



СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
ТРИНАДЦАТОГО МЕЖДУНАРОДНОГО ФОРУМА
**«ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА
И ГРАЖДАНСКОГО ОБЩЕСТВА
ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

22–25 АПРЕЛЯ 2019 г.,
ГАРМИШ-ПАРТЕНКИРХЕН, ГЕРМАНИЯ

АННОТАЦИЯ

В настоящем сборнике представлены тексты выступлений участников Тринадцатого международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» в г. Гармиш-Партенкирхен (ФРГ) (22–25 апреля 2019 г.).

Форум, организованный Национальной Ассоциацией международной информационной безопасности (Россия), был посвящен обсуждению различных аспектов налаживания сотрудничества в области противодействия угрозам безопасности использования информационных и коммуникационных технологий человеком, коммерческими и некоммерческими организациями, государственными органами.

Форум проходил в условиях активизации попыток использования новейших информационно-коммуникационных технологий (ИКТ) в противоборстве в глобальном информационном пространстве, обусловленном стремлением некоторых стран использовать ИКТ для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.

Наиболее убедительна острота проблемы использования ИКТ в контексте международной безопасности проявилась в принятии Генассамблеей ООН в декабре 2018 г. двух резолюций: A/RES/73/27 – инициирована Россией и её партнерами, а также A/RES/73/266 – продвинута США и их сателлитами.

Несмотря на вышеуказанные проблемы, в этих условиях в работе Форума приняли участие свыше 100 экспертов из 17 государств. В центре внимания пленарного заседания Форума и «круглых столов» находились наиболее актуальные проблемы: развития мер укрепления доверия между государствами в ИКТ-среде; противодействия угрозам использования информационно-коммуникационных технологий в военно-политических целях и вмешательства во внутренние дела государств; налаживания государственно-частного партнерства при обеспечении безопасности объектов критической инфраструктуры, включая объекты кредитно-финансовой сферы, безопасности использования ИКТ-среды коммерческими компаниями.

Тексты выступлений, представленных в сборнике на основе расшифровки аудиозаписи, при всем своём разнообразии, отражают единство мнений участников о необходимости формирования системы международной информационной безопасности на основе суверенитета государств, более активного изучения правовых и технических аспектов делимитации и демаркации зон ответственности государств в ИКТ-среде, создания системы получения объективной информации об опасных инцидентах в ИКТ-среде и системы атрибуции государств, вовлеченных в эти инциденты.

Продвижение в решении этих вопросов позволит создать условия для применения норм и принципов международного права, включая положения Устава ООН, для предотвращения международных споров, связанных с инцидентами в ИКТ-среде, для мирного разрешения таких международных споров.

Участникам Форума удалось выявить основные проблемы, препятствующие применению международного права к ИКТ-среде, и предложить направления совершенствования системы международных норм для решения данных проблем.

Как отметил Президент Национальной Ассоциации международной информационной безопасности Владислав Шерстюк, Форум оказал значительное позитивное влияние на расширение сотрудничества экспертного сообщества в области формирования системы международной информационной безопасности.

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



Стремительно нарастающие вызовы и угрозы в информационной сфере требуют консолидированных усилий мирового сообщества по созданию мирной и безопасной ИКТ-среды.

Противостоять этим вызовам и угрозам можно только объединив усилия государств, деловых кругов, научного и экспертного сообщества, гражданских институтов.

Форум в Гармиш-Партенкирхене, впервые состоявшийся в 2007 году и ставший за эти годы авторитетной международной дискуссионной площадкой, предоставляет его участникам из многих стран мира уникальную возможность для предметного профессионального анализа существующих проблем в области международной информационной безопасности, поиска взаимоприемлемых путей их преодоления.

Комплексный подход, основанный на рассмотрении ключевых вопросов формирования системы международной информационной безопасности как с общеполитических, так и с научно-практических позиций, является «визитной карточкой» Форума.

Традиционно повестка дня конференции, тематика его пленарных заседаний и круглых столов ориентированы на обсуждение актуальных задач обеспечения безопасности в информационной сфере. На этой площадке ученые и эксперты имеют прекрасную возможность делиться своими взглядами на проблемы в рассматриваемой области, вести доверительный диалог, сближать позиции в поиске эффективных механизмов противодействия угрозам противоправного использования информационно-коммуникационных технологий.

