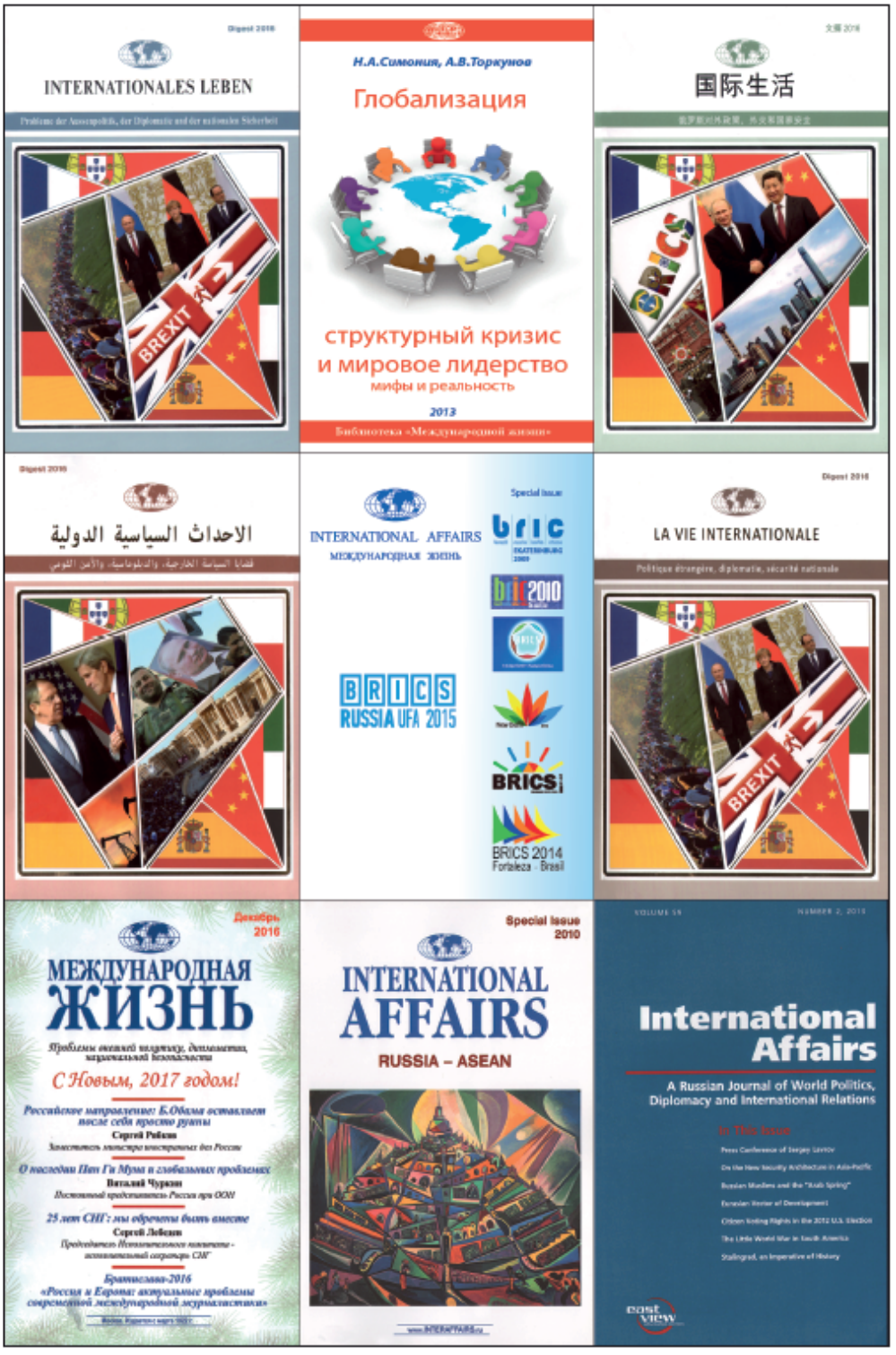
Специальный выпуск

МЕЖДУНАРОДНАЯ ЖИЗНЬ

Россия и информационная безопасность

Москва. Издается с марта 1922 г.


Digest 2016
INTERNATIONALES LEBEN
Probleme der Aussenpolitik, der Diplomatie und der nationalen Sicherheit
BREXIT
Н.А.Симония, А.В.Торкунов
Глобализация
структурный кризис
и мировое лидерство
мифы и реальность
2013
Библиотека «Международной жизни»
国际生活
BRICS
الاحداث السياسية الدولية
INTERNATIONAL AFFAIRS
МЕЖДУНАРОДНАЯ ЖИЗНЬ
Special Issue
BRICS
RUSSIA UFA 2015
BRICS 2014
Fortaleza - Brasil
LA VIE INTERNATIONALE
Politique étrangère, diplomatie, sécurité nationale
BREXIT
Декабрь
2016
МЕЖДУНАРОДНАЯ
ЖИЗНЬ
Проблемы внешней политики, дипломатии, национальной безопасности
С Новым, 2017 годом!
Российское направление Б.Обамы оставляем после себя просто руины
Сергей Рябков
Заместитель министра иностранных дел России
О наследии Пан Ги Муна и глобальных проблемах
Виталий Чуркин
Постоянный представитель России при ООН
25 лет СНГ: мы обречены быть вместе
Сергей Лебедев
Председатель Исполнительного комитета - исполнительный секретарь СНГ
Братислава-2016
«Россия и Европа: актуальные проблемы современной международной журналистики»
Special Issue
2010
INTERNATIONAL
AFFAIRS
RUSSIA – ASEAN
www.INTERAFFAIRS.ru
VOLUME 59
NUMBER 2, 2013
International
Affairs
A Russian Journal of World Politics, Diplomacy and International Relations
In This Issue
Press Conference of Sergey Lavrov
On the New Security Architecture in Asia-Pacific
Russian Muslims and the "Arab Spring"
Eurasian Vector of Development
Citizen Voting Rights in the 2012 U.S. Election
The Little World War in South America
Stalingrad, an Imperative of History
east view

Россия и глобальные вызовы в области информационной безопасности

Десятый международный форум

«Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Гармиш-Партенкирхен, Германия

25–28 апреля 2016 года

Международная конференция журнала «Международная жизнь»

«Актуальные вопросы информационной и кибербезопасности»

Москва

20 декабря 2016 года

Руководитель проекта:
Главный редактор журнала «Международная жизнь»
А.Г.Оганесян

Ответственный редактор:
Ответственный секретарь журнала
«Международная жизнь»,
кандидат исторических наук
Е.Б.Пядышева

Научный редактор:
Редактор журнала «Международная жизнь»
А.Д.Дубина

Литературные редакторы:
О.Н.Ивлиева
Н.В.Карпычева
Л.А.Подчашинская

Выпускающий редактор и дизайн:
И.Н.Знатнова

Верстка:
А.С.Родченкова
М.С.Тюрина

Адрес редакции: **105064, Москва, Гороховский переулок, 14.**
Тел.: 8 (499) 265-37-81; факс: 8 (499) 265-37-71; E-mail: journal@interaffairs.ru

Отпечатано в типографии ООО «Верже.Ру»
Москва, 127055, ул. Сущевская, д. 21 (БЦ «Молодая Гвардия»), подъезд 2, этаж 3, офис 2
www.verge.ru, e-mail: info@verge.ru тел./факс: +7 (495) 727-00-08, 363-61-55

Тираж 1000. Цена свободная.
Дата выхода в свет 15.04.2017. Заказ №.5

МЕЖДУНАРОДНАЯ ЖИЗНЬ

СОДЕРЖАНИЕ

Десятый международный форум

«Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Пленарное заседание

Проблемы современных международных отношений в контексте киберпространства «Круглый стол» журнала «Международная жизнь»

Международная конференция «Актуальные вопросы информационной и кибербезопасности»

Открытие конференции

Сессия 1. Современные вызовы и угрозы в контексте новой Доктрины информационной безопасности и Концепции внешней политики Российской Федерации

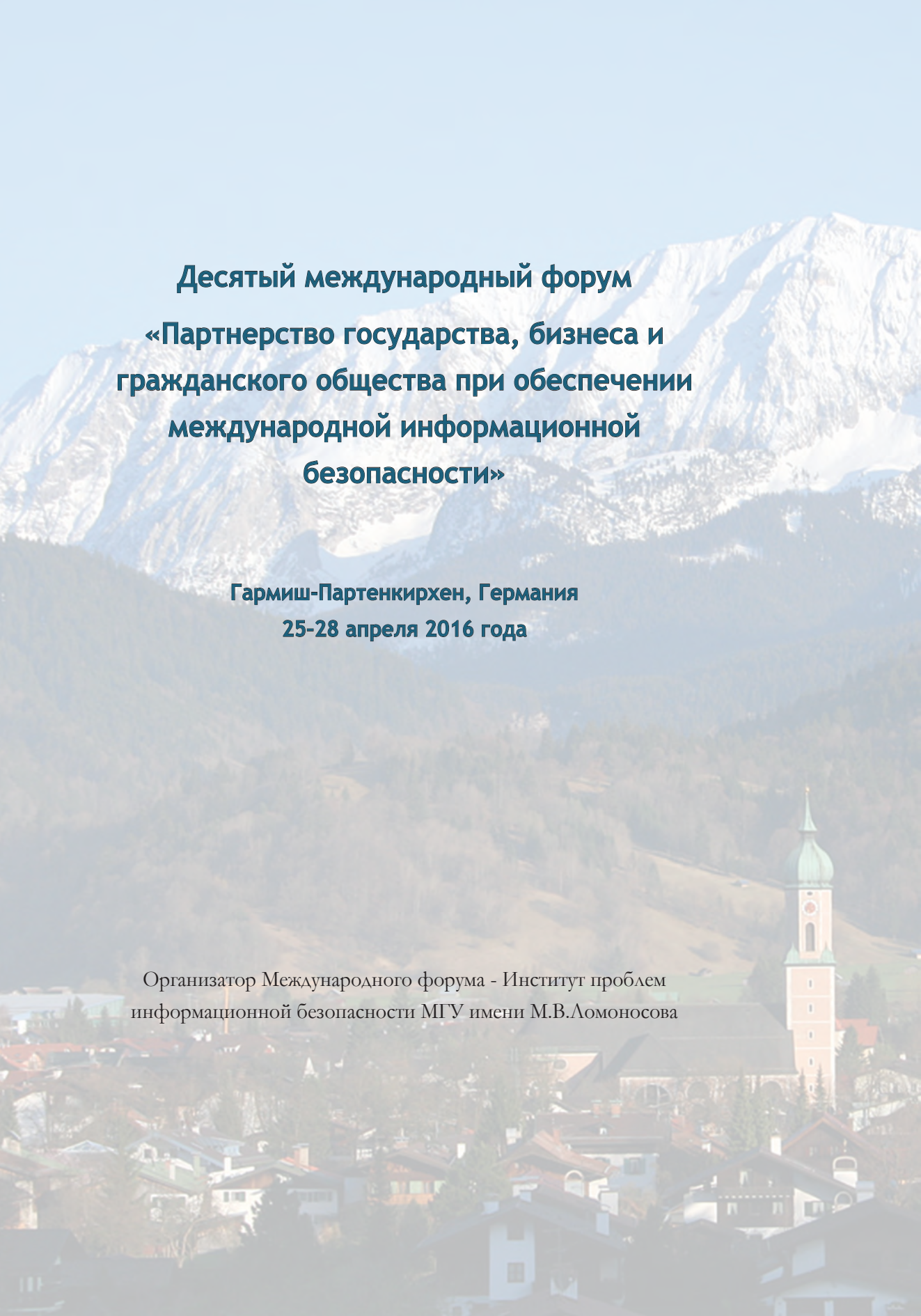
Сессия 2. Гуманитарные аспекты международной информационной безопасности

Десятый международный форум

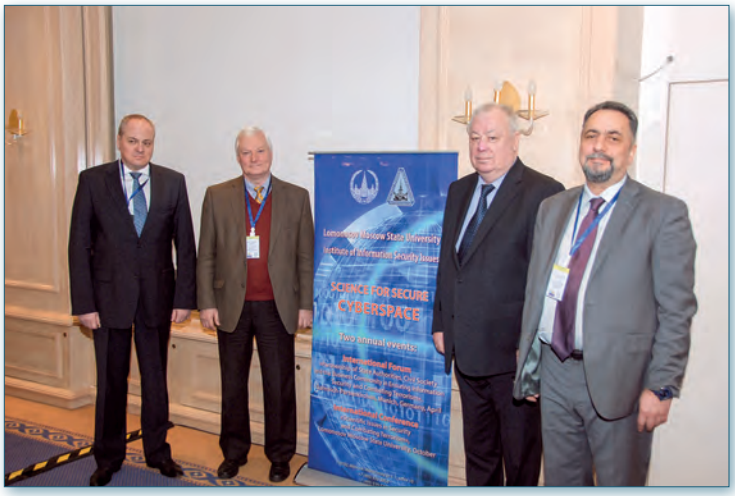
«Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Гармиш-Партенкирхен, Германия

25-28 апреля 2016 года



Организатор Международного форума - Институт проблем информационной безопасности МГУ имени М.В.Ломоносова



Пленарное заседание

Владислав Шерстюк, советник секретаря Совета безопасности РФ, директор ИПИБ МГУ им. М.В.Ломоносова

Многоуважаемые коллеги, хотел бы начать свой доклад со слов искренней признательности руководителям администрации города Гармиш-Партенкирхен, другим представителям Федеративной Республики Германия, которые вот уже десять лет радушно предоставляют нам возможность собираться в этом зале и обсуждать актуальные проблемы обеспечения международной информационной безопасности. За прошедшие десять лет мир существенно изменился. Вопреки нашим ожиданиям и надеждам он не стал более безопасным, более комфортным для проживания людей. Продолжает увеличиваться опасность угроз использования потенциала информационно-коммуникационных технологий для силового разрешения международных споров, осуществления деятельности международных террористических организаций, совершения трансграничных преступлений, корыстной направленности нарушения прав и свобод человека. Все более сложными и изощренными становятся компьютерные атаки на объекты критически важных инфраструктур.

Поисками путей решения проблем международной информационной безопасности, в соответствии с резолюциями

Генеральной Ассамблеи и решениями Генерального секретаря Организации Объединенных Наций, уже длительное время занимается Группа правительственных экспертов ООН. Все это свидетельствует об актуальности и сложности проблем, с которыми столкнулось человечество на настоящем этапе своего развития. Мы помним Всемирную встречу на высшем уровне по вопросам информационного общества, два этапа которой прошли в Женеве и Тунисе в 2003 и 2005 годах. В итоговых документах этой встречи проблемы обеспечения безопасности глобального информационного пространства предлагалось решать прежде всего на основе совершенствования культуры информационной безопасности. Тогда казалось, что достаточно объединить всех лиц, заинтересованных в прогрессивном развитии ИКТ, наращивании его потенциала как фактора обеспечения устойчивого развития человечества, и все проблемы обеспечения устойчивости и безопасности использования ИКТ-среды будут решены.

Сегодня мы знаем, что этого недостаточно для предотвращения использования ИКТ в целях, несовместимых с Уставом ООН. В докладе Группы правительственных экспертов ООН прошлого года (2015 г.) представлены рекомендации по добровольным нормам, правилам и принципам ответственного поведения государств в ИКТ-среде, по мерам доверия и применимости норм международного публичного права к регулированию международных отношений в области поддержания международного мира и безопасности.

Как представляется, определенный вклад в разработку путей решения проблемы обеспечения международной информационной безопасности внес и наш международный форум. Он стал одной из немногих дискуссионных площадок, на которых встречаются специалисты в области информационной безопасности государств, придерживающихся различных политических воззрений, культурных традиций и предпочтений. Мы можем свободно и открыто обсуждать наиболее острые вопросы, опасные угрозы национальной безопасности наших государств, возникающие вследствие злонамеренного использования ИКТ как государствами, так и преступными, в том числе террористическими, организациями.

За прошедшие годы на заседаниях форума мы обсуждали проблемы применения международного права в ИКТ-среде, про-

тиводействия компьютерному терроризму и преступности, обеспечения безопасности объектов критической инфраструктуры, противодействия идеологии терроризма, правила ответственного поведения государств в информационном пространстве, организацию международного сотрудничества в противодействии угрозам международному миру и безопасности, организацию мониторинга этих угроз, терминологического аппарата проблематики международной информационной безопасности и др.

Как постоянно отмечали участники форума, эти обсуждения были полезны для лучшего понимания возможных подходов к решению рассматриваемых проблем, поиску компромиссных решений для предоставления в заинтересованные органы государственной власти. По инициативе участников форума в 2010 году был образован Международный исследовательский консорциум информационной безопасности (МИКИБ). Это позволило не только организовывать встречи экспертов на более регулярной основе, но и заложить основу для проведения совместных научных исследований.

В настоящее время в состав Международного консорциума входят 23 организации из 16 государств. В консорциуме участники представляют Азербайджан, Белоруссию, Болгарию, Германию, Израиль, Индию, Италию, Казахстан, Канаду, Киргизию, Китай, Республику Корея, Россию, США, Швейцарию и Японию. Такое представительство обеспечивает весьма широкий спектр взглядов и позиций по обсуждаемым на заседаниях консорциума вопросам. В консорциуме накапливается положительный опыт по реализации совместных научных проектов. За прошедшее время был создан глоссарий терминов в области кибербезопасности. Эту работу выполнял Институт проблем информационной безопасности МГУ им. М.В.Ломоносова и Международный институт сотрудничества Восток - Запад (США). Доклад «Исследования в направлении снижения рисков компьютерных атак на невоенные ядерные объекты» был доложен на конференции в Мюнхене. Исследование проблемы обеспечения стабильности, устойчивости и безопасности Интернета было выполнено институтом проблем информационной безопасности вместе с компанией «Айтел». Совместная работа участников консорциума «Сравнение национальных практик по

фильтрации контента в Интернете» была проведена и доложена на заседании в Азербайджане, в Баку.

Консорциумом разработан и принят перечень приоритетных направлений исследовательских проектов. По итогам трехсторонней встречи экспертов консорциума Китай - Россия - США, которая состоялась в Пекине в ноябре 2015 года, были подготовлены предложения по организации исследований по четырем новым направлениям, которые планируются рассмотреть на предстоящем заседании консорциума 27 апреля.

За прошедшие десять лет форум стал заметным международным явлением. Интерес к нему непрерывно растет. По сообщению Оргкомитета десятого форума, на нем зарегистрировано 105 человек из 13 стран. На обсуждение участникам вынесены весьма важные и сложные вопросы формирования системы международной информационной безопасности, способной парировать угрозы использования ИКТ для нарушения международного мира и безопасности.

Во-первых, это проблемы толкования основных понятий, принципов и норм Женевских конвенций, применимых к киберпространству. В рамках обсуждения данной проблемы на «круглом столе» предполагается рассмотреть: понятие «ИКТ» как средство ведения военных действий, атрибуцию субъектов вооруженных конфликтов в сфере ИКТ, обозначение объектов и субъектов сферы ИКТ, защищаемых международным правом, комботанты вооруженных конфликтов в сфере ИКТ, права человека в ходе вооруженных конфликтов в сфере ИКТ.

Мы уже обращались к этим вопросам, однако считать их решенными у нас нет никаких оснований. На прошлогоднем заседании форума мы отмечали, что рассматриваем проблемы, связанные не столько с вопросами или противоречиями в международном праве, сколько с новизной в области военных действий, соответственно, с неопределенностью трактовок существующих норм международного гуманитарного права применительно к условиям сферы ИКТ. Требуют развития нормы международного процессуального права, регулирующие отношения в области опознавания гражданских объектов сферы ИКТ, выявления неправомерного применения к ним вредоносных ИКТ противоборствующими сторонами.

Стало понятно, что в условиях глобального общества необходимо определиться и с возможными ограничениями прав человека в сфере ИКТ государствами, участвующими в вооруженных конфликтах. В данном контексте хотелось бы затронуть проблему идентификации объектов киберпространства, защищаемых международным гуманитарным правом. Так, положение 1 к дополнительному протоколу к Женевским конвенциям от 12 августа 1949 года относительно защиты жертв международных вооруженных конфликтов полностью посвящено правилам, касающимся опознавания. Видимо, применение норм данного протокола к условиям киберпространства также потребует отдельного приложения, посвященного правилам опознавания защищаемых объектов.

Сложной проблемой, пока, как нам кажется, не имеющей приемлемого решения, является подготовка объективных документов по фактам нарушения норм международного права в киберпространстве. Мы надеемся, что в ходе работы «круглого стола» будут высказаны идеи, позволяющие объединить усилия всех заинтересованных сторон в данной области.

Второй важной проблемой, выносимой на обсуждение форума, является нераспространение кибероружия и уменьшение опасности его использования. Обсуждению этой проблемы также будет посвящен отдельный «круглый стол». В рамках его работы предполагается рассмотреть следующие вопросы: содержание понятий «информационное оружие» и «кибероружие», договоренность как элемент режима нераспространения информационного оружия, возможные принципы построения режима нераспространения информационного оружия, система международной информационной безопасности как средство предотвращения международных конфликтов, которые могут возникнуть в результате агрессивного применения информационного оружия.

Необходимость разрешения поставленных вопросов с каждым годом становится все более актуальной. Сегодня киберпространство объявлено пятым театром военных действий и целый ряд стран уже разрабатывают для него специализированные средства ИКТ. Вместе с тем Генеральная Ассамблея ООН в 2015 году приняла доклад Группы правительственных экспертов, в котором призывают все государства «способствовать обеспечению открытой, безопасной, ста-

бильной, доступной и мирной ИКТ-среды». В нашем понимании «мирность» ИКТ-среды, в соответствии с Уставом ООН, означает использование государствами потенциала ИКТ-среды для мирного решения международных споров таким образом, чтобы не подвергать угрозе международный мир, безопасность и справедливость, неиспользование государствами потенциала ИКТ-среды для угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, не совместимым с целями ООН.

Третьей важной проблемой, вынесенной на обсуждение участников форума, является определение механизма и инструментов частно-государственного партнерства в области размещения информационной безопасности критически важных объектов. В рамках работы соответствующего «круглого стола» предполагается обсудить вопросы: определение понятия «инцидент» в сфере критически важной инфраструктуры и методов его описания для проведения национального или международного исследования; механизмы взаимодействия частного бизнеса и государства в области совершенствования законодательства, регулирующего отношения в области обеспечения информационной безопасности объектов критически важных инфраструктур; сотрудничество организаций частного бизнеса различных государств по вопросам обеспечения информационной безопасности.

Четвертой проблемой, вынесенной на обсуждение участников конференции, являются меры противодействия интернет-рекрутингу и интернет-пропаганде экстремизма и терроризма. В рамках данной проблемы предполагается обсудить возможные международно-правовые и политические инициативы использования интернет-рекрутинга и интернет-пропаганды, а также лучшие национальные и гуманитарные практики противодействия этим явлениям, проблему научно-технологического обеспечения работ по выявлению деструктивного контента и его источников.

По существу, в рамках данного форума будут анализироваться факторы, определяющие как настоящее, так и будущее гуманитарной составляющей по проблематике международной информационной безопасности. Отдельный «круглый стол» запланировано посвятить обсуждению общих проблем современных международных отношений в контексте киберпространства. Это заседание мы

проведем совместно с авторитетным в России и мире журналом «Международная жизнь», который выпускается под эгидой Министерства иностранных дел Российской Федерации, издается на шести языках ООН и распространяется по всему миру.

Приветствие организаторам, участникам и гостям Десятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» Сергея Буравлева, заместителя секретаря Совета безопасности РФ

Уважаемые коллеги, позвольте приветствовать организаторов, участников и гостей Десятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Ставшие уже традиционными в баварском Гармиш-Партенкирхене апрельские встречи представителей государственных структур, научного, экспертного и бизнес-сообществ, посвященные проблематике борьбы с угрозами в информационной сфере, приковывают внимание специалистов в области информационной безопасности во всем мире. Десятый раз политики, известные ученые, эксперты научных и образовательных центров, различных международных организаций из 13 стран мира примут участие в работе форума.

В этом году повестка дня включает важные вопросы с точки зрения обеспечения безопасности, столь чувствительной области жизнедеятельности, какой на сегодняшний день является информационная сфера. Актуализация заявленных для дискуссии проблем - это не дань моде, а насущная потребность в качестве новых, научно обоснованных подходов и решений, способных оказать реальную помощь государству и бизнесу в обеспечении информационной безопасности в условиях нарастания новых вызовов и угроз, с учетом их трансграничного характера.

Традиционно повестка дня форума, его пленарных заседаний и «круглых столов» ориентирована на обсуждение актуальных задач обеспечения безопасности в информационной сфере. Комплексный подход к всестороннему рассмотрению основных проблемных вопросов в формировании системы международной информационной безопасности давно стал визитной карточкой конференций в Гармиш-Партенкирхене. Полагаю, что в центре

внимания участников встречи будет обсуждение проблем международного правового регулирования сферы использования информационных и коммуникационных технологий, а также перспектив установления режима нераспространения информационного оружия и принятия правил ответственного поведения государств в информационной сфере.

Итогом встречи в Гармиш-Партенкирхене должно стать определение приоритетных направлений совершенствования системы международной информационной безопасности. Желаю успешной и плодотворной работы.

Приветствие организаторам, участникам и гостям Десятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» Виктора Садовничего, ректора МГУ им. М.В.Ломоносова

Уважаемые коллеги, позвольте мне от лица многотысячного коллектива Московского государственного университета приветствовать вас в связи с открытием Десятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Вот уже десятый год подряд МГУ приглашает ученых, политиков, представителей международного экспертного сообщества к обсуждению важнейших проблем международной информационной безопасности. Спектр этих проблем непрерывно расширяется. Безусловно, выдающиеся свершения в сфере развития информационных технологий меняют в жизни все, включая нас самих. Информационные технологии превратились в мощный фактор общественного развития, обусловивший существенное усиление зависимости человека, общества и государства от устойчивого функционирования информационной инфраструктуры.

В этом контексте трудно переоценить важность выработки совместных действий по обеспечению международной информационной безопасности. Мне, как ректору крупнейшего в России университета, особенно приятно отметить, что в рамках форума крепнет и развивается сотрудничество с нашими давними партнерами: Университетом штата Нью-Йорк, Китайским народным обществом дружбы с зарубежными странами, Университетом Корё

(Республика Корея), Евразийским национальным университетом им. Л.Н.Гумилёва (Казахстан) и другими нашими международными партнерами. Желаю участникам форума плодотворной работы и достижения значимых результатов.

Андрей Крутских, специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, профессор

Значимость рассматриваемой проблематики информационной безопасности и интерес к ней в Москве, Вашингтоне, Пекине, Лондоне, да где угодно, обуславливается острейшим политическим противоборством, которое разворачивается на международной арене с использованием информационно-коммуникационных технологий. Уступить в этом противоборстве, идущем по всем направлениям, ни один, по крайней мере, из основных игроков позволить себе не может. Соответственно и отношение России к этой теме.

Кибертехнологии, как в свое время ядерные технологии, определяют не только развитие, но всю суть национальной безопасности в третьем тысячелетии. Поэтому Президент В.В.Путин держит эту тему под личным, непосредственным контролем. Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности определено руководством страны как одно из важнейших, приоритетных, стратегических направлений внешнеполитической деятельности. Россия сделает все, чтобы не уступить и не проиграть киберсоревнование.

Ответственно могу сказать, что общая ситуация в глобальном информационном, или, как говорят наши партнеры, киберпространстве пока имеет тенденцию к ухудшению. А в свете известных региональных событий - даже к обострению. Если позволить себе рассуждать с теоретической точки зрения, то я бы определил геополитическое состояние современного мира, в силу специфики революции в области ИКТ и методов их использования, ужасным словом «мировойна» или «Peace for the War». Можно сказать и проще - «мир и война в одном стакане». Причем эта «мировойна» не является виртуальной. Она наносит реальный ущерб и ведется,

прекрасно сочетаясь с сохранением дипломатических отношений. В целом ситуация ужасная и весьма лицемерная.

Растет число компьютерных атак. Президент РФ В.В.Путин еще два года назад говорил о том, что в 2014 году на российские интернет-ресурсы было совершено 74 млн. атак. В 2015 году чуть меньше, но количество ежегодных кибератак не становится меньше 70 миллионов. Примерно также, если не хуже, обстоят дела между США и Китаем.

Жесткая конфронтация ведется и на других этажах международных отношений. Это относится и к малым странам, зависимым как от основных игроков, так и беспредела, который творят криминальные элементы и террористы. Ущерб, наносимый хакерскими атаками, составляет астрономическую сумму. Мировая статистика на этот счет просто зашкаливает. Цифры реального ущерба колеблются в районе 3 трлн. долларов в год. Технология атак становится, с одной стороны, все более изощренной, а с другой - доступной даже для непрофессионалов. На качество и мощь кибератак Москва не может не обращать внимания, мы видим все подобные атаки. Наши технологические возможности позволяют это.

Резонансной террористической акцией недавнего времени можно назвать удар по французскому медиаконцерну «Монд». Его можно расценивать, и мы едины в этом с американскими коллегами, как репетицию мощнейшей террористической вылазки в Париже. Москву не то чтобы удивила, а привлекла интерес оценка директора ФБР США, который заявил, что французские силовики были просто ослеплены («they were dazzled blinded»). А те, кто отвечает за национальную кибербезопасность, дезориентированы. Еще хуже примеры недавних событий в Бельгии, где преступники имели полную киберсвободу, нападения на промышленные объекты «Круппа» в Германии, нападение, весьма успешное, на польский парламент.

Может, это звучит странно, но нет худа без добра. Подобные действия, масштабы вредоносного использования ИКТ серьезно встряхнули и напугали мир, лишили иллюзий. Наши оппоненты стали восприимчивее к нашим предупреждениям, логике понимания развития событий. Нас стали слушать более внимательно, не как дилетантов, стали разделяться некоторые из наших подходов к обеспечению информационной безопасности.

Растет осознание того факта, что созданные блоковые защитные «киберзонтики» либо слишком дырявы, либо, как в Москве начинают думать, не рассчитаны на обеспечение реальной информационной безопасности младших партнеров. Ни один из упомянутых мной - а имеется масса других - крупных инцидентов в западном мире не удалось ни предотвратить, ни предупредить с помощью отстроенной за немалые деньги совместно с Вашингтоном системы информационной безопасности. Как показали наши консультации с американцами, США признают свою киберуязвимость. Мы тоже говорим о своей киберуязвимости. И это честное признание реальности киберуязвимости, мне кажется, очень важно.

Все это объективно способствует усилению в международном сообществе настроений в пользу того, чтобы договариваться. В пользу этого свидетельствуют и доклад 2015 года Группы правительственных экспертов, и резолюция Генеральной Ассамблеи по информационной безопасности, соавторами которой выступили 84 государства. Отдельно стоит обратить внимание на российско-американские переговоры в Женеве, куда съехалось по шесть заместителей министров в сфере информационной безопасности с обеих сторон, несколько десятков экспертов. Два дня шел интересный прагматичный разговор обо всех аспектах обеспечения информационной безопасности, взаимодействии на международных форумах, совместной борьбе с терроризмом. Речь идет не просто о мерах российско-американского доверия и предупреждения друг друга, а Россия выдвинула идею выработки договоренностей, связанных с предотвращением инцидентов в этой сфере. Как вы понимаете, это новое качественное движение вперед.

Особо хочу остановиться на вопросе, связанном с выработкой и принятием, без этого просто нельзя, универсального международного режима, регулирующего деятельность государств в глобальном информационном пространстве, кодекса ответственного поведения государств в информационном пространстве. Основной площадкой для выработки такого кодекса станет Группа правительственных экспертов ООН по международной информационной безопасности. Группа выступает в новом революционном качестве, поскольку впервые в истории ООН ее пришлось расширить до 25 пяти стран, стандарт был 15. Многие страны хотят участвовать в этой груп-

пе, потому что будут вырабатываться правила поведения. Как говорил заместитель Генерального секретаря ООН: «Больше 60 стран подали заявки, и 45 стран на уровне министров иностранных дел лавируют перед Генеральным секретарем ООН, чтобы их страну включили».

Когда эта группа только организовывалась, Россия как страна - инициатор резолюции довела до сведения Генерального секретаря ООН свое мнение, что при формировании ее состава, возможно впервые, нужно дополнить принцип справедливого географического представительства принципом, чтобы в группе участвовали все основные игроки в информационном пространстве. Для России было бы странно не увидеть Германию в этой группе, а так вопрос стоял, странно не увидеть Японию или Израиль. Обнадеживает ситуацию то, что есть общее понимание проблемы.

Но противоречия, к сожалению, сохраняются очень серьезные. Главным образом они методологически связаны с содержанием самих правил поведения. Наши западные партнеры воспринимают эти правила в основном в виде мер укрепления доверия и программ так называемого наращивания потенциала, рассматривают правила в максимально необязывающем виде. Одновременно звучат предложения принять некие нормы для мирного времени и отдельно - для военного, которые, по-видимому, будут по-разному работать. Сами правила предлагается наполнить в основном техническими по смыслу договоренностями.

Для нас - не скажу сразу, что это неприемлемо, но это не то, что мы хотим видеть. При таком подходе размывается смысл целеполагания, принятия правил, а именно предотвращение конфликтов. Нам нужно мирное, стабильное, глобальное информационное киберпространство. А если мы сосредоточим свои усилия на выработке правил ведения конфликтов, то это либо развяжет руки для экспансии в отношении малых стран, либо приведет к третьей мировой войне в отношении главных игроков в стратегическом мировом пространстве.

Что же вселяет оптимизм?

В общем, удается более-менее выработать определенные параметры правил поведения. Большой вклад в это внесла Группа правительственных экспертов в 2010, 2013 и 2015 годах. Разработан целый перечень очень важных положений, которые

могут составить основу будущих правил поведения. Это принципиальнейшие вещи. Первое - ИКТ должны использоваться исключительно в мирных целях, а международное сотрудничество необходимо направить на предотвращение конфликтов в информационном пространстве.

Во-вторых, в цифровой сфере действуют такие общепризнанные международно-правовые принципы, как неприменение силы или угрозы силой, уважение суверенитета, невмешательство во внутренние дела государства. С учетом уникальных особенностей ИКТ могут вырабатываться дополнительные правовые нормы для регулирования международных отношений. Государства обладают суверенитетом над информационно-коммуникационной инфраструктурой на своей территории. А если суверенитет, то, соответственно, ответственность. Любые обвинения в адрес государств в причастности к кибератакам должны быть подкреплены доказательствами, а не просто так каждый президент, особенно сильной державы, объявляет сразу кого-то преступником, не утруждая себя доказательствами.

Государства не должны использовать посредников для осуществления кибератак и не допускать того, чтобы их территория использовалась в этих целях, для враждебных целей против третьих стран. Это принципиально, потому что в противном случае мы можем быть жертвами непреднамеренных атак, совершаемых через третьи территории.

Мы сформулировали определенные параметры будущих правил, принципов или норм ответственного поведения государств.

Первое - это универсальность. Правила должны быть выработаны под эгидой ООН. Если идти по пути выработки региональных, так сказать «местечковых», правил, есть риск того, что они в рамках различных организаций будут противоречить друг другу и давать возможность осуществлять нападение через третьи страны. Чтобы это перекрыть надежно, должна быть единая система правил. Нельзя допустить того, чтобы информационное глобальное пространство раскололось на инфоальянсы, потому что отношения между ними могут в любой момент стать конфронтационными и тогда рухнет вся эта система.

Второе - это миротворческий характер. Правила должны распространить на информационное пространство действие

принципов неприменения силы, уважения государственного суверенитета, невмешательства во внутренние дела. В этом основной смысл - не воевать в киберпространстве, не поражать друг друга киберсредствами, а предотвращать это. Правила должны отображать принципы неконфронтационного взаимодействия в информационной сфере и содержать однозначно не допускающее двойное толкование недопустимых действий. Нужно выработать общие понятия в этой сфере. Необходимо, чтобы правила закрепляли обязанности государств не совершать подобные противоправные действия ни напрямую, ни через посредников.

Третье - это государствоцентричность. Запад долго в этом отношении испытывал недоверие к России, хотя напрасно. Правила должны быть нацелены на формирование такой модели взаимоотношений в информационном пространстве, в рамках которой будут четко определены обязанности всех участников. В настоящее время в информационной сфере, наряду с государствами, действует множество игроков. Их влияние на процессы весьма ощутимо. Мотивация этих игроков разнообразна и включает в себя интересы коммерческого, научного, любого другого характера. Важно, чтобы каждый актер не только играл свою роль и вносил свой вклад, но и имел соответствующие обязанности. Ведущая роль при этом должна оставаться за государством. Этот постулат уже подтвержден в прошлом году в итоговом докладе группы.

Четвертое - рамочный характер. Правила должны быть рамочными, политическими договоренностями, а не техническими мерами. Они должны образовать международно-правовой реальный защитный «зонтик», под которым должны приниматься более узкие специальные меры. Наряду с базовыми принципами неконфронтационного взаимодействия государств в информационном пространстве, правила, на наш взгляд, просто обязаны охватывать такие вопросы, как укрепление доверия в информационном пространстве, наращивание потенциала.

На передний план выходит защита прав человека в информационной сфере. В последнее время складывается впечатление, что тема прав человека - известный козырь Запада - исчезла в свете развития кибертехнологий. Никакой частной жизни больше в мире нет. Люди предпочитают безопасность частной жиз-

ни правам человека. Так не должно быть, надо восстановить тему прав человека.

Важно ориентировать политику государств в отношении программных уязвимостей. Государства не должны использовать или оказывать давление на коммерческие компании, с тем чтобы те встраивали скрытые вредоносные функции (harmful hidden functions) в свои коммерческие продукты.

Пятое - это постоянное действие. Правила должны действовать постоянно. Принятие отдельных норм для мирного времени или отдельных - для военного, на наш взгляд, девальвирует саму идею правил поведения. Как отличить мирное время от военного, когда в международном праве нет определения не просто киберагрессии, а вообще слова «агрессия», нет определения, что такое кибероружие?

Границы в киберпространстве должны быть четкими и не допускать лазеек. Несмотря на то что правила относятся к так называемому «мягкому праву», не должно складываться впечатления, что их безнаказанно можно нарушать.

По инициативе российских военных, мы, дипломаты, пытаемся привлечь внимание еще к одной проблеме. Решая проблему адаптации развития правового регулирования сферы использования ИКТ, международному сообществу потребуется озаботиться еще одной исключительно важной проблемой. Это обеспечение технической возможности оперативной и достоверной идентификации источников компьютерных атак и определение их мотиваций, а также условий преодоления анонимности вредоносных действий в информационном пространстве. Длительные годы приходилось слышать, что это несбыточно, фантастично, что этого не может быть, потому что это технически нерешаемо. Есть деликатная проблема: увидеть-то мы можем, но мы не хотим раскрывать свои способности и возможности. А ведь надо не просто увидеть, надо сделать это публичным и иметь возможность это доказать.

В заключение хочу отметить, что в целом на поприще обеспечения международной информационной безопасности предстоит серьезная, масштабная, ответственная работа. Еще раз подчеркну, что есть тяга международного сообщества договориться, поэтому обращаюсь ко всем своим коллегам

с просьбой не позволить нам упустить возможность получить Нобелевскую премию мира.

