Даже когда выяснилось, что произошедшее было инсценировкой властей Украины, в социальных сетях распространяли информацию о причастности России к этому происшествию и активно обсуждали стремление России к насилию. Антироссийской пропаганде все же удалось привлечь внимание к ряду событий, связанных с покушением.

«Дело Марии Бутиной», «Допинговый скандал» и другие спецоперации МИ-6, ЦРУ применяют весь спектр ИКТ, используя в том числе влияние социальных сетей и видеохостингов на массовое сознание. Даже при последующем опровержении или разоблачении того или иного фейка, подобные фальшивые вбросы в информационное пространство воздействуют на международное сообщество и как минимум достигают цели дестабилизации определенного политического, социально-экономического или иного процесса.

А вот классический «фейк о фейке». Посол в Великобритании Андрей Келин прокомментировал материал газеты The Times о якобы имевших место попытках РФ распространять дезинформацию о вакцине против коронавируса, разработанной Оксфордским университетом совместно с британско-шведской фармацевтической компанией AstraZeneca. (16.10.2020 газета The Times опубликовала расследование о том, что россияне якобы распространяют фейковые новости о вакцине от коронавируса Оксфордского университета. Кампания якобы нацелена на страны, в которых Россия хочет продавать свою вакцину «Спутиник V», а также на западные страны, указывается в статье). По словам А. Келина, речь идет о конкуренции, с учетом того, что российская вакцина «Спутник V» была создана на основе человеческого аденовируса, а вакцина от AstraZeneca и Оксфорда — на основе аденовируса шимпанзе, который до сих пор не исследовался. Дипломат отметил, что научный, медицинский вопрос используют в политическом ключе. Посол добавил, что Россия не старается кого-то очернить, а выступает за объединение усилий.

Бороться с фейковыми новостями недавно начал основатель соцсети Facebook Марк Цукерберг, после давления со стороны властей и общественности. Сейчас проверкой информации занимаются вручную несколько тысяч сотрудников в рамках соглашения с агентством Reuters. Однако есть данные, что сторонний фактчекинг для Facebook проводят 60 проектов, которые должны быть связаны с теми, кто заинтересован в том, чтобы признавать ложными невыгодные им новости. Российские пользователи отлично знают, что, например, антироссийские материалы нацистской и экстремистской направленности ФБ не блокирует, однако любое осуждающее мнение, например, о событиях «Евромайдана» на Украине, ФБ тут же удаляет и блокирует пользователя. И никакие жалобы администраторам сети не помогают разблокировать профиль.

В контексте борьбы с неправомерным использованием ИКТ в военно-политических и преступных целях, государством подготовлен ряд важных изменений в российское законодательство.

Так, в апреле 2020 антифейковое законодательство ужесточили 2-мя статьями Уголовного Кодекса. За публикацию опасных фейков физлицам грозит штраф до 400 тыс. рублей, юрлицам – до 1,5 млн. Решение о блокировке информации принимает Генпрокуратура. С 2014 запрещено продавать «симки» без паспорта, тем не менее только за 2019 год Роскомнадзор изъял свыше 54 тыс. «серых» SIM-карт. Ранее в России не было законодательных требований по самоконтролю Интернет-площадок. Сейчас до конца 2020 года ожидается подписание Президентом России ряда законопроектов, которые прошли необходимые обсуждения в Парламенте:

- **О самоцензуре соцсетей** – с 1 февраля 2021 года соцсети, мессенджеры, видеохостинги с охватом более 500 тысяч человек в сутки обязаны модерировать деструктивный контент, мониторить свои площадки с целью выявления незаконной информации, рассматривать обращения о нарушениях, удалять запрещенную информацию, клевету, принимать меры по защите чести, достоинства и деловой репутации. Так, соцсети обязаны модерировать и удалять запрещённую к распространению среди детей информацию о наркотиках и суицидах.

Владельцы соцсетей обязаны не допускать их использования в целях совершения уголовно наказуемых деяний (например, распространения экстремистских материалов, сообщений, содержащих публичные призывы и оправдывающих терроризм).

Запрещается распространять в соцсетях информацию «с целью опорочить гражданина или отдельные категории граждан». Если площадки не могут сами квалифицировать тип контента, то они обязаны приостановить его распространение/размещение и обратиться к Роскомнадзору.

Интернет-компаниям также предписывается соблюдать ограничения, предусмотренные законодательством РФ в отношении выборов и референдумов.

- **о противодействии цензуре западных ИТ-платформ в отношении российских СМИ.**

Роскомнадзор сможет блокировать полностью или частично Интернет-ресурсы, огра-

ничивающие значимую информацию на территории России по признакам национальности, языка, происхождения, имущественного и должностного положения, профессии, места жительства и работы; отношения к религии; в связи с введением иностранными государствами политических или экономических санкций в отношении России или россиян. Присваивать Интернет-ресурсу статус «причастного к нарушению основополагающих прав и свобод человека, прав и свобод граждан РФ» сможет генпрокурор РФ и его заместители по согласованию с министерством иностранных дел РФ. Роскомнадзор сможет блокировать YouTube, Facebook и Twitter или замедлять доступ к ним на территории России.

- **о поправках в Уголовный кодекс России, усиливающий ответственность за клевету в Интернете.**

Законопроектом предусмотрено, что клевета в Интернете, СМИ или в публичном выступлении грозит крупным штрафом, либо обязательными работами, либо принудительными работами на срок до двух лет, арестом на срок до двух месяцев или лишением свободы на срок до двух лет.