Из дискуссий в Гармиш-Партенкирхене родились многочисленные идеи и решения, способствующие сохранению стратегической стабильности в глобальном информационном пространстве.

Представленные в сборнике материалы состоявшегося в апреле 2019 г. Тринадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» наглядно демонстрируют стремление его участников сделать наш мир более безопасным.

Сопредседатель Оргкомитета,
заместитель Секретаря Совета Безопасности
Российской Федерации

О. ХРАМОВ

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Шерстюк В.П.,

Сопредседатель оргкомитета Форума, советник Секретаря Совета Безопасности Российской Федерации, Президент Национальной Ассоциации международной информационной безопасности 10

Крутских А.В.,

Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Чрезвычайный и Полномочный Посол Российской Федерации 15

Плохой О.А.,

Первый заместитель Министра юстиции Российской Федерации 22

Ганс-Вильгельм Дюнн (Hans-Wilhelm Dünne),

Президент Совета по Кибербезопасности Германии 24

Бойко С.М.,

Начальник департамента аппарата Совета Безопасности Российской Федерации 27

Гасумянов В.И.,

член Президиума Национальной Ассоциации международной информационной безопасности, Старший вице-президент ГМК «Норильский никель», Россия
СТРАТЕГИЧЕСКИЕ НАПРАВЛЕНИЯ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА ПРИ
ФОРМИРОВАНИИ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:
ПОДХОДЫ КОМПАНИИ «НОРНИКЕЛЬ» 31

Мирошников Б.Н.,

член Президиума Национальной Ассоциации международной информационной безопасности, вице-президент ГК «Цитадель», Россия 36

Дэвид Конрад (David Conrad),

Старший вице-президент, главный технический директор ICANN,
Вени Марковски (Veni Markovski),
вице-президент ICANN по взаимодействию с ООН 38

Лебедь С.В.,

Руководитель службы информационной безопасности Сбербанка России
ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ ГЛОБАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 42

Чарльз Барри (Charles Barry),

Независимый эксперт, США 45

СЕМИНАР–КРУГЛЫЙ СТОЛ № 1

О ДЕЯТЕЛЬНОСТИ МЕЖДУНАРОДНОГО ИССЛЕДОВАТЕЛЬСКОГО КОНСОРЦИУМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (МИКИБ)

Стрельцов А.А.,

член Президиума Национальной Ассоциации международной информационной безопасности, Институт проблем информационной безопасности МГУ имени М.В. Ломоносова
ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ 48

Энекен Тикк (Eneken Tikk),

независимый эксперт, Эстония
О МЕХАНИЗМАХ УРЕГУЛИРОВАНИЯ СПОРОВ И РАЗВИТИЯ МЕЖДУНАРОДНОГО
СОТРУДНИЧЕСТВА В ИКТ-СРЕДЕ 52

Ноюн Пак (Nohyoung Park),

Центр киберправа Университета Корё, Мён Хюн Чун (Myunghyun Chung),
Юридический факультет Университета Корё, Республика Корея
К ВОПРОСУ О ПРОГРЕССИВНОМ РАЗВИТИИ НОРМ ОТВЕТСТВЕННОГО
ПОВЕДЕНИЯ ГОСУДАРСТВ 54

Мён Хюн Чун (Myunghyun Chung),

Юридический факультет Университета Корё, Республика Корея
КИБЕРОПЕРАЦИИ ПРОТИВ ФИНАНСОВЫХ СИСТЕМ ДОЛЖНЫ ОСУЖДАТЬСЯ
В МЕЖДУНАРОДНОМ МАСШТАБЕ 57