Игорь Дылевский*, начальник управления Генерального штаба РФ, генерал-майор

Уважаемые коллеги! По нашим оценкам, угроза возникновения военных конфликтов в результате агрессивного или иного враждебного использования информации и современных информационно-коммуникационных технологий в последнее время существенно обострилась.

Она существует не только в воображении военных теоретиков, которые разрабатывают апокалипсические сценарии «мировой информационной войны». В архивы уже вписаны имена целого ряда военных конфликтов, в которых ИКТ широко использовались для их развязывания и последующей эскалации.

Обратите внимание на то, как мировые СМИ отреагировали на операцию российских ВКС в Сирии. Как только по просьбе законного правительства Сирии она началась, на нашу страну обрушилась массированная пропагандистская атака. Некоторые публичные высказывания высоких должностных лиц ряда стран дают основания полагать, что ложь и искажение фактов стали основой их политической позиции. Покатился вал бесконечных обвинений российской стороны в «бомбежках жилых кварталов» и «гибели мирных жителей». Леденящие душу постановочные кадры заполонили Интернет и телевидение. В итоге мировое общественное мнение и сознание мировых политико-формирующих кругов постепенно стало дрейфовать в направлении «осознания» неотвратимости очередной крупной войны.

Следует отметить, что подобные методы пропаганды ранее неоднократно применялись в периоды военного обострения израильско-палестинского конфликта.

Возникает вопрос: как долго человечество будет мириться с тем, что безнаказанная ложь, распространяемая благодаря современным ИКТ по всему миру со скоростью света, ведет к различного рода междоусобицам, развязыванию агрессивных войн,

*Выступление подготовлено авторским коллективом в составе: Дылевский И.Н., Запивахин В.О., Комов С.А., Кривченко А.А.

массовой гибели ни в чем не повинных граждан, миграционной катастрофе, гибели целых государств, разрушению вековых ценностей мировой культуры?

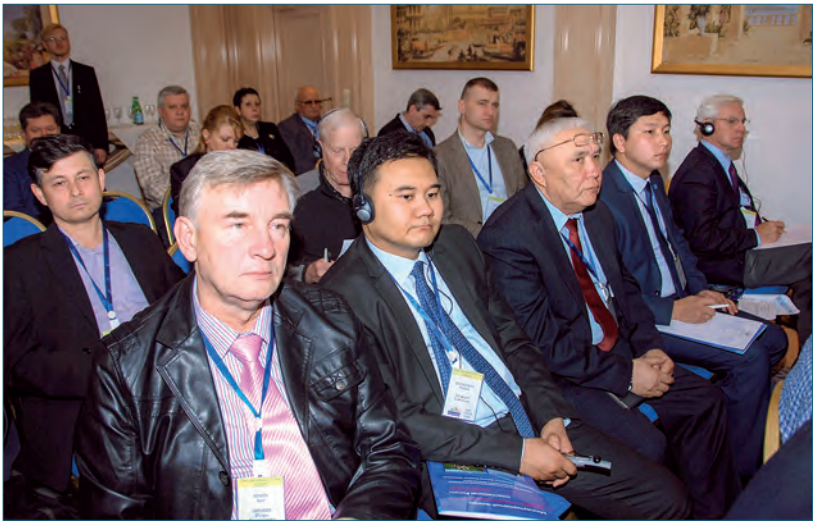
Мы знаем, что этот вопрос волнует не только нас. Например, США и их союзники также озабочены усилением угрозы возникновения военных конфликтов вследствие враждебного использования ИКТ. НАТО к своему июльскому саммиту в Варшаве готовит новую стратегию, призванную повысить эффективность реагирования на нетрадиционные угрозы, в том числе и угрозу информационной войны. При этом наиболее действенным ответом на нее считается метод «сдерживания» геополитических соперников, основанный на демонстрации, а при необходимости и применении военной силы в информационном пространстве.

Полагаем, что реагирование военной силой на какие-либо реальные или мнимые информационные угрозы может серьезно дестабилизировать ситуацию во всем мире. Слишком много соблазнов «поиграть мускулами» в условиях, когда ежедневно и ежечасно неисчислимое множество компьютерных атак обрушивается на информационную инфраструктуру, а потоки экстремистских идей - на головы простых граждан.

К тому же в очередной раз хочется напомнить, что даже воля 28 стран - членов НАТО не может узаконить применение статьи 51 Устава ООН (право на самооборону) в отношении угроз, исходящих из информационного пространства.

Для этого нужен глобальный консенсус, достичь которого можно только путем формирования *всеобъемлющей системы безопасности*, как это было сделано в конце 80-х годов прошлого века.

В те непростые годы большинство государств - членов ООН пришло к пониманию того, что обеспечение всеобъемлющей безопасности возможно лишь на основе соблюдения *общепризнанных принципов международного права* (уважения суверенитета, политической независимости и территориальной целостности государств, отказа от интервенции и вмешательства во внутренние дела, неприменения силы или угрозы силой, мирного урегулирования споров, равноправия и самоопределения народов, уважения прав человека и основных свобод, сотрудничества между государствами, добросовестного соблюдения принятых ими обязательств в соответствии с Уставом ООН).



При этом *механизм коллективной безопасности,* воплощенный в Уставе ООН, был признан фундаментальным и незаменимым инструментом для сохранения международного мира и безопасности. Эффективное функционирование этого механизма должно дополняться усилиями государств мирового сообщества по всемерному ограничению гонки вооружений и снижению уровня военного противостояния.

В свою очередь, решение этих задач немыслимо без *укрепления доверия* между государствами на основе преодоления конфронтационных подходов, укрепления норм цивилизованного поведения и атмосферы гласности и открытости в международных отношениях. И, наконец, всеобщей безопасности не может быть без *обеспечения стабильного и справедливого международного климата* во всех областях сотрудничества (экономике, финансах, торговле, экологии и др.).

Представляется, что, опираясь на этот багаж, мировому сообществу следует принять *универсальные правила предотвращения военных конфликтов,* которые могут возникать вследствие враждебного использования информации и ИКТ. Кроме того, необходимо установить *международную ответственность* за нарушение этих правил и незыблемо их соблюдать.

Ни одно должностное лицо органов государственной власти всех стран мира не должно распространять с использованием ИКТ непроверенную, а тем более лживую информацию, кото-

рая затрагивает национальную гордость других народов, а также честь и достоинство руководства зарубежных государств, подрывает уважение к государственному суверенитету, позволяет влиять на внутренние дела других государств. За эти деяния должна быть предусмотрена строгая международная ответственность, а руководство суверенных государств обязано твердо следовать этим правилам. Такая же ответственность должна налагаться и на тех, кто использует ИКТ для трансграничного воздействия на критически важные инфраструктуры и другие социально-значимые информационные объекты.

В отношении возможных правил предотвращения военных конфликтов, которые могут возникнуть в результате враждебного использования информации и ИКТ, на наш взгляд, должны выполняться определенные требования.

Во-первых, до принятия правил необходимо выработать единый общепризнанный международный словарь терминов и определений в области их юрисдикции. К таким терминам, ждущим своего определения, например, относятся «информационный инцидент», «информационное нападение», «информационная война» и др. Полагаем, что в международном праве, регулирующем вопросы войны и мира в информационной сфере, каждый термин должен быть понятен, прозрачен, иметь единообразное понимание и единообразно понимаемые критерии.

Во-вторых, новые правила должны иметь одинаковую юридическую силу с нормами и принципами существующего международного права, регулирующего вопросы войны и мира. Недопустимо, чтобы какому-нибудь юному хакеру на основе косвенных улик правоохранительные органы соседнего государства вменяли совершение преступления против мира и безопасности человечества за то, что он по своей глупости заблокировал работу органов государственного управления в этой стране. И в это же время глава государства, по указанию которого осуществляется массированная компьютерная атака на коммерческие банки соседней державы, не нес за это никакой международной ответственности. Предусмотренные на этот счет американские санкции во исполнение соответствующего указа Президента США Б.Обамы не в счет. Российская Федерация

не поддерживает санкционную политику в принципе и считает санкции, принятые в обход ООН, противоречащими международному праву.

В-третьих, правила существующего международного права должны быть адаптированы к специфике информационного пространства. По этому поводу в последнее время ведется бурная дискуссия с нашими западными партнерами во главе с США на всех международных площадках и форумах. Они призывают признать автоматическую применимость норм и принципов международного права к регулированию военного использования информационно-коммуникационных технологий. В первую очередь, по их мнению, это относится к возможности применения военной силы в ответ на трансграничное информационное воздействие, опираясь на положения статьи 51 Устава ООН (о праве на самооборону) и статьи 5 Вашингтонского договора (о коллективном реагировании на агрессию в отношении какого-либо члена НАТО).

Российская позиция состоит в том, что, не отрицая незыблемость права на самооборону, необходимо провести большую работу по созданию международно-правовой базы, с использованием которой можно будет адекватно осуществлять его реализацию применительно к специфике информационной сферы. В ее состав должны войти:

- универсальные критерии отнесения различного типа информационных воздействий к актам агрессии (вооруженного нападения);

- методология организационно-правового и технологического характера, предназначенная для регламентации процессов выявления и достоверной идентификации источников информационных воздействий;

- процессуальные нормы, регламентирующие порядок расследования фактов проведения информационных воздействий, включая методику сбора доказательной базы, позволяющей предъявить обвинение виновным лицам в осуществлении акта агрессии с использованием ИКТ.

Убеждены, что первым шагом на пути формирования правил предотвращения военных конфликтов, которые могут возникнуть в результате враждебного использования ин-

формации и ИКТ, являются «Правила поведения государств в области международной информационной безопасности», разработанные государствами - членами Шанхайской организации сотрудничества и вынесенные на рассмотрение 69 сессии Генеральной Ассамблеи ООН.

Они развивают и дополняют концепцию всеобъемлющей международной безопасности применительно к информационной сфере и создают хороший задел для последующего формирования всеобщей системы международной информационной безопасности.

Ее основу могут составить региональные системы международной безопасности, создаваемые на пространстве Содружества независимых государств, Организации Договора о коллективной безопасности и Шанхайской организации сотрудничества.

Полагаем, что эти международные форматы, в силу их привлекательности для развивающихся стран и равноправной основы сотрудничества, будут выступать гарантами мира, основанного на твердом соблюдении правил предотвращения военных конфликтов, развивающих общепризнанные принципы международного права применительно к специфике глобального информационного пространства.

Мы призываем наших западных коллег внимательно рассмотреть наши предложения и присоединиться к ним.

Алексей Солдатов, председатель Совета Фонда развития Интернет

Система - это сеть Интернет. Все информационные технологии, может быть за очень редким исключением, включают в себя использование Интернета. Поэтому, на мой взгляд, очень важно, чтобы этот инструмент был доступен всем.

Что такое критическо-информационная инфраструктура? В США тоже есть определение критической инфраструктуры, это то, что может оказывать пагубное влияние на национальную, экономическую безопасность, здоровье и т. д. Звучит тоже довольно обобщенно, по крайней мере к ней относятся финансовый, банковский секторы, телекоммуникационные средства. В России издан документ, в который

включены объекты государственного управления, финансово-кредитной, информационной, телекоммуникационной инфраструктур и др.

Какие определения есть в мире? Мы отыскали 40 определений критической инфраструктуры - четыре интернациональных и 36 национальных. Дальше их можно классифицировать: что больше понравилось, что меньше. Нет единых четко выработанных критериев, но видно, что, прямо скажу, все идут порознь - как понимают, так и пишут. Хочу напомнить, что Интернет - все-таки глобальный инструмент, а подход к нему различный. И это опасно.

Попробуем конкретизировать: что же такое критическая инфраструктура глобального Интернета? Есть три очевидные вещи - это каналы передачи данных, корневые серверы и маршрутизация. Хочу подчеркнуть, что, конечно же, сюда можно прибавить и обмен трафиком, и платежные системы, потому что если они перестанут работать, то все встанет.

Моя цель - убедить вас, уважаемые коллеги, что есть абсолютно конкретное дело, в продвижении которого заинтересованы абсолютно все присутствующие здесь, - чтобы Интернет во всем мире работал. Вот это крайне важно.

Какие встречаются угрозы? Несанкционированное внесение изменений в корневую зону. Это отсутствие хоста. Некоторые авторы именуют это как прекращение предоставления услуг сервиса. Каналы передачи данных могут рваться. Очень важно, когда каналы работают. Еще один момент: каналы бывают наземные, спутниковые и т. д. Всем предельно ясно значение маршрутизации. В основном борьба с угрозами осуществляется дублированием.

Чем бы хотелось закончить? Первое - сеть Интернет стала сама по себе критическим элементом в инфраструктуре. Второе - если это глобальная система, то необходимы согласованные действия. Третье - это то, что бывает всегда с новыми технологиями: международные соглашения, законы, определения правил всегда опаздывают. Это нужно учитывать и стараться продуцировать документы с нужной скоростью. Понимаю, что будет опоздание, но пусть будет на день, а не на пять лет.

Михаил Якушев, вице-президент корпорации «ICANN» по Восточной Европе и Средней Азии

Вкратце расскажу о том, какие в настоящий момент происходят изменения в корпорации «ICANN» и как они могут повлиять позитивным образом на вопросы информационной безопасности. Моя главная задача - пробудить в вас интерес к тому, что я говорю.

Когда мы говорим об Интернете, то имеем в виду как минимум три разных момента, как достаточно подробно было изложено в выступлении предыдущего докладчика, что есть разные критические элементы в той инфраструктуре, которую мы называем Интернетом. Существует нижний уровень - это железо, физика, каналы связи. Дальше идет уровень логический, где, собственно, размещен Интернет, «ICANN» и его функции. И, наконец, верхний уровень - это социально-экономический, где оказываются те услуги, которые делают Интернет Интернетом. То есть мы отвечаем за промежуточный уровень, который позволяет каналы связи, линии связи объединять в единую сеть и с их помощью оказывать услуги более высокого уровня.

И еще одна тема. То, чем занимается «ICANN» - как организация, распределяющая адреса и нумерации, - это обеспечение доверия между всеми участниками системы. Интернет начинался как доверенная среда. Соответственно, исходим из того, что основа всех социальных институтов - доверие - это ровно то, чем мы должны заниматься. Хотелось бы проиллюстрировать, каким образом вопросы доверия укрепляются в ходе самого важного проекта этого года, который реализуется нашей корпорацией «ICANN» и называется «Передача контролирующей функции от правительства США». Вот три основных направления, по которым «ICANN» осуществляет регулирование характеристической инфраструктуры. Это технические параметры протоколов автономных систем. То есть то, что с технической стороны делает Интернет Интернетом. Во-вторых, администрирование системы корневых серверов DNS. Это те доменные номера, когда после точки пишется «.ru», «.de», «.com» и т. д., а также многочисленные интернационализированные доменные номера, которые написаны кириллицей, по-арабски, по-китайски и т. д.

И, наконец, распределение IP-адресов Интернета, которое мы осуществляем вместе с пятью региональными регистратурами. Делается это, разумеется, не в одиночку, мы этим занимаемся в глобальном сообществе, где огромное количество разных заинтересованных лиц. У каждого из них есть и свои права, и обязанности, и функции. Все вместе взятое - достаточно сложная система, но которая тем не менее обеспечивает ее устойчивость.

Два года назад правительство США заявило о своей готовности отказаться от последней координирующей роли, которая у нее до сих пор существует в отношении контроля за «ICANN», а именно: утверждение изменений в корневые файлы. Алексей Анатольевич сказал, что возможность несанкционированного внесения файла действительно представляет собой максимальную угрозу информационной безопасности. В этой связи существует многоступенчатая система контроля за тем, как эти изменения вносятся на глобальном уровне. И если речь идет просто об изменении, скажем, телефонного номера администратора домена, то это делается по достаточно простой процедуре, где проверяется, насколько тот человек, который себя заявляет администратором и вносит изменения информации о себе, реально таковой и есть. Если же речь идет о перелегировании домена, о создании новых доменов, а сейчас новых доменов будет уже почти 2 тыс., то это совершенно другой ландшафт, совершенно другая картина Интернета.

Так вот, до настоящего момента любые изменения, которые корпорация «ICANN» предлагает в корневых файлах, утверждаются Министерством торговли США. Что и позволяет формально говорить о том, что глобально эти функции находятся под контролем правительства США, но за все годы существования нашей корпорации никаких в этом плане конфликтов или отказов утверждения изменений в корневую зону не происходило, что и означает, что корпорация выполняет свои функции адекватно.

Соединенные Штаты, в частности американское правительство, заявили о готовности отказаться от этой функции. Был установлен ряд ограничений или требований к тому, как это может быть. Во-первых, данный процесс должен быть

одобрен всеми, то есть он не должен противоречить чьим-то интересам. Безопасность корневых функций Интернета должна быть сохранена. Один из важных факторов состоит в том, что американское правительство категорически отказалось передать эти контролирующие функции какому-либо другому правительству или межправительственным организациям ровно по тем причинам, по которым критикуют правительство США за такую роль, которая здесь является якобы доминирующей.

Соответственно, в процессе обсуждения того, каким должен быть будущий механизм этого контроля, выяснилось еще одно очень важное обстоятельство. Недостаточно просто разработать предложение по изменению структуры управления. Очень важно также подумать о том, как теперь и перед кем будет отчитываться, условно говоря, «ICANN». Формально можно сказать, что до настоящего момента идет отчетность перед правительством США. Когда исчезает из системы этот орган, то как мы можем быть прозрачными, подотчетными всему глобальному международному сообществу?

В связи с этим можно говорить о подотчетности и прозрачности управления. Предложения состояли из двух частей. Процесс был достаточно сложный. Он продолжался почти два года. Здесь приведена некоторая статистика. Были десятки тысяч разного рода обсуждений, предложений, встреч, телефонных конференций и тому подобное. Вследствие чего были скомпонованы предложения от трех направлений, трех источников, о которых уже упоминалось. Это - сообщество доменных имен, сообщество сетевых адресов и сообщество технических протоколов, параметров портов и т. д.

Сообщество доменных имен предложило следующее. Когда такая функция уйдет, создать новое юридическое лицо, новую организацию, которая пока еще не имеет своего названия. Она будет выполнять технические функции, контролировать организации, рабочие группы со всех стран мира. То есть система чуточку усложняется, исчезает верхняя надстройка, которой была NTIA - подразделение правительства США.

Что касается предложения сообществ ресурсов нумерации - пяти региональных центров, которые распределяют по всему миру сетевые адреса, - то их предложение было следующим. Они, понимая, что исчезает надстройка, которая в этом смысле занималась именно распределением адресов, предложили подписание так называемого соглашения об уровне обслуживания, или по-английски service level agreement. И возникает ревизионная комиссия, которая контролирует выполнение этих соглашений. То есть этот американский как бы аппендикс исчезает. Он заменяется юридическим документом и ревизионной комиссией, которая следит за его исполнением.

И наконец, сообщество протокола пришло к выводу, что устранение американского правительства из системы управления глобальной инфраструктурой ни к чему негативному не приведет. Предлагается эту настройку убрать как лишнюю. Выяснилось, что все три предложения друг другу никоим образом не противоречат, их можно реализовывать одновременно.

Собственно, эта работа как раз и происходила. В прошлые месяцы на всемирной встрече «ICANN» в марокканском городе Марракеше были рассмотрены предложения по передаче функций этой корпорации. При этом все группы, рабочие и постоянные, включая «ICANN», где работают и представители Российской Федерации, одобрили данные предложения, после чего их передали правительству США для окончательного утверждения.

Что касается подотчетности, то был подготовлен, как я уже говорил, целый комплекс предложений, о которых мне не хотелось бы сейчас подробно говорить. Это очень интересно, но эту информацию требуется изучать достаточно вдумчиво.

То есть выделены четыре структурных элемента, включая разного рода механизмы независимых апелляций, изменения полномочий правления и внесения изменений в устав нашей организации, что очень важно, потому что все-таки, когда меняется основополагающий документ той или иной организации, - это серьезно.

Что мы имеем сейчас - процесс не закончен. Во-первых, мы ждем утверждения наших предложений правительством США. Эти предложения, которые занимают около 200 стра-

ниц (на нашем сайте есть русский вариант), достаточно интересны, но их внимательное прочтение может привести к выводу о том, что они достаточно компромиссны. То есть они сложны, но компромиссны и, соответственно, направлены на то, чтобы американцы все-таки их утвердили.

Тем не менее есть еще недоработанные механизмы, касающиеся подотчетности. Все мы имеем возможность участвовать в обсуждении и принятии документов. Поскольку эти меры, как можно видеть, действительно направлены на укрепление доверия к нашей организации, хотел бы в качестве позитивного привести пример взаимодействия с Институтом проблем информационной безопасности МГУ. На протяжении ряда лет осуществлялся исследовательский проект, который «ICANN» очень поддерживал, в котором участвовали специалисты института, российских экспертных организаций и ряда зарубежных организаций, в первую очередь из США и Болгарии. Был подготовлен всеобъемлющий документ на высоком уровне с объективным представлением о том, что такое правовые и технические аспекты глобальной инфраструктуры Интернета, где расписываются терминология и основные факты того, что есть глобальная инфраструктура. Впервые сжато и понятно, как на русском, так и английском языках, изложены технические стандарты и начата работа по изложению правовых аспектов того, что относится к управлению и регулированию глобальной инфраструктуры Интернета.

Владислав Гасумянов, вице-президент компании «Норильский никель»

Хотел бы от имени горно-металлургической компании «Норильский никель» поприветствовать в первую очередь организаторов и участников Десятого международного форума и 13-й научной конференции Международного исследовательского консорциума информационной безопасности. Должен сказать, что участие ведущих национальных корпораций, таких как «Норильский никель», в подобных мероприятиях принципиально важно для формирования новых мировых трендов и повесток. Эта деятельность касается не только бизнес-стратегий, но и самой философии бизнеса.

Наша компания включилась в «гармишский процесс» по ряду веских причин. Крупный бизнес заинтересован в бесперебойной работе всех производственных, финансовых, логистических, транспортных, сбытовых цепочек своих предприятий. Коммуникационные сети - это кровеносные сосуды единого экономического организма. Нарушение, а тем более насильственное вторжение в их работу может привести к негативным последствиям для акционеров и вообще к снижению инвестиционной привлекательности компании. Не хочу уже говорить о том, что компания «Норильский никель» - один из критических объектов экономики России. И в этом заключается наш основной мотив - участие в обсуждении проблематики информационной безопасности.

Вторая причина связана с глобализацией мировой экономики и как следствие - вовлечением ведущих мировых корпораций в процесс выработки решений на международном уровне по широкому кругу актуальных проблем, включая социальные. В миссии нашей компании говорится, что, эффективно используя природные ресурсы и акционерный капитал, мы обеспечиваем человечество цветными металлами, которые делают мир надежнее и помогают воплощать надежды людей на развитие и технологический прогресс.

Как уже было сказано, «Норильский никель» - это одна из системообразующих компаний в российской экономике. Она является одним из главных игроков мирового металлургического рынка, и от ее позиций зависит развитие отрасли. Мы крупнейшие в мире производители никеля и палладия. 40% мирового палладия вырабатывается и продается «Норильским никелем», компания - четвертая в мире по производству платины и одна из ведущих по производству меди, кобальта и родия. Должен сказать, что география бизнеса включает как Красноярский край, Мурманскую область, Забайкальский край, Финляндию, Южно-Африканскую Республику, Ботсвану, так и Соединенные Штаты Америки, Великобританию, Швейцарию, Китай и другие страны.

Направление деятельности предприятий «Норильского никеля» охватывает геологоразведку, производство, сбытовую сеть, транспорт, в том числе морской и авиационный, энерге-

тику, информационную структуру и научные комплексы. Нелишним будет сказать, что «Норильский никель» - это крупнейший налогоплательщик в различные уровни бюджета на территориях присутствия своих предприятий, сумма налоговых отчислений которого только в 2015 году составила более 1 млрд. долларов.

Показатели безработицы среди населения в регионах присутствия компании - одни из самых низких в стране, и очевидна тенденция к еще большему их снижению. Это способствует обеспечению социальной стабильности и экономическому развитию территорий. Например, масштабный проект планового развития устаревшего производства никелевого завода, расположенного в пределах городской черты Норильска, имеет наряду с экономической составляющей также социально-экологическую направленность. В результате ее реализации не просто снизится выброс вредных веществ, но и радикально оздоровится экологическая обстановка в Арктическом регионе в целом.

Компания «Норильский никель» реализует ряд крупных IT-проектов и решений в области информатизации и информационной безопасности в соответствии со стратегией развития и принципами корпоративной и социальной ответственности. Компания в тяжелых условиях Крайнего Севера ведет активное строительство волоконно-оптической линии связи (ВОЛС) по маршруту Новый Уренгой - Норильск длиной около 1 тыс. километров, которая радикально снизит нагрузку на действующие линии спутниковых коммуникаций. Проект нацелен не только на обеспечение потребностей компании в современных системах связи, но и на предоставление с его помощью жителям норильского промышленного района дополнительного доступа к широкополосному Интернету. Должен сказать, что деятельность компании в социальной сфере также достойно оценена как на правительственном уровне, так и экспертным сообществом. В начале марта 2016 года компания признана победителем национального конкурса «Лучшие социальные проекты России».

Масштаб и мультивекторность бизнеса компании требуют комплексного подхода к выстраиванию современной мобиль-

ной системы защиты корпоративных интересов. Ее руководство, учитывая все аспекты обеспечения экономической, корпоративной, объектовой, транспортной безопасности, особое внимание уделяет, конечно, обеспечению комплексной информационной защиты. Эффективная реализация процессов IT-безопасности компании в значительной степени способствовала изменению методологических основ построения системы корпоративной защиты для «ГМК «Норильский никель». Компания перешла на новый программно-целевой принцип работы, сосредоточившись на упреждении аналитики и внедрении передовых технологий.

В рамках программно-целевого подхода были разработаны и реализуются программы защиты персональных данных, противодействия утечке информации и содействия защите государственной тайны, противодействия несанкционированному вмешательству в работу информационных систем, обеспечения лицензирования в области информационной безопасности и т. д. Активно работает НПО «Институт современных проблем безопасности», методологический и экспертный центр группы «Норильский никель» в сфере IT-защиты. Поэтому процессы модернизации производства, связанные с внедрением новых информационных и коммуникационных технологий, таких как комплекс радиосвязи и позиционирования на рудниках, создание баз данных промышленных активов, систем мониторинга ремонтной деятельности, введения в эксплуатацию системы SAP ERP, решений по обеспечению современного документооборота, строительство ВОЛС, модернизация Центра обработки данных, создание Общего центра обслуживания, проходят в полной синхронизации с мероприятиями по обеспечению информационной безопасности.

Должен сказать, что мы являемся одним из ключевых элементов экономической безопасности страны, и в современном мире такие структуры представляют повышенный интерес для киберпреступников и кибертеррористов, использующих электронные коммуникации в качестве средства нанесения материального и репутационного ущерба. По оценке специалистов «Лаборатории Касперского», Россия в 2015 году вошла в топ-5 стран, подвергшихся массированным действиям хакеров.

Более 92% российских компаний и госструктур столкнулись с попытками вторжения в свои IT-системы. При этом 55% атак на российские компании были направлены против их веб-сайтов, 34% - против коммуникационных сервисов, 18% - на файловые хранилища, 12% - на сервисы для совершения финансовых операций.

По данным российских и зарубежных экспертов, ущерб, нанесенный экономике России в 2015 году от действий киберпреступников, оценивается в 203,3 млрд. рублей, что составляет 0,25% от ВВП страны.

Криминализация киберсреды, безусловно, стала проблемой глобального порядка. Согласно данным компании «Symantec», ущерб от киберпреступлений в 2015 году в мире составил 158 млрд. долларов. При этом отмечается, что атакам подвергаются как ресурсы бизнес-сектора, так и государственных органов, общественных организаций и СМИ. В США хакеры получили доступ к информации ограниченного пользования в результате атаки на IT-инфраструктуру дамбы в Нью-Йорке. Посредством кибератаки были выведены из строя два энергоблока Приднепровской и Углегорской теплоэнергостанций на Украине. В Польше были отменены более десятка рейсов крупнейшей авиакомпании «Лот» из-за вторжения в IT-систему аэропорта Варшавы. Взломав доступ к сайту газеты «Лос-Анджелес таймс», хакеры получили возможность самовольно изменять содержание материалов издания.

Для нас как горно-металлургической компании, конечно, особый интерес представил факт взлома хакерами системы управления печами на металлургическом заводе в Германии, что привело к выводу из строя механизма их отключения.

Итоги ситуационных анализов подобных инцидентов, результаты моделирования киберугроз привели нас к решению, что приоритетным направлением в обеспечении информационной защиты нашей компании должна стать безопасность автоматизированных систем управления технологическими процессами. Прежде всего системы диспетчерского управления и сбора данных, распределенных си-

стем управления, систем на программируемых логических контроллерах.

Говоря об актуальности темы информационной безопасности как в корпоративном секторе, так в глобальной перспективе, полагаю необходимым отметить ряд негативных трендов на их влияние, на информационную экосистему в целом.

Кризисные явления в мировой экономике привели к значительным сокращениям бюджетов в области информбезопасности. Как следствие, отмечается рост активности групп, занимающихся противоправной деятельностью в киберпространстве, повышение их профессионального уровня, переход от примитивных массовых атак к адресным нападениям с применением всего арсенала технических средств, включая элементы социальной инженерии и психологического воздействия через электронные средства коммуникации. Учитывая фактическую внегосударственность и внетерриториальность подобных хакерских сообществ, мы вполне можем столкнуться с таким явлением, как условный «киберИГИЛ», логику и мотивацию поведения которого просчитать весьма проблематично.

Указанные реалии накладывают дополнительную ответственность на структуры корпоративной информационной безопасности. «Норильскому никелю» удалось существенно укрепить эту функцию как с кадровой точки зрения, так и в плане ввода в эксплуатацию передовых решений, включая продукты российских производителей, - обновить системы предотвращения утечек конфиденциальной информации, контроля мобильных корпоративных устройств, решения по обработке событий информационной безопасности, заменить системы криптографической защиты. Активность ГМК в сфере безопасности не ограничивается ареалом группы «Норильский никель».

Компания обладает богатым плодотворным опытом международной деятельности. Возглавляя Комитет безопасности Международной ассоциации металлов платиновой группы (IPA) совместно с Межрегиональным научно-исследовательским институтом ООН по вопросам преступности и правосудия (ЮНИКРИ), «Норильский никель» активно участвует в программах по противодействию незаконному обороту

сырья драгоценных металлов и борьбе с транснациональной преступностью. Наша инициатива об усилении взаимодействия государственных и частных структур получила высокое признание, и благодаря усилиям МИД России, МИД Южно-Африканской Республики и «ГМК «Норильский никель» принята резолюция Экономического и социального совета ООН «О борьбе с транснациональной организованной преступностью и ее возможными связями с незаконным оборотом драгоценных металлов». В настоящее время готовится доклад ЮНИКРИ, в котором будут обозначены перспективные направления борьбы с международной контрабандой драгметаллов.

Уверен, что опыт «ГМК «Норильский никель» в сфере международной борьбы с незаконным оборотом цветных и драгоценных металлов может быть успешно применен в процессе создания глобальной системы информационной безопасности и стать модельным для других ведущих российских и зарубежных корпораций. Анализируя опыт участия «Норильского никеля» в мероприятиях Международного исследовательского консорциума информационной безопасности в Гармише и Сеуле, мы констатируем взаимную заинтересованность всех участников «гармишского процесса» в снижении угроз использования информационно-коммуникационных технологий в преступных целях, создании предпосылок для повышения уровня доверия к поставщикам оборудования и программного обеспечения, добросовестной конкуренции среди вендоров IT-решений и формировании общей среды нетерпимости к проявлениям электронного экстремизма и терроризма.

Участвуя в работе консорциума, «Норильский никель» исходит из принципа ответственного IT-прагматизма, то есть комплексной вовлеченности компании в актуальные процессы, затрагивающие ее деятельность как на технологическом уровне (производство и поставки IT-продукции и технологий), так и на глобальном (выработка принципов мирного сосуществования в информационной среде). Данный подход является прямым воплощением миссии нашей компании и соответствует основным принципам ее развития. Программа сегодняшнего мероприятия затрагивает фундаментальные вопросы международной информационной безопасности.

Полагаю, что всем нам, представителям государства, бизнеса и гражданского общества, необходимо приложить максимум усилий в поиске решений таких актуальных вызовов, как формирование универсальной культуры информационной безопасности, минимизация рисков недружественных действий в информационном пространстве по политическим, экономическим, идеологическим и иным причинам, обеспечение конфиденциальности, целостности и доступности информации в корпоративных сетях и Интернете, применение международного права к процессам, протекающим в киберпространстве. Представляется принципиально важным совместно разработать и запустить действие инструмента государственно-частного партнерства, противодействия использованию информационно-коммуникационных технологий в преступных целях. Не вызывает сомнений, что столь высокий состав и уровень участников обеспечит форуму максимальную эффективность и качество работы.

В этом году «Норильский никель» принял решение присоединиться к консорциуму в качестве полноправного члена. Компания обладает статусом и компетенциями крупнейшего российского потребителя информационных и коммуникационных технологий в сочетании с уникальным практическим опытом государственно-частного партнерства на международном уровне, что делает ее участие в консорциуме знаковым. Мы готовы приложить все наши усилия для формирования на базе Международного исследовательского консорциума информационной безопасности площадки для профессионального диалога и, самое важное, выработки универсальной повестки дня в области глобальной информбезопасности. Достигнув этого, мы сможем актуализировать указанные вопросы уже при участии таких организаций, как ООН, ЕС, ОБСЕ, АСЕАН, ШОС, БРИКС и др.

В завершение своего выступления хотел бы выразить искреннюю благодарность организаторам форума, сопредседателю Оргкомитета конференции, директору Института проблем информационной безопасности Владиславу Петровичу Шерстюку за приглашение и возможность поделиться с вами нашими подходами и предложениями.

Проблемы современных международных отношений в контексте киберпространства

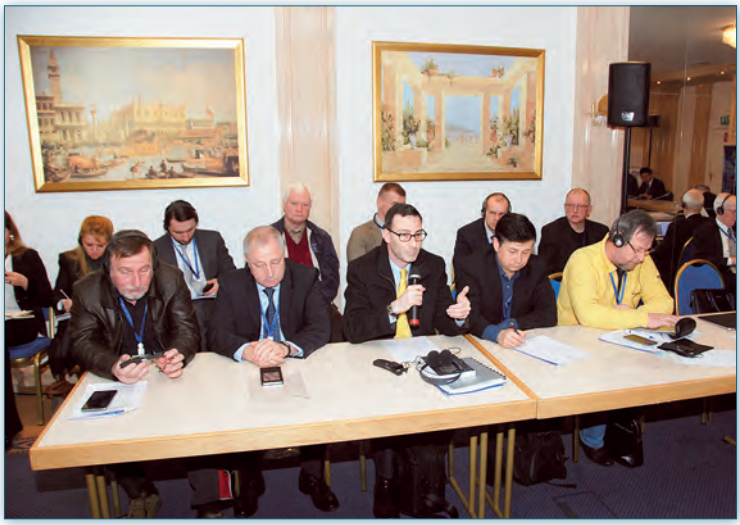
«Круглый стол» журнала «Международная жизнь»

Четвертая промышленная революция: информационные риски - взгляд из России

Анатолий Смирнов, президент АНО «Национальный институт исследований глобальной безопасности», доктор исторических наук: Дорогие друзья, коллеги, формулировка «Проблемы современных международных отношений в контексте киберпространства» предполагает широкое рассмотрение проблемы. Поэтому своим докладом попытаюсь дать пищу для размышлений, критики, конструктивных предложений. Не секрет, что весь мир охвачен беспрецедентной четвертой промышленной революцией. Генеральная Ассамблея ООН приняла повестку дня в области устойчивого развития до 2030 года. Она определила 17 целей и 169 задач, цель №9 - это создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям. А подпункт «С» предполагал именно максимальное развитие Интернета.

Этому было, в частности, посвящено выступление министра иностранных дел России С.Лаврова, который предлагал сделать неделимым устойчивое развитие в сфере инноваций, что нашло отражение в итоговой резолюции, принятой Генассамблеей.

В Давосе на Всемирном экономическом форуме президент форума К.Шваб откровенно говорил, что человечество стоит перед вызовами четвертой революции - «Industry 4.0», которая кардинально изменит нашу жизнь. «Industry 4.0» как концепция была создана в ФРГ. Что это такое? Это сочетание, конвергенция технологий: физической, цифровой и биосферы, в том числе интернет-вещей, индустриальных интернет-вещей, равно как и киберфизических систем, и многого того, что называется сегодня инновационным компонентом в мире цифровых технологий.



Шваб сказал, что трудно предвидеть, по какому сценарию будет развиваться «Industry 4.0», но он подчеркнул, что в выигрыше от нее останется интеллектуальный и физический капитал.

В своей книге «The Fourth Industrial Revolution» («Четвертая промышленная революция») Шваб предупреждает, что как все позитивное, несущее благо человечеству, эта революция несет в себе и огромные, абсолютно непознанные вызовы. Поэтому соглашусь с выступлением Андрея Крутских, который сказал, что мы находимся в цейтноте, нам некогда погружаться в детали. Сегодня передовые страны уже вплотную работают над когнитивным web, то есть используются когнитивные агенты, которые обладают знаниями, они способны к самообучению и рассуждают как люди в виртуальной среде, то есть наблюдается подход вплотную к искусственному интеллекту. Это заставляет совершенно по-иному посмотреть на модели угроз, модели нарушителей, которые обычно классически составляет любой специалист, эксперт по информационной безопасности. Шваб изрек очень глубокую мысль: история войн - это история технологических прорывов, и существует искушение воспользоваться преимуществом, которое получили те, кто уже сегодня перевел экономику на рельсы «Industry 4.0».

Напомню, что предыдущий такой цикл был в 1939 году, а что было после - мы знаем. Лауреат Нобелевской премии по эконо-

мике профессор Йельского университета Роберт Шиллер сказал, что «вы не будете ждать пожара, чтобы застраховать дом». Мы не можем также ждать революционных сдвигов в обществе, чтобы начать готовиться к четвертой промышленной революции и ее негативным последствиям. Кстати, американская компания «Cisco» в целом проанализировала достаточно глубоко ситуацию интернет-вещей. По ее данным, система без человека, машина к машине, то есть одна, скажем, компонента интернет-вещей, достигнет уже к 2020 году 24 млрд. датчиков и объема рынка свыше 1,2 трлн. долларов. Совершенно гигантские объемы. И это уже через три-четыре года. Естественно, что в конкурентной борьбе многие забывают о защите данного продукта, и это особенно необходимо там, где есть критически важные инфраструктуры, будь то электросеть, атомная электростанция, транспорт, авиация - все что угодно. Там, где встроены сенсоры, - это все объект для атак террористов, и мы обязаны на это трезво и очень адекватно реагировать. Причем очень трудно выработать единый стандарт. Предложение поработать юристам вместе с технарями в Шестом комитете ООН (Комитете по правовым вопросам), мне кажется очень правильным. Это пространство уже сегодня изучается специалистами, в том числе террористическими, как объекты для суперобогащения.