Клевета, совершенная с использованием своего служебного положения, будет грозить лишением свободы на срок до трех лет; клевета о том, что лицо страдает заболеванием, представляющим опасность для окружающих, – лишением свободы на срок до четырех лет.

- **о регулировании деятельности лиц и объединений, признанных в России иноагентами.**

Физлица, которые получают финансирование на политическую деятельность из-за рубежа, признаются иностранными агентами. Таким же статусом могут наделить незарегистрированные политические НКО с иностранным финансированием. Перечень иноагентов будет в открытом доступе в Интернете. Члены НКО-иноагентов смогут входить в состав общественных советов в федеральных органах власти.

В связи с таким «обновлением» законодательства, со стороны определенных сил могут возникнуть «вопросы» и «побочные эффекты», например:

- Как государство собирается обязать иностранные соцсети выполнить требование, если иностранные соцсети игнорируют другие требования российских законов, по году не оплачивая штрафы? Как будет происходить администрирование исполнения этого законопроекта?
- Крупные Интернет-компании, владеющими доменами в ру зоне, как только достигнут планки в 500 тыс будут регистрироваться, например, в Эстонии или us. После блокировок – не исключено существенное расширение рынка VPN, с нелегальным обходом блокировок за доплату. Как с этим бороться?

Безусловно, будут добавляться необходимые корректировки в соответствующие законы и подзаконные акты, с учетом обеспечения имплементации последних.

Кроме того, надо быть готовыми к обвинениям Запада в репрессиях в России в отношении независимых СМИ, в том числе в связи с поправками в Закон «Об иностранных агентах». Будут выражаться очередные «обеспокоенности» с так называемыми «нарушениями свободы слова» в России. Однако российской стороне есть чем ответить на подобные обвинения, например:

- Российские законы имеют право оценивать только российские граждане или специализированные международные организации.
- Российский закон никак не препятствует деятельности СМИ-иноагентов, а только обязывает их надлежащим образом регистрировать эту деятельность и соотносить с российской юрисдикцией.
- Российский закон об иноагентах в том числе является зеркальной мерой на репрессивные действия американских властей в отношении отечественных СМИ. Не лишне напомнить, что в США с 1938 года действует, например, Закон о регистрации иностранных агентов, который открыто препятствует обеспечению свободы слова и свободной журналистской деятельности, причем Закон применяется избирательно, по указанию американских госорганов. (Вспомним примеры с ущемлением прав журналистов RT) .
- Российское законодательство по иноагентам не сравнимо с американским, которое, в нарушение международных прав и свобод, преследует и наказывает СМИ, занимающих альтернативную позицию.

Примеров нарушений прав журналистов в США множество: при освещении протестов у Белого дома в июне 2020 г. американские правоохранители ранили резиновыми пулями журналистку «Спутник», в июле 2020 г. избили съемочную группу Первого канала и разбили камеру в Портленде, в октябре 2020 г. от рук бандитов пострадали корреспонденты Первого канала в Филадельфии. Расследование и наказание виновных в нападениях на работников российских СМИ не проводилось, несмотря на требования российской стороны.

Можно вспомнить о многочисленных примерах задержаний российских журналистов в аэропортах США; широкую известность приобрел допрос американскими спецслужбами журналиста RT(2020) – при прибытии в Нью-Йорк и при отлете. Среди других мер воздействия на иностранных журналистов в США - закрытие счетов в американских банках; российских журналистов местные американские спецслужбы периодически пытаются «завербовать» предложениями о сотрудничестве. Вопиющим примером удушения свободы слова является преследование Вашингтоном Дж. Ассанжа, фактически его целенаправленное физическое и моральное уничтожение.

Россия последовательно отстаивает на международных площадках такие основные международно-правовые принципы, как уважение государственного суверенитета, неприменение силы, невмешательство во внутренние дела других государств, соблюдение основных прав и свобод человека и равных прав для всех государств на участие в управлении сетью Интернет. Наша страна проводит политику по предотвращению конфликтов и противоборства в информационном пространстве, по противодействию использования ИКТ в террористических и преступных целях. Одной из недавних наших дипломатических побед было принятие в ноябре 2020 г. Первым комитетом 75-й сессии Генассамблеи ООН проекта российской резолюции по МИБ «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в соответствии с которой в 2021 году сроком на пять лет (2021–2025 гг.) будет учреждена новая РГОС (Рабочая группа ООН открытого состава). Ее мандат будет расширен. Так, например, новая группа будет уполномочена рассматривать национальные инициативы в области МИБ. По-прежнему максимум внимания будет уделяться деятельности по выработке правил, норм и принципов ответственного поведения государств в информационном пространстве.

РГОС будет рассматривать инициативы государств, направленные на обеспечение безопасности в сфере использования ИКТ, организовывать под эгидой ООН регулярный диалог с государствами-участниками. Она также продолжит исследовать потенциальные угрозы в сфере информационной безопасности и другие вопросы, в том числе о том, как международное право применяется к использованию ИКТ государствами. Не касаясь сложных моментов, связанных с противодействием по голосованию, можно утверждать, что Россия вносит конструктивный вклад в переговорный процесс по МИБ, при поддержке группы единомышленников.

Выступление Министра иностранных дел Российской Федерации С.В. Лаврова на XVIII Совещании руководителей спецслужб, органов безопасности и правоохранительных органов иностранных государств, Сочи, 16.10.2019: «Особое значение имеет борьба с экстремистской идеологией, в том числе в информационном пространстве. После ликвидации угрозы халифата ИГИЛ эволюционирует в разветвленную подпольную террористическую сеть, ставит на развертывание вербовочной деятельности, прежде всего среди молодежи, в том числе с использованием соцсетей. Все актуальнее задачи выработки системных подходов против использования Интернета в террористических и экстремистских целях».