Камино Кавана (Camino Cavanagh),

Королевский колледж Лондона
ПРОГРЕСС В РАЗВИТИИ МЕЖДУНАРОДНЫХ КИБЕРНОРМ 59

Жданов Ю.Н., Российская секция Международной полицейской ассоциации РОССИЯ И АКТУАЛЬНЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ.	61
Савенков А.А., Полякова Т.А., Институт государства и права РАН ТЕНДЕНЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И ВОПРОСЫ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ	63
Курбацкий А.Н., Белорусский государственный университет О РОЛИ ЭКСПЕРТНОГО СООБЩЕСТВА В ОБЕСПЕЧЕНИИ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ	66
Андреас Кюн (Andreas Kuehn), Институт Восток-Запад, США АТРИБУЦИЯ В КИБЕРПРОСТРАНСТВЕ И ПРОБЛЕМЫ ОТВЕТСТВЕННОСТИ	68
Якушев М.В., ПАО «Вымпелком», Россия О ВОЗМОЖНЫХ МОДЕЛЯХ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.	70
СЕМИНАР–КРУГЛЫЙ СТОЛ № 2 ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИКТ ВО ВРАЖДЕБНЫХ ВОЕННО-ПОЛИТИЧЕСКИХ ЦЕЛЯХ	
Смирнов А.И., Национальная Ассоциация международной информационной безопасности, Национальный институт исследований глобальной безопасности, Россия НОВЕЙШИЕ ИКТ КАК ФАКТОР ГЛОБАЛЬНОЙ НЕСТАБИЛЬНОСТИ: КАК ДОСТИЧЬ КИБЕР МОДУС ВИВЕНДИ?	74
Рафал Рогозинский (Rafal Rohozinski), SecDev Group, Канада, Международный институт стратегических исследований, Великобритания ТРИ НИТИ – ОДНА СЕТЬ	78
Карнаух В.В., Генеральный штаб Вооруженных Сил Российской Федерации О МЕРАХ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИКТ ВО ВРАЖДЕБНЫХ ВОЕННО-ПОЛИТИЧЕСКИХ ЦЕЛЯХ	84
Гэри Браун (Gary Brown), независимый эксперт, США ПРАВИЛА ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ И ЭЛЕКТРОМАГНИТНОМ ПОЛЕ. ...	87
Карасев П.А., Институт проблем информационной безопасности МГУ имени М.В. Ломоносова, Россия УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМЫ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ	90
Надя Костюк (Nadiya Kostyuk), Мичиганский университет, США КОМПЛЕМЕНТАРНОСТЬ КИБЕРОПЕРАЦИЙ: ПОЧЕМУ ГОСУДАРСТВА ВЕДУТ ПРОТИВОБОРСТВО В КИБЕРПРОСТРАНСТВЕ В ДОПОЛНЕНИЕ К ПРОТИВОБОРСТВУ В ДРУГИХ СРЕДАХ ИЛИ ВМЕСТО НЕГО?	95
Зинченко А.В., Центр международной информационной безопасности и научно-технологической политики (ЦМИБ) МГИМО МИД России ИКТ-ФАКТОР В СОВРЕМЕННОЙ МЕЖДУНАРОДНОЙ СТРАТЕГИЧЕСКОЙ НЕСТАБИЛЬНОСТИ	99
Джон Мэллори (John Mallory), Массачусетский технологический университет, США ПРАКТИЧЕСКИЕ МЕРЫ УКРЕПЛЕНИЯ ДОВЕРИЯ ДЛЯ КИБЕРСТАБИЛЬНОСТИ	102
Ромашкина Н.П., Институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ В ЭПОХУ ИКТ.	106