В Давосе министр экономики ФРГ Зигмар Габриэль сказал, что данные для «Industry 4.0» в ФРГ собираются не национальными компаниями, а четырьмя фирмами из Кремниевой долины. Мы все так или иначе технологически зависим от поставщиков, вендоров всех центров обработки данных и иных инфраструктур, которые обеспечивают продвижение и развитие новых технологий. Другая проблема - это создание безопасных сетей. Интеграция физических систем с Интернетом делает их уязвимыми к кибератакам, причем самыми разными, в том числе коварными методами, с использованием так называемых двойных логических люков, известных всем, кто занимается проблематикой информационного оружия и системами кибератак.

В этом контексте Россию не могло не обеспокоить принятие в США в прошлом году новой стратегии Министерства обороны, мы назвали ее «Стратегией наступательной кибервойны», потому что предыдущая стратегия 2011 года не предполагала проведения кибератак, а только лишь защиту. А что

мы читаем здесь? «Решение о кибератаке принимает Президент США и министр обороны… вывести из строя командные сети противника и лишить его способности применять оружие». В интервью CNN первый заместитель министра обороны Роберт Уок заявил, что Соединенные Штаты сбросили кибербомбы против ИГИЛ (ДАИШ).

Мы за то, чтобы уничтожить ДАИШ, но мы и за то, чтобы знать, что это за кибербомба, к какому классу оружия ее отнести. Мы ничего не знаем, поэтому пытаемся узнать у наших американских коллег в целом, что это такое, так как никакой расшифровки не было. А проект бюджета на 2017 год предусматривает 35 млрд. долларов на кибербезопасность.

Конечно, это дело Соединенных Штатов, но не может не настораживать, по крайней мере, Россию, да и многие другие государства, переход от оборонительной к наступательной кибервойне. В силу этого в России была принята в последний день 2015 года Стратегия национальной безопасности, которая в пункте 21 констатировала, что конфронтация в глобальном информационном пространстве преследует геополитические цели и некоторые государства пытаются манипулировать информацией, прибегая в том числе и к фальсификации истории. Кстати, в этом же документе говорится, как мы будем решать данную проблему для России - в первую очередь путем развития высоких технологий, то есть роботов, биологической, информационной, компенсационной, когнитивной технологий, нанотехнологии, конвергентной технологии и т. д.

У нас принят исторически важный документ, о чем посол Андрей Крутских говорил на пленарном заседании, - это основы государственной политики в области международной информационной безопасности. В нем четко определены все четыре угрозы и наша позиция, причем мы везде подчеркиваем противоречие определенных шагов международному праву, нарушение цифрового суверенитета стран, что позволяет террористам оказывать деструктивное воздействие на элементы критической инфраструктуры, пропагандировать терроризм, в том числе с использованием новейших наработок науки меметики.

Террористы ее уже хорошо освоили, и то, что появляются новые люди в составе ИГИЛ (ДАИШ), тому подтверждение. Напомню и об инициативах членов ШОС в ООН в области

обеспечения международной информационной безопасности. Мы говорим о правах человека в офлайне, как и в онлайне, согласно статье 19 Международного пакта о гражданских и политических правах. Сноуден разоблачил беспрецедентную тотальную слежку за всеми нашими действиями, подготовку информационных досье на каждого человека.

Что касается интернационализации управления Интернетом. Мы слышали на пленарном заседании доклад господина М.Якушева о том, что в течение 90 дней Соединенные Штаты должны рассмотреть предложения о переходном периоде для того, чтобы управлять Интернетом по-иному. На наш взгляд, интернационализация, принцип суверенного равенства, заложенный в Уставе ООН, должен быть соблюден и здесь, в киберпространстве. Актуален и вопрос наращивания информбезопасности и преодоления цифрового разрыва. В этой ситуации, учитывая острейшие вызовы и угрозы, нельзя погрязнуть в деталях, искать недоработки в предложенных документах, мы просто обязаны подняться над ними.

Наша российская компания «Positive Technologies» провела колоссальную работу по анализу «Industry 4.0» с точки зрения безопасности. Выяснилось в частности, что система управления технологическими процессами, или называйте это промышленным контролем, даже в таких компаниях, как «Siemens», «Emerson», «Honeywell», «Schneider Electric», «Bombardier» и т. д., фактически не защищена, а это ведь и атомные станции, и аэропорты, и железные дороги, и химические предприятия и т. д. Все эти системы доступны кому угодно, в том числе и террористам, в целях, не совместимых с целями развития международного сообщества. Кстати, в Москве проходит Positive Hack Day, то есть день, где «позитивные хакеры» пытаются помочь фирмам закрыть свои бреши.

Можно сделать следующий вывод: «Industry 4.0» кардинально меняет модель глобальных информационных угроз и модель нарушителя, в том числе террориста. Поэтому с учетом экспоненциального скачка объемов «Industry 4.0» необходимо срочно договариваться по правилам поведения, в том числе в формате группы экспертов ООН по международной информационной безопасности. Иначе нас ждет «Cyber Armageddon». Наш Национальный институт исследований глобальной безопасности выпустил ряд работ: «Глобальная

безопасность в цифровую эпоху: стратагема для России», «Глобальная безопасность и «мягкая сила 2.0», а также другие достаточно интересные труды по инновационному анализу конфликтов и т. д.

Выстраивание мер доверия между государствами и нормы ответственного поведения государств в киберпространстве: две стороны одной медали

Бен Хиллер, специальный представитель ОБСЕ в области кибербезопасности: Мы, несомненно, добились определенного прогресса в нашей деятельности. Прежде всего хотелось бы отметить некоторые положительные сдвиги и сообщить обнадеживающую новость, способную, как мне кажется, опровергнуть мрачные прогнозы, которые мне пришлось здесь услышать. В течение последнего месяца все 57 стран, объединенных в нашей организации, договорились о расширении мер с целью повышения взаимного доверия в этой области, что, безусловно, приведет к уменьшению риска возникновения киберконфликтов. На мой взгляд, это достойный внимания факт, тем более на фоне политической обстановки, которая, отнюдь не улучшилась за последний период.

В этой связи хотелось бы еще раз процитировать слова, сказанные российским представителем: «Подписание дополнительного протокола является результатом конструктивного сотрудничества всех участников переговорного процесса». Заключение такого рода соглашения свидетельствует о том, что, независимо от политической ситуации, можно достичь консенсуса по основным вопросам, касающимся международной безопасности, в том числе в киберпространстве, и мы считаем, что международное сотрудничество в данной области должно развиваться именно в этом направлении.

Далее, в интересах дальнейшего расширения мер по обеспечению прозрачности информации необходимо наметить несколько конкретных сфер межгосударственного взаимодействия в этом плане. Следует отметить, что данный комплекс мер будет преследовать цель защиты интеллектуальной собственности - это одна из самых чувствительных тем в настоящий момент. В общем ключе наша работа должна быть направлена на повышение взаимного доверия между всеми участниками данного процесса и сторонами,

заинтересованными в дальнейшем развитии сотрудничества в сфере защиты электронной информации, что будет способствовать повышению у каждого из них способности противостоять угрозам со стороны сообщества киберпреступников. После принятия комплекса мер по организации всестороннего сотрудничества необходимо приступить к разработке так называемых «мер стабильности». В этой области также имеется несколько весьма интересных, на наш взгляд, предложений и проектов.

Обстоятельства сложились так, что Соединенные Штаты вносят основной вклад в разработку стандартов ответственного поведения и поддержания стабильности в киберпространстве. От них также исходит предложение провести обсуждение комплекса мер по обеспечению стабильности в ходе очередного заседания Рабочей группы. В общем и целом, признаки прогресса у нас налицо.

Позвольте суммировать некоторые сложности. В разных странах по-разному представляют себе обеспечение кибербезопасности в контексте международной безопасности, и это, несомненно, накладывает свой отпечаток на общий киберконтекст. Тем не менее сотрудничество в этой области может продвигаться вперед, и нам хотелось бы определить основные модели государственной политики в этом направлении, увязав каждую из них с нормами международного права.

Хотелось бы отметить важность открытости информации в процессе сотрудничества, а также важность стабильности и необходимость повышения способности каждой из сотрудничающих сторон к противодействию международной киберпреступности. Все государства-участники, безусловно, понимают необходимость сотрудничества в различных рабочих пространствах. Также вполне очевидно наличие прогресса в плане укрепления стабильности в сфере информационно-коммуникационных технологий по всем четырем направлениям, упомянутым выше.

Вот лишь один пример: зачем одному государству вводить ограничения и запреты по отношению к другому, когда существует уверенность, что там будут следовать тем же принципам? Отмечается существующая на государственном уровне тенденция не только осуществлять такую политику на практике, но и всячески демонстрировать приверженность данной системе мер по обеспечению киберстабильности. Аналогично приверженность нормам

международного права служит обеспечению открытости в том, что касается обмена информацией, что, несомненно, можно отнести к важнейшим достижениям в информационной сфере в последнее время. В реальном ключе, однако, это отнюдь не означает отказа от всех ограничений по обмену информацией, способной оказать влияние на принятие решений на официальном уровне.

Следует отметить, что принципы, о которых только что говорилось, должны подкрепляться практическими мерами с целью создания условий, обеспечивающих их эффективное функционирование, причем независимо от той или иной ситуации.

Что касается «разделения труда» между ООН и региональными организациями, здесь, на мой взгляд, основополагающим принципом будет выработка генеральной стратегии мирного развития ИКТ-рынка наряду с одновременным вводом в действие механизмов ее осуществления на региональном уровне. Главной причиной создания региональных организаций стала необходимость разработки и осуществления комплекса всеобъемлющих мер в свете новых задач в области информационного киберпространства в XXI веке.

Здесь стоит отметить необходимость создания эффективно работающей обратной связи регионального уровня с уровнем глобальным, а также подумать, как предпринимаемые на региональном и глобальном уровнях усилия будут дополнять друг друга как в стратегическом, так и практическом плане. Областью, где исследователи могли бы внести ощутимый вклад, является оказание помощи в ходе осуществления мер, договоренность о которых была достигнута на государственном уровне. Мы отмечаем наличие значительного прогресса в том, что касается концептуализации укрепления ИКТ-стабильности в межгосударственном киберпространстве.

Существует также возможность дальнейшего усовершенствования и доработки достигнутых ранее договоренностей. Уровень и объем обмена информацией в этой области не перестают удивлять в положительном смысле слова. На сегодняшний день достигнутые договоренности осуществлены на 68%, и это, несомненно, выдающийся успех, хотя такой обмен и носит порой вынужденный характер. Однако хочется верить, что заключившие соглашения государства располагают неиспользованными до сих пор возможностями по их внедрению.

В этой связи возникает желание еще раз напомнить о тех трудностях, с которыми государство может столкнуться в ходе осуществления вышеназванных мер, а также показать, как обмен информацией на практическом уровне может получить стратегическую поддержку. Важно заниматься не только мерами по обеспечению этого обмена, но также уделять внимание тому, как сделать их более эффективными и всеобъемлющими, заставить их работать наилучшим образом в ИКТ-среде. На мой взгляд, такую задачу должны поставить перед собой во всех странах - участницах нашего форума.

Что касается планов практической деятельности многочисленных исследовательских институтов, то мне хотелось бы еще раз подчеркнуть нашу безусловную заинтересованность в дальнейшем развитии всеобъемлющего обмена электронной информацией. И, конечно, буду рад обсудить вопросы, о которых только что упомянул, с генеральным секретарем ОБСЕ, а также с представителями сотрудничающих с нами организаций в Швейцарии и Италии.

Подводя итог, хочу сказать: у нас было много событий, мы немало сделали, и нам предстоит сделать еще больше в том, что касается осуществления достигнутых договоренностей, если мы хотим следовать по пути дальнейшего прогресса. На этом пути нам, несомненно, могут оказать помощь такие организации, как ООН и ОБСЕ, прежде всего в том, что касается сотрудничества стран-участниц и неприсоединившихся стран. Слова должны подкрепляться делами.

Суверенитет и Интернет

Санджай Гоел, профессор Университета штата Нью-Йорк (США): Не надо рассматривать данный вопрос в черно-белом свете, хотя зачастую дело обстоит именно так, в чем я, к сожалению, неоднократно убеждался в ходе этой конференции. Интернет - это не только огромный ресурс и мощное средство соревнования, он оказывает огромное воздействие на общество и политику. Киберпространство - прекрасная среда для пропаганды и утверждения тех или иных социальных ценностей, а политическая ситуация в отдельных странах нередко формируется при активном участии интернет-сообщества. Могущество и всеобъемлющий характер

Интернета вызывают обоснованную тревогу, поскольку он представляет собой некую виртуальную угрозу историческому праву государственных властей на управление национальными территориями и обеспечение суверенитета.

Складывающееся положение вещей становится неприемлемым для многих стран. Возникает некий дисбаланс между киберпространством и государственными границами. Согласен, этот процесс, несомненно, носит негативный характер. Но решением, по-моему, будет нахождение приемлемого выхода из подобной ситуации. Причем делать это нужно общими силами, и не дожидаясь, когда она выйдет из-под контроля. Технологии нахождения соответствия между государственными и интернет-ценностями уже существуют и начинают применяться на практике. Вопрос стоит лишь о приемлемости самих технологий как таковых.

Национальные государства испытывают озабоченность по поводу содержащейся в Интернете информации, которая может быть опасной для политической стабильности и вредной для граждан, и это беспокойство охватывает одну страну за другой. Речь идет о пропаганде радикальных идей, безнравственности, сексуальной эксплуатации и коррупции - в разных странах находят разные причины установления контроля за Интернетом. Благодаря Интернету любая пропаганда легко преодолевает границы, и это создает проблему для служб, отвечающих за обеспечение государственной безопасности, создает угрозу для внутренней стабильности, особенно в тех странах, где изначально существовали радикальные тенденции. Здесь Интернет особенно опасен.

В период, следующий за информационной революцией, все более сложной становится задача по регулированию воздействия электронных источников информации на формирование общественного мнения, причем в глобальном масштабе. В таких условиях общественное мнение может стать мощным оружием, направленным одними странами против властей других стран.

Интернет также можно с успехом использовать для мониторинга общественного мнения и внутриполитических тенденций в других государствах и в качестве мощного средства пропаганды и открытой агитации. Здесь главная трудность заключается в том, чтобы разумно уравновесить необходимость эффективного контроля над распространением

информации и ее свободное распространение, что в конечном счете будет способствовать укреплению внутренней и всеобщей стабильности.

Процесс контроля постепенно принимает форму скрининга средств массовой коммуникации на предмет достоверности информации с целью отсева сомнительных или провокационных сообщений. В некоторых странах эта мера осуществляется, так сказать, «в гласном режиме». Уровень и масштаб контроля также различаются в зависимости от той или иной страны, но сам факт осуществления контроля следует обязательно брать в расчет. В настоящее время причиной осуществления подобного контроля является в первую очередь осознание степени воздействия Интернета на общественное сознание. Но какими бы ни были причины контроля и введения ограничений, этот процесс неизбежно нуждается в юридическом регулировании, отправной точкой которого станет разработка соответствующего международного законодательства.

Необходимость поддержания разумного равновесия связана также с огромной важностью Интернета для ведения бизнеса, для экономики отдельных стран и мировой экономики в целом, и здесь необоснованные ограничения могли бы нанести серьезный ущерб. В этой связи вопрос о юридическом обеспечении процесса контроля приобретает особую актуальность. Судя по первым практическим результатам, данный аспект является наиболее сложным, прежде всего ввиду отсутствия необходимого опыта на государственном уровне.

В целом вопрос стоит о создании глобальной системы всеобъемлющих мер, с тем чтобы не допустить возникновения взрывоопасных ситуаций. Интернет не может функционировать в условиях абсолютной независимости от глобальной социальной и политической среды. Он нуждается в пристальном внимании мировой общественности с целью поддержания стабильности в кибернетическом пространстве, поскольку от этого теперь все больше зависит стабильность в мировом сообществе. И чем скорее эта взаимосвязь станет очевидной для всех, тем лучше.

Чтобы лучше представить себе концепцию национального суверенитета, давайте посмотрим, как работают различные ресурсы, от которых зависит ее обеспечение. Концепция националь-

ного суверенитета означает право осуществления неограниченного контроля над национальной территорией без какого-либо вмешательства извне. Государство берет на себя функцию обеспечения территориальной целостности страны всеми доступными способами. Остальная часть мирового сообщества действует в рамках юридических норм, обеспечивающих суверенитет отдельных его членов и одновременно возможность принятия коллективных решений.

Один из примеров - международное морское право, в соответствии с которым Мировой океан и моря являются общим ресурсом всех стран, частично принадлежащим отдельным собственникам, обладающим правом организации судоходства в своих территориальных водах и их экономического использования. Отчасти это можно сравнить с киберпространством, которое тоже является коллективной собственностью. Но здесь пока не достигнут консенсус относительно разграничения полномочий в области суверенитета. И процесс этот развивается недопустимо медленно в сравнении с темпом развития современных интернет-технологий, а задачи, которые необходимо решать международному сообществу, абсолютно не похожи на все то, с чем приходилось сталкиваться раньше. В общем, вопрос в том, как следует работать с данным ресурсом - в «суверенном», так сказать, режиме или объединив усилия всего мирового сообщества. Ведь права «плавания» в электронном пространстве в равной степени принадлежат всем государствам, независимо от национальных границ.

Итак, ключевая проблема заключается в том, сумеют ли суверенные государства создать некий орган, предназначением которого станет управление потоками информации, неограниченно распространяемой в Интернете. Вопрос также и в том, будет ли этот орган способен предоставить необходимую инфраструктуру и наметить границы в интернет-пространстве. Возникает также вопрос, что эти интернет-границы будут представлять собой в действительности. И еще один вопрос: чем будет отличаться международная интернет-инфраструктура от инфраструктуры национальной? Интересно также, как международный контроль над Интернетом будет сочетаться с контролем, осуществляемым в пределах отдельной страны.

В этой связи можно предположить, что во многих странах контроль над Интернетом будет усилен и ужесточен, исходя из необходимости защиты национального суверенитета. Контроль над обменом сообщениями в Интернете между частными лицами довольно сложен, но здесь будет уместно обратиться к опыту американских властей, имеющих доступ практически ко всему объему проходящей через Интернет информации.

Теперь о концепции интернет-границы. Ее главное отличие от границы физической вполне очевидно: географическую границу никому не позволят пересечь анонимно, не имея необходимых документов и не выполнив необходимых процедур, чего не скажешь о границе в Интернете. Для осуществления интернет-трафика не нужен даже национальный паспорт, не говоря уже о заграничном. Свобода доступа создает такие проблемы, как возможность пропаганды радикализма, насилия и многие другие. Но главная беда, похоже, отнюдь не в этом. Дело в том, что огромная масса проходящей через Интернет информации не имеет конкретного адресата. Поэтому, на мой взгляд, нужно более тщательно мониторить и «просеивать» эту информацию, отделяя, так сказать, зерна от плевел. Такой контроль, конечно, должен осуществляться в пределах вышеупомянутого «разумного равновесия». Необходимо четко осознавать, чем можно поделиться и что должно находиться под контролем.

Осуществление интернет-контроля в мировом масштабе - это огромная ответственность, связанная с возможностью предотвратить враждебные действия, направленные против других стран, опасность которых исходит с вашей национальной территории. Ведь непринятие или несвоевременность необходимых мер может повлечь за собой ответную реакцию, чреватую порой непредсказуемыми и даже непоправимыми последствиями. Поэтому ошибки здесь неприемлемы.

Предпринимая любые меры с целью осуществления контроля над Интернетом, следует помнить о необходимости поддержания стабильности в киберпространстве, что в конечном счете чрезвычайно важно в плане сохранения национального суверенитета. Совершенно очевидно, что в условиях, когда государственные границы сделались абсолютно про-

зрачными для любой электронной информации, государственный контроль над Интернетом имеет тенденцию к постоянному усилению.

В этой связи особенно остро встает вопрос о том, в каком объеме должен осуществляться комплекс мер, призванных обеспечить сохранение государственного суверенитета на разных уровнях. Неограниченное распространение любой интернет-информации в странах Северной Африки и Ближнего Востока, к сожалению, стало одной из причин подрыва стабильности и создания предпосылок для постепенного погружения мировой цивилизации в пучину хаоса. В этом случае Интернет является, по существу, одним из дестабилизирующих факторов и контроль над его дальнейшим развитием жизненно необходим - опять же в интересах сохранения национального суверенитета государств, заинтересованных в поддержании стабильности на мировом уровне.

С другой стороны, сколь велика ни была бы наша забота о сохранении суверенитета, нельзя и, наверное, практически невозможно установить абсолютный контроль над распространением электронной информации в киберпространстве. В этой связи приобретает первостепенную значимость задача по отслеживанию интернет-трафика с целью выявления информации, исходящей из сомнительных и потенциально опасных источников. Однако решить проблему распространения нежелательной информации на межгосударственном уровне вряд ли удастся даже с помощью создания глобальной идентификационной системы, поскольку реакция мировой общественности на такое нововведение будет абсолютно непредсказуемой.

Так, например, дальнейшее усиление государственного контроля над частной перепиской в Интернете неминуемо приведет к массовому недовольству, чреватому стать причиной глубокого раскола в обществе. Поэтому необходимо понимать, что будет представлять собой международный контроль над Интернетом и каковы будут его границы и рамки, а также не будет ли принесен принцип свободного обмена информацией в жертву необходимости защиты национального суверенитета и государственной безопасности.

В условиях, когда в разных странах существуют разные стандарты определения степени доступности электронной информации, создание действенной международной системы контроля над ее распространением может оказаться невыполнимым вообще. Поэтому необходимо выработать новые международные нормы по определению качества информации и ее правовой оценки. Этот революционный шаг, несомненно, будет способствовать созданию новой парадигмы, позволяющей уравновесить действующие в Интернете разумные ограничения с необходимостью осуществления в нем свободного обмена информацией. Это представляется нам вполне возможным в плане существующих на сегодняшний день технических и материальных возможностей. Не хватает лишь надлежащей заинтересованности и проявления доброй воли, в первую очередь со стороны интернет-пользователей, обладающих необходимыми полномочиями и государственным суверенитетом.

Хочу подвести итог, назвав комплекс первоочередных мер и задач в этой области. Во-первых, суверенный контроль над Интернетом, проведение суверенных границ в киберпространстве, выработка норм правового, государственного и общественного контроля в данной области. Во-вторых, осознание степени ответственности за характер распространяемой на международном уровне информации, определение понятия потенциально опасных информационных действий. В-третьих, разработка комплекса конкретных мер по обеспечению международной кибербезопасности в коммуникационной сфере и смежных с ней областях. Лишь в этом случае существующие на сегодняшний день трудности будут успешно преодолены и задача по защите национального суверенитета от угроз, исходящих из всемирного информационного пространства, станет практически осуществимой в обозримом будущем.

Найджел Инкстер, исследователь Международного института стратегических исследований (Великобритания): Затрону вопросы международных отношений в киберпространстве и обеспечения кибербезопасности и стабильности. Хотелось бы сделать пару замечаний по поводу того, о чем говорил на

этой презентации господин Смирнов. Имею в виду вопрос о Сноудене, поскольку он очень интересен сам по себе и оказал заметное влияние на размышления о кибербезопасности, стал причиной нескольких дискуссий на эту тему.

Прежде всего надо отметить, что выводы, сделанные на основе разоблачений Сноудена, нельзя считать абсолютно правильными, отчасти из-за того, что сам Сноуден не понимал значительную часть материалов, которые он похитил, а также потому, что пресса, распространявшая эту информацию, тоже в основном не понимала ее. Поэтому утверждение о том, что Агентство национальной безопасности США просматривает все электронные сообщения и прослушивает все телефонные звонки, мягко говоря, весьма далеко от истины. В действительности АНБ в любое время могло отслеживать лишь очень небольшую часть интернет-трафика по причине весьма ограниченного количества сотрудников, и в первую очередь аналитиков, обладающих необходимыми лингвистическими познаниями. Это накладывало очень серьезные ограничения в плане объема материалов, которые можно было просматривать.

С этим, по-моему, тесно связан вопрос о шпионаже в международных электронных системах и о той роли, которую он играет на государственном уровне. На мой взгляд, отдельные люди и целые страны зашли слишком далеко в своих суждениях. Все встревожены - в этом нет никаких сомнений, - США, конечно, виновны, но, однако, в какой степени? Их вина, как мне кажется, прежде всего в использовании преимущества и господствующего положения, которыми они обладали. Ведь США первыми создали эту систему новых возможностей и во многом способствовали ее распространению по всему миру.

Определяя понятие шпионажа, международное право никак не отражает шпионаж электронный, не говорит о законных или незаконных способах и средствах его осуществления. В этой связи хочу обратиться к Женевской конвенции, согласно которой шпионаж не является оправданием применения силы пострадавшим от него государством. То есть

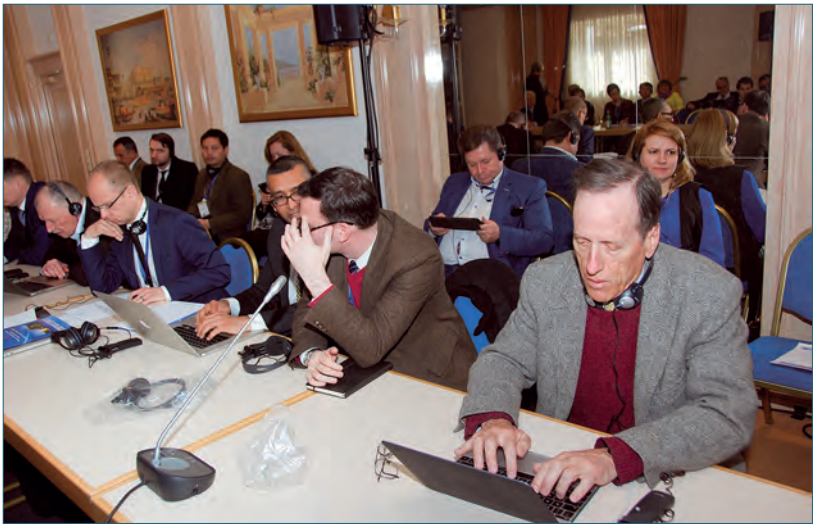
шпионаж, по существу, является инструментом управления государственными делами.

Однако при всем при том шпионаж не обладает статусом в международном праве. Когда речь заходит об охране данных частных лиц, международным правом предусмотрены определенные меры защиты, осуществления которых могут требовать отдельные люди. Идея заключается в том, что государства с недавнего времени гарантируют гражданам других стран такую же правовую защиту, как и собственным гражданам. Раньше такого в международной практике не наблюдалось, поскольку государственные власти всегда стремились покровительствовать «своим». Но международный «настрой» теперь, похоже, стал меняться, и эту тенденцию, проявляющуюся пока не слишком ярко, на мой взгляд, обязательно нужно иметь в виду.

Но зашел ли государственный кибершпионаж слишком далеко? Возможно, это действительно так. Но, с другой стороны, я не побоюсь заявить, имело место лишь новое определение тех параметров, в пределах которых собранные с помощью этих средств разведданные воздействуют на процесс проведения политики, и в этом нет ничего нового.

Скажем, если вернуться в XVI век и посмотреть, какую разведывательную информацию собирали голландцы в католических странах, которые были их главными противниками, то теперь большую часть этой информации можно почерпнуть из учебника географии для начальной школы. В те времена люди знали очень мало, сегодня нам известно гораздо больше. И в этой связи я готов утверждать, что, вероятно, происходит своего рода перестройка, новая калибровка ситуации, и прогнозы того, что можно сделать с помощью разведданных, переместились на другой уровень. Так что, на мой взгляд, ничего особенно страшного не происходит.

Но существует область, в которой разоблачения Сноудена оказывают очень серьезное практическое воздействие. Дело в том, что они дали толчок началу того, что можно назвать «кибернетической гражданской войной» между правительством США и крупнейшими американскими технологическими компаниями по вопросу кодирования информации. Вскоре после



разоблачений Сноудена мы увидели, как американские технологические компании стали лихорадочно вкладывать деньги в организацию кодирования данных.

Многие скажут, что аналогичный процесс имел место и до разоблачений Сноудена, однако теперь причиной такого инвестирования является не стремление защитить информацию, а опасение лишиться своей доли рынка в связи с тем, что часть конфиденциальной информации о продуктах компаний становится достоянием АНБ.

Это стало одной из причин того, что переговоры между компанией «Эппл» и ФБР по вопросу о создании надежных закодированных айфонов зашли в тупик. Теперь нередко в ходе мониторинга того или иного объекта службы безопасности и разведчики фиксируют лишь сам факт переговоров объектов наблюдения, не имея представления об их содержании и о том, с кем они велись. И даже если они предъявляют судебный ордер компании, разрабатывавшей систему кодирования, там тоже не могут помочь, возникают проблемы в связи со сложным кодированием средств, поскольку кодирование предполагает надежную защиту от несанкционированного проникновения. Это еще один из примеров работы принципа «действие-противодействие», который также отнюдь не нов.

Мне кажется, что разведывательным и правоохранительным органам придется адаптироваться в мире, где прежние способы их работы стали неэффективными и неприемлемыми. Несомненно, во всех странах западной либеральной демократии доступ правоохранителей к средствам телекоммуникации с целью мониторинга расширялся со времени изобретения телефона. Поэтому опять же хочу сказать: не надо паниковать - мир сумеет «перенастроиться» в очередной раз.

Анатолий Смирнов: *Если есть вопросы - пожалуйста. Анатолий Стрельцов.*

Анатолий Стрельцов: *Большое спасибо за хорошее выступление. Вопрос, который остался за кадром. Шпионаж в традиционной форме более-менее связан со сбором информации. Скрытые действия в киберпространстве могут преследовать не только сбор информации, но и создание площадок для размещения элементов вредоносного программного обеспечения. И все это будет прикрываться названием «шпионаж», и легализация такой деятельности как-то не очень вписывается в здравый смысл. Если проводить аналогии с фортификацией или подготовкой к военным действиям, то, если бы в рамках шпионажа кто-то начал строить окопы и готовить площадки для размещения самолетов, танков, артиллерии, вряд ли все это отнесли бы к форме ведения шпионской деятельности. Как вы думаете?*

Найджел Инкстер: *Это справедливое замечание, поскольку тема использования киберсредств, вообще, весьма проблематична. Мы, конечно, имеем в виду разведывательную деятельность, повлекшую за собой определенный ущерб в реальности. Примером того могут служить точечные удары, для нанесения которых необходимо располагать абсолютно точными развединформацией, как это было, например, в Ираке. На мой взгляд, этот вопрос в определенной степени связан с темой, которая обсуждалась сегодня утром. Имею в виду оружие. Речь шла об использовании киберсредств таким обра-*

зом, когда результат будет напоминать применение средств прямого кинетического воздействия, то есть когда шпионаж автоматически переходит в разряд способов ведения военных действий. И это, возможно, наиболее полезный способ проведения границы между этими двумя видами деятельности. Полностью согласен с таким подходом и разделяю точку зрения, согласно которой использование киберсредств в целях похищения информации или каких-либо других в принципе является одним и тем же.

Андрей Крутских: *У меня есть несколько вопросов, но это вопрос непосредственно к Найджелу с небольшим комментарием. Готов продолжать аплодировать выступлению Найджела, потому что, на мой взгляд, это был гимн роли государств в осуществлении контроля над киберполитикой, но, думаю, очень важно все-таки различать два понятия - шпионаж и диверсия. Давайте посмотрим на иранские события, связанные с вирусом. Два года определенная страна занималась шпионажем в разных формах, в том числе и в электронном виде, а потом была совершена диверсия. Сначала это был кибершпионаж, а потом кибердиверсия. Что такое шпионаж? Если красиво назвать, то это «сбор информации», а некрасиво - «поиск уязвимостей». Но ведь уязвимости ищут для того, чтобы потом их эксплуатировать и через эти уязвимости уже управлять целыми государствами, их лидерами, формировать общественное мнение и дестабилизировать обстановку. На каком этапе кончается шпионаж и начинается практическое использование уязвимостей - очень большой вопрос и далеко не совсем понятный.*

Как дипломат, вынужден констатировать, что, конечно, венские конвенции о дипломатической и консульской деятельности никакой шпионаж не легализуют и не считают это допустимой формой деятельности. И если даже дипломаты занимаются шпионажем, это называется «деятельность, не совместимая со статусом», то они подлежат высылке и наказанию. Но это если они занимаются физическим шпионажем.

А вот как нам быть с кибершпионажем? Частично на этот вопрос дала ответ встреча в верхах «двадцатки», которую американская сторона трактует как свой большой успех, потому что там четко записано, что интеллектуальную собственность воровать киберспособами нельзя. Но для того чтобы ее своровать киберспособами, ее надо сначала обнаружить. И киберворовство от кибербора информации отличить невозможно, насколько я понимаю. И тем не менее Россия, Китай и многие другие страны «двадцатки» подписались под этим положением. Поэтому кибершпионаж - это очень мощное средство, но проблема состоит в том, что есть разница между сбором информации и нанесением ущерба стране через сбор информации. Потому что любой физический шпион - он как бы украл кошелек, но уже деньгами из этого кошелька воспользуются другие. А в кибермире этой разницы в процессе нет. Кибершпион - он, получается, уже и кибердиверсант. Но это мнение дилетанта. Как вы, Найджел, согласны с такой трактовкой?

Найджел Инкстер: *По-моему, у вас слишком негативное и пессимистичное представление о том, что называют сбором разведданных. Могу с уверенностью утверждать, что в большинстве случаев, занимаясь сбором информации, я и мои коллеги не наносили какого-либо ущерба другому государству. Это делалось лишь с целью, чтобы мое правительство могло лишний раз убедиться, что проводимая в этом государстве политика - порой не слишком популярная внутри страны - являлась именно такой, какой ее представляли. И наше правительство получало тому подтверждение, поскольку информация, добытая нами, так сказать, «с черного хода», выглядела более убедительной, чем полученная от официальных лиц. Это в конечном счете было весьма полезно, так как способствовало проведению более позитивной и конструктивной политики в сравнении с той, проводить которую предполагалось первоначально. Так что сбор разведданных не всегда и, не побоюсь заявить, отнюдь не из-*

начально осуществляется со злонамеренными или антагонистическими целями.

Вопрос из зала: *Не могли бы вы более подробно остановиться на этическом аспекте кодирования информации? В этой связи хотелось бы привести один, на мой взгляд, весьма характерный пример: некая итальянская фирма продает через своих агентов программное обеспечение, с помощью которого службы безопасности получают возможность прослушивать разговоры итальянских юристов между собой. Но аналогичные программы того же производителя имеются и в свободном доступе. Возможно, такая позиция оправдана, поскольку тенденция к кодированию информации получает все более широкое распространение. Но при этом существуют, так сказать, «хорошие» государства и «плохие», и провести грань между «плохим» и «хорошим» порой почти невозможно. В этой связи можно упомянуть Северную Корею и сложившуюся там ситуацию с правами человека, а также аналогичную ситуацию на Кубе. Так вот, может быть, это правильно - возможность кодирования информации любым заинтересованным лицом или организацией. Но как вы относитесь к тому, что любые государственные службы - в «плохих» и «хороших» странах - теперь практически не могут осуществлять мониторинг частных переговоров в надлежащем для обеспечения безопасности объеме?*

Найджел Инкстер: *Вопрос справедливый. На мой взгляд, соответствующие технологии развиваются именно в таком направлении, и в результате государственным органам становится все сложнее сохранять за собой возможность контролировать обмен информацией и ее содержание. В такой ситуации властям приходится отказываться самим от использования вышеупомянутых средств и запрещать их использование частными лицами, тем более когда речь идет о продуктах, произведенных в других странах. При этом как бы ставится условие: или мы получаем доступ к вашей ин-*

формации, или использование тех или иных устройств будет запрещено. Здесь я бы посоветовал трезво смотреть на вещи, ведь, например, ни один зарубежный бизнесмен не сдаст свой айфон на хранение в аэропорту, чтобы пользоваться местным эквивалентом. Раньше так делали в Японии, но теперь там пользуются программами, адаптированными под мировой стандарт. Так что, на мой взгляд, решение этой проблемы лежит в технологической плоскости.

Андрей Крутских: *Хочу продолжить дискуссию о шпионаже и привести совершенно поразивший меня пример того, что такое шпионаж. Я работал в Канаде в 1990-х годах, тогда были опубликованы мемуары канадского «электронного» разведчика, который помогал на крыше канадского посольства в Москве оборудовать систему подслушивания, чтобы можно было подслушивать и Кремль и т. д., потом канадцы убрали эту систему. Там приводился потрясающий пример, что такое кибершпионаж. В России был неурожай зерна, и в этот момент еще и Китай хотел закупить миллионы тонн зерна. За эти два рынка, за эти два контракта бились Соединенные Штаты и Канада. II вопрос разрешился с помощью сотрудника канадской секретной службы «Канадиан роял маунтед полис», который сумел подслушать электронно и узнать конечную цену Соединенных Штатов при продаже этого зерна. Канадцы после этого понизили свою конечную цену на полцента и получили многомиллиардные контракты с Россией. II эта заслуга того, кто воспользовался системой «World Wide Web», что нельзя, наверное, и диверсией назвать. Это именно то, о чем говорил Найджел. Была предоставлена канадскому правительству правильная информация, но именно таким способом.*

Джон Мэллори: *Прежде всего, хотелось бы отдать должное высокому профессионализму разведчиков в некоторых странах, особенно в России. Про нас этого, к сожалению, сказать нельзя. IIмею в виду экономический шпионаж, со-*

хранение коммерческой тайны и многое другое. В условиях постоянного снижения уровня компьютерной безопасности и недостаточно адекватных мер, принимаемых государством с целью ее обеспечения, те, кто принимают соответствующие решения, обязательно должны озаботиться данной проблемой и принятием необходимых мер противодействия. В настоящее время ущерб от промышленного шпионажа конкурентов частично нейтрализуется благодаря работе служб безопасности, чьей задачей является охрана собственной конфиденциальной информации наряду с получением доступа к аналогичной информации конкурирующих фирм и организаций, а также информации из соответствующей сферы деятельности вообще. При этом государство в силу очевидных причин не может дистанцироваться от сложившейся ситуации, сохранив за собой лишь роль стороннего наблюдателя.