Мы подошли к важному вопросу – откуда, собственно, берутся участники протестных движений и «цветных революций»? В. Жириновский о корнях событий 2014 на Украине: «Пока мы давали им скидки на газ, Запад работал с неправительственными организациями». И это тоже одна из многих причин. Можно также привести в пример украинских боевиков, которые с 2006 г. проходили обучение

в структурах НАТО, – или вспомнить офицеров НАТОвских кибервойск, которые в 2014 г. прибыли на Украину и из Борисполя осуществляли атаки на наши ресурсы (Российская газета, Центробанк и др.).

Надо обратить внимание, что более половины подписчиков в сети составляет молодежь до 18 лет – это группа лиц высокой внушаемости. К сожалению, современные исследования молодежи в России сосредоточены лишь на изучении «доступной» аудитории (например, студенты, получающие высшее образование). Основная же масса «обычных» молодых людей как бы выпадает из поля зрения ученых. Это подтверждает почти полное отсутствие исследований так называемых «маргинальных групп». Молодые инвалиды, сельская и «переферийная» молодежь, ВИЧ-инфицированные, иностранная молодежь (из числа мигрантов, например), в исследованиях представлены крайне редко. Соцсети как мощный медийный инструмент используется для тиражирования контента экстремистской направленности и представляющего потенциальную и реальную угрозу национальной безопасности страны. При этом зарубежные соцсети находятся вне поля российского законодательства, потому фактически являются открытой площадкой для публикации таких материалов. Социальные сети контролировать гораздо сложнее, чем обычные Интернет-сайты. Группу, где звучат прямые призывы к свержению действующей власти или нарушение территориальной целостности РФ, можно закрыть по предписанию прокуратуры, но с пропагандой религиозного экстремизма сложнее, так как этим занимаются группы по религии, а они тесно связаны с религиозным фундаментализмом. Экспертизы могут не признать публикуемые материалы экстремистскими, либо о них не становится вовремя известно. Кроме того, существует «мягкая» пропаганда фундаменталистких религиозных течений, которая не нарушает правил соцсетей и законодательства РФ, для вовлечения как можно большей массы людей. Для оказания максимального влияния на аудиторию используется целенаправленное распространение контента, например, реклама для определенной профессиональной, географической, социальной, возрастной группы пользователей. И если ранее важным было эмоциональное воздействие на жертву через живое общение, то сегодня в секты нового образца стало возможно привлекать людей лишь с помощью переписки в сети – для этого достаточно выхода в Интернет. Варвара Караулова, которая стала жертвой вербовщиков ИГ, золотая медалистка, студентка философского факультета МГУ была завербована через «Вконтакте» и «Skype» – при этом она относилась к представителям образованной молодежи и выросла в интеллигентной семье. После того, как школьник учинил массовый расстрел в Керчи в 2018 г. в своем родном колледже, правоохранительные органы изучили странички подростка-убийцы в соцсетях и пришли к выводу, что если бы компетентные органы обратили внимание на их содержание раньше, трагедии можно было бы избежать. Не менее серьезным вызовом для вербовки определенных слоев молодежи являются суицидальные группы. Между жертвами групп смерти и вербовки в ИГИЛ есть единый корень проблемы: отсутствие духовного иммунитета. В группах смерти покончившим с собой обещают «тихий дом» после суицида, а в ИГ обещают рай, где будет ждать блаженство за помощь террористам осуществлять «джихад». В сегодняшнем обществе, за редким исключением, нет сильной воспитательной идеологии. Освободившееся место легко заполняется вредоносными установками. В обществе, где размываются нормы морали, принадлежность к определённому народу, государству уже не имеет большого значения, и человек начинает чувствовать себя изолированным. А потребность в общении и причастности к какой-либо группе у них остаётся, что повышает возможности вербовки в секту. 15 августа 2017 года ситуацию вокруг «групп смерти» прокомментировал президент России Владимир Путин. Он заявил: «Те, кто вовлекает детей в «группы смерти» в Интернете, ничем не отличаются от убийц».

Можно говорить о новом типе психологического оружия ИКТ — манипуляции людьми через переписку в соцсетях.

ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА ПРОТЕСТНОЕ ПОВЕДЕНИЕ

Прокатившиеся на постсоветском пространстве «цветные» и «твиттерные» революции продемонстрировали, что любому протесту предшествует работа организаторов по «десоветизации» общества не просто с населением, а в первую очередь с его наиболее подверженной внешнему воздействию частью – с молодёжью. Она – движущая сила протестов, основной человеческий таран. Надо рассматривать ИКТ **не только как инструмент вмешательства во внутренние дела государства.** Следует говорить о воздействии на граждан конкретного государства: это угроза конкретной личности, а не только угроза государственному строю.

«Цветные революции» (ЦР) – это технологии осуществления государственных переворотов с преимущественным использованием методов ненасильственной политической борьбы и внешнего управления политической ситуацией в стране в условиях искусственно созданной политической нестабильности, где давление на власть осуществляется в форме политического шантажа с использованием в качестве инструмента шантажа молодежного протестного движения.

Президент Путин: «Мы видим, к каким трагическим последствиям привела волна так называемых цветных революций, и мы сделаем всё для того, чтобы это никогда не случилось в России».

Необходимое условие для ЦР – наличие политической нестабильности в стране, сопровождающейся кризисом действующей власти. Если политическая ситуация в стране стабильна, ее нужно искусственно дестабилизировать.