Дженис Хэмби (Janice Hamby), контр-адмирал ВМС США (в отставке), Колледж информационного и киберпространства, Университет национальной обороны США СТРАТЕГИЯ НЕПРЕРЫВНОГО ВОЗДЕЙСТВИЯ: ОПИСАНИЕ И ВЗГЛЯД НА ПРЕИМУЩЕСТВА И РИСКИ . . .	112
Татту Мамбеталиева, ОФ «Гражданская инициатива Интернет-политики», Кыргызстан ПРОБЛЕМЫ ПРОФИЛАКТИКИ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В ИКТ-СРЕДЕ	116
Тяжлова И.А., Министерство иностранных дел Российской Федерации К КИБЕРДИАЛОГУ С ВАШИНГТОНОМ ГОТОВЫ, НО НАВЯЗЫВАТЬСЯ НЕ БУДЕМ	119
Фролов Д. Б., Российская телевизионная и радиовещательная сеть (РТРС), Россия УГРОЗЫ И РИСКИ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ	123
СЕМИНАР-КРУГЛЫЙ СТОЛ №3 НАУЧНО-ТЕХНИЧЕСКИЕ И ЮРИДИЧЕСКИЕ ПРОБЛЕМЫ УСТАНОВЛЕНИЯ РЕЖИМА «ЦИФРОВОЙ ГРАНИЦЫ» ГОСУДАРСТВ: ПУТИ ИХ РЕШЕНИЯ	
Пилюгин П.Л., Институт проблем информационной безопасности МГУ имени М.В. Ломоносова, Россия ТЕОРЕМА О «ЦИФРОВОЙ ГРАНИЦЕ»	130
Кевин Лимонье (Kevin Limonier), Университет Париж-8 «ЦИФРОВЫЕ ГРАНИЦЫ» И «СУВЕРЕНИТЕТ» С ТОЧКИ ЗРЕНИЯ ТОПОЛОГИИ МАРШРУТИЗАЦИИ	133
Сурма И.В., Дипломатическая академия МИД России ВНЕШНЕПОЛИТИЧЕСКИЕ ВЫЗОВЫ И УГРОЗЫ ЦИФРОВОМУ СУВЕРЕНИТЕТУ ГОСУДАРСТВА	136
Бабекин Д.В., Министерство юстиции Российской Федерации, начальник отдела ПРАВОВЫЕ АСПЕКТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА И УСТАНОВЛЕНИЯ РЕЖИМА «ЦИФРОВОЙ ГРАНИЦЫ» ГОСУДАРСТВ	147
Од Жери (Aude Géry), Университет Руана, Франция ПРАВОВЫЕ ОСНОВЫ ЭКСТЕРРИТОРИАЛЬНОЙ ЮРИСДИКЦИИ И ИХ ВЛИЯНИЕ НА ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ	149
Чухи Пак (Joohee Park), Центр киберправа Университета Корё, Республика Корея ПРАВОВЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ ПРАВА МЕЖДУНАРОДНОЙ ОТВЕТСТВЕННОСТИ К КИБЕРОПЕРАЦИЯМ	152
Цветкова А.Г., Национальная Ассоциация международной информационной безопасности, старший эксперт НАМИБ ПРОБЛЕМА МЕЖДУНАРОДНОГО УПРАВЛЕНИЯ ИНТЕРНЕТОМ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	155
СЕМИНАР-КРУГЛЫЙ СТОЛ № 4 РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	
Григорьев Д.И., Национальная Ассоциация международной информационной безопасности, ГМК «Норильский никель», Россия ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО И МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПОДХОДЫ КОМПАНИИ «НОРНИКЕЛЬ»	160
Джэнис Хэмби, контр-адмирал ВМС США (в отставке), Колледж информационного и киберпространства, Университет национальной обороны США ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО ПРИ ЗАЩИТЕ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ	162
Ганс-Вильгельм Дюнн (Hans-Wilhelm Dünne), Президент Совета по Кибербезопасности Германии ТРАНСПАРЕНТНОСТЬ, ДОВЕРИЕ И СОТРУДНИЧЕСТВО: ПРЕДПОСЫЛКИ МЕЖДУНАРОДНОЙ КИБЕРБЕЗОПАСНОСТИ	163
Ярных А.Ю., Лаборатория Касперского, Россия ОПЫТ ЛАБОРАТОРИИ КАСПЕРСКОГО ПО РАЗВИТИЮ ДОВЕРИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ . .	165