Найджел Инкстер: *По-моему, вы сделали ценное замечание, Джон. Существует риск нестабильности в киберпространстве, и вы правы, сказав, что в определенных, наиболее тяжелых случаях возникает опасность неверного восприятия ситуации, как это было, например, во время ситуаций «ракетного неравенства» в 1960-х или 1970-х годах. Никакого «разрыва», никакого отставания не существовало, но уверенность американской стороны в обратном вызвала к жизни процесс эскалации развития собственных возможностей в этой области, что в конечном счете способствовало созданию очень опасной ситуации. Если бы США в то время располагали более точной информацией о Советском Союзе, нам бы это совершенно не понадобилось.*

Анатолий Смирнов: *Цифровая революция и «Industry 4.0» уже озаботила и вице-канцлера Германии, который выразил опасения, что из всех «Industry 4.0» объектов на территории Германии данные попадают в Силиконовую долину раньше, чем даже в центры Германии. А ведь используемые технологии позволяют вести не только контент-анализ, но*

и интент-анализ, коннект-анализ, то есть кто, с кем, по каким каналам контактирует. А еще и - геолокационный анализ. На основании всех этих составляющих появляется досье, которое сделало возможной, скажем, известные операции с дронами в Пакистане, когда было уничтожено немало людей, которые случайно попадали под эти массивы информации. Это как бы излишки или издержки шпионской или военной области. На основании этих составляющих - контент- и лэнд-коннекта и геолокационного анализа появляется интент, то есть то, что можно спрогнозировать о человеке, корпорации, государстве, группе государств на основании big data. Это сегодня абсолютно реально, считают многие эксперты. Мы должны понимать, что дальнейшая задержка принятия решений по торможению этой безумной гонки технологических, военных в том числе, составляющих может привести к «Cyber Armageddon».

Что делать с использованием социальных сетей террористами?

Фил Гурски, SecDev (Канада): Как бывший канадский шпион, буду говорить о таких вещах, которые моим российским коллегам нужно будет либо подтвердить, либо опровергнуть. Как бывшему разведчику мне гораздо ближе практическая сторона дела, поскольку я не был дипломатом, не занимался разработкой политического курса, я не политик, но знания, которыми я обладаю, и мой практической опыт имеют непосредственное отношение к теме радикализации. Один из предыдущих докладчиков прослужил 33 года в финских Вооруженных силах, а я отдал службе в канадской разведке 32 года, и мне тоже есть что рассказать. Хочу также предупредить, что мои личные замечания и комментарии не следует рассматривать как выражение официальной позиции канадских властей или каких-либо других государственных структур.

Речь пойдет об использовании террористами киберпространства, Интернета и социальных сетей. Подчеркиваю, именно террористами, поскольку до этого мы говорили больше о поль-

зовании Интернетом, так сказать, «на государственном уровне». Хочу демистифицировать, демифологизировать ту роль, которую играет социальная среда в бурном процессе радикализации, хочу сказать, что́ нам следует делать в связи с этим и что́ - это, на мой взгляд, является более важным - делать не следует.

На протяжении моей более чем 30-летней работы в разведке мне неоднократно приходилось заниматься проблемой терроризма применительно к такой области, как радикализация, то есть я изучал причины, заставляющие наших граждан воспринимать идеологию насилия, вступать в террористические организации и отправляться в другие страны для совершения террористических актов. Я слышал много разговоров о том, какая роль в этом процессе принадлежит и Интернету, и средствам массовой информации.

Вне всяких сомнений, платформам массовой коммуникации отводится главенствующая роль в этом деле, но вы наверняка удивитесь, узнав, что всевозможные запреты, связанные с пропагандой насилия в Интернете, приводят к прямо противоположным результатам, особенно среди молодежи, что в конечном счете способствует радикализации немалой части наших юношей и девушек. Я помню себя молодым, каким тоже был несколько десятилетий назад. Но сегодняшние молодые люди не похожи на нас в годы нашей юности. Они живут и действуют в режиме онлайн, в их распоряжении огромный набор средств электронной коммуникации, и нет ничего удивительного в том, что эта необъятная платформа широко используется ими с самыми разными целями.

Неслучаен тот факт, что онлайн-средства социальной коммуникации (социальные сети) обрели огромную популярность в исламских странах, что там выросло целое поколение пользователей электронных социальных сетей. В результате мы имеем все более расширяющуюся пропасть между цивилизационными понятиями и системами ценностей, и огромное количество людей, присутствующих в социальных сетях, попадает под влияние распространителей идей насилия.

Не следует думать, что Интернет способствует радикализации людей, Интернет сам по себе ничего не может сде-

лать. Это всего лишь носитель, средство коммуникации. Даже у тех, кто радикализируется, находясь в онлайн-среде, всегда присутствует некий «человеческий фактор». Мы имеем коллективный разум с тех пор, как кто-то сел на стул, пристроив на коленях ноутбук. Я, например, пропустив через себя огромное количество информации самого разного содержания, тем не менее почему-то не сделался радикалом. За 30 лет службы в разведке не знал ни одного случая, чтобы это произошло само собой. Всегда имеет место взаимодействие людей, вопросы - ответы, сомнения - решения.

Радикализация всегда происходит приблизительно по следующей схеме: я достаточно талантлив, чтобы понять, о чем говорят другие. Далее идут религиозная, историческая, политическая или культурная составляющие. Итак, первое, что мне хотелось бы, это демифологизировать Интернет как главного «виновника» радикализации. Это не так. Радикальные идеи распространяются через Интернет, но восприятие их вовсе не неизбежно.

Так что же нам следует делать? Звучат многочисленные призывы закрывать сайты, удалять аккаунты, взять под строгий контроль электронные средства массовой информации, «почистить» «Твиттер», то есть удалить 1250 тыс. аккаунтов. Вдумайтесь - миллион 250 тысяч! И тогда, дескать, с терроризмом будет покончено… Сколько времени, по-вашему, потребовалось пользователям, чтобы создать новые аккаунты? 10 секунд? Минута? Сторонники ИГИЛ, другие экстремисты гордятся и хвастают тем, сколько раз удалялись их аккаунты в «Твиттере». То же самое происходит с веб-сайтами. Если на заре Интернета на восстановление удаленного сайта уходило несколько месяцев, теперь это занимает три минуты. С учетом того, какие светлые умы сидят в этом зале, вскоре это будет делаться почти мгновенно.

Возникает закономерный вопрос: как нам быть с террористами в Интернете? Мы убираем платформы, убираем аккаунты, а они появляются вновь чуть ли не сразу. Что нам следует делать в этой связи? Нужно ли закрывать сайты в Интернете?

К чему приведет проявление излишних эмоций? Но я, как бывший разведчик, меньше всего хочу, чтобы дело обстояло таким образом. Удалив аккаунт в «Твиттере», мы ничего не добьемся. Надо выяснить, кто его создал, где этот человек находится, чем занимается, кого представляет и какие у него планы. Удалив информацию, мы будем блуждать в потемках - никудышная перспектива, с точки зрения разведчика. И еще - удалив очередную платформу, мы вряд ли заставим террориста бросить свое дело. Как бы не так! Он, как справедливо заметил Найджел, лишь позаботится о более совершенном кодировании, и это только добавит нам проблем. В общем, исходя из чисто эгоистических побуждений, советую не закрывать сайты, поскольку считаю это бесполезным делом - они все равно будут создаваться снова и снова, а нам, опять же повторяя сказанное Найджелом, нужно как можно больше информации, причем самой разносторонней.

Так что же нам следует делать? В начале 2000-х годов бывший министр обороны Дональд Рамсфелд задал вопрос: убиваем ли мы их больше, чем появляется новых? И ему ответили: «Вероятно, да». Интересно, что совсем недавно Президент Обама задал своему советнику по компьютерным технологиям аналогичный вопрос, который, однако, прозвучал несколько иначе: «Мы согласились с тем, что не можем уничтожить всех, не можем всех арестовать». И советник добавил: «Мы не можем удалить их всех». Потому что покончить с этим нельзя - удаленные сайты сменяют другие. Так как же тогда быть? Не побоюсь утверждать - на социальном медийном фронте мы как страны, как общества не принимаем достаточных мер противодействия терроризму. В этой связи считаю необходимым вести собственную информационную пропаганду и агитацию в электронном пространстве, поскольку она по своему содержанию будет намного превосходить все измышления террористов.

Подавляющее большинство людей, просматривающих такой контент, не становятся террористами. Это значит, что информация террористов не слишком привлекательна, дело не

в этом. Данная проблема важна, но она, так сказать, не смертельна. И если мы изначально уделяли бы ей достаточно внимания, сейчас ситуация выглядела бы намного лучше. Думаю, американская администрация поняла, что государственные контртеррористические пропагандистские онлайн-программы, разработанные в прошедшее десятилетие Государственным департаментом и АНБ, оказались провальными и вдобавок непомерно дорогими. Поэтому, на мой взгляд, задача в том, чтобы сделать это лучше, привлечь побольше светлых голов. Нам нужно лишь «поведать свой собственный рассказ», если можно так выразиться, и это будет достойным ответом поползновениям террористов в Интернете. В общем, чтобы количество людей, воспринимающих идеологию насилия, неуклонно сокращалось, нам нужно как можно лучше доносить до них наши слова. И тогда мы победим, потому что наши «рассказы» звучат более убедительно.

Комментарий из зала: *Два очень коротких комментария. Первый - если я сейчас захочу дать вам взятку и приготовлю деньги, то это не значит, что деньги надо запретить и что они во всем виноваты. Во всем виноват я, который дает взятку. Поэтому у профессионалов нет иллюзии, что мы боремся с компьютерами, или Интернетом, или с ИКТ как таковыми. Мы боремся с вредоносным использованием ИКТ. Но проблема в том, что в разных странах неодинаково определяется, что такое вредоносное использование. Поэтому в ООН мы не смогли определить все аспекты вредоносного использования ИКТ, но мы, по крайней мере, договорились, что Интернет и ИКТ не надо использовать во вредоносных целях, поэтому мы не боремся с самими средствами, мы боремся против их вредоносного использования, и я призываю договориться о главных параметрах - что такое вредоносная деятельность, чтобы определение и понимание такой деятельности в Канаде и России совпадало, чтобы, когда делается что-то вредоносное в России, оно подпадало бы под законодательство - и канадское, и российское.*

Второй момент связан со степенью радикализма используемых средств. Когда шла война против общего врага - фашизма в Германии и когда уже было ясно, что мы побеждаем, кто подверг Германию бессмысленной бомбардировке? Погибли сотни тысяч людей, по-моему, в Лейпциге, Дрездене. Какая была нужда уничтожать немецкое население? Там не все были нацисты. Кто бросил бомбу на Нагасаки и Хиросиму, и погибли полмиллиона человек? Там не все были из императорской армии.

Теперь берем другой пример - Югославия. Сам участвовал в переговорах в Англии, в Кардифе, где требовали полностью отключить Югославию от Интернета и всех ИКТ. Тогда только две страны из 60 - Россия и Армения - проголосовали против этого абсурдного акта. В кулуарах мне говорили: «Андрей, извини, это юридический абсурд, потому что в Eutelsat никого нельзя лишить доступа к информации с европейского спутника, если вы платите деньги. Но нашелся американский генерал, который посчитал, что радио Сербии слишком националистично. И это мнение генерала было использовано как юридический предлог, чтобы Югославию полностью отключить.

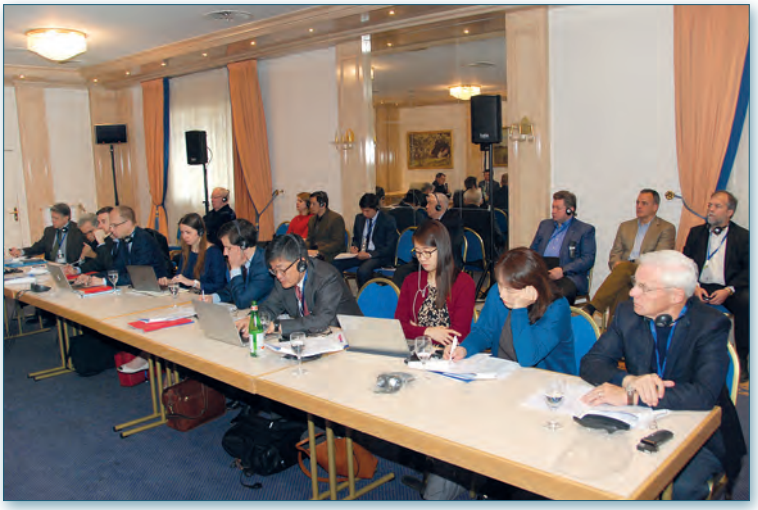
Возвращусь к тому, что Соединенные Штаты бросили кибербомбу на ИГИЛ - нашего общего врага. Это признано в ООН. Так, давайте не жалеть. Раз мы не жалели немецких фашистов, почему мы должны жалеть арабских фашистов, мусульманских? Значит, надо уничтожать, значит, надо принимать радикальные решения во имя будущего человечества. Значит, надо отключать все, что связано с Интернетом, и решать это радикально. А потом уже думать о том, как с теми, кто уцелеет, вести работу и как помочь им все восстановить.

А если мы будем придерживаться избирательных, основанных на идеологии подходах - Югославию будем отключать, а ИГИЛ с опозданием на два года будем отключать, - мне кажется, это неправильно.

Энекен Тикк-Рингас, Международный институт стратегических исследований (Великобритания): Итак, вот несколько тем, которые я не собиралась выносить на обсуждение, считая, что это должны сделать серьезные юристы с международным статусом. Темы эти относятся к области международного права, политики и дипломатии. Мне кажется, представляя себе международное право как таковое, каждый из нас помнит, что все мы придерживаемся разных взглядов и точек зрения на него и его отдельные аспекты. Я бы сказала, нам нужно прилагать дальнейшие усилия с целью утверждения полновластия международного права, всеобъемлющего утверждения его духа и буквы.

И в этой связи хочу вспомнить о человеке, который давно умер, но принятые им решения - а решения в конечном счете принимаются людьми, а не государствами - актуальны по сей день. Этот человек пользовался заслуженным уважением в Эстонии и России. Его звали Фридрих Мартенс (это его эстонское имя). Он известен также как Федор Федорович Мартенс. И не собираюсь спорить, каким ученым он был - эстонским или русским. Главное, он представлял Россию на Гаагской мирной конференции много лет назад. Как ученый-гуманитарий он также принимал участие в издании 15-томного сборника российских и международных договоров с 1874 по 1909 год.

Но почему я обратилась к столь далеким временам? Конечно, не для того, чтобы обсуждать юридические нормы того периода. Хотелось бы подчеркнуть его достижения на службе мировому сообществу, поскольку в ситуации, сложившейся накануне Гаагской конференции, когда государства решили договориться о международных правовых нормах, сделать это было совсем не просто. И тогда, понимая, что это займет много времени, он предложил временное решение, названное в дальнейшем «перекрестком Мартенса». До тех пор, пока не будет принят новый всеобъемлющий свод законов, война остается грязным делом, и высокие договари-



вающиеся стороны вправе декларировать, что в случаях, не подпадающих под принятые ими нормативные правила, оказавшееся в зоне военных действий мирное население остается под защитой основных принципов права, поскольку это проистекает из обычаев общения цивилизаций, из общечеловеческих законов и требований общественного сознания.

Почему это столь важно теперь? Конечно, за прошедшее с тех пор время международное право стало гораздо более сложным, но нам нужен принцип, нужно, как мне кажется, устранить противоречие конкретных (отдельных) норм и принципов. И, может быть, стоит воспользоваться принципом Мартенса применительно к кибербезопасности, я бы назвала это так, до тех пор, пока не будет выработан более комплексный подход, не будут разработаны всеобъемлющие принципы ответственного поведения государств в области международной безопасности в киберпространстве.

В киберпространстве продолжают действовать все нормы, правила и принципы, обусловленные международными соглашениями, международными традициями и общими принципами права. Даже при том что такое решение не будет полностью адекватным, удастся, как мне кажется, избежать ситуации, когда один процесс осуществляется при условии наличия дру-

гого процесса. С данным принципом мы имеем возможность продвигаться вперед в деле укрепления кибернетической безопасности на межправительственном уровне.

Возникает вопрос: является ли международное право достаточно объемным, адекватным применительно к комплексу проблем, с которыми теперь приходится иметь дело? И я не могу на него ответить. Но у меня есть предложение относительно путей подхода к некоторым из них, по-прежнему сохраняющим актуальность.

Отвечая на вопросы, какие нормы, кроме Устава ООН, могут применяться с целью обеспечения безопасности в области ИКТ, мне хотелось бы привести целый список, чтобы вы убедились, насколько богат и разнообразен набор средств, имеющихся в нашем распоряжении. Вот лишь несколько норм и инструментов, которым, на мой взгляд, стоило бы уделить внимание.

Я уже упоминала Устав ООН. В нем прописан статус Международного суда. Назвала бы также декларацию о дружественных отношениях 1970 года - статьи об ответственности государств; декларацию о недопустимости вмешательства во внутренние дела 1965 года; декларацию о недопустимости создания помех передаче данных 1981 года; декларацию об упрочении принципа от отказа применения силы в международных отношениях 1987 года; определение понятия «агрессия»; международную конвенцию по средствам связи; международное соглашение о гражданских и политических правах; устав Международного союза электросвязи; Конвенцию по правам ребенка; венскую конвенцию о юридических договорах; венскую конвенцию о дипломатическом иммунитете, а также многие другие соглашения, например, в области космической и морской информационной инфраструктуры или прав и обязанностей государств. Почему упоминаю об этом? Потому что это не упоминалось у нас до сих пор.

А теперь перейду к теме моего выступления: юристы принадлежат к тем школам, где обучались, - независимо от того, признают ли они это сами или нет, - и с этим связаны разногласия относительно норм применения права. В этом

контексте следует, на мой взгляд, искать ответ на вопрос о конкретных областях применения данных правовых норм. Параллельно на государственном и научном уровнях следует организовать инвентаризацию существующих норм, правил и принципов, изучить их и прокомментировать, выявить общие составляющие и определить пути их сближения, а также наилучшим образом разобраться в их содержании. Нам никогда не удастся достичь полного единообразия в толковании юридических норм и законодательных актов, такую задачу не следует ставить вообще, поскольку она практически недостижима, и в этом смысле нас не ожидает ничего, кроме разочарования.

Однако нам удалось достичь того, что в Женеве получило определение предсказуемости подхода разных стран к одному и тому же вопросу. Это может осуществляться в рамках специального комитета или каком-либо другом формате, включающем в себя разные школы права.

В дальнейшем участвующим в этом процессе государствам следует проанализировать и вынести на обсуждение понятия и принципы, проистекающие из первоначальных и специализированных соглашений, в ключе их перспективного применения в соответствии с существующими традициями трактовки международного права, поскольку в рамках международного права действительно существуют разные традиции. Поэтому нельзя утверждать, например, что российское представление о международном праве является примитивным и устаревшим, - существует лишь российский «взгляд на вещи».

Это позволит начать консультации в рамках Шанхайской организации сотрудничества, в рамках Конвенции о правах и обязанностях государств, принятой в Монтевидео, а также в рамках конвенции о киберпространстве. Все эти инструменты должны обсуждаться без каких-либо приоритетов и исключений.

В ходе такой работы неизбежно будет проводиться оценка степени аналогии. Но это отнюдь не будет означать простую констатацию аналогий в результате сравнения тех или иных документов. Поиском аналогий следует заниматься в случае

отсутствия нормы регулирования конкретного принципа, то есть какой-либо специализированной нормы. Тогда аналогию следует искать и в способах интерпретации определенных норм, в том, как организована их юридическая защита.

И почти в завершение моей темы - следует иметь в виду, каким образом осуществлялся поиск данной нормы, с помощью каких инструментов. Лишь тогда можно будет сделать правильные выводы о характере применения норм международного права и соответствующих результатах. Ведь в конечном счете как неоднократно отмечалось здесь, разработка норм применения информационных технологий и борьба с их использованием в преступных целях наряду с созданием глобальной системы кибербезопасности может осуществляться лишь в условиях взаимообмена информацией о целях и задачах всех заинтересованных сторон.

Считаю также, что на государственном уровне следует организовать изучение прецедентов практического применения традиционных правовых норм, которые могли бы «работать» в киберпространстве. Подчеркиваю, имеется в виду именно государственная практика, так как многие юристы будут возражать, упоминая применение общего (обычного) права. Но, повторяю, речь идет о государственной практике, о чем, надеюсь, нас обязательно будут информировать.

И последнее. Если мы будем предпринимать такие шаги, надо позаботиться о том, чтобы все эти процессы не зависели от успешности каждого из них. Выполнение этой задачи в параллельном режиме и вне определенной последовательности позволит производить «перекрестное опыление» каждого процесса. При этом мы должны также помнить о необходимости продолжить разработку новых норм и принципов, которые будут включены в законодательство заинтересованных стран. И сделать это можно уже в ходе следующей встречи. Может быть, этим следует заниматься на постоянной основе, поскольку очевидно, что в условиях растущей технологической взаимозависимости необходимо уделять больше внимания вопросам правового сотрудничества применительно к киберсфере.

Дэниел Штауффахер, фонд «ICT4Peace» (Швейцария): Мне хорошо знакома тема «ИКТ за мир» и связанные с ней проблемы, поэтому с интересом присоединяюсь к развернувшейся здесь дискуссии. Я также хорошо знаком с мирными инициативами, на протяжении многих лет исходящими из Москвы, и готов всецело поддержать эти благородные начинания.

Сегодня хочу ознакомить вас с так называемыми «уроками Джонсона» - передать ценный опыт работы в мировом информационном сообществе, поскольку в ходе всемирной встречи удалось сплотить правительства разных стран, а также гражданское общество вокруг идеи консенсуса и норм взаимопонимания, в том что касается нашей насущной проблемы, которая звучит так: «Как создать всеобъемлющее глобальное информационное сообщество, включающее в себя и развивающиеся страны, которое будет открытым для всех и жизнеспособным».

Конечно, это было очень сложной задачей - объединить усилия всех правительств, а также подключить бизнес и гражданское общество. Поэтому, может быть, из нашего опыта стоит извлечь уроки, поскольку, изучая документы GGI и другие нормативные акты, понимаю, что они принимались ради создания максимально безопасной и стабильной, мирной ИКТ-среды с единственной целью – в интересах экономического и социального развития, так как политика тесно связана с экономикой и проводится ради достижения экономических целей, что в конечном счете обеспечивает жизнеспособность правительств. Для этого необходимо наличие всеобъемлющего процесса, и VC-процесс, по-моему, был именно таким. VC, кстати, включает в себя параграф 36, где речь идет о мерах предотвращения (о превентивных мерах), обеспечивающих мир в области ИКТ. И это, на мой взгляд, всегда следует иметь в виду.

Обращаясь к участникам конференции GGI, хотелось бы отметить наш очевидный успех, но этого, как мне кажется, еще недостаточно, поскольку мы имеем дело с очень сложным вопросом и весьма разнообразным составом участ-

ников, имею в виду государственные структуры и организации, а также частный сектор. Поэтому в дальнейшем нас ожидают невероятно трудные задачи. Прежде всего это связано с тем, что GGI продолжает оставаться небольшой группой стран и система, которую мы пытаемся выстроить, должна включать в себя развивающиеся государства, чтобы быть достаточно сильной. В этой связи возникает важная задача: как сделать их участниками конференции и, главное, как вывести на одинаковый с нами уровень понимания важности вопросов, которые обсуждают здесь юристы и дипломаты. По-моему, - об этом уже упоминалось в отчете со всеми надлежащими выводами - мы тем не менее должны продолжать этим заниматься.

Средства и деньги тоже становятся важной темой. В рамках программы «ИКТ за мир» и в рамках других инициатив мы организуем работу по всему миру с целью обучения дипломатов в Латинской Америке, Азии, Африке. И конечно, то, что мы там видим, сильно различается между собой. В целом наши успехи довольно велики, но что касается Африканского союза, Организации африканских государств и даже Азии, то там наше влияние пока остается недостаточным. Поэтому актуальным становится вопрос: как заставить эти государства осознать необходимость создания глобальной юридической системы, глобального правового поля, развиваться опережающими темпами?

Другая трудная задача, если обратиться к процессам в рамках ООН, - в принимаемых там документах никак не отражены наши проблемы, несмотря на их глобальный характер. Имею в виду безопасность и мир и развитие. Отсюда разобщенность между двумя сообществами дипломатов, разногласия в гражданском обществе и т. д. Это еще одна задача, которую пытаемся решить, - преодоление, так сказать, «раскола». С этой целью мы уже занимаемся киберстроительством в рамках нашей системы, создали несколько подотчетных вспомогательных организаций.

И в заключение хочу сказать несколько слов о частном секторе. Несмотря на выдающуюся роль в энергетике и VC-про-

цессе, о чем говорил здесь господин Крутских, частный сектор до сих пор не принимал участия в какой-либо дискуссии и не был ее объектом. Конечно, он является частью конструкции, поэтому при обсуждении правовых норм необходимо иметь в виду не только регулирование взаимоотношений между государствами, между государствами и фирмами, но также организацию отношений между фирмами и потребителями, всеми, кто является частью системы.

Система образована не только крупными компаниями, в Швейцарии, например, мелкие предприятия и индивидуальный бизнес защищены в одинаковой степени. В этой связи, как мне кажется, стоит подумать о том, как стимулировать активность частного бизнеса, с чего следует начать. Возможно, частным компаниям следует предоставить более широкий выбор сферы деятельности. И право такого выбора должно найти отражение в действующем законодательстве. В Швейцарии, как известно, существует развитая финансовая индустрия, и крупные кредитные организации уже предлагают конкретные пакеты мер, весьма выгодные для частного сектора. Это способствует повышению безопасности всей системы в целом. Наверное, на уровне правительств следует проводить консультации относительно способов налаживания контактов с частным бизнесом и его поддержки. Нужно создать специальную инфраструктуру, в которой частному сектору отводилось бы соответствующее место.

В общем, необходим более комплексный подход к решению тех задач, о которых я упомянул.

Новые медиа и киберпространство: современные способы производства и распространения информации

Михаил Поляков, МГИМО МИД РФ: Хочу вкратце ознакомить вас с e-media в киберпространстве, со способами производства и потребления в Интернете. Почему я заговорил об e-media? В последние годы эта область неуклонно расширяется и очень быстро развивается, становится все более популярной, поскольку люди (пользователи) проводят все больше

времени в этой среде. Постараюсь показать, как устроена ее «глобальная кухня», что представляют собой новые технологические парадигмы, расскажу об основных тенденциях в e-media, скажу пару слов о e-media-экономике и, может быть, попытаюсь сделать прогноз на будущее.

Итак, давайте познакомимся с краткой характеристикой глобального цифрового пространства. Сейчас население Земли составляет около 7 млрд. человек, и более половины из них живут в крупных городах. 3,5 млн. человек пользуются Интернетом. Это 46-процентный охват. Многие из них активно пользуются социальными сетями, это более 2 млрд. человек. 3070 млн. человек имеют мобильные телефоны, это 50-процентный охват. Обратившись к перспективам распространения Интернета, станет очевидно, что нам предстоит охватить еще полмира. Более половины населения планеты пока еще не имеют доступа к Сети. И что в данной связи собираются предпринять крупнейшие мировые медийные магнаты? Давайте попробуем выяснить это.

Как известно, «Google» начал широко внедрять программу лумов (looms), чтобы распространить Интернет на территориях, где это невозможно сделать с помощью кабельных средств. Этот лум летает над территорией Шри-Ланки, обеспечивая работу Интернета во всей стране. Другой проект получил название «Killer». Так назван потребляющий солнечную энергию беспилотник, разработанный «Facebook» с аналогичной целью. Неделю назад его продемонстрировал Марк Цукерберг на конференции в США. Аппарат еще не поднялся в воздух, но, насколько я знаю, событие должно произойти в следующем году, когда, кстати, начнется серийное производство таких устройств.

Почему же медийные боссы так заинтересованы в распространении Интернета среди широких масс людей? Назову несколько цифр, определяющих численность населения пяти крупнейших стран мира. Две из них - это Китай и Индия, а третья - «Facebook». Это около 1 млрд. человек. Следом идут США и Индонезия. «Facebook», как вы поняли, сейчас занимает третье место, и население этой «страны»

увеличивается очень быстро. Через несколько лет она станет крупнейшей в мире. Согласно определению, государство - это пространство, где проживают люди. Подумайте, пожалуйста, сколько времени в своей жизни люди проводят в «Facebook». Такова краткая характеристика социальной медийной среды.

Социальная медийная среда (социальные сети) является крупнейшим в мире киберпространством - 2030 млн. человек в настоящее время. Одна треть населения Земли приобщена к социальной медийной среде. 27% этих людей пользуются мобильными телефонами для связи с ней. Уверен, прямо во время нашей дискуссии большинство тех, кто присутствует в этом зале, могут войти в медийную среду с помощью мобильников, причем некоторые находятся там практически постоянно. Вспомните такое понятие, как определение «глобальная деревня», введенное Маршаллом Маклюэном в книгах под общим названием «Гутенбергова Галактика». Еще в начале 1960-х годов Маршалл Маклюэн показал, во что превратился мир после появления радио и телевидения. Он утверждал, что мир стал намного меньше из-за огромной массы стремительно распространяющейся информации. А теперь скорость распространения информации выросла настолько, что «глобальная деревня» уменьшилась, я бы сказал, до размеров «глобальной кухни», где любое событие, личная жизнь любого человека мгновенно приобретают глобальный масштаб. Поэтому каждый из нас, кто является пользователем глобальных сетей, сидит теперь на «глобальной кухне», если можно так выразиться.

Вот некоторые статистические данные бизнес-разведки, ежегодный отчет бизнес-инсайдера, в котором показано, что представляли собой различные медийные среды на протяжении последних четырех лет. Как видите, телевидение, радио, печать и все другие средства массовой информации постоянно сокращаются в течение истекших четырех лет. Рост отмечается лишь в цифровой среде, и самый высокий показатель этого роста приходится на мобильные устройства, о которых мы тоже поговорим.

Чем люди занимаются в Интернете? Вот отчет участника рынка электронных средств коммуникации (e-marketer), охватывающий последние семь лет. Он демонстрирует, чем в действительности заняты люди в Интернете. В США люди проводят в цифровой среде не менее пяти часов в сутки. Как вам кажется, пять с половиной часов в сутки - это много? По-моему, это целые полдня. Значит, в США люди находятся в цифровой среде полдня.

А как обстоит дело в Индии, например? Вот другие данные, статистика по Индии. Там ситуация несколько иная. Больше всего времени люди тратят на общение в режиме онлайн, преимущественно в социальных сетях. Они также тратят время на развлечения, интернет-шопинг и приобретение билетов через Интернет. Вот чем заняты люди. Вспомните выступление господина Якушева из «ICANN», говорившего о трех уровнях Интернета. Это инфраструктура - первый уровень; передача (транспортировка и кабели) - второй уровень; третий уровень - социальные сети (медиа) и цифровые медиа.

Теперь несколько слов о производстве медийных средств. Существуют две производственные модели: старая и новая. Старая модель предполагает наличие нескольких уровней между автором и читателем (потребителем). Это автор, дизайнер или ведущие и дикторы, если речь идет о телевидении, производственная группа, печатающая газету или создающая телепередачу, дистрибуция - продажа печатных изданий (в киосках, например); это спутники - в случае с телевидением, а также ручное распространение продукции и, наконец, читатель или те, кто получает телевизионный сигнал. Это старая модель. Новая модель гораздо проще и короче. Между автором и читателем нередко нет никого, иногда даже редактора. Что это дает? Многое, потому что автором может быть практически каждый.

Теперь я попытаюсь классифицировать медийные средства. Их можно разделить на пять групп: средства, предназначенные для общения (связи), такие как социальные медиа (сети); средства, созданные для распространения информа-

ции, точек зрения, изображений; средства, созданные для развлечения; средства, созданные для поиска; средства, созданные для осуществления обмена, покупок и приобретения собственности.

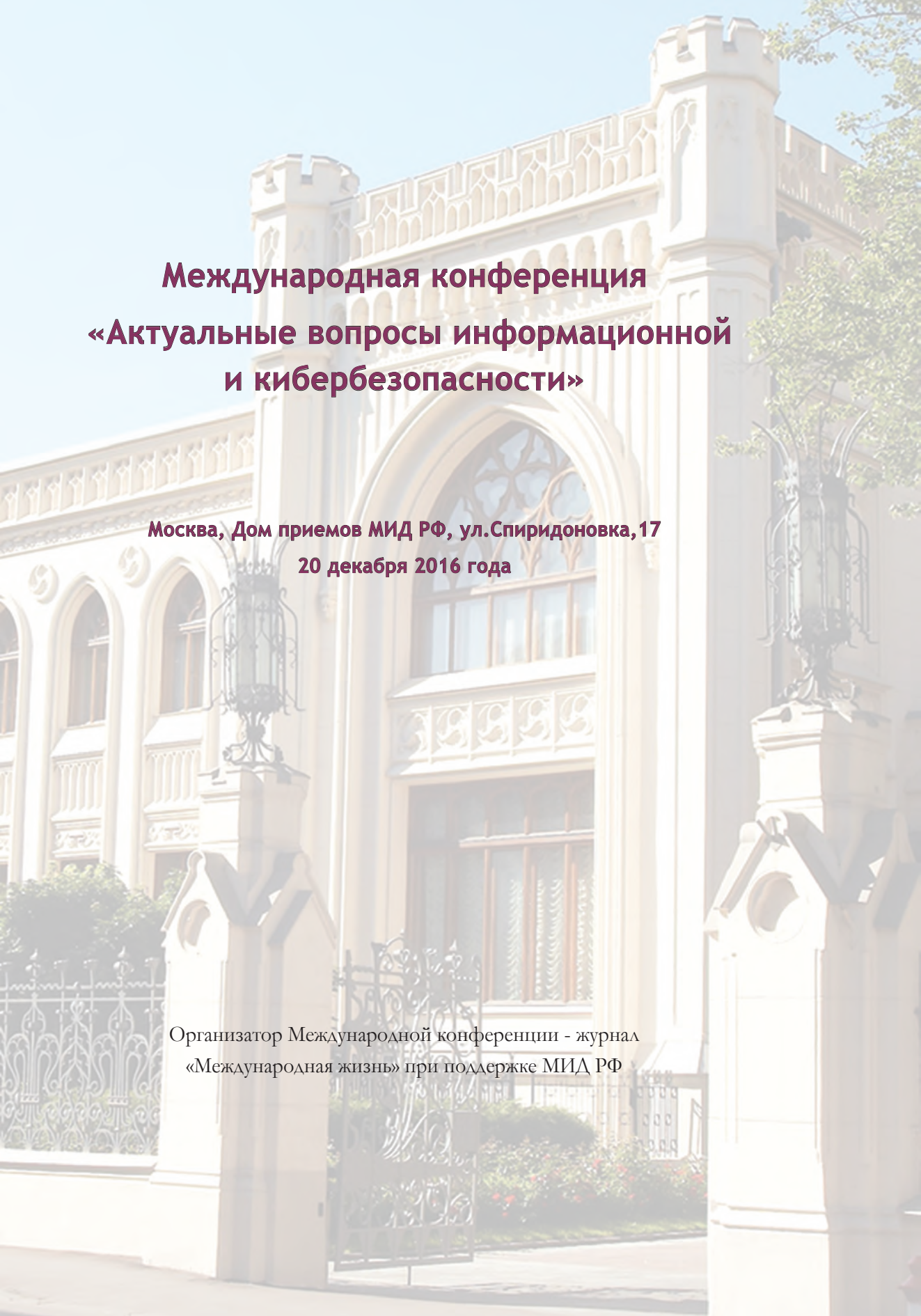
Вот один из примеров мгновенной публикации, взятый из «Twitter». Широко известный пример с фотоснимком, сделанным на церемонии вручения «Оскара», который в течение короткого времени посмотрели 2 млн. человек. Теперь, когда существует цифровая среда, появилось много авторов, и в дальнейшем их будет еще больше. Некоторые ученые утверждают, что автором становится каждый, кто приобретает смартфон. Осуществлять мониторинг такого огромного количества авторов, на мой взгляд, далеко не просто.

Поговорим теперь о тенденциях. Основной тенденцией в новой медийной среде стало превращение мобильных телефонов в главный слоган для всех разработчиков программных продуктов (publishers). Теперь все разработчики «завязаны», так сказать, на мобильные устройства. На телевидении тоже происходят перемены. Крупные каналы постепенно сдают позиции. Мессенджеры (messengers) стали новой средой (медийным средством), и даже социальные сети переживают спад. Мессенджеры быстро идут на подъем, и это движение в будущем лишь еще больше ускорится. Power распространяется все больше на уровне индивидуальных пользователей, и, мне кажется, государства не могут осуществлять надлежащей контроль в этой новой медийной среде, там действуют свои собственные законы.

Несколько слов насчет будущего. Вот прогноз относительно количества пользователей и устройств, которые появятся в Интернете в ближайшие три года. Количество интернет-участников, как известно, растет в геометрической прогрессии. Причем это не только люди, но и разнообразные устройства - смартфоны и т. п. Таким образом, мы имеем так называемый «неодушевленный Интернет». Устройства стремительно завоевывают интернет-пространство. Пройдет еще около двух лет, и в Интернете будет 18 млрд. пользователей, но лишь половина из них - люди.

Марк Цукерберг - один из самых могущественных людей в новом медийном пространстве и цифровом мире. Вот его представление о том, что будет происходить в Интернете в ближайших три года. Если посмотреть на «Дорожную карту», можно увидеть, что первые два этапа уже позади. Это экосистема и общество. Теперь на очереди технология - создание искусственного разума, виртуальной реальности, а также того, что называется… «киберсингулярность». В общем, мы не можем даже четко представить, что будет происходить в Интернете, но количество участников и размер киберпространства растут в геометрической прогрессии, и ученые не в состоянии предсказать, что нас ждет через пять-десять лет.

Это все, что мне хотелось сказать. Но как обстоит дело с трудностями, о которых сегодня шла речь? Медийная популяция очень велика и продолжает расти, и ее не контролирует государство. Кто вообще контролирует кого? Логическое развитие данной субстанции показывает: изменения с целью обеспечения безопасности должны происходить не только в медийной среде, эта среда также оказывает большое влияние на государства, и они, может быть, тоже должны изменяться. Надеюсь, что лидеры медийной среды в состоянии осуществлять контроль на третьем уровне ее развития, и в будущем некоторые из них помогут в ходе выполнения тех задач, которые обсуждаются здесь сегодня.



Международная конференция «Актуальные вопросы информационной и кибербезопасности»

Москва, Дом приемов МИД РФ, ул.Спиридоновка,17

20 декабря 2016 года

Организатор Международной конференции - журнал «Международная жизнь» при поддержке МИД РФ

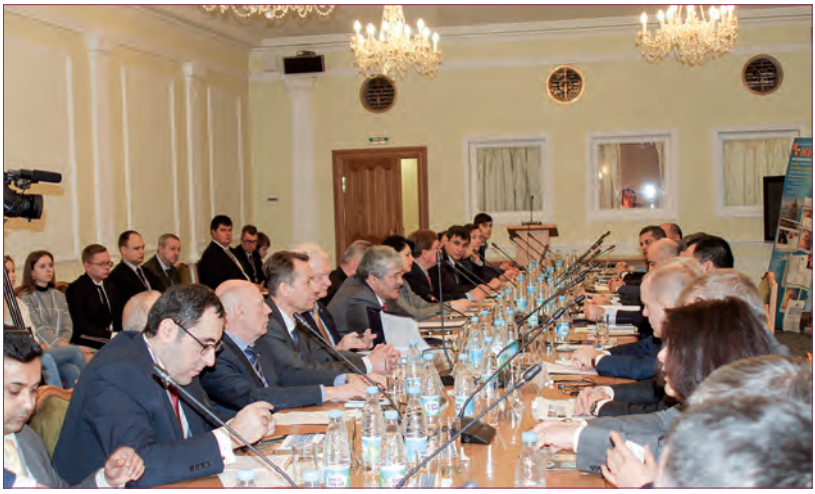
Армен Оганесян, главный редактор журнала «Международная жизнь»

Наша конференция посвящена теме, которая за последнее время стала весьма актуальной. Если пользоваться журналистскими терминами, то есть ощущение, что мы идем по минному полю: то ли нет саперов, то ли мины особого свойства, на которые не нашли средств противодействия. Опасность стала настолько всеобъемлющей, что охватывает все сферы личной жизни человека, общества, государства. Наша конференция затрагивает темы межгосударственной безопасности, борьбы с терроризмом, криминалом и военными угрозами. Бизнес проявляет заинтересованность в решении этих вопросов. Поэтому сегодняшняя программа сложнокомпозитная. У нас присутствуют представители всех тех сфер, которые я сейчас перечислил.