Достаточное условие – наличие специально организованного (по особой сетевой форме) молодежного протестного движения.

Отличительные черты «цветных революций»:

- в «цветных революциях» воздействие на власть осуществляется в особой форме – форме политического шантажа.
- основным инструментом воздействия на власть выступает молодежное протестное движение.

Западные политологи пытаются выдать ЦР за стихийное проявление воли народа, внезапно решившего вернуть себе право управлять собственной страной.

Любая ЦР начинается с формирования в стране организованного протестного движения – основной движущей силы будущей «цветной революции».

На начальном этапе, до открытого выступления, протестное движение формируется в виде сети конспиративных ячеек (лидер и 2–4 активиста). Такие сети объединяют тысячи активистов (ядро будущего протестного движения), многие из которых проходят обучение в специальных центрах, специализирующихся на вопросах содействия «демократизации». Рекрутируют активистов из легко увлекаемой различными яркими призывами и лозунгами молодежной среды. Сетевой принцип организации протестного движения напоминает принцип организации глобальных террористических сетей – по сути, это одна организационная технология.

Из подполья эта сеть выходит на улицы крупных городов одновременно и по условному сигналу, – «инциденту», часто созданному искусственно. Инцидентом может стать любое шокирующее событие, получившее мощный общественный резонанс (например, «сакральная жертва»). Инцидент должен стать предметом широкого обсуждения, интерпретации, нарастания всеобщего возбуждения и инициирования стихийных форм массового поведения.

Далее протестная сеть выходит из подполья на улицы, где группы активистов становятся катализатором стихийных массовых процессов, вовлекающих все больше людей в протестное движение, которые движимы в основном страхом за свое будущее.

Сознание людей переходит в состояние всеобщей истерии, часто на уровне рефлексов и инстинктов.

Следующий шаг в ЦР – формирование политической толпы из протестных масс. Для этого выбирается большая площадь для значительных масс народа.

В ходе бесконечного митинга происходит эмоциональное слияние активистов с протестной толпой; для идентификации свой-чужой используется яркая «революционная» опознавательная символика.

Именно такие технологии воздействия на подсознание, перепрограммирования человека применяются в протестантских тоталитарных сектах. Создаются условия для поддержания устойчивого существования и функционирования толпы – материальное обеспечение, палатки, горячее питание, одежда, деньги активистам, средства нападения (арматура

и др.) и т.д. Действует хорошо организованная «служба тыла».

К власти выдвигаются ультимативные требования, под угрозой массовых беспорядков или физического уничтожения.

Если власть не выдерживает этого напора, ее может смести стихия. Если власть начинает сопротивляться, толпа становится основным тараном удара, который наносят авторы ЦР. Такая революция может перерасти в мятеж, а в некоторых случаях – в гражданскую войну.

Например, на украинском Евромайдане обязательным элементом сценария ЦР стала работа снайперов по активистам майдана и мирным гражданам («сакральные жертвы») с целью повышения агрессивности толпы. Это пример жесткой силы, замаскированной под «мягкую» структуру ЦР. Почти всегда следствием ЦР, помимо осуществления главной задачи – совершения государственного переворота, становится погружение страны в политический хаос, переход под внешнее управление (например, назначение иностранцев на ключевые посты в Кабмине Украины), а также гражданская война, геноцид мирного населения и военная интервенция.

В качестве инструментария, используемого для влияния на протестный потенциал населения, используются все новейшие ИКТ, в том числе сайты социальных сетей.

Обмен информацией через виртуальные социальные сети, блоги и т.д. отличается **оперативностью**, позволяет **преодолевать физическое пространство**, оповещать жителей отдаленных районов о происходящем в центре событий, создавая схожие представления и **синхронизируя действия** участников коммуникации.

Виртуальная коммуникация между различными слоями населения содействует **сплочению людей с разным уровнем благосостояния,** что особенно актуально в обществах с неравномерным распределением доходов. Виртуальный протест, хоть и временно, объединяет богатых и бедных, городских и сельских жителей.

Информация с мобильного телефона (например, заснятое участником протеста видео) или предварительно заснятый пропагандистский сюжет может попасть на сайт социальной сети или YouTube, оттуда – на телеканал. Соцсети обладают эффектом мультиплицирования информации. Они также позволяют журналистам оперативно находить контакты участников протестных движений, провести с ними интервью онлайн и транслировать его через официальные СМИ.

Лидер политических протестов в Армении весной 2018, премьер-министр Армении Пашинян, охарактеризовал роль соцсетей: «В течение моей политической деятельности и протестов телевидение фактически было закрыто для оппозиции. Очень важно иметь альтернативный канал общения с народом. Сейчас у моей страницы в Facebook большая аудитория, которую можно сравнить с аудиторией телевидения. Это очень эффективный путь диалога с обществом, с гражданами. Facebook сыграл большую роль в нашей революции и был очень эффективным каналом для информационных потоков, чтобы пригласить людей на митинги». После событий в Нагорном Карабахе ИКТ-оружие ударило по самому Пашиняну, когда оппозиция собрала через соцсети десятки тысяч протестующих в центре Еревана, требуя его отставки. Представитель оппозиционной партии «Дашнакцутюн» Сагателян: «Если он этого не сделает, по всей стране начнутся акции неповиновения».

В России можно вспомнить протесты в Екатеринбурге (поводом стало строительство храма «не на том месте»), которые оппозиция всеми силами пыталась вывести на уровень политической борьбы. Или, например, митинги в Москве несогласных с выборами в Мосгордуму. Организация и ход протестов, руководство массами идет именно из соцсетей, – это относится и к «Болотным» протестам.