Марков А.С., Группа компаний «НПО «ЭШЕЛОН», Россия ВОПРОСЫ ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СИСТЕМ.	167
Тихонов А.И., Лаборатория Касперского, Россия ДОВЕРИЕ И БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ	170
Баранов А.П., ООО «Сов-технология», Россия ТЕХНОГЕННАЯ УСТОЙЧИВОСТЬ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПОНЕНТЫ МИРОВОГО ИНТЕРНЕТА . .	172
Толстухина А.Ю., Российский совет по международным делам ИНИЦИАТИВЫ БИЗНЕСА ПО ФОРМИРОВАНИЮ ПРАВИЛ И НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ В ЦИФРОВОМ ПРОСТРАНСТВЕ.	175
Чарльз Барри (Charles Barry), независимый эксперт, США МЕЖДУНАРОДНЫЕ ГОСУДАРСТВЕННО-ЧАСТНЫЕ ПАРТНЕРСТВА: ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ.	177
Сычев А.М., Банк России МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ИНФОРМАТИЗАЦИИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ НА ПРИМЕРЕ СОТРУДНИЧЕСТВА ЦЕНТРАЛЬНЫХ БАНКОВ ЕАЭС	180
Шэнь И (Shen Yi), Директор центра БРИКС, Фуданьский университет, Китай ПОЗИЦИЯ БРИКС В УПРАВЛЕНИИ КИБЕРПРОСТРАНСТВОМ.	183
Толорая Г.Д., Национальный комитет по исследованию БРИКС, Россия БРИКС И ВОПРОСЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	185
Лебедь С.В., Руководитель службы информационной безопасности Сбербанка России	189
СЕМИНАР – КРУГЛЫЙ СТОЛ № 5 ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИКТ ДЛЯ ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ, ВКЛЮЧАЯ ГУМАНИТАРНОЕ ИЗМЕРЕНИЕ	
Куракин М.Б., журнал «Международная жизнь», Россия	192
Хиро Фудзимаки (Hiro Fujimaki), Университет Токай, Япония ВОПРОСЫ БЕЗОПАСНОСТИ ЧЕЛОВЕКА В КИБЕРПРОСТРАНСТВЕ.	193
Скворцов Я.Л., Факультет международной журналистики МГИМО МИД России ТРАДИЦИОННЫЕ ЦЕННОСТИ В УСЛОВИЯХ НОВЫХ МЕДИА	195
Бирюков А.В., Центр международной информационной безопасности и научно-технологической политики (ЦМИБ) МГИМО МИД России К ВОПРОСУ О ТЕХНО-ГУМАНИТАРНОМ ДИСБАЛАНСЕ ЦИФРОВОЙ ЭПОХИ.	201
Воробьев А.А., Координационный центр национального домена сети Интернет, Россия ОТВЕТСТВЕННЫЙ ПОДХОД К РАЗВИТИЮ СИСТЕМЫ DNS КАК ВАЖНОГО ЭЛЕМЕНТА ПУБЛИЧНОГО ЯДРА ИНТЕРНЕТА	205
Новикова Т.И., Координационный центр национального домена сети Интернет, Россия ПРОБЛЕМЫ ЦИФРОВОЙ ГИГИЕНЫ ДЕТЕЙ.	208
Солдатова Г.У., Фонд «Развитие Интернет», Россия КИБЕРБЕЗОПАСНОСТЬ И ЦИФРОВАЯ ГРАМОТНОСТЬ ПОДРОСТКОВ.	211
Михайлова Е.А., Факультет государственного управления МГУ имени М.В. Ломоносова НОВЫЕ МЕДИА В ИНФОРМАЦИОННОМ СОПРОВОЖДЕНИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ: СЛАКТИВИЗМ	214

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Ведущий:

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

В.П. Шерстюк

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

Уважаемые участники конференции!¹
Уважаемые гости!
Дамы и господа!

1. Позвольте мне открыть очередной, тринадцатый Международный Форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Хотелось бы начать со слов искренней признательности руководителям администрации города Гармиш-Партенкирхен, на территории которого уже в 13 раз собирается наш Форум. Мы с удовольствием информируем всех присутствующих о том, что в этом году в работе Форума принимают участие президент Германского совета по кибербезопасности г. Ганс-Вильгельм Дюнн и другие представители Германии. Рассчитываем, что это окажет позитивное воздействие на сотрудничество России и Германии в области создания открытой, безопасной, стабильной, доступной и мирной среды информационно-коммуникационных технологий.

Наш Форум проводится в непростое время. Прошедший год показал, что угрозы миру становятся все более опасными. В Вашингтоне взят курс на демонтаж договоренностей в сфере контроля над вооружениями, можно прийти к выводу о том, что возобладали сторонники запуска новой гонки вооружений.

На Конференции по разоружению, состоявшейся месяц назад в Женеве, Министр иностранных дел Российской Федерации Сергей Лавров отметил: «Сегодня мы сталкиваемся с агрессивным внешнеполитическим эгоцентризмом, подпитываемым претензиями на единоличное право определять «правила» мирового порядка и судьбы народов, стран и целых регионов. Нарастают попытки разрушить базовые договорённости, перекроить под свои конъюнктурные интересы всю



многостороннюю архитектуру контроля над вооружениями. В стремлении к доминированию бесцеремонно уничтожаются механизмы, десятилетиями работавшие на поддержание стабильности и предсказуемости в международных отношениях».