Олег Сыромолотов, заместитель министра иностранных дел РФ

Тематике безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) или международной информационной безопасности (МИБ) как в России, так и во всем мире уделяется повышенное внимание. Повсеместный интерес к ней обуславливается тем острейшим политическим противоборством, которое разворачивается на международной арене с использованием ИКТ.

За этот год ситуация в международном информационном пространстве резко ухудшилась. Основной причиной тому стало не только увеличение случаев использования ИКТ террористами и рост числа хакерских атак, наносящих колоссальный ущерб мировой экономике, но и создание некоторыми государствами ситуации тотального недоверия в информационном пространстве путем выдвижения беспочвенных обвинений в адрес других стран о причастности к хакерским атакам, якобы совершенным на их политические и частные интернет-сайты. Считаем, что это порочная практика, которая не только препятствует обеспечению МИБ, но способствует эскалации напряженности между государствами.



Очевидно, что в этом контексте особое значение приобретает желание и умение договариваться. Россия последовательно выступает с концепцией предотвращения военно-политических конфликтов в информационном пространстве, неприменения силы в этой сфере, уважения принципов национального суверенитета и невмешательства во внутренние дела. Нашей ключевой инициативой и приоритетом на данном направлении является разработка и принятие под эгидой ООН универсальных правил ответственного поведения государств в информационном пространстве. В условиях, когда принципиальные противоречия не позволяют выйти на заключение универсального международного договора, разработка и принятие добровольных правил поведения позволит оформить широкую политическую договоренность о неконфронтационном статусе информпространства.

В этом контексте особое значение приобретает деятельность новой Группы правительственных экспертов (ГПЭ) ООН по МИБ, которая в соответствии со своим мандатом занимается выработкой подобных правил. Надеемся на успешное завершение ее работы в следующем году.

На национальном уровне Россия также предпринимает активные шаги для обеспечения информационной безопасности. Главным событием этого года в области МИБ считаем утверждение Президентом Российской Федерации новой Концепции внешней политики Российской Федерации. В соответствии с ней обеспечение национальной и международной информационной безопасности является одним из условий поддержания междуна-

родной безопасности и стабильности. Данный документ закрепляет намерение России противодействовать использованию ИКТ в военно-политических целях, не соответствующих нормам международного права, а также добиваться выработки под эгидой ООН универсальных правил ответственного поведения государств в области обеспечения МИБ.

Еще одним знаковым событием стало принятие новой Доктрины информационной безопасности Российской Федерации. Рассчитываем на то, что данная доктрина станет основой для обеспечения эффективного взаимодействия с государствами - членами ОДКБ, СНГ, ШОС, государствами - участниками БРИКС, а также другими государствами и международными институтами в области информационной безопасности.

Надеюсь, что данная конференция будет способствовать развитию конструктивного диалога российских и зарубежных экспертов и обмену опытом между ними, а соображения, высказанные участниками конференции в ходе дискуссии, помогут сделать международное взаимодействие в области противодействия современным вызовам и угрозам в информационной сфере более эффективным.

Желаю вам успешной и плодотворной работы.

Григорий Рапота, государственный секретарь Союзного государства России и Белоруссии

Уважаемые участники и гости конференции, проведение подобной конференции полагаю крайне своевременным и полезным.

В современном обществе информационная безопасность является системообразующим фактором практически всех сфер его жизни. Она оказывает влияние на состояние экономической, оборонной, социальной, политической и других составляющих национальной безопасности. При этом информационная безопасность сама выступает составной частью национальной безопасности, значение которой неуклонно растет.

В новой Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 года №646, учитывается современная международная обстановка, положение России в мире, дается четкое определение национальных интересов в сфере информационной безопасности, указываются основные информационные угрозы и формируются стратегические цели национальной политики,

касающиеся защиты суверенитета, политической и экономической стабильности, обеспечения основных свобод и прав человека, экономики, военной сферы, дипломатии, науки и образования в информационной сфере.

Принятие этой доктрины очень важно и для Союзного государства, в котором практически создано единое информационное пространство.

В основу обеспечения его информационной безопасности была положена в том числе реализация мероприятий программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий».

В настоящее время идет процесс утверждения программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств - участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере».

В рамках реализации программы предусматривается:

- защита системного и прикладного программного обеспечения автоматизированных систем управления технологическими процессами критически важных объектов Республики Беларусь и Российской Федерации;

- разработка перспективных способов, средств и систем защиты информации на основе применения новых технологий, в том числе технологий виртуализации, элементов искусственного интеллекта, использования новых криптографических методов и аппаратных средств в интересах повышения защищенности информации в автоматизированных системах управления технологическими процессами критически важных объектов;

- повышение защищенности информации от несанкционированного доступа и от ее утечки по техническим каналам;

- создание средств обнаружения компьютерных атак, а также перспективных телекоммуникационных технологий и оборудования для защиты общих информационных ресурсов Союзного государства.

Естественно, что при реализации этой программы будут учитываться основные положения принятой в России доктрины.

Одним из механизмов согласованных действий по обеспечению информационной безопасности Союзного государства являются также ежегодно проводимые научно-практические кон-

ференции «Комплексная защита информации». Очередная конференция планируется в 2017 году.

Разрешите пожелать участникам конференции успешной работы. Уверен, что сегодняшняя дискуссия будет способствовать нахождению ответов на многие актуальные вопросы информационной и кибербезопасности.

Сессия 1. Современные вызовы и угрозы в контексте новой Доктрины информационной безопасности и Концепции внешней политики Российской Федерации

Об итогах работы Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в 2016 году

Андрей Крутских, посол по особым поручениям, специальный представитель Президента РФ по вопросам международного сотрудничества в области информационной безопасности

Для Группы правительственных экспертов ООН 2016 год был сложным и под конец трагическим.

Если говорить о каком-то большом политическом позитиве в политической сфере кибербезопасности, то, безусловно, созыв по инициативе России Группы правительственных экспертов ООН по международной информационной безопасности - это очень актуальное, вовремя организованное мероприятие. Россия долго его «пробивала», и группа состоялась. Она собиралась уже дважды - в августе и ноябре. Это очень позитивный момент.

Группа имеет расширенный состав, что является прецедентом в ооновской практике. Надо отдать должное бывшему Гене-

ральному секретарю ООН и его помощникам, которые сумели сделать ее достаточно представительной и объективной. 56 стран активно лоббировали себя в участники этой группы, в конечном итоге было отобрано 25 стран. Ее основной мандат был сформулирован Россией и поддержан международным сообществом. Его суть заключается в том, чтобы от философских, общеполитических дискуссий и изучения общих моментов международное сообщество решило перейти к практическим шагам, именно к выработке принципов, норм, правил, ответственного поведения государств в информационном пространстве, что является практической мерой. Больше того, в рамках данной группы Россия (до этого она «обкатывала» это на международных конференциях, которые проводились в Женеве и Пекине) предложила новый вариант резолюции Генеральной Ассамблее ООН - как будут работать правила, если их одобрит международное сообщество. Резолюция, безусловно, не будет носить обязательного характера, но станет прелюдией к более серьезному, проработанному и детализированному международному договору, который позволит прекратить кибербеспредел, происходящий в мире.

Под кибербеспределом я понимаю следующее. Начну с России. Президент РФ В.В.Путин озвучил цифры: в среднем в год на Россию совершается более 70 млн. кибернападений, что даже можно назвать прямой кибервойной. Это не мировой рекорд. В ходе наших консультаций в Вашингтоне и Пекине стало известно, что между Китаем и США существуют взаимные проникновения и нападения и их число еще выше. Идет проверка уязвимости, и где гарантия того, что обнаруженные «слабые места» другого государства не будут использоваться. По данным нашей и американской разведок, более 140 государств активно занимаются подготовкой, проводят учения, создают специальные силы для ведения кибервойн. Два года назад министр обороны Великобритании прямо заявил о том, что его страна намерена наращивать наступательный кибернотенциал. Она будет наращивать, а мы все будем смотреть? Да нет, конечно. Мы все будем втягиваться в эту безумную гонку вооружений с совершенно непредсказуемыми последствиями.

Как представитель России в этой группе могу сказать, что у меня сдержанный оптимизм, поскольку, несмотря на то что пра-

ктически все участники, 25 государств, придерживаются разных точек зрения, блокируясь по-разному, они тем не менее исходят из того, что правила нужны. В какой форме они должны быть - это предмет обсуждения внутри группы.

В июне 2017 года группа должна завершить свою пятую сессию. Доклад, соответствующие рекомендации и проект резолюции с правилами поведения будут представлены Генеральному секретарю ООН и Генеральной Ассамблее. Основное противоречие среди участников группы состоит в следующем: Россия в принципе выступает за предотвращение конфликтов в киберпространстве. США возглавляют блок тех стран, которые считают, что милитаризация киберпространства произошла, ее нельзя повернуть вспять или остановить, поэтому, дескать, надо договариваться о регулировании конфликтов в киберсфере.

Хочу перейти к тому моменту, который вызывает у нас реальную озабоченность - у Президента РФ, силовых структур, на политическом уровне, да и в мире, это вызывает озабоченность. Если западная философия предполагает доведение до этих конфликтов, а не их предотвращение в зародыше, то как тогда надо воспринимать слова Байдена, когда он говорит, что Америка задумала нанести ответный кибердар по России. При этом, как всегда, доказательств нет. На что же тогда они рассчитывают? Что Россия смирится, испугается?! К счастью, наш президент зарекомендовал себя как человек, который не подставит другую щеку. Наши политические руководители неоднократно заявляли о том, что у нас не повторится 22 июня 1941 года в киберпространстве.

В данном случае возникает вопрос: почему США до сих пор не нанесли такой удар? Частично это объясняется тем, что, как считает Б.Обама, Америка не обеспечила себе дислокационного преимущества. Американцы хорошо проинформированы о том, что мы эту атаку просто так не оставим, вторую щеку не подставим. В результате получилось, что американцы начали считать варианты: они ударят - мы ответим.

На официальных консультациях с ближайшими союзниками США я задавал один и тот же вопрос: давайте вспомним американскую атаку на Иран, она ведь осуществлялась не только напрямую, но в том числе и через киберпространство с использованием инфраструктур других стран. А если удар будет нане-

сен через вас, то вы ни при чем? Или это прелюдия к мировой войне? Как это все воспринимать? И мне было отрадно услышать, что умирать в мире никто не хочет - ни за Клинтон, ни за Трампа. У всех своя жизнь, все рассчитывают на оборону, а не на нападение. А в данном случае речь идет о нападении с непредсказуемыми последствиями.

Но поскольку дислокационного преимущества у американцев нет, видимо, в ходе внутриполитической борьбы, в условиях экономического кризиса стало модным разыгрывать антироссийскую политическую карту, чтобы найти виноватого. Нас считают главной причиной проигрыша Х.Клинтон, как будто не было провалов политики всей администрации Б.Обамы в течение многих лет.

На западных конференциях, встречах и переговорах считается плохим тоном ссылаться на Сноудена и на те разоблачения, которые он сделал. Нет Сноудена - нет глобальной американской системы информационного шпионажа, нет прослушек. Есть только одни российские хакеры. США важно сформировать такую ментальность в мире, которая легко позволяет приписывать другим то, что делают сами американцы. В этом и кроется суть истеричной кампании, которая развернута в США, по закреплению образа России как врага и в данном случае врага, действующего в киберпространстве. Это скоординированная кампания идет в Европу, где подспудно проводится мысль, что Россия обрела новые способы подорвать всю западную демократию, всю западную цивилизацию. Вот тот политический заряд, который сейчас пытаются взорвать.

Прагматизм Д.Трампа основан именно на том, что он по-другому смотрит на то, как можно Америку сделать реально сильнее, в перспективе это сделает нашу жизнь сложнее. Но никто в мире не хочет умирать, все хотят лучшей жизни, хотят преодоления противоречий. И в этой связи мне кажется, что есть шансы договориться, возобновить активный кибердиалог с США. Между Россией и США уже заключены три весьма впечатляющих соглашения, которые позволяют исчерпывать инциденты до того, как они переросли в конфликты. Но есть еще другая наша идея - договариваться с Америкой о реальном, практическом предотвращении конфликтов в киберсфере. Нужно договариваться, а не переносить диалог в политическую плоскость, СМИ и нагнетать напряженность.

О новой Доктрине информационной безопасности Российской Федерации

Дмитрий Грибков, референт аппарата Совета безопасности РФ

Как уже было сказано, Доктрина информационной безопасности Российской Федерации в новой редакции была утверждена 5 декабря 2016 года. Национальные интересы в документе определяются как объективно значимые потребности личности, общества и государства, касающиеся их защиты.

Хотел бы обратить особое внимание, что обеспечение безопасности и при этом обеспечение развития проходит красной нитью через весь документ. Во многих пунктах при внимательном рассмотрении эта связка присутствует. Это неслучайно, поскольку все-таки понятно, что мы живем в новых условиях развитых ИКТ, понимая все возможности, которые дают данные технологии, и те угрозы, которые они несут вместе с собой. Мы должны четко представлять, что одно от другого неотделимо и что эта связка должна, безусловно, соблюдаться. Один из принципов, который в документе прописан - это достижение баланса между свободным обменом информацией и теми ограничениями, которые влечет за собой обеспечение безопасности.

Грустный факт: до последнего времени любое развитие и внедрение информационных технологий уже на начальном этапе связывается с проблемой обеспечения безопасности. Что, собственно говоря, является сферой регулирования в информационном пространстве? В новой редакции это определено более четко по сравнению с прошлым документом (прошло 16 лет). Сфера регулирования - это совокупность информаций как таковых и информационные инфраструктуры, то, что на языке специалистов называется «железками», и, конечно, регулирование тех отношений, которые возникают в этой области у всех участников. Данная тема - рассмотрение или нерассмотрение этих информаций - стара как мир. Эти

аспекты, связанные с информацией как таковой, можно и нужно называть информационно-психологической сферой. Все, что связано с инфраструктурными моментами, объектами информатизации, сетями, информационными системами, - это информационно-психологический аспект. Такое деление, безусловно, присутствует.

Национальные интересы в документе почти такие же, какие были в документе 2000 года, некоторые формулировки претерпели изменения, но главный национальный интерес - это защита конституционных прав и свобод человека и гражданина, что является приоритетом их деятельности. В этой области мы заостряем внимание на том, что здесь есть информация и вопросы защиты интересов граждан, которые непосредственно связаны с веб-технологиями.

Когда новая доктрина была опубликована, в СМИ появились высказывания, что в новом документе, в новой редакции стратегии, нет четко и внятно написанного тезиса или положения о том, что цензура запрещается. Кто-то считает, что она должна быть. Боже упаси! Во второй части Конституции четко прописаны права и свободы человека и гражданина. В пункте 5 ст. 9 так и звучит, как было написано в предыдущей редакции стратегии: гарантируется свобода массовой информации, цензура запрещается. Если мы ссылаемся на Конституцию, то трудно обвинять Россию в том, что у нас есть цензура.

К этому же аспекту, который связан с информацией, относится и защита духовно-нравственных ценностей человека. Этот момент в документе тоже присутствует.

Второй национальный интерес - защита информационной структуры, кибербезопасность, о которой мы все говорим. И наши оппоненты, и наши коллеги это прекрасно понимают, поскольку реально существуют кибератаки и кибернападения.

Следующий национальный интерес связан с развитием отрасли информационных технологий. Для России это вопрос не праздный, как дураки и дороги. Имеются еще наши отставания. Сейчас наблюдаются, безусловно, прорывы, хороший задел на будущее. Были постобсуждения после публикации доктрины, что как-то все плохо, слишком сгущены краски, все как-то мрачно. Но документ ведь направлен на предотвращение угроз.

Что касается развития. Сейчас на сайте Совета безопасности идет обсуждение документа «Стратегия развития информационно-

го общества в Российской Федерации», который был утвержден в 2008 году. Вот там как раз уместно вести речь о развитии, тенденциях, перспективах тех наших достижений, которые, естественно, есть и будут.

Еще один момент - доведение достоверной информации о государственной политике РФ как внутри страны, так и за рубежом. Наши оппоненты могут называть это пропагандой. В этой связи следует говорить о трудностях работы средств массовой информации. Недавним примером того служит попытка или решение Европарламента отнести «Russia Today» к игиловской пропаганде - как к этому относиться?! Национальный интерес нашего государства был и в той редакции доктрины и, естественно, присутствует в новой.

Следующий блок вопросов - формирование системы международной информационной безопасности. Этот момент более выпукло сформулирован в новой доктрине. Сейчас это очень серьезная составляющая безопасности России. Зачастую наши партнеры по переговорам стараются свести все к кибербезопасности, потому что тема весьма актуальная. Но проблемы, связанные с информацией как таковой, имеют право на обсуждение.

Возвращаясь к вопросу о том, что Россия влияет на американские выборы. В начале года это трудно было даже представить. Если американцы так серьезно об этом говорят, то это проблема. Мы за то, чтобы открыто и широко обсуждать с нашими партнерами такой вопрос. Говорилось о взломе почтовых ящиков демократов, о влиянии на голосование - подобная риторика нарастала, чем ближе к выборам, тем больше говорилось. За неделю до выборов американская сторона обратилась официально к России с запросом: давайте разберемся. Мы с самого начала говорили, если есть факты, давайте разберемся. Отрадно, что это взаимодействие было реализовано на основе тех решений, которые были приняты еще в 2013 году.

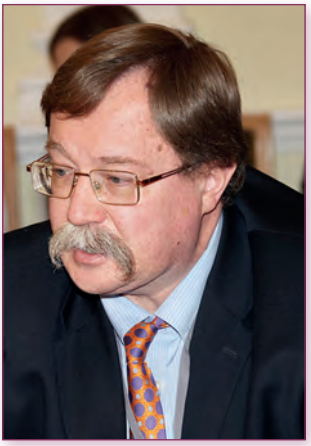
Каналы связи, которые были обозначены, работают. С одной стороны, приятно, что все сложности решаются, а с другой - проблема столь велика и значима, что никто этот механизм не откладывает в долгий ящик. Мы готовы к совместному сотрудничеству и решению всех вопросов со всей ответственностью. Документ содержит и оценку тех угроз, которые существуют в военно-политической сфере. Исходят от террористическо-экстремистских

и криминальных группировок, в нарушении национальной стабильности. Все вмешательства во внутренние дела других государств в разных регионах недопустимы, имею в виду «цветные революции». Без ИКТ ничего не бывает, мы это понимаем. Надо обязательно налаживать международные связи и по возможности предотвращать теракты. В банковской сфере кража денег с карт - сейчас это только капля в море. Когда ФСБ было заявлено о возможности хакерских атак голландцев, стало понятно, что надо друг с другом договариваться.

В документе «О Стратегии национальной безопасности Российской Федерации» обозначено девять приоритетов, а у нас написаны только пять, такие, как качество жизни, здравоохранения и т. д. Угрозы, связанные с использованием ИКТ, не так ярко выражены. А в оборонной области, в области экономической и государственной безопасности есть своя специфика, свои нюансы. Мы за то, чтобы предотвращать конфликты. В новом документе есть новый аспект - защита сегмента Интернета. Проблемы, конечно, присутствуют. Устойчивость нашего сегмента Интернета - тоже проблема номер один. В этой связи наши партнеры то готовы, то не хотят ее обсуждать.

О безопасности личности, общества и государства

Илья Рогачев, директор Департамента по вопросам новых вызовов и угроз МИД РФ



Хотел бы «разворошить» еще один пласт. Речь шла о военно-политической, стратегической безопасности, об отношениях между государствами в информационной и киберсфере. Есть другая область безопасности - безопасность личности, общества и государства. В этой области прежде всего надо говорить о криминальных угрозах и вызовах. Национальная стратегия это, в частности, учитывает. Здесь огромный

океан угроз. Мы знаем, что через Интернет продают наркотики. В результате очень большое количество людей гибнет. Есть случаи, когда раскрывались интернациональные интернет-сети педофилов, полицейские операции проводились одновременно в разных государствах, и подозреваемые преступники задерживались многими десятками.

Сегодня приводились примеры в основном в области стратегической безопасности. Террористы очень умно, умело используют современные ИКТ в своих целях, и в экспертной среде принято считать, что они выигрывают. Мы пока не можем выиграть войну за умы и сердца людей. Пропаганда, которая ведется ИГИЛ и другими террористическими организациями, очень сильная, происходит террористическое рекрутирование, например на Ближнем Востоке - в Сирии и Ираке. Поток новобранцев-рекрутов продолжается, хотя и сократился во много раз. Во-первых, люди едут, поддаются пропаганде, во-вторых, используются на широкой основе различные возможности ИКТ для передачи всевозможных сообщений, обмена информацией между террористическими лидерами, организациями и руководителями среднего звена. Данные сигналы просто посылаются в пространство для анонимных пользователей и адресатов. Эти возможности, к сожалению, пока перекрыть не удается. У террористов очень хорошие психологи, теологи, пропагандисты, частично они известны, но также среди них очень много умелых, технологически подготовленных людей.

Приведу примеры из своей практики. В антиигиловской коалиции, возглавляемой США, в которой уже около 70 государств, есть несколько рабочих групп. Одна из них называется «Стратегическая коммуникация». Задача этой группы состоит в том, чтобы нарушить связи, которые используют террористы между собой. На одном из мероприятий - мы в этой коалиции не участвуем, встречаемся только на третьих площадках - выступал руководитель такой группы, англичанин, эксперт, дипломат. Посыл его был следующий: к сожалению, мы, антитеррористы, проигрываем террористам по всем статьям. Я его спросил, не задавался ли он вопросом, который для наших спецслужб является очевидным: в коалиции находятся такие государства, как США и практически все развитые государства с огромным потенциалом ИКТ, и как же

получается, что они проигрывают террористам. У кого террористы учились? Как они приобрели такие навыки и знания? Почему теперь все лучшие специалисты коалиции оказываются бессильными перед террористами? Нечасто приходится видеть опытного английского дипломата, которому нечего ответить. Понятно, что это самый насущный вопрос. По большому счету это не вопрос о каком-то одном дипломатическом «уколе».

С другой стороны, можно продолжать данный список угроз: это и криптовалюты, и преступность, которая имеет экономический смысл, и преступления, совершаемые с целью наживы, или просто киберхулиганство, когда используется именно анонимность среды для того, чтобы о себе заявить, зачастую самым безобразным образом, без большого смысла. Как мы все хорошо знаем, часто такие действия приписываются русским хакерам, русским преступникам.

Механизмы взаимной помощи в этой области ничем не отличаются, они не специфические. Используются те, которые применяются в случаях любого правового взаимодействия между государствами. Эти механизмы громоздки, процедура очень длинная, использовать их регулярно просто невозможно, поэтому требуется взаимодействие в реальном времени, а не путем обмена запросами, которые переводятся, передаются по каналам или еще как-то. На это уходят месяцы, а то и годы. Конечно, должна быть какая-то международная инстанция, на наш взгляд, которая бы осуществляла международное регулирование, разрабатывала бы новые практики, правила, уже более детальные стандарты в этой области. Но даже на очень высоком уровне национальное государственное законодательство то и дело просто не развито.

В большинстве случаев все это квалифицируется национальными судами как мошенничество. По одной статье проходят очень разнообразные деяния, люди, совершившие очень разные незаконные поступки. Говорю это к тому, что мы в Российской Федерации данной теме придаем большое значение, и практически уже несколько лет назад был разработан объемный документ - проект конвенции о борьбе с информационной преступностью. Можно спорить о его названии, но этот проект носит всеобъемлющий характер. Там есть положения о криминализации определенных деяний, есть положения

о международном сотрудничестве, об уголовно-правовом взаимодействии между государствами, о международной организации - инстанции, которая управляла бы международным сотрудничеством в этой области и т. д.

Но странное дело, наши партнеры блокируют даже возможность обсудить эту тему, не говоря уже о нашем проекте. Теоретически есть еще одна группа экспертов - Рабочая группа в Вене на базе Комиссии ООН по наркотическим средствам Управления ООН по наркотикам и преступности, которая рассматривает вопросы киберпреступности. Ее даже не удается собрать, потому что наши партнеры, прежде всего западные, чинят препятствия начиная с процедурного уровня. Решение о созыве группы должно принять расширенное бюро, а оно не может собраться, потому что западные партнеры не предоставляют своего представителя. Вот на такие ухищрения они идут, чтобы не дать возможности заняться вплотную этой темой.

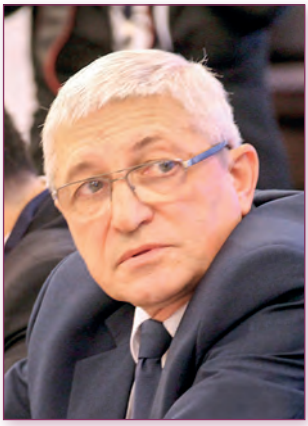
С одной стороны, это удивительно, а с другой - понятно, потому что если бы международное сообщество работало на этом направлении, то, скорее всего, не было бы возможности обвинять русских хакеров во всех мыслимых и немыслимых прегрешениях. Если бы было нормальное взаимодействие по уголовным делам, то было бы невозможно хватать наших людей в разных странах мира, требовать экстрадиции, как это делает сейчас США, потом их сажать - давать от 8 до 24 лет. Вот это окно возможностей огульной критики России было бы в значительной мере закрыто. И здесь приходится говорить не только о каких-то двойных стандартах, а о 100-процентной лицемерной лживой политике, которая направлена на то, чтобы не дать возможности развивать международное сотрудничество и формировать международные правила поведения государств в этой области.

К сожалению, с такими проблемами приходится сталкиваться довольно часто в разных областях, мы далеко не все затронули. Любая технология сама по себе нейтральна, ее можно использовать во благо, на развитие, а можно использовать с криминальными и преступными целями. Мы активно стараемся работать, чтобы эту вторую часть закрыть, нивелировать,

чтобы государства договорились о тех правилах, которые, по крайней мере, сокращали бы эти возможности.

О «сдерживании и предотвращении» в информационной сфере

Сергей Комов, ведущий научный сотрудник Военной академии Генерального штаба Вооруженных сил РФ, профессор, доктор военных наук



Уважаемые коллеги, в своем выступлении хочу проиллюстрировать взаимосвязь современной военной политики Российской Федерации с государственной политикой в области информационной безопасности и внешней политикой нашего государства на примере задачи сдерживания и предотвращения военных конфликтов.

Начну с того, что как в обсуждаемой сегодня новой редакции Доктрины информационной безопасности Российской Федерации, так и в действующей Военной доктрине Российской Федерации, введенной в действие в 2014 году, содержатся близкие по смыслу ключевые положения.

Оба документа с единых позиций трактуют основные военные опасности и угрозы, исходящие из информационной сферы. К ним, в частности, отнесено «информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей», а также «использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу междуна-

родному миру, безопасности, глобальной и региональной стабильности».

Стратегическая цель обеспечения информационной безопасности в области обороны - «защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности» - совпадает с целью обеспечения военной безопасности Российской Федерации.

Доктрина информационной безопасности развивает положение Военной доктрины о «стратегическом сдерживании и предотвращении военных конфликтов» как одном из приоритетных направлений военной политики Российской Федерации, распространяя его действие на информационную сферу.

В свою очередь, задача Российской Федерации по сдерживанию и предотвращению военных конфликтов, которые могут возникнуть в результате использования ИКТ, закреплена в Военной доктрине.

Следует отметить, что меры сдерживания и предотвращения военных конфликтов диалектически взаимосвязаны и имеют взаимодополняющий и взаимообусловленный характер.

Так, меры сдерживания противника от совершения актов агрессии основаны на создании военного потенциала государства, позволяющего в случае необходимости нанести ему неприемлемый ущерб в ходе оборонительных (контрнаступательных) военных действий. Меры предотвращения военных конфликтов основаны на формировании и использовании потенциала международной системы безопасности, базовые принципы построения и функционирования которой закреплены в Уставе ООН.

Основные направления деятельности Российской Федерации по предотвращению военных конфликтов, которые могут

возникнуть в результате использования ИКТ, определены в ст. 12 «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». К ним относятся:

- *развитие диалога* с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием ИКТ в военно-политических целях;

- участие в выработке на двустороннем и многостороннем уровнях мер *укрепления доверия* в области противодействия угрозам использования ИКТ для осуществления враждебных действий и актов агрессии;

- содействие развитию *региональных систем и формированию глобальной системы международной информационной безопасности* на основе уважения государственного суверенитета, невмешательства во внутренние дела других государств, неприменения силы и угрозы силой в международных отношениях, уважения прав и основных свобод человека;

- содействие подготовке и принятию государствами - членами ООН международных правовых актов, регламентирующих применение принципов и норм международного *гуманитарного права* в сфере использования информационных и коммуникационных технологий;

- создание условий для установления международного правового *режима нераспространения информационного оружия.*

Практическая работа на этих направлениях, проводимая в последние годы, наглядно подтвердила их взаимосвязь с мерами сдерживания.

Приведу только один пример - вопрос применимости международного права к деятельности в информационной сфере, активно обсуждаемый в ООН, «Большой двадцатке», «Большой семерке», НАТО и других международных форумах. Коалиция стран Запада во главе с США призывает признать автоматическую применимость норм и принципов международного права к регулированию военного использования ИКТ. В первую очередь такой подход они пытаются применить к возможности использования военной силы в ответ на трансграничные агрессивные кибератаки. При этом

предлагается опираться на положения ст. 51 Устава ООН (о праве на самооборону) и ст. 5 Вашингтонского договора (о коллективном реагировании на агрессию в отношении какого-либо члена НАТО).

Российская позиция состоит в том, что, не отрицая незыблемость права на самооборону, необходимо провести работу по созданию международной правовой базы, с использованием которой можно будет адекватно осуществлять его реализацию применительно к специфике информационной сферы. В ее состав должны войти:

- универсальные критерии отнесения различного типа информационных воздействий к актам агрессии (вооруженного нападения);

- методология организационно-правового и технологического характера, предназначенная для стандартизации процессов выявления и достоверной идентификации источников информационных воздействий;

- общепризнанные процессуальные нормы, регламентирующие порядок расследования фактов проведения информационных воздействий, включая методику сбора доказательной базы, позволяющей предъявить обвинение виновным лицам в осуществлении акта агрессии с использованием ИКТ.

Если этого не сделать, то в условиях существующей правовой неопределенности, задача оценки соответствия принимаемых государствами мер военного реагирования на какое-либо информационное воздействие нормам международного права объективно и беспристрастно решена быть не может. В свою очередь, это может привести не к разрядке, а к обострению международной обстановки со всеми вытекающими последствиями.

В заключение следует отметить, что критериями сбалансированности выработки и реализации мер сдерживания и предотвращения военных конфликтов являются стабилизация международной обстановки, снижение угрозы развязывания агрессивной войны, обуздание гонки вооружений и создание условий для снижения оборонных расходов.

Взгляды мирового экспертного сообщества на проблемы международной киберстабильности

Анатолий Стрельцов, советник директора ИПИБ МГУ им. М.В.Ломоносова, начальник Департамента обеспечения безопасности в области информации и информационных технологий аппарата Совета безопасности РФ

В этом году по поручению руководства мне удалось поучаствовать в нескольких крупных международных конференциях и семинарах. В принципе международное сообщество авторитетно должно заниматься предотвращением злонамеренного использования ИКТ. Другое дело, что к этому вопросу относятся по-разному, видят решение этой проблемы по-разному. Но в целом все поддерживают необходимость разработки принципов и правил, норм поведения, все понимают, что это основа в системе международной информационной безопасности. Данную тему обсуждали и в Гармише в 2016 году, там была высказана очень, на мой взгляд, полезная идея создания еще одной группы при ООН из специалистов-юристов, военных и инженеров, которая смогла бы на базе тех политических принципов, норм, правил поведения, которые были сформулированы в докладе Группы правительственных экспертов ООН, прийти к общему пониманию того, как именно надо трактовать вопросы выработки правил, принципов, норм поведения.

Что такое суверенитет государства в ИКТ-среде? Совершенно очевидно, что ИКТ-среда - это не территория, а нечто особое. Мало кто сейчас понимает, что такое инцидент в ИКТ-среде. У нас в Уставе ООН в ст. 24 записано, что международные вопросы надо решать мирными средствами. Какие документы нужно положить на стол переговоров, чтобы

обсуждать проблемы, связанные с инцидентами в ИКТ-среде? По-этому вопросу, как мне представляется, еще надо подискутировать.

Отдельно хотел сказать несколько слов о праве. У меня такое ощущение, что мы стоим на пороге в этой области, потому что условия, в которых мы вынуждены применять существующие методы, механизмы, принципы, правила, правовые институты для регулирования общественных отношений, претерпевают существенные изменения, когда речь идет об ИКТ-среде. Прежде всего, ИКТ-среда создает достаточно серьезную виртуальную обстановку, в рамках которой очень трудно проследить проявление юридических фактов и правоотношений и изменение этих правоотношений и т. д.

Я был на конференции в Бостоне, посвященной стратегической стабильности в киберпространстве. Там в разговоре со многими специалистами мне открылись новые тенденции. Во-первых, с американской стороны было высказано пожелание перейти к более конкретному взаимодействию по поводу событий, происходящих в ИКТ-среде, и опознавания субъектов, которые в этих событиях участвуют. Высказана была идея, что нужно наладить взаимодействие на профессиональном уровне при появлении таких озабоченностей, которые в настоящее время возникли в США относительно того, что российские хакеры проникли куда-то.

Аналогичные озабоченности возникают и в России, и, думаю, не беспочвенно относительно соответствующих специалистов в ИКТ-среде. В этом плане необходимо создание некоторой системы или нужна интеграция возможностей, которая бы существенным образом помогла прояснить вопрос, с чем мы имеем дело. Во-вторых, возникла новая тема о вмешательстве СМИ во внутренние дела других государств, которая очень болезненная. Американские эксперты сказали, что целесообразно вернуться к разработке третьей корзины Совещания по безопасности и сотрудничеству в Европе, которая в прошлый раз осталась незаполненной. Она должна быть посвящена именно этой тематике.

Американцы настолько озабочены нашим пресловутым влиянием на выборы, что готовы обсуждать все что угодно. По всем телепрограммам идут дебаты, как российские специалисты влия-

ют на результаты выборов в США. Даже их политологи находятся под большим впечатлением от происходящего. Никто не берет в голову, что Клинтон набрала немереное количество денег на свою кампанию, под эти деньги розданы обещания, но американцы-то озабочены не этими деньгами, а влиянием России на выборы. В этих условиях нам не грех предложить руку помощи в плане наполнения третьей корзины Совещания.

Многие государства мира ощущают необходимость продвижения вперед в этой области. Очевидно, что складывается некий потенциал взаимопонимания, который позволяет хотя бы на уровне экспертов начать проработку данных вопросов.

План работы по проведению стратегической стабильности, в том числе и в киберпространстве, будет доложен на очередном заседании международного форума в Гармише в 2017 году.

Современные угрозы террористического и экстремистского характера в информационной сфере

Александр Смирнов, заместитель начальника отдела Главного управления по противодействию экстремизму МВД РФ

Хотелось бы отметить, что в докладах предыдущих выступающих очень четко прозвучал тезис о том, что среди блоков угроз информационной безопасности выделяются угрозы с проявлением террористическо-экстремистской деятельности в информационной сфере. Этот тезис очень четко зафиксирован во всех основополагающих документах стратегического планирования РФ, в частности в Стратегии национальной безопасности и новой Доктрине информационной безопасности, характеристика которым была подробно дана. Наряду с традиционными каналами распространения экстремистской идеологии, безусловно, в настоящее время приоритет отводится сети Интернет.

Это тоже очень четко прописано в документах. Характеризуя основные направления использования Интернета в террористических и экстремистских целях, следует выделить пропаганду идеологии экстремизма, осуществление вербовочной деятельности, сбор финансовых средств, а также проведение компьютерных атак на информационные ресурсы. Какие информационные ресурсы используются для этих целей? Это экстремистские интернет-сайты. Кроме того, активно применяются видеохостинги для размещения различных видеороликов, а также индивидуальные групповые аккаунты в основных социальных сетях, чаты и каналы в наиболее популярных мессенджерах, прежде всего мессенджерах телеграмм. Для этих целей, конечно, используется и закрытый сегмент Интернета, прежде всего система Tor.

К сожалению, в данной области мы также наблюдаем те же тенденции, на которые часто обращает внимание МИД России, - прямая или косвенная поддержка деятельности террористических и экстремистских организаций со стороны нескольких государств. Вот, в частности, действующий русскоязычный ресурс сторонников «Джабхат ан-нусра», хостинг и информационная поддержка которого осуществляются на территории Украины. Безусловно, здесь некий новый стандарт международной террористической организации «Исламское государство», которая запрещена в нашей стране.

На наш взгляд, секрет кроется в двух составляющих: во-первых, наличие притягательной идеологии и, во-вторых, использование для ее трансляции самых разных передовых информационных технологий. Что касается первой составляющей и какие средства они применяют. Во-первых, это реализация идеи об исламском халифате, которая и раньше декларировалась другими террористическими организациями, но, по сути, впервые воплощена. Конечно, это псевдохалифат, что понятно всем.

Во-вторых, это искусственное использование авторитета ислама и религиозной мифологии. Все пропагандистские тексты ИГИЛ сопровождаются выдержками из Корана с соответствующими символами и т. д. Важным аргументом, при-

меняемым пропагандистами ИГИЛ, является могущество этой организации. Они всегда говорят, что ведут войну против всех стран мира и что в конечном итоге львы халифата побеждают в этой борьбе.

Далее - это интернационализм, делается акцент на то, что неважно, какой национальности, из какой страны приезжаешь в халифат и воюешь за «Исламское государство». Как это ни парадоксально, экстремальное насилие, которое очень активно транслируется через медийные каналы, также является фактором привлекательности для большой части его потенциальных сторонников.

Что касается самих инструментов, то здесь мы имеем ситуацию, беспрецедентную в истории, когда у террористической организации, по сути, создан мощнейший медиахолдинг, который включает в себя и печатные издания, и различные новостные ресурсы, наиболее известным из которых является информационное агентство «Аль-Амак». Кстати, они разработали специальное приложение для Андроид Маркета, правда компанией «Гугл» оно было заблокировано. Они очень активно информационно освещают их борьбу, в частности, есть инфографика, посвященная битве за Мосул, которая в настоящее время ведется, где четко указано, сколько проведено операций смертников, сколько уничтожено вражеской техники, убито вражеских солдат и т. д. Также выпускаются специальные пресс-релизы и, конечно, ведется огромная работа в социальных сетях. Все социальные сети задействуются для этой цели. Очень активно ИГИЛ освоила чаты в мессенджерах. Здесь, на наш взгляд, ИГИЛ была на шаг впереди многих ведущих СМИ, которые только сейчас начинают такую работу.