Почему был сорван «быстрый» западный план по типу Евромайдана в Белоруссии?

Ослабленные пандемией, «чернокожими» протестами в Америке, США и Евросоюз торопились «поменять геополитику», развернуть большую геополитическую игру, где Беларусь была бы «разменной картой».

Ряд причин помешал западным странам:

- Западные НКО в Беларуси есть, но их гораздо меньше, чем на Украине, они не успели «масштабно насадить» десоветизацию, антисоветские настроения, не проникли глубоко в сознание граждан. Они не успели подготовить боевиков, – последних активно готовили на Украине – но в Беларуси «не успели». (Кстати, если говорить о группах вербовки и суицидальных сообществах, то из стран Постсоветского пространства в этом отношении наиболее благополучной можно считать Беларусь: ее молодежной среде присущи политическая уравновешенность, отсутствие массовых религиозных и национальных экстремистских настроений. В молодёжной политике всегда отдавался приоритет гражданско-патриотическому воспитанию, это повлияло на духовно-нравственное развитие белорусов). ВВП втрое выше, чем на Украине, и дело далеко не только в помощи России. Белорусы талантливый, трудолюбивый народ. Там не развалена экономика, производство.
- Там нет олигархов, которые финансируют протест и управляют им извне. Белорусский ОМОН работал очень жестко, они в том числе и боевиков задерживали. Оппозиция и провокаторы в ответ на жесткий ответ силовиков, стали угрожать им и их семьям, через соцсети и мессенджеры запугивать, травить их детей, пытались сделать аналог горящего майдана. Это вызвало отторжение большей части населения – люди поддерживали мирный протест, но не вооруженный.
- Лидеры оппозиции «далеки» от народа. Например, Колесникова – из специфических нетрадиционных движений прозападной прослойки. Тихановская – слабая фигура, достаточно вспомнить ее некомпетентные, примитивные ответы в интервью. Алексиевич поддерживала убийство Олеся Бузины. Это все населению не близко.
- Кроме того, они задумали задушить производство: призывали всеобщую стачку из Польши, Литвы – призывы шли через все возможные соцсети, блоги и мессенджеры, пока практически полностью не заблокировали Интернет – это и было ИКТ в действии. Оппозиция намеревалась остановить государственные предприятия, развалить государственную экономику, выбить ее из состава союзного государства.

Это не одобрило большинство населения, консервативная часть активизировалась и поддержала стабильность.

- За «лидеров» никто не голосовал, из них ни одного кандидата на выборах Президента Беларуси не было! Получились самозванцы вне правового поля. Официально оппозиция не стала обжаловать выборы на участках, не пошла в суд. То, что они предлагали свержение власти незаконными методами, подорвало их позицию.
- В стране отсутствовал сильный кандидат, который мог стать новым Президентом.
- Лукашенко нельзя сравнивать с Януковичем на Украине, хотя ранее он и вёл политику двойных стандартов – достаточно вспомнить о его предвыборной антироссийской риторике, приеме М. Помпео, – или как задерживали российских журналистов. Он своей антироссийской риторикой потерял часть избирателей.
- Почему Лукашенко «застали врасплох»? Он был уверен в своей неприкасаемости, в неограниченной власти, не был готов сражаться за неё ежедневно. Лукашенко боялся создания пророссийской партии – боялся потерять свою партийную поддержку. В результате у него нет опорных точек, нет своей преданной партии.
- Сейчас Лукашенко мобилизовал государственную систему – и конфликт принял вялотекущий характер. Ему надо запускать обновление политической системы, в рамках конституции – чтобы оппозиционно настроенная часть общества поняла, что государство и ее услышало.
- Чтобы выявить нарушения со стороны силовиков и других структур, власти надо использовать ИКТ. России следует помочь Лукашенко с точки зрения политических технологий, применения ИКТ, в том числе в качестве воздействия на население. Ему еще раньше надо было обратиться за содействием.

России выгодно, чтоб Лукашенко разрешил конфликт мирными политическими методами, без непосредственного участия России. **Наш геополитический интерес** – чтобы была мирная страна и братский белорусский народ в союзном государстве, который не повторит трагической судьбы украинского народа, кровопролитного Майдана. Мы отстаиваем национальные интересы России в союзном государстве.

УРОКИ БЕЛАРУСИ ДЛЯ РОССИИ: нашей стране необходимо создавать в Беларуси свои НКО, СМИ, продвигать ИКТ. Необходимо помочь беларусам организовать там российские НКО. Например, литовские, польские НКО там есть, а российских – нет! Нету СМИ, относящихся к России. Мы должны присутствовать в стране.

В России нам надо формировать «улицу». Главная сила протестов – молодежь. За неё надо бороться, иначе государство потеряет поколение. Политический режим должен иметь мобилизуемый социальный ресурс. У нас нет времени «на раздумье».

В этом направлении:

- Совершенствовать образовательную и молодежную политику, сделать ее адресной.
- Развивать страницы российских ведомств, наполнять их актуальной информацией – это позволит построить диалог с пользователями.
- Активная информационная деятельность на международной арене, в том числе аккаунтов российских зарубежных ведомств, направленных на иностранных пользователей и учитывающих языковые особенности и специфику информации.

Важным элементом такой работы являются и страницы в социальных сетях крупнейших теле- и радиоканалов, целевой аудиторией которых выступают и российские, и иностранные граждане.