К сожалению, данная тенденция отражается и на международном сотрудничестве в области использования ИКТ. Это явно проявилось в работе Группы правительственных экспертов ООН по достижениям в области информатизации и коммуникаций в контексте международной безопасности (2016–2017 гг.) и на 73-ей сессии Генеральной Ассамблеи ООН.

Мировое сообщество раскололось при обсуждении рекомендованных Группой правительственных экспертов консенсусом в Докладе 2015 года норм, правил и принципов ответственного поведения государств в ИКТ-среде. Принятые Генеральной Ассамблеей ООН две резолюции по данному вопросу означают существование серьезных противоречий между государствами мира по проблемам правового регулирования отношений в ИКТ-среде, а также отсутствие общего видения подходов к разрешению этих противоречий. Позитивной стороной сложившейся ситуации можно, наверное, считать только то, что у двух Групп экспертов ООН задекларирована

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

общая цель – создание открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Сегодня мы собрались здесь для того, чтобы обменяться мнениями и предложениями экспертов о путях достижения этой цели и определить возможные направления сотрудничества по реализации согласованных предложений.

2. Организатором Форума в этом году выступает Национальная ассоциация международной информационной безопасности. Мы обещаем, что будет сделано все возможное для того, чтобы участники могли свободно и открыто обсуждать любые вопросы международного сотрудничества в области обеспечения национальной и международной информационной безопасности.

3. Одним из таких вопросов является, в частности, обсуждение результатов проекта МИКИБ «Методические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды». В чем здесь проблема? Международное право пока не стало инструментом, способным предотвращать использование ИКТ для нанесения ущерба правам и свободам человека и гражданина, законным интересам коммерческих и некоммерческих организаций в области информационной деятельности, а также деятельности государственных органов по обеспечению безопасности использования глобальной информационной инфраструктуры.

С принятием норм, принципов и правил ответственного поведения государств в ИКТ-среде в качестве норм «мягкого» права особую актуальность приобретает проблема обеспечения практического применения этих норм. В условиях обострения международной обстановки эксперты многих государств мира полагают, что необходимо разработать конкретные рекомендации по практическому применению норм, правил и принципов ответственного поведения в ИКТ-среде, использование которых могло бы способствовать снижению опасности возникновения конфликтов, связанных с «враждебным» и злонамеренным использованием ИКТ государствами для разрешения межгосударственных противоречий.

Решение о начале работ по этому проекту было принято год назад по инициативе участ-

ников МИКИБ – экспертов Института проблем информационной безопасности МГУ, Института Восток-Запад, Института киберполитики, Центра киберправа Института Корё и Фонда ИКТ для мира. На первом этапе объектом исследования были выбраны три нормы ответственного поведения государств, представленные в рекомендациях Доклада ГПЭ ООН 2015 года.

В рамках круглого стола, посвященного обсуждению деятельности МИКИБ, будут доложены основные результаты проекта, а также будут определены направления дальнейших исследований в области практического применения норм, правил и принципов ответственного поведения государств в ИКТ-среде.

Выяснение причин, почему международное право не работает в ИКТ-среде, приобретает особое звучание в связи с предстоящим началом работы двух Групп ООН – Группы открытого состава (инициатива России) и Группы правительственных экспертов, сформированной на основе принципа географического представительства (предложена США).

4. Разделяя справедливые опасения ГПЭ ООН об опасности использования информационно-телекоммуникационных технологий для враждебных военно-политических целей, организаторы Форума предлагают обсудить пути противодействия этой угрозе.

По мнению многих государств мира, вредоносный потенциал ИКТ, предназначенных для использования в рамках «силового» разрешения межгосударственных противоречий, продолжает увеличиваться. Убедительным примером этому, на наш взгляд, является принятая в США в сентябре 2018 г. Национальная киберстратегия. Её уже многие эксперты называли преамбулой войны.

Если еще недавно к числу угроз ИКТ эксперты относили, прежде всего, использование специального программного и технического обеспечения для нарушения деятельности критически важных объектов информационной инфраструктуры, то в настоящее время количество таких направлений использования ИКТ резко возросло.