Хотелось бы отметить проигиловские хакерские группы, такие как киберхалифаты, которые совершают компьютерные атаки на сайты и размещают пропагандистскую информацию в поддержку ИГИЛ. Пропагандисты ИГИЛ очень активно отрабатывают все террористические акты, которые происходят в мире, причем даже те, где причастность сторонников данной организации к тому или иному теракту, по меньшей мере не

очевидна, в частности пропагандистский постер, размещенный после совершения террористических актов в Париже. Данная группировка неоднократно размещала пропагандистские материалы, в которых высказывались прямые угрозы в адрес России, например самый известный видеоролик «Скоро, очень скоро».

Хотелось бы обратить внимание на относительно новую тенденцию, которая, на наш взгляд, представляет серьезную опасность, - это смещение акцентов в пропаганде ИГИЛ с эмиграции в халифат, как они в своих материалах пишут, на совершение хиджры - переселение в исламскую страну, призывы к совершению терактов в местах проживания. Такие посылы адресуются не только членам спящих ячеек и другим членам данной террористической организации, но и так называемым волкам-одиночкам, то есть любому лицу, которое подверглось саморадикализации в Интернете и может совершить теракт с использованием разных подручных средств - ножей, молотков, автотранспортных средств и т. д. Соответственно, прямые призывы такого рода публикуются на подконтрольных информационных ресурсах.

Характеризуя противодействия данной пропагандистской деятельности террористических и экстремистских организаций, нужно выделить два направления. Это, во-первых, технологическое противодействие. В частности, одним из традиционных и уже обкатанных его инструментов является ограничение доступа к интернет-ресурсам экстремистского характера. Во-вторых, идеологическая составляющая - разъяснительная работа по развенчанию тех идеологических постулатов, которые транслируются пропагандистами международных террористических организаций. Хотелось бы привести пример такого рода деятельности при поддержке МВД. В текущем году завершена работа над художественным фильмом «Рядом с нами», режиссер которого протоиерей Александр Новопашин. Сейчас эта лента активно участвует в фестивальной программе, где уже завоевала ряд призов. Приятно было узнать, что фильм получил первое место на фестивале православного кино в Киеве.

Технологические аспекты безопасности в Wi-Fi и 3G/4G

Рустам Газиев, директор компании «Whirl Software»

Хочу кратко рассказать о том продукте, который разработан нашей компанией «Whirl Software». В частности, технологические аспекты безопасности в Wi-Fi-сетях и 4G-сетях. Развитие мобильного Интернета идет очень бурными темпами. На сегодня уже 50% пользователей Интернета выходят в сеть на личных мобильных устройствах. По прогнозам, до 2020 года количество пользователей вырастет до 75%. Соответственно, это довольно большой пласт, который необходимо конструировать, анализировать. Всю данную информацию необходимо иметь для обеспечения безопасности. В этом смысле наша компания разработала продукт, который является платформой доставки управления информационного контента на мобильные устройства пользователей Wi-Fi-сетями и 4G-сетями.

Продукт представляет собой единый инструмент коммуникации с населением, чтобы проводить консультации, иметь отзывы, размещать рекламу и многое другое. Это является неким ключом к сбору данных, потому что такая коммуникация находится в постоянном режиме. Например, если пользователь зарегистрирован в определенной сети с неким продуктом, то в этой системе при обновлении своих данных в социальных сетях в автоматическом режиме такая информация обновляется. У нас постоянно появляются новые данные.

Как всем известно, есть постановления Правительства РФ №758 и 801, в рамках которых должны быть обязательные идентификации пользователей Интернета в публичных сетях. Мы не единственные, есть и другие компании, которые этим занимаются. Сбор данных происходит на основании профилирования пользователя на уровне MAK-адреса (индивидуальный идентификацион-

ный атрибут), который присваивается любому устройству еще на заводе, а также идет профилирование на уровне международного индивидуального идентификационного абонента и, конечно, используется социальный демографический профиль, который собирается через социальные сети в открытых источниках.

Что такое модуль безопасности в рамках СМС? Когда человек заходит в открытую Wi-Fi-сеть, например в кафе, вместо того чтобы просить код у официанта, он просто получает сообщение о том, что находится в публичной сети, вводит номер телефона, получает СМС-код, после чего проходит идентификацию. Соответственно, его номер телефона привязывается к тем паспортным данным, которые находятся у оператора.

Система собирает данные и в автоматическом режиме выстраивает различные графики по возрасту, полу, интересам, по посещениям тех или иных локаций. Там есть огромный пласт аналитической информации, которая может быть полезна для той или иной стороны.

Одним из важных моментов является тот факт, что такая система может собирать большое количество данных, это модуль безопасности. В этом смысле «пакет Яровой» создает предпосылки для движения в сторону развития интернет-технологий с точки зрения безопасности.

На сегодняшний день, кто бы что ни говорил, такие крупные компании, как «Гугл», «Яндекс», так или иначе собирают огромное количество информации. Вы заходите в Интернет, по сути, вы выходите на киберулицу и везде оставляете свои следы. Оставляя такой след, вы в следующий раз получаете какой-то рекламный посыл в Интернете и можете его использовать с точки зрения безопасности. Благодаря таким атрибутам можно определить точное местонахождение пользователя, независимо от того, где установлен Wi-Fi. При всем при этом можно производить мониторинг неправомерной активности пользователей при помощи всех данных средств, а также при помощи выслеживания ключевых слов, при этом можно делать уведомления на электронный адрес или СМС-сообщения. При получении той или иной информации можно получать имя пользователя, время посещения, его MAK-адрес, его е-мейл, возраст, пол, номер телефона, сведения об операционной среде, в которой он работает, его аккаунт в «Фейсбуке».

Например, сегодня коллеги из МВД сообщили, что ИГИЛ ведет очень серьезную деятельность. Нужно идти в направлении того, чтобы выстраивать в системе такие ключевые слова, как «ИГИЛ», «Джихад», «наркотики», «детская порнография» и т. п., у этой системы появляется возможность реагировать на активность от пользователя.

Можно получать в режиме онлайн информацию по ключевым словам или по другим параметрам уведомления. После этого можно проводить какие-то другие мероприятия. Если двигаться дальше, то нужно развивать программы таким образом, когда определяется так называемая группа пользователей, группа устройств. Когда два пользователя друг друга знают, ходят в одну локацию, тогда можно выстраивать какие-то аналитические данные, составлять списки пользователей, которые находятся в розыске, а они могут появиться в сети.

С учетом того, что сейчас идет бурное движение в сторону трафика, который, к сожалению, тяжело расшифровать, имеет смысл заниматься анализом доменных имен и адресов в целях противодействия противоправным пользователям. Оперативная работа настолько глубокая, что ограничиться такими данными будет достаточно тяжело.

Общая информационная стратегия стран БРИКС - от идеи к практической реализации

Денис Тюрин, директор Делового клуба Шанхайской организации сотрудничества

Мы сегодня говорили о национальном суверенитете в киберпространстве, хотел бы затронуть тему многополярности в киберпространстве. Можно ли сегодня говорить, что политическая многополярность, которую возможно с той или иной уверенностью описать в современном мире, существует и в информационном пространстве. Думаю, что нет. Во-первых, потому что

Интернет по-прежнему является безграничной областью практического доминирования США. Во-вторых, потому что вслед за монополией американских и европейских компаний - производителей программного и аппаратного обеспечения - следует их безусловная монополия информационно-идеологических стандартов. Кстати, это касается и ставшего уже нормой всемирного знания английского языка, без которого человек фактически остается за бортом информационного обмена. Можно говорить, что сам по себе латинский алфавит представляет определенную угрозу национальному суверенитету стран, который до поры до времени находится в рапиде жесткого идеологического влияния Запада.

Надо сказать, что существуют некие изолированные островки, сохранившиеся в этом информационном океане, сохраняющие национальный интерес. Это прежде всего происходит благодаря обладанию собственными системами поиска, пользованию социальными сетями, собственным алфавитом. Кстати говоря, я бы сказал, что существуют только два острова - Россия и Китай, в которых есть достаточно мощная инфраструктура общения, поиска в Интернете. Но их влияние, как вы можете видеть на примере нашего отечественного «Яндекса», постепенно снижается, потому что большинство пользователей предпочитает использовать поисковые сервисы, где можно читать и по-русски, и по-английски, что для такого глобализованного сообщества гораздо удобнее.

Однако на уровне политического осмысления этих процессов в странах БРИКС такая опасность осознанна. Например, в ШОС рабочими языками выбраны два языка - русский и китайский. В БРИКС, несмотря на то что рабочим языком выбран английский, каждая страна настаивает на том, чтобы и ее национальный язык принимался в качестве языка общения. Это видно и на примере сайта виртуального секретариата БРИКС. Индия настояла на том, чтобы языком национального представительства этой страны, которая сейчас является председателем БРИКС и представители которой присутствуют на нашем мероприятии, стал язык хинди.

С точки зрения многополярности в информационно-коммуникационной среде мы должны понять и осмыслить угрозы,

исходящие от навязывания монополий в информационно-идеологических стандартах, осмыслить новые потребности человека в защите своих естественных прав, в том числе права на защиту национальной идентичности, которое незаслуженно долгие годы сознательно исключается из тех основных прав и свобод человека, которые обеспечивают свободу и равноправие в современном мире.

Сайт виртуального секретариата БРИКС представляет собой платформу, на которой это общее информационное пространство смыслов может развиваться и становиться действующей силой. Сайт создан по инициативе России и официально презентован на саммите БРИКС в июле 2015 года в Уфе. Главной и основной причиной для его создания послужило заключение меморандума МИД стран - участниц БРИКС о взаимопонимании по созданию общего сайта группы, который был подписан 9 июля 2015 года. Этот портал разрабатывался как ресурс бесплатного пользования для освещения деятельности БРИКС, а также в качестве официальной площадки для того, чтобы информировать мировую общественность о деятельности БРИКС.

Основная мысль проекта состоит в том, чтобы укреплять сотрудничество между странами БРИКС, использовать новейшие технологии для развития диалога, развивать отношения между государствами и ведомствами стран - участниц группы, а также активно вести информационную работу на экспертное сообщество и население тех стран, которые формально к БРИКС не относятся, но тоже испытывают интерес либо к участию в этом международном форуме, либо к участию в отдельных мероприятиях, которые проводятся в его рамках. Конечная цель проекта - именно формирование общего пространства идей и смыслов, связанных с информационной координацией работы стран - участниц группы в условиях такого неблагоприятного политического окружения.

Сейчас, конечно, много говорится о том, что Дональд Трамп представил новую парадигму внешней политики США, но вряд ли США откажутся от тех выгод и преимуществ, которое дает монопольное положение в ИКТ. Мы знаем, что

ближайшие союзники США по так называемой группе «Пять глаз», куда входят ведущие англосаксонские страны мира - США, Великобритания, Канада, Австралия, Новая Зеландия, удерживая в своих руках это монопольное право на распространение неких идеологических установок в другие страны, не откажутся от таких монополий. Поэтому странам БРИКС имеет смысл, безусловно, более активно действовать сообща по преодолению этих исторически сложившихся неблагоприятных условий для их созидательного развития.

В настоящее время основная аудитория сайта в первую очередь состоит из дипломатического сообщества стран БРИКС, дипломатов других стран, представителей международных организаций, представителей международных центров, научных организаций, из политических деятелей, журналистов, студентов и учащейся молодежи в разных странах. При создании виртуального секретариата БРИКС был учтен опыт функционирования международных организаций. Важно, что идеологически правильно это было зафиксировано в документах, на основании которых разрабатывался виртуальный секретариат. Он разрабатывался программистами не с закрытыми сложными шифрованиями и закрытым кодом, а на прозрачной платформе - доступной, открытой для международного сообщества. Сайт создан на основе «Юникс», он удобный и понятный, распространенный в знакомой международному сообществу оболочке WordPress.

Коротко о принципах работы портала: абсолютный доступ всех стран БРИКС к его содержательному наполнению; каждая страна имеет право по своему усмотрению публиковать материалы на любом языке из представленных на портале. Это возможность освещать любые темы независимо от того, касаются ли они напрямую деятельности БРИКС или относятся к каким-то другим важным для того или иного государства политическим моментам.

Хотел бы обратиться к партнерам БРИКС, присутствующим в зале: активно подключайтесь к работе данного ресурса, который предоставляет по-настоящему интересную и важную возможность для информационной деятельности наших стран.

Разработчики экспертного программного обеспечения и оборудования как участники системы обеспечения информационной безопасности Российской Федерации

Анатолий Земцов, директор Ассоциации производителей программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий «ЭКСПИТ»

Хотелось бы рассказать о той роли, которую мы на себя берем как производители специализированного программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий, о той роли, которая описана и в новой Доктрине информационной безопасности, - роли участника системы обеспечения информационной безопасности. Многие участники конференции уже упоминали о большом списке угроз, которые декларированы в Доктрине информационной безопасности. Все эти угрозы, по сути дела, - это преступления, всякого рода опасности и инциденты в информационном пространстве.

Как любое преступление, логично, что данные мероприятия злонамеренных, еще неустановленных лиц являются поводом для начала разбирательства в форме расследования или другой процессуальной форме. А для любого разбирательства существуют определенные процессуальные моменты, определенные действия - это особого рода исследования, экспертизы, которые назначаются в рамках расследования. Понятно, что для специализированных расследований в сфере ИКТ существуют, давно разработаны и применяются различного рода специализированные инструменты, представленные на мировой арене.

С чем мы сталкиваемся почти каждый день по работе с различными органами? Десятки инструментов используются в работе представителей правоохранительных органов, причем не только отечественных, но и ФБР, и АНБ, и ЦРУ. Любой профессионал в сфере компью-

терной криминалистики, так называемый форензик, использует высококлассный продукт. Большинство из них произведено в США, есть производства в Японии, Германии, довольно серьезная школа существует и на Украине. Все данные программные продукты аппаратного комплекса - это инструментарий с закрытым кодом. Мы не знаем, что происходит внутри этих программных продуктов, какие недекларированные возможности оставили за собой производители, находящиеся в своих странах. Еще очень важно, такие продукты в большей части, хотя и используются в расследовании преступлений, не сертифицированы в РФ.

В России еще до декларирования этих угроз в доктрине пришли к выводу, что необходимо приступить к разработке программного обеспечения. Рад тому, что в нашей стране есть серьезные инструменты и игроки, которые уже сделали ставку на развитие инструментария по защите угроз в сфере информационной безопасности. Есть конкурентоспособное решение, реальные поставки и продажи за рубеж. Любая из российских компаний, организаций готова к сертификации, аккредитации и т. д. К сожалению, пока эти компании еще разобщены и не могут единым фронтом представлять свои интересы. Но тем не менее мы уже пришли к мысли, что нуждаемся в едином представительном органе в данной отрасли. Мы приняли решение объединиться в Ассоциацию производителей программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий.

Прежде всего это развитие средств и методов, которыми мы пользуемся в наших разработках в сфере криминалистики. Очень важным моментом является участие в разработке целевых программ развития, потому что мы видим, какое внимание уделяет государство этой проблеме, готовы принять участие в процессе - советом, делом. Если государство активно включилось, то, как ни странно, российские компании не всегда готовы к активному взаимодействию. Чуть менее локальный, но очень важный вопрос популяризации и продвижения отечественного производства таких специализированных инструментов.

Понятно, что локально работать на территории РФ в данном случае, когда ИКТ - международная субстанция, наверное, не очень правильно, поэтому перед любой серьезной российской компанией в хорошем смысле стоит задача показать не только России, но и всему миру, что российские производители являются серьезными игроками на этом рынке. Опять же немаловажный вопрос - это специалисты, которые работают с данным программным обеспечением оборудования. Необходимо приоритетное внимание к подготовке соответствующих специалистов по российским программам. В российских университетах такая тяжелая и каждодневная работа ведется, например в Бауманском институте и др. Нам нужно озадачиваться и вопросом, чтобы в этой отрасли были единые правила, единый стандарт для всех игроков.

Тенденции развития киберпреступлений

Сергей Золотухин, менеджер по развитию бизнеса ООО «Группа информационной безопасности» («Group-IB»)

Расскажу о тенденциях развития киберпреступлений на основе 13-летнего опыта работы в компании «Group-IB». Эта российская компания занимается выявлением, предотвращением, расследованием компьютерных преступлений в области высоких технологий.

Современный мир характеризуется значительным ростом рисков, связанных с высокими технологиями. В обществе все больше появляется информации, связанной с последствиями действий хакеров, - это финансовые мошенничества, хищения персональных данных, шпионаж, вмешательство в работу критически важных объектов. Перечень постоянно расширяется. Можно констатировать, что сегодня глубина

проблемы еще не до конца осознана российским сообществом. В то же время и организации, и государства предприняли серьезные меры по повышению информационной безопасности.

Все мы знаем, что стандартом де-факто стало использование антивирусного программного обеспечения межсетевых экранов, несанкционированного доступа. Вместе с этим количество атак постоянно увеличивается. Казалось бы, средств защиты становится больше, они эффективнее и количество атак должно снижаться, а они растут. Почему так происходит? По оценкам нашей компании, объем хищений с конца 2015 до конца 2016 года составил почти 4 млрд. рублей. Это на 44% больше, чем в прошлом году. Современные злоумышленники научились обходить те средства защиты, которые мы используем.

Атаки становятся целевыми, направленными. Нужно учитывать и расходы, потраченные на средства защиты, которые не смогли уберечь от атак. Основная причина, на наш взгляд, такого положения дел - плохая осведомленность участников рынка о проведении атак, о тактике, методах преступников, которыми они пользуются. Вторая причина - это излишняя вера в то, что стандартные средства защиты сработают, остановят злоумышленников на каком-то этапе атаки. Тенденция роста направленных атак - это самый основной и тревожный тренд в развитии киберпреступности.

Еще одна тенденция - атаки становятся глобальными. Все больше и больше преступники проявляют черты организованного характера на международном уровне. Сложился международный рынок купли и продажи вредоносных программ, аренды бот-сетей, ориентированный не только на российские, но и на иностранные банки. Здесь надо отметить, что, к сожалению, происходит захват рынка вирусописательства русскоязычными специалистами. Обращаю внимание: не русскими, а русскоязычными. Это практически все русскоговорящие люди из бывших стран СНГ - Украины, Белоруссии, Казахстана, соотечественники, живущие за границей. К разработке 16 из 19 «троянов», кото-

рыми сейчас пользуются для хищения по всему миру, причастны русскоязычные люди. Мы понимаем, что это только часть проблемы программного обеспечения, оно разрабатывается, передается: одни люди осуществляют атаки, другие уводят деньги.

Еще одна тенденция, которая затрагивает нас с вами, - это взрывной рост атак на андроиды. На 470% за прошлый год увеличилось количество атак на наши мобильные устройства, основные из которых андроиды. Это большая проблема для общества и государства, поскольку сейчас атакуются простые частные пользователи, их мобильные кошельки, привязанные к банковским счетам, и т. д. Тут мы говорим о развитии новых технологий в информационной сфере и домашних интернетах. Гаджеты, которые находятся в личном пользовании, являются обьектами частых хакерских атак. Они имеют постоянный доступ в сеть. Чаще всего используются пароли по умолчанию, антивирусы практически не контролируются пользователем. Именно поэтому мы все больше слышим об атаках умных телевизоров, холодильников, скоро дело дойдет до утюгов и кофеварок, камер.

Далее - увеличение атак на промышленные предприятия, объекты критической инфраструктуры. Мы видим, что такие атаки развиваются, они идут и со стороны кибермии других государств и направлены в основном на получение контроля над информацией. Для кибертеррористов стоит задача провести как можно больше разрушений и получить общественный резонанс и т. д. Технологии борьбы с такими направленными атаками преступников существуют. Мы разрабатываем и стратегические средства защиты киберразведки, тактические средства выявления атак.

Считаем, что совместная работа человека, общества, государства, межгосударственное партнерство, международный обмен информацией очень важны для борьбы с киберпреступностью. Хотим мы или не хотим, но киберпреступность вышла за рамки одного государства, это стало межгосударственной проблемой со всеми ее аспектами и проявлениями, хищениями, шпионажем, терроризмом и т. д.

Современная защита от масштабных кибератак

Дмитрий Белявский, директор по развитию ООО «Иновентика технолоджес»

Мы являемся разработчиками российской системы защиты от сетевых масштабных, глобальных атак, которые переходят границы стран, организаций, строим и программируем разработку системы, которая помогает выявлять, детектировать и предотвращать сетевые атаки, в том числе дезатаки. В сегодняшней мировой обстановке целями атак является практически каждое государство. Необходимо следить за тем, что от чего мы защищаем. Результатами прогресса в области информационных технологий в полной мере пользуются злоумышленники. Они получают достаточно «удобные» средства организации таких атак. Ими формируются большие потоки данных определенных ресурсов, например СМИ, политические ресурсы, которые также влияют на восприятие различных ситуаций в мире.

Сейчас атаки, в том числе DDoS-атаки, достигают высочайшей мощности, и технические ручные средства и механизмы, которые могут быть использованы специалистами по информационной безопасности, недостаточны. Тем более что атаки постоянно совершенствуются, они происходят в коротком режиме. По нашей статистике, 70% атак осуществляется в течение 30 минут. Этого времени недостаточно, чтобы выявить атаки вручную, можно увидеть только последствия. С ними можно бороться следующим образом - фильтровать весь трафик, который проходит в сетях, но такой путь весьма дорогостоящий. Подобный вопрос стоит перед многими сетями, операторами связи и государством. Для защиты таких сетей недостаточно применение систем, которые действительно фильтруют трафик. В этом случае используются системы, кото-

рые выявляют поведение пользователей. Мы применяем как раз эту идеологию, мы строим систему согласно этому построению. Система собирает статистику со всех сетевых устройств, через которую проходит трафик сети, выявляет аномальные ситуации и согласовывает их с базой данных типов атак, дает подробную информацию, откуда, на какие объекты идут атаки, как они были организованы, в каких странах. То есть система позволяет в автоматическом виде предоставить эту информацию. Самое главное, что такая система может предотвратить данные атаки полностью в автоматическом режиме.

Система может быть настроена таким образом, что предотвращение атак включает согласованные действия с операторами связи, которые предоставляют доступ в Интернет организациям, к которым они подключены. В России такая система уже реализована двумя крупными операторами связи - «Транстелекомом» и «Ростелекомом». Операторы связи могут получить полный сервис и защититься, по крайней мере на двух уровнях, но мы идем дальше - на мировой рынок. К примеру, у нас уже есть инсталляции за рубежом - в дружественной Армении, мы начинаем строить систему на Кубе. Они уже в течение полугода используют систему для демонстрации операторам связи, партнерам по Латинской Америке.

Мы считаем, что это направление действительно интересно и нам как разработчику, и странам как средство для выявления и предотвращения атак, в том числе и других стран. Система состоит из двух компонентов: анализа трафика и фильтрации трафика, но это относится к технической информации. Мы сотрудничаем с достаточно большим количеством компаний, занимающихся антивирусной защитой, информационной безопасностью. В сотрудничестве рождаются определенные алгоритмы, которые мы внедряем в наши системы, они позволяют четко определять компьютерные атаки с точностью до IP-адреса со скоростью менее 30 секунд для того, чтобы гарантировать работоспособность информационных сетей и сервиса.

Андрей Крутских: *С учетом услышанного, благодаря вашим докладам, назвал бы это мероприятие, организованное журналом «Международная жизнь», как одно из наиболее важных в 2016 году,*

потому что здесь за столом собраны силы очень профессиональные - и представители IP-бизнеса в области кибербезопасности и научно-исследовательских институтов, и политики.

Наша работа навеяла много мыслей, но я «зацеплюсь» за Стрельцова Анатолия Александровича. Он говорил про «третью корзину», а именно: затронул вопрос о роли СМИ в кибервойне. Что надо понимать под кибервойной?

Напрашивается определенная аналогия. Будучи еще мальчишкой, в СССР я слушал радио «Свобода», «Свободная Европа», «Голос Америки». Ведь тогда Запад, наоборот, боролся за то, чтобы открыть все идеологические границы и чтобы эти радиостанции имели свободный прием у нас в стране.

Кибервойна обретает разные очертания и направления. Прежде всего, это когда с помощью кибервойны, виртуальных средств можно наносить материальный ущерб. И голливудские фильмы нам показывают, как это делается. Если все заслонки электростанций открыть с помощью киберсредств и затопить миллионные города в России и США, шлюзы или плотины поднять, то мощные электростанции можно вразнос пустить. Мы знаем, что сделали американцы со Stuxnet - 1200 центрифуг были выведены из строя, ядерную программу Ирана задержали на два года. А если бы это было доведено до взрыва? Если бы ветер не туда подул, то вся радиация пришла бы в СНГ, в том числе и Россию. Вот это ядерная война.

Американцы обвиняют китайцев, когда проводятся двусторонние переговоры их групп, в краже интеллектуальной собственности. Американцы вкладывают многие миллиарды, чтобы сделать какие-то продукты, в том числе военные, а китайцы все крадут. Это тоже направление, возможно, кибервойны.

И еще. Вернемся к пресловутой избирательной кампании в Америке. Ведь когда начинают говорить о российских хакерах, они не говорят, что хакеры нанесли какой-то материальный ущерб, что вывели компьютеры из строя. Нет, речь идет о том, что наши СМИ - «RT», «Спутник» и другие - вбросили в американскую аудиторию такое количество интересной информации, и это не комплимент нашим СМИ, просто признание факта их профессионализма, что ее стали слушать, из нее стали делать выводы, хотя эта информация в основном идет от «Викиликса» и др. Так, нас

стали обвинять в том, что якобы наши хакеры вбросили информацию на американский информационный внутренний рынок, и эта информация якобы повлияла на умы американцев. Так это война или нет?

Сегодня никто бы и не узнал - американская пресса этим не занималась, - что у Клинтон деньги формируются из украинских фондов. Так это попало на американский информационный рынок.

Кстати, скажу, что информационная работа МИД России поставлена на высоком уровне, к его информации прислушиваются, поэтому и просмотры мидовской информации растут, отсюда и популярность российской внешней политики.

Я, Анатолий Александрович, не очень четко понимаю, как мы сможем договариваться по поводу «третьей корзины», потому что СМИ - это святое, и надо бороться за информационные рынки. И если у нас это стало лучше получаться, то мы никогда не пойдем на самоограничение наших возможностей действовать на других рынках.

Эту идею я хотел бы подчеркнуть, наступательность наша стала профессиональнее, мы многому научились, надо выживать. Это не война.

Дмитрий Геннадьевич Грибков упомянул очень важный момент: что вообще стоит считать правом на ведение ответных действий? Процитирую снова 51-ю статью, вокруг которой и на двусторонних консультациях, и в ООН велась большая борьба. Там четко записано, что право на ответные действия возникает в случае вооруженного нападения, вооруженной агрессии. Должен обратить ваше внимание, что нет в международном обществе, даже внутри НАТО, и внутри, казалось бы, братьев по разуму единого понимания: считать ли кибернападение вооруженным нападением, а соответственно, с правом на ответ с применением всех сил, которые у вас есть.

Что из этого вытекает? Вытекает обамовщина. В мае 2011 года он опубликовал под претенциозным названием свою стратегию кибербезопасности. Там он впервые высказался без всяких ссылок на международное право: если на США кто-то нападет, то они ответят всеми имеющимися у них средствами, включая вооруженные. Когда я в Белом доме спросил их «киберцаря», предполагает ли это нанесение ответного ядерного удара, сразу все затушевались, замолчали, но сказали твердое «нет».

Поэтому договориться о правилах, что можно, что нельзя, стало сейчас принципиально важным и актуальным, пока мы не зашли слишком далеко или не нанесли ответный кибердар. Но это отнюдь не значит, что должны быть ограничения на работу СМИ и нужно в извращенном виде представлять деятельность «RT». Это не хакеры, они действуют на основе официальных разрешений. Ставить вопрос, что Россию надо наказать за то, что мы эффективнее представляем свою информацию, недопустимо.

Сессия 2. Гуманитарные аспекты международной информационной безопасности

О гуманитарном аспекте международной информационной безопасности

Александр Бикантов, заместитель директора Департамента информации и печати МИД РФ

В вопросах международной информационной безопасности важное место занимают гуманитарные аспекты. В современном мире все более злободневной становится тема не только распространения неправомерной информации, но и объективного распространения информационного контента. Все мы знаем, что в мире развернулось жесткое информационное противостояние между западными масс-медиа, претендующими на своего рода монополию истины, и другими СМИ, включая российские, которые представляют альтернативные точки зрения. К сожалению, до сих пор журналисты Азии, Африки, Латинской Америки, а также дружественных стран ориентируются на новостной контент, предлагаемый ведущими западными медиаграндами. Даже в рамках

БРИКС прямые контакты между СМИ наших государств пока только формируются.

Медийные компании нацелены на максимальную дискредитацию России и ослабление ее позиций. Ведется широкомасштабная антироссийская пропаганда по всем возможным сюжетам. В октябре 2016 года в интервью «Воскресному времени» на Первом канале С.В.Лавров отметил, что в основе политики уходящей администрации США лежит именно русофобия. Причем речь идет не только об исторической русофобии, а о конкретных агрессивных шагах в информационной сфере, которые реально ставят под угрозу нашу безопасность. Будем надеяться, что при новой администрации в Вашингтоне такое положение дел изменится.

Надо отметить, что западными СМИ взяты на вооружение не просто критика наших действий, но и подтасовка фактов, и клевета, и провокации. Так, некоторые сирийские правозащитные НКО заявляют о массовой гибели сирийского гражданского населения в результате якобы действий сирийской армии при поддержке российских ВКС. Не сбавляет обороты и кампания по очернению отечественных спортсменов и российского спорта в целом. Один за другим всплывают журналистские псевдорасследования и заявления спортивных функционеров о якобы годами отработанной системе допинговой поддержки на государственном уровне. Поэтому мы не удивляемся, что по мере приближения чемпионата мира по футболу 2018 года появляются спекуляции о якобы неготовности нашей страны к проведению этого крупного международного мероприятия.

Развивается практика информационных вбросов в международное пространство с непроверенными, предполагаемыми данными по типу публикаций о панамских офшорах, финансовых связях отдельных бизнесменов с российским руководством. Вбросы с официальных баз данных происходят вследствие взломов информационных сетей, а это уже напрямую относится к информационной безопасности. Соответственно, гуманитарный аспект этой проблемы становится все более острым. Со своей стороны в МИД мы за последние годы много занимались работой с общественным мнением для того, чтобы противостоять негативным решениям западных стран, ложным установкам в отношении нашей страны.

Как вы знаете, в Концепции внешней политики в последней редакции отмечено, что Россия будет добиваться объективного восприятия в мире, развивать собственные эффективные средства информационного влияния на общественное мнение за рубежом, содействовать усилению позиций российских и русскоязычных СМИ, включая соотечественников, в мировом пространстве, предоставляя им при этом господдержку. Наша страна активно сотрудничает в мировом сообществе в информационной сфере. В этих целях предполагается широко использовать ИКТ, для безопасного использования которых мы с западными партнерами пытаемся формировать комплекс правовых норм. В рамках МИД России решаются вопросы координации по распространению за рубежом сведений о внутренней и внешней политике, а также формированию объективного образа России на международной арене, отчасти этими вопросами занимается и Россотрудничество.

Позиция России по актуальным международным вопросам находит отражение в ходе конференций и заявлений руководства страны, в официальных заявлениях внешнеполитического ведомства России, в ходе еженедельных пресс-брифингов официального представителя МИД России. Брифинги проходят не только с российскими, но и иностранными участниками. Мы обеспечиваем в массмедиа публикации выступлений, интервью министра, заместителей министра, руководителей загранучреждений. В дополнение к традиционным методам работы с максимально широкой аудиторией, включая граждан России, мы используем новые инструменты дипломатии - это сайты министерства, РЗУ, а также присутствие в отечественных соцсетях, включая и личные аккаунты.

Мы уделяем большое внимание содействию российским массмедиа в обеспечении их безопасности, профессиональных прав, поддерживаем СМИ своих соотечественников, стараемся выстраивать долгосрочные доверительные отношения с иностранными корреспондентами. В целом наша линия показывает свою эффективность. В последние годы нам удалось значительно повысить оперативность реагирования на крупные информационные поводы, а также мы стараемся небезуспешно

выстраивать собственную позитивную повестку дня. По нашей оценке, в основном нам пока удается противостоять нападкам, идущим от западных оппонентов, в которых также используют СМИ и НКО. Мы все отмечаем повысившийся уровень недоверия граждан западных стран к своим руководителям.

Понимаем, что, с одной стороны, надо дальше предпринимать усилия для пресечения грязных приемов в международном медийном пространстве, а с другой - распространять объективную информацию о нашей стране, позиции России по актуальным международным проблемам. Будем продолжать свою работу по этим направлениям.

Максим Григорьев, член Общественной палаты РФ, директор Фонда исследования проблем демократии: *На специальном заседании Контртеррористического комитета ООН мы недавно обсуждали эти вопросы, даже название мероприятия было абсолютно сходное - «Предупреждение использования информационных технологий в террористических целях». Мы здесь пересекаемся. Журнал «Международная жизнь» - организатор нашей конференции - стоит на ведущих позициях в обсуждении этой актуальной международной проблемы, что очень позитивно.*

Подписанная в декабре 2016 года Президентом РФ Доктрина информационной безопасности - очень правильный документ, во многом носит исчерпывающий характер. Там выделяется ряд сфер, которые мы уже упоминали, - и информационно-техническое воздействие в военной сфере, и информационно-психологическое воздействие, которое направлено на дестабилизацию внутренней политической ситуации.

За последние годы мы видели много примеров, особенно яркий из них - конституционный переворот на Майдане в Киеве. Какое-то время представители нашего фонда находились там, даже вышла книга «Евромайдан».

Представители псевдонезависимых организаций не скрывают, что они прошли соответствующий тренинг и подготовку. Мы видели это по результатам нашего мониторинга в сетях Интернета. Когда, например, на конференции ОБСЕ приглашают десятки украинских организаций, которые проводят мероприятия против России. Когда в прошлом году на площадке ООН мы пред-

ставляли доклад о системном использовании пыток украинскими вооруженными силами, спецслужбами, о действиях против граждан в Донбассе, то опросили более 100 человек - жертв этих пыток, которых Украина передавала в обмен на пленных. Я лично присутствовал при некоторых таких обменах, потом общался с этими людьми.

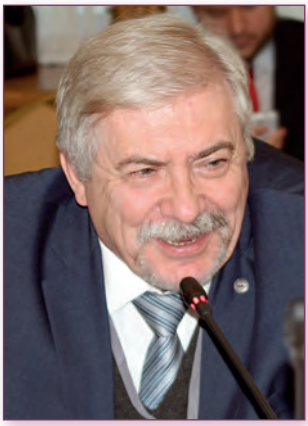
Мы рассылали свои доклады по электронной почте. У нас 60 тыс. адресов депутатов парламентов Европы и США, ведущих журналистов западных СМИ. Вскоре мы увидели, как западные структуры оперативно выпустили свой доклад в целях противодействия в том числе и нашей деятельности. Польский сенатор опубликовал свой доклад о российских военных преступлениях в Восточной Украине, использованные сведения не были документально подтверждены. Мы видели, как дипломаты Евросоюза практически координировали эти действия. Более 30 человек на мероприятии, у нас есть даже фотографии, в режиме онлайн вели антироссийскую пропаганду в социальных сетях. Нам удалось преодолеть это, внося поток нашей информации. Все делалось с напряжением определенных сил.

Другое направление, которое здесь тоже уже обсуждалось: мы видим, какое психологическое давление оказывается на ситуацию в Сирии, как ряд западных стран выстраивает сотрудничество с террористическими организациями. Все знают ситуацию с «Белыми касками» - только по открытой информации, финансирование составляет более 50 млн. долларов, даже не надо доказывать их связь с террористами, участие в казнях мирных граждан, создание фальсифицированных постановочных сюжетов, использование «Белых касок» для передвижения вооруженных боевиков, не говоря уже о сообщениях, что русские якобы в очередной раз бомбили последний госпиталь, 50-й по счету.

Хотелось бы отметить, что мы недооцениваем эффективность проведения антироссийской кампании, которая направлена на российских мусульман. Мы в нашем фонде ведем ежедневный мониторинг российских официальных сетей. В дальнейшем можно отслеживать, как меняются результаты данных отчетов.

Образование и информационная безопасность

Александр Стоппе, начальник аналитического отдела Постоянного комитета Союзного государства России и Белоруссии, профессор МГИМО МИД РФ



В своем выступлении я остановлюсь на проблеме, которая на первый взгляд может выпадать из привычной тематики подобных конференций, однако без нее представляется невозможным полноценное обсуждение стоящих на повестке дня вопросов. Речь идет о сфере образования и его месте в системе информационной безопасности.

Эта тема присутствует в новой Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 5 декабря 2016 года, в разделе, посвященном национальным интересам в контексте применения информационных технологий для сохранения культурных, исторических, духовно-нравственных ценностей, в разделе угроз, когда речь идет о размывании российских духовно-нравственных ценностей и недостаточной эффективности научных исследований в области образования и т. д.

Необходимо отметить, что в Российской Федерации все нормативные правовые документы в сфере обеспечения национальной безопасности постулируют безопасность личности, общества и государства, причем именно в таком порядке.

В современном мире, когда личность подвергается массированным атакам в информационной сфере, она должна быть защищена не только всей системой информационной безопасности государства, но и сама быть информационно устойчивой. И если человек не имеет достаточного уровня образования, сам не готов к противодействию негативному информационному воздействию, не умеет отделять «зерна от пле-

вел», никакие самые изощренные системы парирования угроз в информационной сфере не будут достаточно эффективны.

Представляется, что сегодня, говоря о безопасности личности в информационном пространстве, кроме понятия «угроза», к сожалению, можно уже применять термин «информационное насилие». В процессе глобальной информатизации человек стал информационно «прозрачен». При наличии желания и средств любая имеющаяся информация о конкретной личности может стать доступной и быть использована в своих целях как другой личностью, группой лиц, так и различными организациями, фондами, партиями и т. п.

В этой связи, как и в любой другой сфере общественной жизни, человек не вправе рассчитывать только на помощь государства, но и сам должен уметь противостоять этим угрозам, уметь дать им отпор.

В России, особенно в последнее десятилетие XX века, мы наблюдали деструктивную роль различных форм мифологизации сознания, «бригадизации», культа денег, падение престижа и ослабление важнейших социокультурных институтов государства - науки, культуры, образования, воспитания, в том числе физического и психологического.

Все это имело свои последствия, которые мы чувствуем и сегодня. Они не могли не сказаться в негативном плане на устойчивости личности, ее психики к различным информационным воздействиям. При этом надо понимать, что личность может считаться устойчивой в коммуникационной сфере, если она способна провести критический анализ, оценку воспринимаемой информации, а также принять объективное решение на основе этой информации.