- Работа с «троллями» и ботами в рамках социальных сетей, которые призваны распространять зачастую ложную информацию,а также направлять дискуссии и мнение аудитории в выгодное оппоненту русло.

Отслеживание фейковых публикаций и аккаунтов, с которых может вестись работа по подрыву стабильности внутри государства и распространение ложной информации.

- Регулярная актуализации имеющихся нормативно-правовых актов, касающихся информационной безопасности и эффективного контроля за деятельностью пользователей в сети.

Некоторые особенности противодействия «Цветным Революциям» – российский контекст:

- Против технологий государственных переворотов использовать все новейшие ИКТ.
- Перекрывать каналы получения средств для организации ЦР – протест начнется только когда будут размещены большие суммы денег в национальных банках.
- Работать с основной ударной силой ЦР – активной молодежью, развенчивать идеологию ЦР. (Требуется грамотная молодежная политика).
- Уделить внимание проблемным регионам – Дальнему Востоку, Сибири, Кавказу, где региональная политика федерального центра периодически «проседает»: ЦР в России может начать развиваться под лозунгами регионального сепаратизма.
- Разработать российскую модель противодействия ЦР, в том числе на пространстве СНГ, в Азии и других регионах, где Россия имеет свои национальные интересы. (Например, переключение внимания населения на другие проблемы; задействие инструментов «мягкой силы» и т.д.)
- Создание общегосударственной системы противодействия ЦР и подготовки специалистов в области информационных и гибридных войн.

Применение новейших ИКТ как действенного инструмента влияния в системе международных отношений и, в частности, в информационной сфере требует непрерывного практического изучения (с учетом быстрого обновления ИКТ-технологий) и является одним из условий обеспечения национальной безопасности России и повышения внешнеполитического престижа страны.

А.Ю. Раззоренов
Депутат городской Думы Краснодара

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ВМЕШАТЕЛЬСТВУ ВО ВНУТРЕННИЕ ДЕЛА С ИСПОЛЬЗОВАНИЕМ ИКТ НА РЕГИОНАЛЬНОМ УРОВНЕ: ОПЫТ КУБАНИ

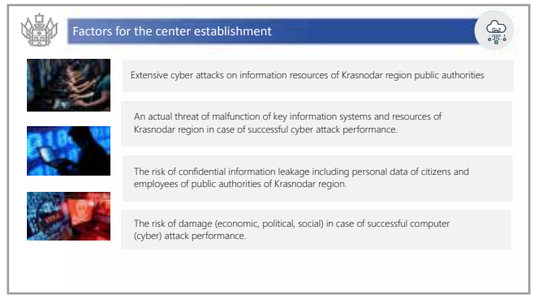
Актуальность угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты. 20 лет назад задача обеспечения безопасности информации решалась при помощи средств криптографической защиты, установления межсетевых экранов, разграничения доступа. Сейчас этих технологий недостаточно, любая информация, имеющая финансовую, конкурентную, военную или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления критическими объектами информационной инфраструктуры.

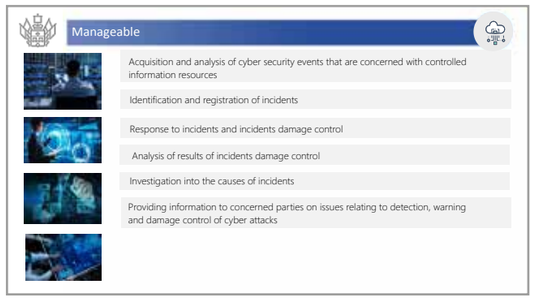
Именно поэтому для обеспечения безопасности органов государственной власти Краснодарского края был создан Центр мониторинга информационной безопасности, осуществляющий выявление инцидентов информационной безопасности, связанных с информационными ресурсами, системами и иными компонентами региональной мультисервисной сетью органов государственной власти. Центр является структурным подразделением организации, подведомственной ответственному за информационную безопасность органу власти Краснодарского края, имеющим соответствующие лицензии ФСТЭК России.

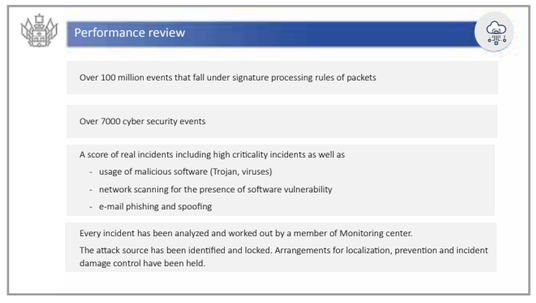
За год средствами мониторинга регистрируется более 100 миллионов событий информационной безопасности, попадающих под сигнатурные правила обработки пакетов:

- более 13 млн событий, носящий информационный характер и не относящихся напрямую к инцидентам, однако способных предоставить дополнительную информацию по сетевой активности;
- более 16 млн событий, связанных с попытками сканирования служб контролируемых информационных ресурсов и систем на предмет наличия уязвимости;
- порядка 200 тыс. событий, связанных с попытками подбора паролей к открытым службам;
- более 60 млн. событий, информирующих о попытках эксплуатировать потенциально опасные службы и внешние сервисы;
- более 500 тыс. событий, связанных с активностью вредоносного кода и программного обеспечения;
- более 100 тыс. событий, связанных с попытками вызвать приостановку работы сервисов контролируемых информационных систем и ресурсов;
- более 400 тыс. событий, связанных с попытками эксплуатации уязвимостей в сервисах и службах контролируемых информационных ресурсов и систем;
- более 16 млн. прочих событий, попавших под сигнатурные правила.