Активно развиваются смертоносные автономные системы с искусственным интеллектом, который широко внедряется в военную технику, подстегивая гонку вооружений. Исследуются способы и методы создания и бое-

вого применения автономных боевых роботов различного назначения. ИКТ широко применяются для повышения эффективности средств ведения вооружённой борьбы. Увеличивается количество объектов инфраструктуры государства, поражение которых способно привести к возникновению межгосударственных конфликтов. К таким объектам теперь относят не только объекты военной инфраструктуры государства, но и целый ряд объектов экономической и социальной инфраструктур общества.

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

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

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

По существу человечество столкнулось с вызовом, обусловленным необходимостью применять международное право для регулирования отношений в принципиально новой среде, в которой пока не представляется возможным объективными способами зафиксировать как признаки нарушения международных обязательств, так и установить субъектов международного права, причастных к этим нарушениям.

Отсутствие механизмов применения международного права для регулирования международных споров в ИКТ-среде создает угрозу сохранению стратегической стабильности. При этом у некоторых юристов и полити-

ков возникает иллюзия свободы «силовых» действий в ИКТ-среде. По их мнению, когда не работает сила права, начинает работать право силы. Представляется, что этим путем нельзя достигнуть закреплённой в Уставе ООН цели – избавить грядущие поколения от бедствий войны.

В рамках круглого стола №3 предполагается обсудить приоритетные направления международного сотрудничества в области предотвращения использования ИКТ во враждебных военно-политических целях.

5. Одним из малоизученных, крайне сложных, но настолько же важных вопросов является вопрос о порядке установления пространственных пределов государственного суверенитета в ИКТ-среде.

Как известно, эта среда принципиально отличается от традиционных сред реализации международных отношений – суши, моря, воздушного и космического пространства. На наш взгляд, именно новизна ИКТ-среды, как пространства международных отношений, является основной причиной эрозии и кризиса международного права.

Во-первых, ИКТ-среда имеет искусственный характер. Она образовывается совокупностью сетей связи, коммуникационных и вычислительных устройств, функционирующих в пространстве глобальных цифровых идентификаторов (доменных имен, IP-адресов). Основным назначением этой среды является обеспечение взаимосвязанного выполнения программ автоматизации обработки и передачи информации, реализующих определенные информационно-коммуникационные технологии. Этот процесс имеет виртуальный характер и не предоставляет возможности использовать средства объективного контроля регулируемых процессов.

Во-вторых, функционирование ИКТ-среды обеспечивается, прежде всего, деятельностью негосударственных организаций, находящихся в различных юрисдикциях. Это накладывает определенный отпечаток на содержание суверенитета государств в ИКТ-среде и, соответственно, – на содержание международных обязательств государств и на возможности объективной фиксации признаков их нарушения.

С точки зрения международного права ИКТ-среда представляет собой юридическую

фикцию, заключающуюся в том, что техническую систему рассматривают как одну из составляющих территории для распространения на нее понятия «суверенитет».

По существу, человечество столкнулось с вызовом, обусловленным необходимостью применять международное право для регулирования отношений в принципиально новой среде, в которой не представляется возможным использовать хорошо знакомые и отработанные процедуры «делimitации» и «демаркации» границы. Решение столь важной проблемы способно очертить контуры будущей системы международной информационной безопасности.

В связи с этим представляется исключительно важным обсудить научно-технические и правовые аспекты выделения таких зон ответственности государств как одного из неперемennых условий атрибуции сторон инцидентов в ИКТ-среде.

6. Особенности ИКТ-среды обуславливают необходимость обеспечения безопасности ее использования на основе взаимодействия государственных органов и негосударственных организаций. Это сотрудничество часто называют государственно-частным партнерством. Данное партнерство, как правило, базируется на системе национальных нормативных правовых актов, которые регулируют отношения, в частности, в области безопасности организаций бизнеса, критической информационной инфраструктуры, а также использования в этих целях потенциала центров реагирования на чрезвычайные ситуации в ИКТ-среде.

По мнению многих экспертов, за последние годы опасность злонамеренного использования информационных технологий для нападения на критическую информационную инфраструктуру, осуществления других преступных деяний не стала меньше. Еще в 2013 году в докладе ГПЭ ООН отмечалось, что «угрозы частным лицам, компаниям, национальной инфраструктуре и государственным органам приобретают все более острый характер, и соответствующие инциденты имеют все более тяжелые последствия». В 2015 году ГПЭ ООН пришла к выводу, что «к числу наиболее пагубных нападений с использованием информационных и коммуникационных техно-

логий относятся нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств. Опасность вредоносных нападений с использованием информационных и коммуникационных технологий на критически важную инфраструктуру является реальной и серьезной».