Все это во многом зависит от качества образования. Не лишним будет вспомнить слова О.Бисмарка о том, что именно прусский учитель обеспечил политические и военные победы Пруссии и создание единой Германии.

Государство сегодня зависит от своих граждан в не меньшей, а может быть и в большей степени, чем они от него. И неспособность обеспечить им условия для самореализации приведет к отставанию страны. Отсюда одна из главных стратегических целей обеспечения безопасности - кардинальное

наращивание и улучшение качества человеческого капитала нации, радикальное повышение эффективности его использования, его информационная безопасность.

Нельзя забывать и о том, что многие достижения научно-технической мысли использовались не только во благо людей. Достаточно вспомнить открытия в ядерной физике, приведшие к созданию атомной бомбы, в оптоэлектронике - лазерное оружие, в химии - отравляющие газы, в биологии - биологическое оружие и т. д. Всегда находились силы, которые стремились использовать в своих интересах открытия в научно-технической сфере. Еще более это заметно в области информационных технологий, потому что информация, как библейский змий-искуситель, может пролезть в любую щель: социальные сети, различные блоги и даже компьютерные игры, нацеленные на деградацию личности. По сути, сегодня можно говорить о новом наркотике, но уже информационном.

Советское образование, а до него образование в Российской империи, было одним из лучших в мире. Большинство самых выдающихся изобретений XIX и XX веков имеют российские корни. Советские студенты постоянно побеждали на международных олимпиадах по физике, математике, химии, биологии, потому что школа учила думать. Сегодня мы не можем этим похвастаться, а наши вузы - за исключением МГУ, МГИМО, Санкт-Петербургского государственного университета, МИФИ, МФТИ - далеки от позиций лидеров рейтинга ведущих мировых учебных центров.

Здесь можно вспомнить и известный план Аллена Даллеса в отношении СССР, и «вражьи голоса» из-за кордона, которые кажутся сегодня достаточно примитивными по сравнению с современными возможностями, и учебники, финансируемые Фондом Сороса, и т. д. Цель была не только воздействовать на личность, но сделать все возможное для снижения уровня образования.

Не могу не коснуться и набившей оскомину темы ЕГЭ, не говоря уже о том, как реализовывалась в России Болонская декларация о зоне европейского высшего образования 1999 года. Как-то на семинаре я задал студентам вопрос, на который надеялся получить быстрый и верный ответ. Ожидания оказались тщетными. Тогда я предложил им четыре варианта ответа, из которых толь-

ко один был верным, как на ЕГЭ. Девять из десяти студентов сделали правильный выбор. Школа не научила их думать. Она даже если и дала знания, то только для того, чтобы, в лучшем случае, определить, а то и просто угадать верный вариант ответа. Поэтому в том числе так сильно воздействие социальных сетей, которые зачастую предоставляют решение проблем, не требуя их анализа, «освобождая» пользователя от раздумий.

При этом и школа, и вуз, как правило, не учат размышлять, анализировать, формировать возможные сценарии, варианты решения задачи. Можно соглашаться или не соглашаться с сатириком Задорновым в определении американцев, но свое «отставание» от нас в живости ума, в умении анализировать, принимать неординарные решения они компенсируют умением предусматривать различные сценарии, пусть приемлемым окажется далеко не первый. Вспомните американские фильмы, где достаточно часто звучит вопрос: а какой у нас план «В»?

Поэтому, пока мы не сможем восстановить способность воспитывать, формировать образованную, активную, патриотичную личность, все наши действия по созданию информационной безопасности при самом высоком ее научном, технологическом, программном обеспечении будут недостаточно эффективны.

В этой связи, когда мы говорим об информационной безопасности, мы просто не имеем права не рассматривать личность как самостоятельную «боевую единицу» в информационном противостоянии, а ее главным оружием, наряду с программными продуктами и техническими средствами, должны стать образование, культура, духовность.

В заключение хотел бы привести слова П.А.Столыпина о том, что «народ, не имеющий национального самосознания, - есть навоз, на котором произрастают другие народы». Очень резкие слова, но они подчеркивают крайнюю злободневность необходимости в повышении уровня образования, а также культуры в современном мире информационного противоборства, потому что без этого невозможно сохранение национального самосознания, неразрывно связанного с толерантностью в том числе как защиты против негативного для безопасности страны информационного воздействия.

Что необходимо для принятия взвешенных решений при выборе средств киберзащиты

Михаил Лядов, вице-президент по Центральной и Восточной Европе компании «ATOS» (Франция), председатель Комитета по информационным технологиям Франко-российской торгово-промышленной палаты

Добрый день, уважаемые дамы и господа!

Компания «ATOS» является ведущей сервисной IT-компанией в Европе с оборотом 12 млрд. евро, штатом сотрудников 100 тыс. человек и представлена в 72 странах мира. В России компания «ATOS» представлена 1 тыс. сотрудников и обладает множеством сертификатов и лицензий, в том числе сертификатами ISO 9000, 21000 и 27000.

Сегодня хотелось бы осветить четыре пункта:

1. Кибербезопасность как глобальная угроза.
2. Пример решения такой угрозы в виде бизнес-кейса Олимпийских игр в Рио в 2016 году.
3. Принятие решений об оценке рисков по кибербезопасности советами директоров.
4. Небольшое напоминание о личной безопасности руководящего состава.

Извне может показаться, что вести бизнес просто. Вы создаете продукты и продаете их клиентам. Но когда вы смотрите на картину мира шире, то понимаете, что экосистема включает всех стейкхолдеров: регулятора, мобильную рабочую силу, хакеров, облачный сервис, идентификацию, управление поставками и снижение издержек. Каждый из этих компонентов представляет для вашего бизнеса как вызов, так и новые возможности.

Как показывает «Gartner», один из ведущих аналитиков в этой сфере, более 60% компаний подвергнутся кибератакам в ближайшем будущем. Также он указывает, что атаки на компании растут в

количественном измерении на 20% в год. Влияние этого фактора на жизнеспособность бизнеса будет только увеличиваться.

Олимпийские игры привлекают внимание миллиардов зрителей по всему миру, и значение этого события не только спортивное, но и геополитическое. Ну и, безусловно, оно влияет на имидж страны, где проходят соревнования. Чтобы понять сложность этого события, хотел бы сказать, что подготовка к Олимпийским играм начинается за четыре года и включает в себя так называемый мастер-план с обратным отчетом времени, построение инфраструктуры, создание приложений, набор и обучение IT-персонала в количестве нескольких тысяч человек и последующее сворачивание проекта. А цена ошибки видна всем - нет возможности повторить и исправиться. Именно в этом данный пример похож на реальную ситуацию в бизнесе, с которой может столкнуться Совет директоров, - отсутствие второго шанса.

Как я и говорил, проблема кибербезопасности - это глобальная проблема, с которой невозможно бороться локально, поэтому для выполнения таких сложных задач «ATOS» построил сеть глобальных центров, которые решают данные вопросы.

Подходя к проблеме кибербезопасности в работе Совета директоров, хотел бы привести примеры из опроса членов Совета директоров по кибербезопасности. Как показывает отчет, члены Совета директоров воспринимают угрозы кибербезопасности очень серьезно и две трети готовы менять работников IT-подразделений в случае проблем в направлении кибербезопасности.

Практически все члены Совета директоров знают, что делать с информацией по кибербезопасности и как оценивать риски. Две трети верят, что действия IT достаточны. 70% членов Совета директоров понимают техническую информацию, хотя 50% из них говорят, что эта информация слишком технична. 75% членов Совета директоров хотят получать информацию, не требующую навыков в области кибербезопасности.

Первый вопрос: кто в Совете директоров отвечает за кибербезопасность? Обычно этот вопрос делегируется комитету по аудиту или комитету по рискам, если такой существует в структуре Совета директоров. Он обязан периодически предоставлять отчеты для всего Совета директоров.

Однако часть компаний контролирует вопрос безопасности. На уровне менеджмента - это генеральный директор и структура IT.

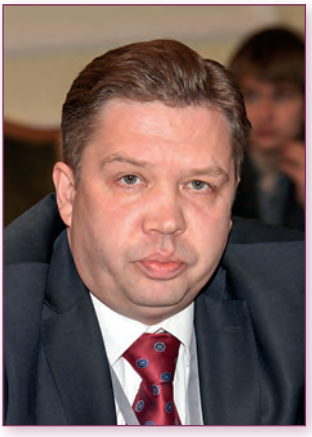
Техническая экспертиза и платформа IT - это только часть системы. Каждая часть организации играет свою роль в кибербезопасности и должна понимать приоритет этой задачи. Это отдел персонала, бизнес-подразделения, коммуникации, финансы, закупки, внутренний аудит, отдел слияний и поглощений.

Подход к оценке кибербезопасности основан на оценке риска, потому что защита периметра не может обеспечить полную защиту. Поэтому использование Dashboard-панелей с основными KPI, определенными руководством компании, является одним из типичных примеров работы с рисками кибербезопасности в советах директоров.

Последний, но немаловажный пункт, на который я хотел бы обратить ваше внимание, это личная безопасность. К сожалению, этим пунктом пренебрегают руководящие работники и члены Совета директоров.

Прогрессивное развитие международно-правовых основ внешней политики и информационной безопасности Российской Федерации

Алексей Моисеев, вице-президент Российской ассоциации международного права, член Международно-правового совета при МИД РФ, доктор юридических наук



За короткий промежуток времени в России были приняты два основополагающих документа - Концепция внешней политики (30 ноября 2016 г.) и Доктрина информационной безопасности (5 декабря 2016 г.).

Концепция внешней политики представляет видение Россией современных мировых проблем в быстроменяющейся «мозаично-противоречивой» международной обстановке. Документ формулирует дипломатические ответы на весь спектр вопросов внешнеполитической повестки в рамках определенного исторического периода. Концепция под-

черкивает, что «Россия проводит самостоятельный и независимый внешнеполитический курс, который продиктован ее национальными интересами и основой которого является безусловное уважение международного права».

Внешнеполитическая деятельность государства направлена на дальнейшее продвижение курса по укреплению международного мира, обеспечению всеобщей безопасности и стабильности в целях утверждения справедливой демократической международной системы, основанной на коллективных началах в решении международных проблем, верховенстве международного права, прежде всего, на положениях Устава ООН, при центральной координирующей роли ООН.

Важно, что в новой Концепции внешней политики России отражено единство и преемственность российской внешней политики не только в пространстве, но и во времени, без противопоставления одних исторических периодов другим. Неслучайно МИД называют самым консервативным ведомством. Общее направление российской внешней политики всегда сохранялось, несмотря на смены режимов, трагедию Второй мировой войны, «борьбу за мир», за которой последовал крах СССР и «геополитическая катастрофа конца прошлого века». Принципиальных отличий между внешней политикой Святослава и политикой Молотова - Громыко - Лаврова не просматривается. В этом смысле Россия всегда выступала «уравновешивающим фактором в международных делах и развитии мировой цивилизации».

Приоритетными ценностями российской внешней политики являются целостность России и ее органическое геополитическое положение в многополярном мире. Идея «полицентричной архитектуры международных отношений» - это единственный адекватный ответ на пережитую в XX веке геополитическую катастрофу, причем не только для России, но и для всего мира. Для России неприемлемы тоталитарные идеи «мирового правительства» или военно-политической гегемонии, которые не оставляют никакой возможности выбора ни для государств, ни для человека.

Полюса полицентричного мира в целом совпадают с геополитическими «пространствами» экономического и политического влияния, которые следуют собственным историческим путем цивилизационного развития, такие как Китай, Европа, Северная Амери-

ка и Великобритания, исламский мир, Индия, Азиатско-Тихоокеанский регион, Латинская Америка. Для России таким пространством является Евразия, включая «российскую диаспору».

Соединенные Штаты Америки и Великобритания - ядро противоположного мира, мировая экспансия которого при поддержке международного капитала приводит к историческому противостоянию, которое Россия стремится завести в определенные правовые рамки.

По словам министра С.Лаврова, «в идеале полицентричная архитектура международных отношений должна опираться на взаимодействие ведущих центров силы в интересах совместного решения глобальных проблем». Включая проблемы устойчивого мироустройства; верховенства права в международных отношениях; укрепления международной безопасности; международного экономического, гуманитарного и экологического сотрудничества; информационного сопровождения внешнеполитической деятельности.

Кроме этого, сохраняется опасность со стороны «трансграничных вызовов и угроз, таких как распространение оружия массового уничтожения, нелегальная миграция, торговля людьми, незаконный оборот наркотических средств и психотропных веществ, коррупция, морское пиратство, киберпреступность, глобальная бедность, изменение климата, а также угрозы в области продовольственной, экологической и санитарно-эпидемиологической безопасности».

Новшеством концепции является прямое указание в разделе, посвященном верховенству международного права, на недопущение неконституционной смены власти под внешним влиянием. «Глобальные вызовы и угрозы требуют адекватного ответа со стороны международного сообщества при координирующей роли ООН с учетом объективной взаимосвязи вопросов защиты прав человека, обеспечения безопасности и устойчивого развития».

Россия выступает категорически против использования террористических организаций для политических и иных целей.

По своей природе и своему укладу Россия отвергает любое идолопоклонство, включая поклонение «демократии», «правам человека» и т. п. Демократия не существует сама по себе, равно как и другие формы государственного устройства, она является разной для каждого народа и обусловлена его историей и культурой. Так и идеализация «прав человека» ведет к подмене ценностных ориентиров и деградации человека. Утверждение смены пола, эвтаназии нормой может привести только к смене сознания и подмене того,

что считать «нормой». Права человека могут существовать только вместе с его обязанностями - по отношению к государству, народу, семье, Богу. Полагаю, что более точной является концепция «прав нормального человека», «опирающаяся на общий духовно-нравственный потенциал основных мировых религий, а также на такие принципы, как стремление к миру и справедливости, достоинство, свобода, ответственность, честность, милосердие и трудолюбие».

Кроме этого, подрыв духовно-нравственных основ ведет к искажению толкования религиозных ценностей, которые становятся идеологической основой современного терроризма, например исламистов из ИГ и аналогичных структур.

В этой связи принцип невмешательства во внутренние дела, который обычно противопоставляют принципу уважения и защиты прав человека, получает новое звучание в рамках концепции, содействует развитию диалога и партнерства в интересах укрепления согласия и взаимообогащения различных культур и цивилизаций.

К задачам российской внешней политики, помимо распространения и укрепления позиций русского языка в мире, популяризации достижений национальной культуры, национального исторического наследия и культурной самобытности народов России, российского образования и науки, консолидации российской диаспоры, укрепления позиций российских СМИ в глобальном информационном пространстве, добавилась задача доведения российской точки зрения на международные процессы до широких кругов мировой общественности.

«Россия добивается объективного восприятия ее в мире, развивает собственные эффективные средства информационного влияния на общественное мнение за рубежом, содействует усилению позиций российских и русскоязычных средств массовой информации в мировом информационном пространстве, предоставляя им необходимую для этого государственную поддержку, активно участвует в международном сотрудничестве в информационной сфере, принимает необходимые меры по противодействию угрозам своей информационной безопасности».

Концепция подчеркивает тот факт современных международных отношений, что «неотъемлемой составляющей современной международной политики становится использование для решения внешнеполитических задач инструментов «мягкой силы», прежде всего возможностей гражданского общества, информационно-ком-

муникационных, гуманитарных и других методов и технологий, в дополнение к традиционным дипломатическим методам».

Весьма значительный потенциал продвижения объективной информации, позитивного имиджа России, в том числе в русскоязычном сегменте, сегодня не используется. Как следствие, упускаются многие уникальные возможности.

Новая Доктрина информационной безопасности 2016 года вполне соответствует тенденциям, направленным на усиление контроля над российским сегментом Интернета со стороны государства и более активное его использование как площадки и инструмента для ведения информационной работы. Она пришла на смену Доктрине информационной безопасности Российской Федерации от 9 сентября 2000 года и является логическим продолжением Стратегии национальной безопасности Российской Федерации от 31 декабря 2015 года, учитывающим национальные приоритеты.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

В доктрине 2016 года подчеркивается приверженность соблюдению общепризнанных принципов и норм международного права, международных договоров Российской Федерации, несмотря на отсутствие международно-правовых норм и механизмов, регулирующих межгосударственные отношения в сфере информационных технологий, во всех сферах жизни. Вместе с тем в доктрине исчезло положение о недостаточной развитости национального правового регулирования сферы информационных технологий и информационной безопасности.

Положения новой доктрины соответствуют актуальным тенденциям в сфере обеспечения глобальной безопасности, противодействия кибератакам, угроз, связанных с экстремистской деятельностью, а также импортозамещения и снижения зависимости от зарубежных промышленных технологий и др.

В условиях непростой геополитической обстановки ликвидация зависимости от иностранных информационных технологий является частью стратегии информационной безопасности Российской Федерации. Применение информационных технологий с использованием отечественных разработок становится одной из первостепенных задач доктрины.

По-прежнему остро стоят вопросы противодействия методам «информационной войны». Все большую опасность приобретают угрозы компьютерных атак на объекты информационной инфраструктуры.

Новая редакция доктрины нацелена на развитие как национальной системы управления российским сегментом сети Интернет, так и кадрового потенциала в области обеспечения информационной безопасности. В целом Россия движется в сторону смягченного варианта регулирования Интернета государством по китайскому сценарию, где вопросы информационной, разведывательной и военно-политической безопасности имеют приоритетное значение.

В новой версии документа значительно возросло внимание к внешним геополитическим и военно-политическим угрозам, связанным с враждебными действиями со стороны иностранных государств, террористических, экстремистских и криминальных организаций, к проблемам, связанным с препятствием деятельности государственных СМИ по информированию российской и зарубежной аудитории о государственной политике Российской Федерации.

Наряду с органами власти различного уровня впервые участниками системы обеспечения информационной безопасности признаются: собственники объектов информационной инфраструктуры и организации, эксплуатирующие такие объекты; средства массовой информации и массовых коммуникаций; организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка; операторы связи; операторы информационных систем; организации, осуществляющие образовательную деятельность; общественные объединения; иные организации и граждане, которые участвуют в решении задач по обеспечению информационной безопасности.

Положения новой Доктрины информационной безопасности и особенно Концепции внешней политики указывают на изменение всего политического мировоззрения Российского государства. Новые подходы указывают на возвращение к традиционному отношению к власти, культуре, народу, территории и не могут в будущем не отразиться на изменении российского законодательства.

Российско-китайское сотрудничество и информационная безопасность в новую интернет-эпоху

Виктор Сюй, президент глобальной технологической компании «LeEco» в России и Восточной Европе» («LeREE»), академик Международной телекоммуникационной академии (Китай)

Уважаемые участники конференции! Благодарю организаторов этого важного мероприятия - Министерство иностранных дел и редакцию журнала «Международная жизнь» за возможность выступить и высказать свое мнение.

Как руководитель рабочей группы «Интернет + Китай» при Институте развития Интернета я много общаюсь по вопросам интернет-технологий и информационной безопасности с руководителями крупных технологических компаний, таких как «Huawei», «JD.com», «Alibaba», «Chiha 360» и других предприятий, которые занимаются интернет-проектами, большими данными и облачными технологиями.

Говоря об информационной безопасности, важно разграничивать ее уровни. Есть сетевая безопасность и информационная безопасность (security), а есть защита информации частных пользователей (privacy).

Сейчас так или иначе основная часть интернет-активности ориентирована на пользователя, поэтому вопросы защиты персональных данных крайне актуальны и вызывают жаркие дискуссии в обществе. С одной стороны, есть позиция государств, одна из основных задач которых - обеспечение государственной безопасности, и с другой - граждане, которые с беспокойством относятся к вторжению в их частную жизнь и ограничению их свобод. Здесь, как и в любой другой сфере, необходим разумный баланс.

«LeEco» как глобальная интернет-компания и производитель смартфонов, смарт-телевизоров и в перспективе

смарт-автомобилей, имеющая свои интернет-платформы и облачные сервисы, уделяет вопросам информационной безопасности и защиты персональных данных значительное внимание. Очевидно, что массовое проникновение Интернета и доступность абсолютно любого контента, в том числе вредоносного и шокирующего, может нанести ущерб как отдельным гражданам, так и государственной безопасности.

Огромное количество китайцев пользуется сегодня Интернетом - около 800 миллионов. Кстати, онлайн - видеоплатформа «LeEco» - «Le.com» насчитывает те же 800 млн. уникальных пользователей в месяц.

Интернет в Китае появился в 1994 году. В 1998-м правительство осознало, что пришло время подумать о защите народных масс от вредоносной информации, и началась разработка системы «Золотой щит», которая была запущена в 2003 году. От чего защищает «Золотой щит»? Прежде всего от порнографии и политической дезинформации. Критерии блокировки сайтов постоянно меняются и совершенствуются. Блокировка может производиться по ключевым словам и по «черным спискам». В настоящий момент идет переход от «черных списков» к «белым». То есть сейчас китаец может зайти на любой сайт, который не заблокирован. А в будущем сможет посещать только разрешенные ресурсы.

Среди известных в мире сайтов, заблокированных «Золотым щитом», - «Google», «Facebook», «Instagram», «Twitter» и другие глобальные платформы западного происхождения. Для иностранцев в роуминге доступны все интернет-ресурсы. На Гонконг и Макао (регионы с особым статусом) блокировка не распространяется.

С 1 марта 2015 года в Китае был принят закон, согласно которому все аккаунты в соцсетях, микроблогах, на форумах и других сайтах должны регистрироваться с указанием реальных паспортных данных. Несмотря на жесткие блокировки, лишь каждый пятый китаец (среди пользователей Интернета) использует «VPN». Это неудивительно, ведь в китайском сегменте Интернета есть все необходимое для жизни. Все всемирно известные сайты и социальные сети имеют популярные китайские аналоги с десятками миллионов пользователей.

Вместо «Google» у китайцев - «Baidu». Четыре из пяти поисковых запросов в Китае осуществляется через эту систему. Кроме поиска, компания владеет сервисом для хранения файлов, онлайн-картами, социальной сетью и десятками других ресурсов.

«QQ.com» - один из самых посещаемых информационных порталов, а одноименный мессенджер является популярным средством общения. «Taobao» - всемирно известный магазин с огромным ассортиментом товаров. Кстати, собственный онлайн-магазин «LeEco» - «LeMall.ru», продающий продукцию компании и партнеров, - третий по трафику в Китае после «TMall» («Alibaba») и «JD.com». К слову, китайцы очень активно закупаются в интернет-магазинах. Это делает каждый второй пользователь сети.

Вместо «Twitter» и «Facebook» у китайцев - «Weibo».

Этот сервис имеет огромную популярность среди населения (почти 250 млн. пользователей). У меня тоже есть аккаунт в «Weibo» с численностью 0,5 млн. подписчиков.

Вместо «YouTube» китайцы пользуются «Youku», вместо «Facebook» - «Renren», а вместо «Pinterest» - «Huaban».

Еще в Китае не работает «Википедия». Но есть своя энциклопедия «Hudong». Количество статей в ней опережает англоязычную «Википедию». Не менее масштабна энциклопедия «Baidu».

В целом следует отметить, что китайский Интернет обширен и у каждого из вышеназванных сервисов есть огромное количество аналогов.

Одной из характерных особенностей китайского Интернета являются доменные имена, состоящие только из цифр. К примеру, на «4399.com» располагается крупный портал с флеш-играми.

300 млн. китайцев учили/учат английский, но дается он им с трудом. Числовую последовательность многим запомнить легче, чем латиницу. Кроме того, многие китайцы имеют e-mail-адреса, первая часть которых состоит из цифр.

Порядок цифр в названиях сайтов часто бывает совсем не случайным, а фонетически обоснованным. К примеру, по адресу «1688.com» расположен магазин «Alibaba». А числовой ряд «1, 6, 8, 8» звучит по китайски «йау-лийо-ба-ба».

Уровень интернет-цензуры в Китае далеко не самый высокий. В соседней Северной Корее доступ к сети имеют лишь некоторые организации, имеющие специальное разрешение (их около 1,5 тысяч), в частности посольства иностранных государств. Простые корейцы пользуются собственной сетью «Кванмён» (через «Dial-Up»). И даже в эту локальную сеть можно выходить только с рабочих компьютеров.

От Интернета полностью отключали также Египет и Ливию в 2011 году. В 2014 году российские власти стали всерьез задумываться о возможности перекрытия доступа во Всемирную сеть страны в случае чрезвычайной ситуации и угрозы национальной безопасности страны.

Что ни говори, в нашей жизни сегодня многое предопределяется всепроникающим Интернетом. Стираются границы государств, ускоряются экономические, информационные процессы, создаются абсолютно новые межиндустриальные связи и явления.

Мы уже вошли в эпоху информационного общества. В такой динамично развивающейся сфере, как Интернет и информационные технологии, вопросы безопасности и регулирования зачастую отстают на шаг. Здесь необходимы гибкость и скорость, чтобы, с одной стороны, не помешать бурному развитию интернет-технологий и всей экономики в целом, а с другой - не допустить ущерба безопасности государств и рядовых граждан.

Согласно «Common Law», применяются правила из соображений совести и справедливости, как альтернатива континентальному законодательству, где решения принимаются элитными судьями. «Common Law» больше подходит для таких динамично развивающихся и нестабильных отраслей, как Интернет и информационные технологии, где высока скорость развития, но, однако, не определены правила.

В Интернете все развивается по интуитивной модели, ничто не кодируется заранее. Это другая культура, другая философия. И подход к информационной безопасности нужен двоякий. С одной стороны, нужен базовый закон, с другой - невозможно все охватить в такой динамично развивающейся отрасли. Многие вопросы решаются по ходу.

Китайские интернет-платформы и интернет-ориентированные отрасли сегодня на несколько лет опережают в своем развитии российские аналоги, а также многократно превосходят их по масштабу, количеству пользователей. В последние годы мы наблюдаем активную экспансию китайских платформ в Россию. Это очень полезно и для развития российско-китайского сотрудничества в целом, и для российской экономики в частности. Россия, подтягиваясь за Китаем, внедрит новые технологии значительно быстрее, впитывая и адаптируя под себя уже готовые решения.

Кроме того, крайне актуальные сегодня вопросы российско-китайского экономического и культурного сотрудничества будут решаться и уже решаются значительно быстрее и эффективнее, возникают абсолютно новые сферы и формы взаимодействия - и в бизнесе (B2B, B2C), и в информационном культурном взаимодействии.

В 2014 году Генеральный секретарь ЦК КПК Си Цзиньпин выдвинул стратегическую инициативу строительства «Экономического пояса нового Шелкового пути» и «Морского шелкового пути XXI века». В новую интернет-эпоху особым содержанием наполняется концепция «Один пояс - один путь», ставшая важной стратегической мерой, которая соответствует новым экономическим реалиям и направляет их. Основываясь на принципах совместного обсуждения, совместного строительства и совместного использования, все страны вдоль «Шелкового пути» образуют небывалое слияние, организуют все ценные административные, рыночные и социальные ресурсы и оптимизируют распределение, не ограниченное государственными границами. Этот обладающий самым большим потенциалом развития экономический пояс дал огромное количество возможностей для развития бизнеса, культурного взаимодействия всем странам-участницам.

Концепция «Один пояс - один путь» - одна из основ бизнес-модели компании «LeREE» («LeEco Russia and Eastern Europe»), президентом и основателем которой я являюсь. Имея в основе глобальную технологическую интернет-платформу «LeEco», «LeREE» в своем развитии идет по пути вовлечения стран «Одного пояса - одного пути» в экономическое и культурное взаимодействие на основе общей интернет-платформы.

С инициативой «Один пояс - один путь» «LeEco» поразительно роднит особенная ценность - это интегрирование ресурсов, превращение преград в преимущества, оптимизация распределения и взаимовыгодное сотрудничество посредством экоплатформы. «LeREE» в качестве дочерней компании «LeEco» и международной платформы еще больше увеличит эту ценность. По сравнению с множеством предприятий, которые участвуют в инициативе «Один пояс и один путь», у «LeREE» есть особенные преимущества. Выбрав Россию в качестве первого шага участия в инициативе «Один пояс - один путь», «LeRee» выступит интегратором многих бизнес-процессов на основе своей интернет-экосистемы.

Сегодня многие традиционные компании так или иначе ведут бизнес в Интернете. Возникают абсолютно новые сочетания традиционных и недавно появившихся отраслей. Уже сегодня «LeREE» сделала ряд важных шагов на пути к тому, чтобы стать интернет-платформой российско-китайского сотрудничества и в области экономики, и в области культуры.

Так, еще в мае 2016 года мы заключили соглашение с компанией «Цифровое телевидение» (совместное предприятие ВГТРК и «Ростелекома») при поддержке Российского экспортного центра и Института развития Интернета об экспорте российского кино и видеоконтента в Китай на основе интернет-платформы «LeEco». Уже в июне первые три серии мультсериала «Мимимишки» за три дня набрали рекордные 6 млн. просмотров. Список российской видеопродукции, экспортируемой в Китай посредством нашей платформы, постоянно расширяется. Это прекрасный пример экономического и культурного сотрудничества России и Китая на основе интернет-технологий.

В конце августа мы подписали соглашение с Фондом развития Дальнего Востока о создании онлайн-платформы по экспорту российских экологически чистых продуктов в Китай - «LeLive». «LeREE» рассчитывает охватить своей интернет-платформой многие сферы российско-китайского взаимодействия. Сейчас как раз тот период, когда наши страны могут получить максимум от экономического и культурного сотрудничества. Интернет и информационные технологии позволят значительно ускорить эти процессы, создать новые связи между отраслями и

рыночными игроками и, самое главное, донести новые ценности до потребителей наших стран. При этом вопросы информационной безопасности и защиты данных являются для нас одними из приоритетных.

Когнитивные технологии как инструмент ответа на вызовы киберпространства

Кирилл Коктыш, политолог, доцент МГИМО МИД РФ, медиа-эксперт в области внешней политики (Республика Беларусь)

Буду созвучен во многом с Александром Георгиевичем Стоппе в том смысле, что главное не только техника и не то, что происходит в киберпространстве, а кто стоит за этой техникой - то самое гуманитарное измерение, тот самый замысел, который позволяет формировать и реализовывать разнообразные проекты. Всегда за всем стоят люди и, если быть более точным, - социальные сети. Один пример, который буквально две недели назад был на слуху, - это задержание в Белоруссии двух, по сути, блоггеров, журналистами их назвать нельзя, которые на самом деле вполне успешно на российских ресурсах размещали беларусофобские статьи. В Белоруссии достаточно жесткой была реакция на это, после чего некоторые люди шли в администрацию президента и требовали гранты на борьбу с белорусскими националистами.

Учитывая падение общего уровня морали, которое мы сегодня наблюдаем, эта задача достаточно актуальна. Хотелось бы представить проект, который мы сделали для Госдумы. Реализован он был полгода назад, сведения немного устарели, но методология осталась той же. Базируется он на когнитивистике. Она в начале XX века была инструментом в руках международников самых разных стран, начиная с США и Израиля, затем Советского Союза.

Когнитивистика позволяет понять и прогнозировать с той или иной степенью точности, из чего, собственно, исходит ваш контрагент, о чем он думает и из какого замысла исходит. Политик, облеченный властью, всегда действует не по своей воле, а в рамках той социальной сети, в которую он включен. В 2010 году, когда Обама пришел к власти и формировал свою администрацию, мы сделали для правительства РФ анализ его команды, исследовав более 140 человек. Посмотрели те стереотипы, установки, к которым люди апеллируют, рассуждая на тему международных отношений, потом мы получили корреляцию на 93% по поводу всех решений, которые администрация приняла до окончания срока своего существования, включая и нормализацию отношений с Ираном.

Человек сам по себе уникален и неповторим. Как только он действует в рамках сети, он будет всегда ограничен теми стереотипами, которыми мыслит вся сеть. Мы попробовали вычисление этих когнитивных стереотипов заложить в компьютерную программу, в частности по курдской проблематике, характерной для периода российско-турецкого кризиса. Посмотрели на те установки, которые курдские политические деятели легитимировали в той ситуации. Результаты получились интересными. Все мы знаем какие-то очевидные факты, от которых можно отталкиваться, а вот в рамках каких сфер они внедряются, узнать очень интересно. Все установки и те карты курдов, которые мы в результате получили, представились достаточно неожиданными и в плане политической стратегии, и позиционирования идентификации результатов.

Если мы говорим о способах прогнозирования в области предотвращения угроз, то понятно, что их число является приблизительным, понимание того, каким образом существуют социальные сети, на какие стереотипы и установки опираются, возможно, позволит объяснить ситуацию лучше.

Мы получаем обширную информацию, а понимаем ее меньше. Сейчас возникает необходимость в новых инструментах понимания, новых инструментах интерпретации. Базовые зоны их применения могут оказаться достаточно благоприятными и для предотвращения экстремизма, и для налаживания общего понимания ситуации, о каких контрагентах шла речь. Без сомнений, интегрировать можно совершенно разные сети и структуры.

Роль научных и образовательных учреждений в реализации Доктрины информационной безопасности 2016 года

Наталья Ромашкина, руководитель группы по проблемам информационной безопасности ИМЭМО РАН, кандидат политических наук

Хотела бы несколько слов сказать именно о проблеме, от решения которой совершенно точно зависит, как будут выполняться задачи, поставленные в новой Доктрине информационной безопасности 2016 года, как будут решаться вопросы, которые сегодня поднимались. Ведь, по сути, в новой доктрине обосновывается необходимость усовершенствования механизмов принятия государственных решений по минимизации и предотвращению угроз в информационной сфере.

Понятно, что на любом этапе процесса принятия государственных решений экспертное сообщество не всегда играет главную роль. Экспертное сообщество представлено и образовательными, и научными организациями. Для того чтобы оценить эффективность высшего профессионального образования в этой сфере, необходимо подчеркнуть ключевые особенности современной системы обеспечения безопасности в информационном пространстве. Вот только некоторые из них.

В первую очередь это ускоренное нарастание угроз, причем лавинообразное, что выделяет сферу информационной безопасности сегодня из всех других сфер. Это отставание теории - научной, политической, нормативно-правовой - от практики, той теории, которую должны создавать ученые, которая должна стать инструментом для практиков. Связано это напрямую с недостатком специалистов. Ведь еще совсем недавно казалось, что так называемых безопасников - специалистов в основном с техническим образованием в специальных

сферах - вполне достаточно для того, чтобы обеспечивать информационную безопасность.

Жизнь показала, что это не так - специалистов не хватает. Очень важное отличие сегодняшней ситуации от того, что было совсем недавно, - это выход международной информационной безопасности на международный уровень, и в рамках двусторонних отношений, и в рамках ООН. А это значит, что уже сегодня стоит задача подготовки специалистов-международников, которые разбирались бы в вопросах информационной безопасности.

Это совершенно, на мой взгляд, новый пласт специалистов, в которых мы сегодня очень остро нуждаемся. Высшее профессиональное образование в России по соответствующим специальностям, связанным с информационной безопасностью, получают уже более чем в 50 вузах нашей страны - это и технические вузы - МИФИ, в котором есть специальный факультет, Бауманский университет, - и МГИМО, даже Московская духовная академия. Но тем не менее специалистов не хватает, что выводит проблему на уровень необходимости подготовки специалистов на междисциплинарном и мультидисциплинарном уровнях. Сегодня это крайне важно, но пока еще не сделано. Кроме того, приводит к необходимости разработки новой образовательной стратегии для подготовки специалистов, обеспечивающих информационную безопасность.

Подобный процесс - долгий. Понятно, что стратегия должна создаваться в течение многих лет, но хотелось бы сказать несколько слов о том, что сегодня можно сделать и уже делается для того, чтобы эту проблему решить. А она заключается в том, что специалисты технических специальностей не разбираются в политической стороне данной проблемы, недостаточно знают о психологических аспектах. Наоборот, специалисты-гуманитарии не разбираются в технических вопросах, не понимают, что такое критически важные объекты и т. д.

Еще один пласт - юристы. Ведь сейчас в России переизбыток юристов, но юристов - специалистов в информационной сфере недостаточно. Знаю это не понаслышке. Поэтому междисциплинарный и мультидисциплинарный подход в образовании крайне важен во всех специальностях - и в тех-

нических, и гуманитарных. В чем, по сути, заключается проблема? Она на сегодняшний день, к сожалению, представляет замкнутый круг. Не хватает высококвалифицированных специалистов, отсутствует в связи с этим достаточная теория методологии, при этом недостаточно эффективен процесс принятия решений в этой области и недостаточен механизм эффективности реакции на угрозы, которые сегодня существуют в информационном пространстве. Как решать эту проблему? Уже можно предложить несколько практических методик в сфере высшего образования.

Во-первых, что очень важно, нужно уже в существующие образовательные программы включать те дисциплины, те направления, которые будут связаны с ликбезом в сфере информационной безопасности. Это уже делается. Очень интересно, что опыт всего нескольких лет показывает, какой огромный интерес проявляют студенты к данной сфере. Молодежь более восприимчива, чем старшие поколения, к этому направлению. Ребята с удовольствием берут курсовые и дипломные работы, бакалаврские и магистровские диссертации по этой проблематике. Сегодня в ИМЭМО РАН три аспиранта взяли для себя тему, связанную с обеспечением информационной безопасности.

Мы совсем недавно стали применять новую методику обмена, когда двум студентам из разных государств или из разных вузов РФ предлагается одна и та же тема для исследования. Понятно, что студенты могут находиться друг от друга очень далеко, но в постоянной связи, используя современные информационно-коммуникационные технологии. При этом руководители могут в зависимости от договоренности сыграть разную роль в процессе исследования этой темы. Ребята должны обмениваться данными, какую информацию, какие источники они используют, какие задачи ставят, какие научные методы применяют, и тогда действительно можно прийти к очень хорошим результатам. Мы только начали практиковать данную методику. Для этого сотрудничаем с МИФИ, а также с одним из американских университетов, результаты уже очень интересные. Здоровая конкуренция в молодежной среде приносит положительные результаты. Будем надеяться на успех научных исследований.

Что касается задач научных организаций, абсолютно убеждена, что они сегодня носят совершенно другой характер. Очень важно, чтобы проблема обособленности научных учреждений решалась. Думаю, что необходимо создать ассоциацию таких специалистов из разных областей. Перед научными организациями очень остро стоит проблема учета информационной безопасности в проблеме обеспечения стратегической стабильности. Она требует больших научных усилий. В ИМЭМО РАН несколько лет назад было создано подразделение проблем информационной безопасности. В 2016 году у нас вышли уже две монографии на русском и английском языках. Будем рады, если вы с ними познакомитесь, они выставлены на нашем сайте. Совсем скоро у нас выйдет еще одна монография. Таким образом, мы пытаемся решать вопрос обособленности в науке. Авторами являются и специалисты-психологи, и технические специалисты, и практики, которые ведут постоянный контроль за информационной безопасностью в соответствующих сферах.

Роль социальных медиа в борьбе с терроризмом

Рустем Агзямов, координатор проектов МИРаС

Террористы все чаще используют новый вид коммуникации - социальные сети - для разжигания ненависти и привлечения большего числа сторонников. Этот факт ставит под угрозу международную безопасность и стратегическую стабильность государств. Какие уроки мы можем извлечь из трагических событий последних двух лет, произошедших в мире?