Вышеуказанные события коррелируются в комплексные события информационной безопасности (подозрение на инцидент), обычно порядка 7 тыс. Каждое подозрение на инцидент анализируется специалистами Центра мониторинга, в результате анализа которых направляется на детальное изучение специалистам по информационной безопасности порядка 50–100 инцидентов, связанных с ресурсами региональных органов власти и подведомственных им учреждений, далее при необходимости, предпринимаются действия по блокированию, локализации, противодействию и устранению последствий каждого из них.







Все статистические данные представленные выше собираются и обрабатываются в системе мониторинга, организованной в центре мониторинга информационной безопасности. В состав этой системы входят:

- система сбора событий информационной безопасности, автоматического обнаружения компьютерных атак и выявления инцидентов информационной безопасности;
- сетевые сенсоры системы обнаружения вторжений IDS.

Сетевыми сенсорами специализированного программного обеспечения, установленными на сегментах сети региональной мультисервисной сети органов государственной власти, круглосуточно в автоматическом режиме анализируется сетевой трафик и собирается информация о событиях информационной безопасности на основании регулярно обновляемых баз решающих правил. Информация по событиям передается в систему сбора событий информационной безопасности, автоматического обнаружения компьютерных атак и выявления инцидентов информационной безопасности, где проводится ее анализ и корреляция в автоматическом режиме.

Более подробный анализ собранных событий, а также блокирование, локализация, противодействие и устранение возможных последствий инцидентов информационной безопасности осуществляется также специалистами центра совместно с ответственными в органах власти.

Наибольшее количество попыток совершения несанкционированного доступа к государственным информационным ресурсам наблюдается в период социально-значимых мероприятий, в частности массовых спортивных соревнований (Олимпиада, Чемпионат мира по футболу, Кубок конфедерации, Формула-1), а также в период выборов представителей разных уровней власти.

В.И. Булва
Эксперт, помощник Директора. Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России

БОРЬБА С РАСПРОСТРАНЕНИЕМ ПРОТИВОПРАВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ

Сегодня противоправный контент в мировой Сети распространяется с беспрецедентно большой скоростью, генерируя угрозы традиционным устоям общества и национальной безопасности государства. Причём масштаб проблемы увеличивается по мере роста пользователей социальных сетей и расширения доступа ко Всемирной паутине.

По данным глобального отчёта Digital 2020, в мире число Интернет-пользователей выросло до 4,54 млрд (на 7% или 298 млн пользователей по сравнению с 2019 г.), а в России этот показатель достиг 118 млн. Если добавить к этому, что в среднем человек проводит в Интернете 6 часов 43 минуты ежедневно (более 100 дней в год, около 40% времени бодрствования), то становится очевидным, что для подавляющего большинства онлайн-контент служит основным источником информации[1]. Всё это наглядно демонстрирует сильную взаимосвязь степени защищённости общества, национальной безопасности, а также содержания и качества контента.

Условно, можем поделить проблемный контент на две группы:

1) контент, который признаётся противоправным всеми государствами (в этом случае ответственность за его распространение несут не государства, а отдельные личности или группы лиц);

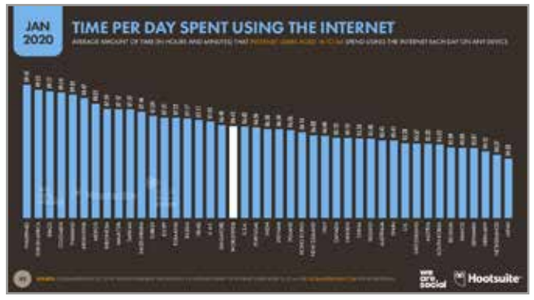
2) контент, который используется государством с целью вмешательства во внутренние дела другого государства.

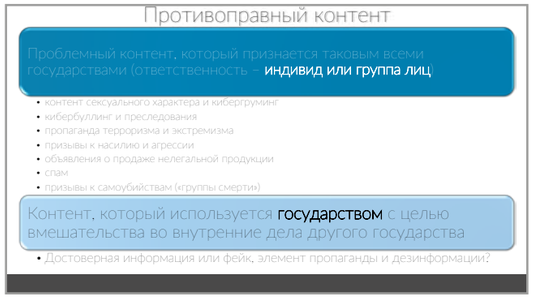
К первой группе относятся: контент сексуального характера и кибергруминг (сексуальное насилие над ребёнком), буллинг и преследования, пропаганда терроризма и экстремизма, призывы к насилию и агрессии, объявления о продаже нелегальной продукции (оружие, наркотики, торговля людьми), спам, призывы к самоубийствам («группы смерти»). На глобальном уровне существует межгосударственный консенсус о важности недопущения распространения подобного контента. Основное противоречия возникает при выборе средств и методов борьбы с киберпреступностью, кибертерроризмом и киберэкстремизмом.

В рамках второй группы разногласия между суверенными государствами более значительны. Это обусловлено тем, что проблемность контента зависит от того, с позиции какого государства он анализируется. Так, одна и та же информации в одном государстве может рассматриваться как точная и достоверная, а в другом – как дезинформация, пропаганда или фейк. Именно поэтому распространение подобного контента нередко выступает поводом для взаимных обвинений и является деструктивным для стабильности межгосударственных отношений.

Проблема усугубляется тем, что государства по-разному трактуют принцип невмешательства во внутренние дела, чёткое следование которому позволило бы минимизировать риск использования информации одним государством против интересов другого. Примером могут послужить преследуемая Соеди-

1 Вся статистика Интернета на 2020 год – цифры и тренды в мире и России // Web Canape – URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (дата обращения: 05.12.2020)





нёнными Штатами тактика содействия установления и поддержания демократии в различных государствах мира. Важно отметить, что пропаганда идеалов западной демократии рассматривается США не как вмешательство во внутренние дела, а как помощь в укреплении режима государства.

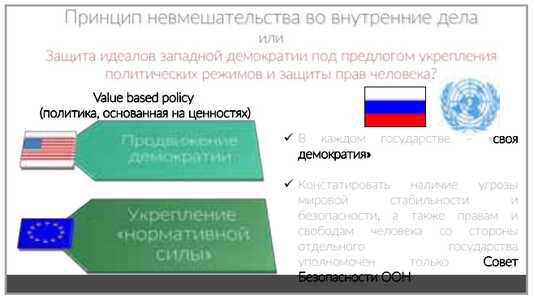
Другой пример – политика, основанная на ценностях (value based policy), проводимая Европейским Союзом. В качестве ключевой стратегической задачи внешней политики европейские страны обозначают необходимость укрепления «нормативной силы» Союза путём продвижения демократических ценностей, причём в таком понимании, как это зафиксировано в Учредительных договорах ЕС.

В обоих случаях «информационное поле» служит идеальной площадкой для воздействия на массовое сознание граждан. Де-факто нарушается принцип суверенитета государства (ограничение его полного контроля над своими гражданами, и, как следствие, над территорией). Более того, подрыв доверия к действующему правительству может стать катализатором реальных внутренних конфликтов, что наглядно было продемонстрировано в ходе «цветных революций» и «Арабской весны».

Российская Федерация, признавая демократические ценности, считает, что важно учитывать различия в их трактовке в зависимости от индивидуальных особенностей государства. Иными словами, единого понимания демократии не существует. Констатировать наличие угрозы мировой стабильности и безопасности, а также правам и свободам человека со стороны отдельного государства уполномочен только Совет Безопасности ООН. В противном случае любая деятельность извне, направленная на дискредитацию действующего режима, в том числе посредством распространения соответствующей информации, нарушает основополагающий принцип международного права – гарантию невмешательства во внутренние дела.

Для эффективной борьбы с противоправным контентом необходимо предпринимать взаимодополняющие шаги на индивидуальном, национальном и международном уровнях. Выбор конкретных инструментов зависит от группы, к которой относится противоправный контент. Так или иначе, главная цель подобной борьбы – построить в России высокоэффективное информационное общество на основе безопасной и этичной Интернет-среды, и в первую очередь для подрастающего поколения.

Что касается индивидуального уровня, приоритет следует уделять развитию таких качеств как критическое мышление и способность к многоаспектному анализу. Необходимо сделать акцент на повышении уровня цифровой культуры (обучение специальным цифровым навыкам), а также на углублении общих знаний, которые бы помогали человеку



выжить и сохранить индивидуальность в информационном хаосе.

Повышение уровня общего образования важно, потому что оно создает определённый защитный барьер в условиях мира постправды. Образованные граждане сложнее поддаются деструктивному воздействию извне. В то же время, манипулировать толпой, в которой подавляющее большинство занимает пассивную позицию и не располагает реальными знаниями, намного легче.

Не стоит забывать, что использование общественного мнения в интересах иностранного государства создаёт угрозу национальной безопасности, нанося огромный ущерб репутации государства и подрывая доверие его граждан. При этом, опасность кроится в том, что нередко противник применяет тактику опосредованной войны (proxy war), которая позволяет оказывать деструктивное воздействие на оппонента, действуя на территории третьего государства, в том числе на его информационном пространстве.

Кроме этого, активную роль в недопущении распространения проблемного контента должно играть государство. На национальном уровне необходимо сочетать меры превентивного характера и меры эффективного реагирования. К первым относятся: формирование культуры населения на основе высоких гуманитарных технологий, создание государственного контента, который бы отражал фундаментальные ценности, устои и традиции общества, развитие образования на основе комплексного и всеобъемлющего подхода как в цифровой области, так и в других областях.

Эффективное реагирование должно строиться на основе сотрудничества различных участников (государственных структур, неправительственных организаций, профильных компаний, добровольцев) в области мониторинга Интернет-контента, блокировку которого должны осуществлять правоохранительные органы. Перманентный мониторинг также может стать одним из направлений международного сотрудничества.

В дополнение к этому, крайне важно развивать институциональную и нормативно-правовую базу, которая регулировала бы сотрудничество государств в области обмена информацией. Этот шаг имеет особое значение в рамках борьбы с киберпреступностью, кибертерроризмом и киберэкстремизмом.

Помимо этого, на международном уровне интересам не только Российской Федерации, но и абсолютно всех государств мира отвечает законодательное закрепление Кодекса поведения. В него также следует инкорпорировать этические нормы деятельности в цифровой среде, а для повышения эффективности действия – учредить специальный контрольный механизм и согласовать комплекс штрафных мер за их невыполнение.

Таким образом, Кодекс поведения станет своего рода универсальным механизмом по противодействию распространения проблемного контента не только в силу широкого географического охвата, но и потому, что будет направлен на регулирование всех видов угроз, связанных с публикацией противоправной информации.

Для заметок

СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
ЧЕТЫРНАДЦАТОГО МЕЖДУНАРОДНОГО ФОРУМА
«ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА
И ГРАЖДАНСКОГО ОБЩЕСТВА
ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Подписано в печать 21.12.2020. Гарнитура Helios.
Формат 60x84/8. Объем 24,64 усл. печ. л.
Тираж 200 экз.