13 ноября 2015 года в концертном зале Батаклан в Париже боевики захватили заложников и расстреливали их одного за другим, а когда полицейские начали штурм, взорвали себя с помощью «поясов смертника». Накануне

теракта один из террористов опубликовал свою фотографию в одной из социальных сетей с подписью: «К тому времени, когда мир увидит это лицо, будет слишком поздно». Так террористы сеют страх через социальные медиа.

Другой эпизод - 12 июня 2016 года 29-летний Омар Матин открыл огонь из огнестрельного оружия в ночном клубе «Pulse» в Орландо, а затем захватил заложников. В результате стрельбы погибло 49 человек, 53 получили ранения. Ответственность за произошедшее взяла на себя запрещенная в России террористическая организация «Исламское государство».

По информации «The New York Times», орландский стрелок использовал несколько учетных записей «Facebook», чтобы писать сообщения и искать записи об ИГИЛ. Матин делал запросы по ключевым словам «Клуб Пульс Орландо» и «Стрельба».

14 июня 2016 года еще один террористический акт произошел в Европе. В пригороде Парижа убиты полицейский и его супруга. И вновь социальные медиа стали соучастниками этого нападения. Находясь в доме семейной пары, преступник опубликовал 13-минутное видео. Во время трансляции он утверждал, что ответил таким образом на призыв лидера ИГИЛ к совершению терактов в Европе и Соединенных Штатах.

Нет сомнений в том, что террористы разбираются в технологиях. Мы живем в такое время, в котором социальные медиа используются так активно, как никогда раньше, и эволюция использования социальных сетей далека от завершения. Последней тенденцией является использование прямых трансляций. Потоковое вещание через соцсети в настоящее время совершает глобальный прорыв в понятии коммуникаций. Но этот прорыв может служить и средством разрушения: потоковое вещание - это новейший инструмент террористов.

Интернет всегда был акселератором и добра, и зла. Так какие уроки можно извлечь (или переосмыслить) в свете последних тенденций?

1) Нужно оценить роль социальных медиа в качестве акселератора и мультипликатора.

Социальные медиа ускоряют распространение практик террористов, облегчая их повторение в краткосрочной и долгосрочной перспективе. Перед нами стоит ряд ключевых вопросов:

если Интернет - это некая «педаль газа», ускорившая распространение информации так же, как 500 лет назад это сделал печатный станок, то где же находятся тормоза в киберпространстве, где каждый жаждет быть услышанным? И как пользоваться этими тормозами?

2) Необходимо разработать открытые и гибкие стратегии и инструменты в борьбе с кибертерроризмом.

Технологические и административные решения должны быть выстроены в соответствии с национальной политикой и ставить цель, с одной стороны, экономическое развитие и благосостояние на мировом рынке, а с другой - конфиденциальность, кибербезопасность и борьбу с терроризмом. Данные группы целей - это две стороны одной медали.

3) Продолжить просвещение общественности в надлежащих формах.

Общественность должна понимать позитивные и негативные аспекты, касающиеся социальных медиа. Это непростая задача, так как общественное доверие к традиционным СМИ в долгосрочной перспективе может снизиться на фоне роста интереса к альтернативным источникам информации. Одна из причин того, что люди смотрят прямые трансляции в соцсетях, - желание услышать тех, кому они доверяют.

Без сомнения, вопросы, касающиеся использования социальных медиа, являются очень сложными и требуют комплексных решений. Выработка таких решений должна происходить с участием правоохранительных органов, некоммерческих организаций (как религиозных, так и светских), политических лидеров.

Вместе с тем мы должны говорить о безопасности в соцсетях дома, в наших семьях, с нашими детьми, в соответствующих возрасту формах.

Борьба в вопросе определения границ между свободой слова и запретными зонами в социальных сетях будет продолжаться и дальше. Платформы социальных медиа продолжают поиск баланса между защитой свободы слова и борьбой с людьми, которые используют соцсети в качестве средства для продвижения терроризма. Каждый из нас должен вносить свой вклад в борьбу с киберзлом, ведь как сказал англо-ирландский деятель Эдмунд Бёрк: «Для торжества зла необходимо только одно условие - чтобы хорошие люди сидели сложа руки».

Языковой аспект в проблеме внутренней и внешнеполитической информационной безопасности

Николай Литвак, доцент кафедры философии МГИМО МИД РФ, кандидат социологических наук

В 1991 году прекратил существование СССР, а вместе с ним завершилось и глобальное противостояние двух общественных систем - капиталистической и социалистической. Принципы и цели международной деятельности современной России излагаются в концепциях внешней политики Российской Федерации, которых к настоящему моменту принято уже пять. Поначалу руководители новой России - основного преемника Советского Союза - на волне отторжения некоторых ценностей прежней, советской системы были готовы чуть ли не «броситься в объятия» Западу. В первой концепции, утвержденной Президентом в 1993 году, главной характеристикой международной ситуации назван «поворот России в сторону демократического развития», который «в корне изменил мировой расклад сил».

Было констатировано, что «прекращение политики, проходившей под знаком борьбы «двух систем»… не только отодвинуло угрозу глобальной войны… но и заложило новые предпосылки конструктивного сотрудничества стран на региональном и глобальном уровнях, в ООН и других международных организациях». Приоритетами внешнеполитической деятельности были объявлены обеспечение безопасности России; защита прав, свобод, достоинств и благополучия россиян; обеспечение благоприятных внешних условий для продвижения демократических реформ, создания эффективной рыночной экономики, развития конкурентоспособности и в том числе «развитие полнокровных отношений с США», способных, в соответствии со своим положением и весом в мировых делах, облегчить создание благопри-

ятной внешней среды для проведения внутренних экономических реформ в России.

Однако уже через несколько лет обнаружилось, что блок НАТО не то что не самораспустился, как Организация Варшавского договора, но продолжил расширяться на Восток; США сохранили свои базы и ядерное оружие в Европе, Японии и военное присутствие во многих других странах, активно участвовали в развале Югославии, применили военную силу в косовском кризисе, вышли из двустороннего с Россией Договора по ПРО, начали войну в Афганистане, Ираке и т. д. В этой связи Россия несколько раз пересматривала свое видение ситуации и цели, принимая новые концепции внешней политики. Но главное, что следует из их сравнительного анализа, заключается в постепенно выходящем на первый план внимании не только к военным, политическим и экономическим, но и к культурным, и цивилизационным вопросам.

Конечно, сегодня, как и раньше, безопасность рассматривается прежде всего с позиции возможного насилия и угрозы его применения в физическом смысле - убийств, разрушений, нанесения ущерба. Но вместе с тем различное оружие в любом случае применяют люди. И история полна примеров, когда исход сражений и войн зависел вовсе не от количества войск и их вооружения, а от боевого духа противников. Так, текущие события в арабском мире показывают, что, с одной стороны, все государства, быстро развалившиеся в результате внешних интервенций, по существу, не задействовали свой оборонительный потенциал, потому что руководство их вооруженных сил не выполнило приказы, не стало воевать, прежде всего с США. С другой же стороны, можно наблюдать, как психологическая, идеологическая и политическая обработка делает людей способными на самые ужасные вещи, преступления, в том числе массовые военные, которые казались давно уже ставшими частью исторического прошлого.

В целом уже прошло несколько десятилетий, как основные сражения переместились в информационную сферу - психологическую, культурную, цивилизационную. Основных причин этого две. Первая - объективные основания конфронтации в международных отношениях, и в нынешних условиях, к сожалению, неустранимые. Вторая - это паритет в ОМУ.

Что касается первой причины, то, несмотря на постоянно подтверждаемое желание России конструктивно сотрудничать со всеми иностранными партнерами, главным содержанием международных отношений является глобальная и тотальная конкуренция, что постепенно и все более четко стало определяться в концепциях внешней политики РФ. Уже в Концепции 2000 года отмечалось, что «в международной сфере зарождаются новые вызовы и угрозы национальным интересам России. Усиливается тенденция к созданию однополярной структуры мира при экономическом и силовом доминировании США». Фактически же с распадом СССР ситуация в мире во многом вернулась к своему состоянию примерно вековой давности. Конечно, есть значительные отличия. Пала колониальная система, появились десятки новых государств, сменились доминирующие центры силы. Вместе с тем по-прежнему главным содержанием международных отношений является вовсе не сотрудничество, и по-прежнему в этой всеобщей конкуренции определяющим является военно-промышленный потенциал, используемый государствами для достижения желаемых экономических и политических результатов, когда мирные средства неэффективны или более сильное государство не хочет ждать, пока они сработают.

Теперь о второй причине и ее следствиях. Конечно, информационный компонент всегда был одним из компонентов «обычных» войн. Но оказалось, что в современных условиях - паритета в ОМУ - он становится главным. Ведь последствия информационного воздействия, информационных войн, информационного оружия не так очевидны, как последствия бомбардировок и тем более публичное отрезание голов. Но главное, противник не всегда в состоянии даже понять, что происходит, какое оружие и с каким эффектом против него применяется. Поскольку мировая конкуренция - настоящая, то при невозможности безнаказанно бомбить неизбежно используются средства конкуренции в информационном пространстве, затрагивающие ценности, культуру, язык.

Уже в упоминавшейся Концепции 2000 года был отмечен рост риска зависимости экономической системы и информационного пространства России от воздействия извне. Кроме того, среди задач были названы «содействие позитивному восприятию

Российской Федерации в мире, популяризации русского языка и культуры народов России в иностранных государствах», «обеспечение информационной безопасности как аспекта укрепления стратегической стабильности». В Концепции 2008 года было заявлено, что «в международной обстановке, наряду с позитивной тенденцией - укреплением позиций Российской Федерации на международной арене, проявились и негативные тенденции... Стираются различия между внутренними и внешними средствами обеспечения национальных интересов и безопасности». В этом же контексте впервые в концепции появляется и занимает значительное место материал о цивилизационных аспектах международных отношений.

Отмечено, что «глобальная конкуренция впервые в новейшей истории приобретает цивилизационное измерение, что предполагает конкуренцию между различными ценностными ориентирами и моделями развития в рамках универсальных принципов демократии и рыночной экономики», а также, что «стратегия односторонних действий дестабилизирует международную обстановку… ведет к росту напряженности в межцивилизационных отношениях; натиску глобализации подвергается культурная самобытность подавляющего большинства стран и народов».

В Концепции внешней политики РФ 2013 года тезис о цивилизационном измерении глобальной конкуренции дополнен тезисом о том, что «неотъемлемой составляющей современной международной политики становится «мягкая сила» - комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии.

Вместе с тем усиление глобальной конкуренции и накопление кризисного потенциала ведут к рискам подчас деструктивного и противоправного использования «мягкой силы». В отношении стран послабее США первые, предложившие и освоившие этот инструментарий, уже перешли к следующему этапу - использованию «умной силы» и трансформационной дипломатии. В отношении же стран, которые по разным причинам нельзя, во всяком случае пока, бомбить или легко «трансформировать», используются мощные информационные средства.

И эта проблема политической независимости как независимости культурной и, конечно, языковой касается всех стран. Поскольку Россия - европейская страна, приведем в этой связи пример Европы, и в частности Франции, где проблема американского культурного влияния обсуждается не только общественностью, но и в научных и политических кругах. Сегодня там постепенно формируется понимание, как Франция и остальной мир в самых разных областях, в том числе в культуре и образовании, проигрывают борьбу Соединенным Штатам, одним из самых острых последствий которой является «утечка умов» за океан. Разделяет это видение и большинство франкофонских стран. Бывший Президент Сенегала и генеральный секретарь международной организации «Франкофония» Абду Диуф в одной из своих широко обсуждавшихся во Франции работ подчеркивал, что «опасно отрицать конкуренцию ценностей и идей, являющихся культурными факторами среди поводов к развязыванию конфликтов в нашу эпоху». Ситуация такова, что либо победит «культурный дарвинизм», либо будет осуществлен политический проект «культурной безопасности», «культурного плюрализма», требующий сознательных совместных усилий. И в этом проекте ключевое место занимает языковой аспект.

Универсальность объективных законов и взаимозависимость современного мира обуславливает необходимость наблюдения за языковой ситуацией и у нас. Уже некоторые наши депутаты обратили внимание на то, что преподаванию иностранного языка в наших школах отводится, как минимум, столько же времени, сколько русскому. Но из школьных программ и министерских планов можно узнать более точные данные.

Сегодня в обычной московской школе у старшеклассников естественно-научного, технологического, социально-гуманитарного и социально-экономического профилей в неделю один урок русского языка, три - литературы и три - английского языка. В других профильных классах - целых два урока русского в неделю и те же три английского. В школе же с углубленным изучением английского языка в расписании на текущий 2016-2017 учебный год значится в первом классе по четыре урока письма и чтения (будущие русский язык и литература) и два - английского языка в неделю; во

втором классе - пять уроков русского языка, четыре - чтения и три - английского языка (пятидневная учебная неделя). В шестом классе (в шестидневную учебную неделю) шесть уроков русского языка, два - литературы, три - английского языка и три - французского языка; в девятом классе - три урока русского языка, два - литературы, пять - английского языка и два - французского языка; в одиннадцатом классе - два урока русского языка, два - литературы, четыре - английского языка и два - французского языка. С 1 сентября 2015 года во всех российских школах введено обязательное изучение *второго* иностранного языка. Притом что большинство школ, кроме столицы и, возможно, некоторых крупных городов, не готовы к этому. Прежде всего нет необходимого количества учителей.

А с 2020 года запланировано введение третьего *обязательного* ЕГЭ - по *иностранному* языку. Можно предположить, что в будущем без его отличного знания просто не будут принимать в отечественные вузы. При этом совсем недавно вице-премьер правительства РФ О.Ю.Голодец и новый министр образования и науки О.Ю.Васильева выразили противоположные точки зрения на преподавание русского языка в отечественных вузах. Голодец считает, что тем, кто не выучил русский язык в школе, нечего делать в вузах и надо проверить «как у нас оказываются в вузах дети, не владеющие русским языком». Васильева же отстаивала необходимость изучения русского и в высшей школе ввиду его недостаточного уровня у выпускников современных средних школ. А руководитель Федерального агентства по делам национальностей Игорь Баринов заявил, что сегодня существует «огромная угроза - снижение уровня владения русским языком, особенно это актуально для национальных республик, для малых населенных пунктов, для сел, это актуально для коренных малочисленных народов, для детей мигрантов». Как же в такой ситуации оказывать влияние на другие народы?

В такой ситуации *обязательное* изучение нескольких иностранных языков - это как раз и есть *идеологическая* установка, описывающая действительность ложным образом. В условиях, когда наш среднестатистический школьник плохо осваивает программу по традиционным предметам (математике, русскому языку), преподающимся уже не одно столетие, ключевым

становится не выяснение причин этого и внимание к качеству образования, а дальнейшие реформы с необъясняемыми четко целями. Отечественный студент, уже и сегодня плохо говорящий и пишущий по-русски по сравнению со своими предшественниками, на что жалуются абсолютно все, разве улучшит эти свои навыки, изучая еще и два иностранных языка? Но предположим, что выпускники вузов и тем более обычных школ, каких у нас абсолютное большинство, выучили какой-то из двух иностранных языков до уровня сдачи ЕГЭ и потратили немало сил на изучение второго. А что они дальше будут делать? С кем общаться на этих языках и по какому поводу? Да, сегодня люди путешествуют гораздо больше, чем прежде. Но языковой барьер преодолевается созданием соответствующих туристической и бизнес-инфраструктур, работники которых и учат специально иностранные языки, и их используют. Потому что большинство путешественников - туристы.

Так, значима ли цель для национальной системы образования, ориентированной на десятилетнее преподавание двух иностранных языков, попросить без акцента на курорте чашку кофе? Государству, обществу вовсе не все равно, где будет работать выпускник. Но если выпускник этот англоязычный, то он может быть отобран для работы в США или на США, в американскую компанию или филиал. И ключевое слово здесь *отобран*, то есть именно меньшинство, но лучших выпускников и будут работать на чужие компании и государства.

Есть и еще два важных аспекта, связанных с этой проблемой. Во-первых, подготовка англоязычных специалистов, впоследствии *не*отобранных, очевидно, не облегчает, а затрудняет их дальнейшую работу на родине. Каждому, наверное, уже приходилось сталкиваться с теми, кто получил образование на иностранном языке и при разговоре по-русски периодически затрудняется подбирать необходимые слова. Но усилия-то уже потрачены. И эта проблема касается не только России, но также и многих государств Европы. Ну а современный российский школьник, с первого класса начиная изучение иностранных языков, в первую очередь английского, получает установку на то, что это едва ли не единственное средство к успеху в его взрослой жизни - в виде работы за рубежом или на зарубежную компанию.

Для сравнения - не в общеобразовательных, а в элитных частных школах, например, Великобритании, где иностранные языки тоже изучают, в старших классах обязательными предметами остаются только *родной* английский язык, математика и блок естественных наук. Более 90% выпускников таких школ продолжают обучение в Великобритании - в подавляющем большинстве в университетах Оксфорда, Кембриджа, Лондонской школе экономики и других подобных вузах. Во все эти школы, кстати, надо сдавать вступительные экзамены, а треть преподавателей в них - выпускники все тех же Оксфорда, Кембриджа и других ведущих университетов.

Второй аспект касается общего психологического развития школьников и формирования их систем ценностей. Современная психология приводит данные о менее качественном интеллектуальном и психическом развитии детей при многоязычии (все-таки лучше иметь один основной, родной язык, а остальные изучать как иностранные и, конечно, по желанию). Кроме того, каждый язык имеет и собственные формы мышления (развитость грамматики, словарного запаса и т. д.). Наконец, при изучении в наших школах иностранных языков речь ведь не идет о переводе русской истории на французский или английский. Французский и английский изучаются на примерах французской или английской истории, литературы, которые обязательно содержат и национальные ценности.

Таким образом, можно сделать следующие выводы.

1. Ни одна сильная страна мира, тем более лидеры Запада, никогда не желали и в условиях жестокой капиталистической конкуренции и не могут желать появления новых конкурентов, в том числе «свободной и сильной России», как многие из них часто повторяют. Стоит помнить, что все прежние войны, особенно самые масштабные и ужасные, были войнами между европейскими странами. Новизна же ситуации заключается в достигнутых и освоенных к настоящему времени результатах научно-технического прогресса. С одной стороны, были произведены и поддерживаются в боевом состоянии средства полного взаимного уничтожения конкурирующих сторон, а с другой - были созданы возможности формирования и использования *культурного* доминирования и, как следствие, управления другими государствами, народами.

Все это можно обобщить в понятии «*информационная война*». Она не так видна, поскольку видимых разрушений нет, но зато эффективна, поскольку победителю достаются все ресурсы. Пока еще в программных внешнеполитических документах всех стран основное место уделено военно-политическим и экономическим факторам. Между тем уже в случае с СССР ни одна бомба или ракета не упала на его территорию, не ступил на нее и ни один вражеский солдат. Но страны не стало, и это потому, что поражение Советского Союза в холодной войне состоялось не в военной и даже не в экономической, но в политической и культурной сферах. И информационное оружие, если так дело будет продолжаться, имеет все шансы стать еще одним видом ОМУ, что косвенно уже признается, хотя пока в основном в связи с возможностями физического подключения или ущерба через компьютерные сети. Но уже есть и антироссийские резолюции в связи с деятельностью наших теле- и радиокомпаний.

2. Необходимо учитывать, что внешняя политика и внешняя безопасность строятся на основе внутренних ресурсов и внутренней безопасности. Пока российская школа реформируется по худшему американскому образцу, а высшее образование - по «болонской системе», которую отвергли ведущие западные вузы. При этом лидер западного мира - США постоянно *импортирует* кадры. А ведь там все школьники учатся на английском, что, оказывается, само по себе еще не делает образование лучшим.

В то же время все страны, которые развивают дву- и многоязычие в школе, либо ориентируются на *экспорт* своей рабочей силы, на экспортное будущее своих детей, либо находятся в плену *мультикультурной идеологии*. Ведь обязательное изучение нескольких языков коренным образом отличается от свободного выбора изучать тот или иной иностранный язык или не изучать никакого. При этом факты показывают, что как в настоящее время у США, так и ранее у Великобритании, Франции или России результаты и отдача от языковой политики были и есть только тогда, когда *иностранцев* обучают, соответственно, английскому, французскому или русскому языку.

В СССР иностранный язык изучался массово только как язык наиболее вероятного противника - до Великой Отечественной

войны немецкий, затем в основном английский. При этом был налажен сбор по всему миру научно-технической и гуманитарной информации, ее перевод, реферирование и издание. И кроме специалистов-международников, только те, кто шли в науку, по-настоящему могли нуждаться в языке для самостоятельного чтения узкоспециальных статей и книг, которые не было смысла переводить. Сегодня же у нас огромные ресурсы затрачиваются и еще большие планируется затратить на всеобщее изучение иностранных языков. Но при этом четко не сформулировано видение текущей и будущей *отдачи* от вложения таких ресурсов.

Нарративы информационной безопасности в дискурсе достижений «Industry 4.0»

Анатолий Смирнов, президент АНО «Национальный институт исследований глобальной безопасности», доктор исторических наук

Канадский социолог Герберт Маршалл Маклюэн говорил, что смена исторических эпох определяется сменой коммуникационных технологий. Третья мировая война будет партизанской информационной войной без разделения между военным и гражданским участием.

Уважаемые коллеги! Мое выступление будет своего рода продолжением презентации на «круглом столе» «Международной жизни» в ходе конференции в Гармише 27 апреля 2016 года.

Начало XXI века способно запечатлеться в скрижалях человечества как один из самых драматичных для глобальной безопасности. Планета вошла в зону ломки миропорядка и Вестфальской системы в целом. Приведу лишь некоторые угрозы:

- адаптивная смена режимов и «цветные революции»;
- терроризм и рецессия;
- рецидивы холодной войны и санкций;

- всплеск локальных и региональных конфликтов;
- пандемии, голод, «цунами» миграции;
- техногенные, природогенные и социогенные катастрофы.

В иерархии угроз резко возрос инфогенный нарратив. Это нашло отражение в целом ряде документов на международном (ООН, ОБСЕ, СНГ, ШОС и др.) и национальном уровнях.

Действительно, весь мир охвачен беспрецедентной технологической революцией, новейший этап которой «Industry 4.0» - это конвергенция технологий, которые размывают границы между физической, цифровой и биологической сферами. Современная концепция конвергенции ИКТ, когнитивных, нано- и биотехнологий, а также «Интернета вещей» и «индустриального Интернета» была разработана в ФРГ в 2011 году. Массовое внедрение киберфизических систем в производство (взаимодействие минуя людей - M2M), обслуживание человеческих потребностей, включая быт, труд и досуг, влекут изменения практически всех страт цивилизации - технологического уклада, политических систем, рынка труда, жизненной среды, человеческой идентичности и т. д.

Уже более полувека драйвером ее феномена являются информационно-коммуникационные технологии. Из технической сферы они трансформировались в один из ключевых факторов геополитической конкуренции, ибо наряду с несомненным позитивом породили и инфогенные угрозы для всех страт цивилизации.

Наиболее емко сложившаяся ситуация оценена в Стратегии национальной безопасности России (2015 г.): «Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать ИКТ для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории».

В Доктрине информационной безопасности России (2016 г.) вышеуказанный посыл был конкретизирован: «Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоор-

динированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации». Об этом очень убедительно уже высказались коллеги.

Кроме того, данная проблема нашла отражение в Стратегии научно-технологического развития России (2016 г.). В документе подчеркнуто, что в ближайшие 10-15 лет приоритетами научно-технологического развития следует считать направления инновационного развития внутреннего рынка продуктов и услуг, устойчивого положения России на внешнем рынке, которые обеспечат «противодействие техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства».

Основатель и президент ВЭФ в Давосе К.Шваб в своей книге «Industry 4.0» предупреждает о ее сильном воздействии на национальную и международную безопасность, ибо история войн - это история технологических прорывов. Конфликты между странами носят все более гибридный характер. Границы между войной и миром, воюющей и невоюющей сторонами, даже между насилием и его отсутствием (вспомним кибервойну) становятся все менее четкими и создают принципиально новые вызовы.

В данном контексте Р.Шиллер, лауреат Нобелевской премии по экономике за 2013 год, профессор экономики Йельского университета, изрек на форуме в Давосе в 2016 году: «Вы не будете ждать пожара, чтобы застраховать дом. Мы не можем ждать сдвигов в обществе, чтобы начать готовиться к четвертой промышленной революции». А вице-канцлер, министр экономики ФРГ З.Габриэль высказал опасение, что большие данные (big data) «Industry 4.0» собираются не в ФРГ, а четырьмя фирмами из Кремниевой долины.

Сенсационное исследование опубликовал 3 декабря 2016 года швейцарский журнал «Das Magazin» - Трамп победил благодаря big data и технологии микротаргетинга. Микротаргетирование - меха-

низм точной настройки социальных медиа для работы с целевой аудиторией - предполагает «интимное знание» любого пользователя социальной сети. Задача, которая ставится перед микротаргетированием в выборной кампании, - побудить избирателя к голосованию за того или иного кандидата.

«Лайк» в соцсети или запрос в «Google» оставляет след. Их совокупность образует big data. По 68 «лайкам» можно определить цвет кожи и ориентацию, пристрастие к политическим партиям, по 150 «лайкам» - узнать человека лучше, чем родители, по 300 - лучше, чем партнер. В дни дебатов в соцсети отправили 175 тыс. вариантов постов в ключевые штаты по 32 психотипам людей с позитивными качествами Трампа и негативными - Клинтон. Услуги компании «Cambridge Analytica» (она оказывала поддержку и в ходе референдума в Великобритании сторонникам выхода из ЕС) обошлись Трампу в 15 млн. долларов.

Возможности технологии микротаргетинга по манипулированию общественным сознанием из-за рубежа высоки и в России, где, по некоторым оценкам, около половины пользователей Интернета имеют аккаунты в «Facebook» и используют поисковик «Google».

Следует подчеркнуть, что НАТО для обозначения якобы негативной роли России в кризисных точках уже активно продвигает интернет-мем «гибридные войны». Весьма характерен в данном контексте тезис из п. 5 Заявления НАТО по итогам встречи на высшем уровне в Варшаве (8-9 июля 2016 г.): «Североатлантический союз сталкивается с рядом вызовов и угроз безопасности, исходящих с Востока и Юга, от государственных и негосударственных субъектов, от вооруженных сил и террористических, кибернетических или гибридных нападений. Агрессивные действия России, в частности провокационная военная деятельность на периферии территории НАТО, и проявленная Россией готовность добиваться политических целей с помощью угрозы силой и применения силы являются одним из источников региональной нестабильности». В силу этого становится понятным создание НАТО у границ России 20 центров передового опыта, в том числе Центра по стратегическим коммуникациям в Риге. Его главная задача - это информационное противоборство в Россией.

О профиле центра убедительно говорят названия лишь некоторых трудов и тем конференций 2016 года:

Социальные медиа как инструмент гибридной войны («Social Media as a Tool of Hybrid Warfare») (07.07.2016);

Кейр Джайлс. Следующая фаза российской информационной войны («The Next Phase of Russian Information Warfare») (20.05.2016);

Обрамление конфликта Украины и России в онлайн и социальных медиа («Framing of the Ukraine-Russia conflict in online and social media») (18.05.2016);

Интернет-троллинг как инструмент гибридной войны: случай Латвии («Internet Trolling as a hybrid warfare tool: the case of Latvia») (25.01.2016).

Тематика проводимых конференций и семинаров:

Конфликт и информационная среда: будущие стратегические коммуникации (22.09.2016);

Презентация предварительных результатов исследования интернет-троллинга (16.07.2015).

Картина становится совсем полной, если учесть, что 6 декабря 2016 года НАТО и ЕС приняли решение о создании в Хельсинки в 2017 году Европейского центра противодействия гибридным угрозам.

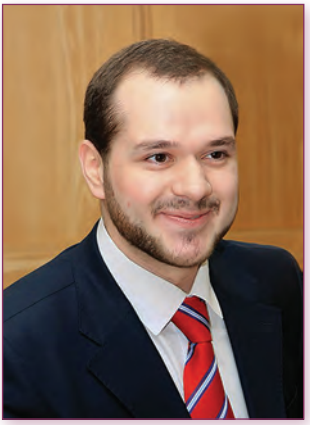
Вышеизложенное в целом убедительно показывает, что та страна, которая овладеет всем потенциалом «Industry 4.0», в том числе в военно-политической сфере, способна получить критически важные преимущества в геополитической конкуренции.

В соответствии с концепциями внешней политики (2013 и 2016 гг.) Россия принимает необходимые меры для обеспечения национальной и международной информационной безопасности. Совместно с партнерами по ОДКБ, СНГ, ШОС, БРИКС подготовлен проект резолюции Генассамблеи ООН «Правила ответственного поведения государств в информационном пространстве в контексте международной безопасности», который активно продвигается в том числе в формате Группы правительственных экспертов ООН.

Резюмируя, воспользуемся метафорой: миру нужен «цифровой Вестфаль», ибо альтернатива иррациональна - «киберАрмагеддон!»

Пятый театр военных действий и военно-сетевой комплекс США: уроки для России

Вахтанг Сургуладзе, ведущий методолог компании «Р.О.С.Т.У.» по стратегическому планированию, кандидат философских наук



Кибервойны стали пятым театром военных действий, являющимся полем противоборства современных развитых государств наряду с воздушным, сухопутным, водным и космическим пространствами.

В силу разоблачений «WikiLeaks» и Эдварда Сноудена и благодаря бурному интересу общественности и научного сообщества к проблемам кибербезопасности, в настоящее время в общих чертах понятны угрозы, с которыми сталкивается Россия на указанном направлении, ясен «портрет» потенциального врага в сфере информационного противоборства. В частности, специалисты понимают механику взаимоотношений между специальными и силовыми ведомствами США и их подрядчиками - «Lockheed Martin», «Raytheon», «General Dynamics», «Boeing», «Northrop Grumman», «Harris Corporation», «Booz Allen Hamilton» и т. д. В частности, известны компании, которые разрабатывают программное обеспечение американских спецслужб - «Computer Associates», «Net Witness» и т. д. Понятна деятельность частных компаний, занимающихся как обеспечением кибербезопасности, так и ведением кибервойн. Многие из этих компаний являются активными игроками черного рынка уязвимостей программного обеспечения и могут оказывать помощь: как сохранять и защищать данные, так и взламывать базы данных и запускать в них сетевых червей.

Одним из ключевых, пользующихся спросом со стороны государственных спецслужб и профильных подразделений крупных корпораций, продуктов этого рынка являются уязвимости нулевого дня - слабые места системы, неизвестные разработчикам

программного обеспечения, при обнаружении которых в случае атаки у разработчика не останется времени для их устранения.

Агентство национальной безопасности (АНБ) США скупает сведения об этих уязвимостях у обнаруживших их хакеров, а также сотрудничает с компаниями - разработчиками программного обеспечения с той целью, чтобы они не раскрывали информацию о наличии таких уязвимых мест при их обнаружении, а также не сообщали пользователям о наличии в их программном обеспечении бэкдоров - специально созданных в программном продукте точек доступа для американских спецслужб.

Всплеск глобальной активности в киберпространстве привел к тому, что в настоящее время существует обширный рынок по продаже результатов трудов хакеров, работающих в нише выявления подобных угроз. При этом на теневом рынке уязвимостей нулевого дня никто не дает гарантий эксклюзивности получаемой информации, в связи с чем можно говорить о значительном потенциале для злоупотреблений со стороны спецслужб, которые тратят миллиарды долларов на приобретение таких данных и способствуют возникновению мыльного пузыря на рынке кибербезопасности.

АНБ скупает уязвимости, чтобы воспользоваться ими в случае войны, когда потребуется дестабилизировать общество, материально-технические средства и инфраструктуру потенциального противника. Частные корпорации приобретают эти же уязвимости для того, чтобы ликвидировать их и улучшить свой продукт. В результате рынок программного обеспечения оказывается вовлечен в невидимое посторонним перманентное соперничество между государством и корпорациями за человеческие ресурсы и информацию. Более того, не имея возможности отвечать на кибератаки конкурентов в легальном правовом русле, корпорации вынуждены принимать собственные меры и вести свою кибервойну, используя в ней все методы, которыми пользуются в данной сфере государственные спецслужбы, а временами предпринимать совместные с государственными органами усилия в данной сфере.

Киберсреда - серая зона, в которой сталкиваются интересы не только соперничающих государств и конкурирующих корпораций, но и государственных органов, которые, казалось бы, должны добиваться одинаковых целей. Так, вызывает интерес ставшее известным общественности столкновение подходов к обеспечению аноним-

ности информационной киберсреды между Государственным департаментом США и АНБ. Внешнеполитическое ведомство Соединенных Штатов вкладывает значительные средства для обеспечения программными продуктами шифрования групп повстанцев в разных дестабилизируемых США государствах, в то время как АНБ тратит ресурсы на то, чтобы ослабить эффективность этого программного обеспечения и иметь доступ к любым шифруемым данным.

Специалисты, анализируя подходы к кибербезопасности, характерные для бизнеса и государственных структур, сопоставляют кибернавыки АНБ с разработками крупных корпораций и приходят к заключению, что достаточно часто большая часть информации АНБ устаревала к тому моменту, когда она поступала получателям. В частности, отставание АНБ выявилось при сопоставлении с системами кибербезопасности, разрабатываемыми финансовыми структурами и крупнейшими банками. Только тесное сотрудничество с бизнесом позволяет эффективно обновлять арсенал киберсредств нападения и защиты. В отсутствие такого сотрудничества работа государственных спецслужб становится менее эффективной, а зачастую выливается в прямое введение в заблуждение лиц, принимающих политические решения.

Заслуженный интерес специалистов вызывают увенчавшиеся успехом методы информационной борьбы американцев на поле контрпропаганды и подрывной деятельности на форумах членов «Аль-Каиды». Тщательно изучается операция кибервойск США против Ирана - разрушение тысячи иранских центрифуг, которое принято связывать с результатом действия вируса Stuxnet.

Для понимания стоящих перед современными обществами проблем обеспечения безопасности или защиты гражданских прав несомненный интерес представляет анализ деятельности ключевых фигур кибернетических спецслужб США и истории их становления в целом. В качестве примера можно привести усилия Джона Майкла Мак-Коннела по созданию киберармии АНБ. Именно Мак-Коннел объяснял американским законодателям, что «большая часть мирового телекоммуникационного трафика проходит через кабели, маршрутизаторы и коммуникаторы, расположенные на территории страны», убеждая их в том, что АНБ не должно получать разрешение на использование этого оборудования в целях шпионажа за гражданами других государств.

С точки зрения защиты национальных интересов России особое внимание вызывает взаимодействие государственных структур США с частными корпорациями. Прежде всего здесь важно отметить систему сбора данных PRISM, благодаря которой АНБ получала от американских компаний массив электронных писем и другой информации о пользователях сети Интернет. Первой компанией, вошедшей в программу PRISM, стала «Microsoft», затем к ней присоединились «Yahoo», «Google», «Facebook», «YouTube» и «Apple». Сегодня эти компании отвечают за огромную часть трафика Интернета в Соединенных Штатах. Одна только «Google» генерирует четверть всего трафика, проходящего через оборудование провайдеров в Северной Америке. Через три года, после того как «Google» вошла в программу PRISM, ее продуктом «Gmail» пользовались 425 млн. человек. В декабре 2012 года почтовый сервис «Yahoo» насчитывал 281 млн. пользователей. А в феврале 2013 года «Microsoft» отчитался о 420 млн. пользователей ее почтовой системы «Outlook».

Военно-сетевой комплекс - гибридный инструмент, результат срастания государственных структур США и частного бизнеса, приведший к тому, что рыночная стоимость ведущих оборонных предприятий превышает ВВП многих стран мира, а создание оружия, транспортировка солдат и даже их питание в зоне боевых действий доверено частным подрядчикам.

Тесная спайка государственных структур и бизнеса - характерная особенность военно-сетевого комплекса США, которую важно учитывать, прорабатывая возможные контрмеры, направленные на предотвращение доминирования Соединенных Штатов в информационном и киберпространстве.

Анализ функционирования военно-сетевого комплекса США заставляет задуматься о том, насколько гибко и дисперсно действуют американские власти, отстаивая собственные национальные интересы, опираясь не только на государственный аппарат, но и мощные транснациональные корпорации, находящиеся на переднем крае научно-технического прогресса.

Армен Оганесян: *Я благодарю всех участников конференции за интересные доклады, выразившие различные точки зрения.*

ПРОГРЭС

Основано в 2009 году

Основной целью компании является обеспечение энергетического комплекса РФ качественными услугами в области ремонта, реконструкции и строительства энергетических объектов любой сложности. Компания сконцентрировала и объединила вокруг себя настоящих профессионалов из сферы энергетики, единомышленников, имеющих многолетний бесценный опыт работы в крупнейших электрогенерирующих компаниях РФ.

Основными заказчиками ООО «ПРО ГРЭС» являются такие крупные компании, как ПАО «Мосэнерго», ПАО «ОГК-2», ОАО «ТГК-1», ПАО «Интер РАО ЕЭС».

Компания предлагает услуги EPC-контрактора (генерального подрядчика), начиная от работ по проектированию, поставке нестандартного оборудования, выполнению строительно-монтажных и пусконаладочных работ, заканчивая вводом объекта в эксплуатацию.

К особо значимым проектам для компании, реализованным собственными силами, можно отнести такие объекты, как Реконструкция энергоблока №2 (330 МВт) на Рязанской ГРЭС – филиале ПАО «ОГК-2» с заменой основного оборудования, а также строительство ХВО на ТЭЦ-12 и ТЭЦ-22 – филиалах ПАО «Мосэнерго», ОРУ и нового КРУЭ на ТЭЦ-20, мазутного хозяйства для энергоблока №10 Троицкой ГРЭС (ПСУ-660 МВт), реконструкцию ОРУ, очистных сооружений и БНС-4 для Троицкой ГРЭС.

Постоянно развиваясь и осваивая новые направления, с 2015 года компания реализует проект по реконструкции энергоблока с турбиной типа Т-250/300-240 ст. №9 на ТЭЦ-22 - филиале ПАО «Мосэнерго», а также осваивает для себя новое направление деятельности по реконструкции гидроэнергетических объектов.

Сегодня компания выполняет весь спектр ремонтных работ на Троицкой ГРЭС, обеспечивая на протяжении многих лет надежность и безаварийную эксплуатацию одной из самых крупных и стратегически важной теплоэлектростанции в регионе. Созданное обособленное подразделение в городе Троицке насчитывает более 800 человек.

На сегодняшний момент в штате ООО «ПРО ГРЭС» трудятся более 2500 человек – профессионалов своего дела с большим опытом работы в энергетике. В числе постоянных поставщиков и партнеров крупнейшие мировые и отечественные изготовители электротехнического, котельного и турбинного оборудования на территории РФ.

За время своего существования ООО «ПРО ГРЭС» реализовало более 100 проектов, направленных на повышение надежности и эффективности энергогенерирующих и промышленных предприятий. В планах компании – расширить круг своих заказчиков по всей территории Российской Федерации, а также освоить серьезнейшую отрасль энергетики – атомную.

WWW.INTERAFFAIRS.RU