Становится все более очевидным, что без взаимодействия с частным бизнесом, с собственниками соответствующих объектов критической информационной инфраструктуры государство вряд ли сможет обеспечить безопасность использования ИКТ в финансовой области, экономике, социальной жизни, управлении государством. Неспособность государства обеспечить достаточный уровень защищенности негосударственных организаций, организаций бизнеса заставляет эти организации активизировать деятельность по защите интересов в ИКТ-среде.

С этой точки зрения заслуживают серьезного внимания инициативы, выдвигаемые организациями бизнеса. Так, на 11-м Форуме в г.Гармиш-Партенкирхене российская компания «Норильский Никель» выступила с инициативой разработки Хартии информационной безопасности критических объектов промышленности. В рамках Хартии компания «Норильский никель» четко обозначает свое представление о том, какое поведение в информационном пространстве бизнес-сообщество должно приветствовать, а какое – осуждать. Компания исходит из того, что любой, кто использует информационные технологии для недобросовестной конкуренции, проникновения в технологические процессы, кражи чувствительной информации у коллег и конкурентов, должен быть осужден бизнес-сообществом. С аналогичной инициативой выступила компания Майкрософт и некоторые другие.

Понимая озабоченность бизнеса ситуацией с обеспечением безопасности информационной деятельности, представляется правильным активизировать усилия государств по адаптации международного частного права к новым условиям применения. Это новое направление развития государственно-частного партнерства, возможно, поможет уравновесить складывающееся сотрудничество бизнеса и государства в решении традиционно государственных задач – обеспечении оборо-

носпособности страны и безопасности государства.

В рамках круглого стола «Механизмы реализации государственно-частного партнерства в области обеспечения безопасности критической информационной инфраструктуры» будут обсуждаться вопросы воплощения положений Хартии в практической деятельности бизнес-сообщества, а также вопросы взаимодействия с государством при обеспечении безопасности критической информационной инфраструктуры.

7. Естественным следствием обострения международной обстановки является реконфигурация привычной структуры межгосударственных взаимодействий по вопросам развития и взаимопомощи. На этом треке все более заметным становится межгосударственное образование Бразилии, России, Индии, Китая и Южно-Африканской Республики, называемое БРИКС.

Как известно, на саммите глав государств этого международного образования в Йоханнесбурге (Южно-Африканская республика) в 2018 году обсуждались вопросы развития, инклюзивности и всеобщего процветания в контексте индустриализации и экономического роста на основе технологического прогресса. Перед лицом международных вызовов, требующих совместных усилий государств БРИКС, участники саммита подтвердили важность разработки под эгидой ООН правил, норм и принципов ответственного поведения государств в информационном пространстве для обеспечения безопасности в сфере использования ИКТ. Они также подчеркнули важность международного сотрудничества в борьбе с использованием ИКТ в террористических и преступных целях и вследствие этого – необходимость выработки

под эгидой ООН универсального, юридически обязывающего нормативно-правового документа по противодействию использованию ИКТ в преступных целях. Главы государств «признали прогресс, достигнутый в области развития кооперации в соответствии с дорожной картой практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ и любыми другими согласованными механизмами, а также значимость создания правовых рамок для сотрудничества между участниками БРИКС в области обеспечения безопасности в сфере использования ИКТ».

В рамках Форума эксперты государств обмениваются мнениями о приоритетных направлениях сотрудничества в этой сфере. Данный вопрос особенно важен для России, которая в 2020 г. будет председательствовать в БРИКС.

8. Наконец, на обсуждение участников Форума будет вынесен вопрос о противодействии использованию ИКТ для вмешательства во внутренние дела суверенных государств, включая вопросы защиты прав человека в ИКТ-среде.

Использование ИКТ для дезинформации международного общественного мнения в отношении действий, направленных на вмешательство во внутренние дела государств, а также в области признания, соблюдения и защиты прав человека в ИКТ-среде, повышает риски возникновения конфликтов, способных нарушить международный мир и безопасность.

Уважаемые коллеги! Программный комитет Форума подготовил довольно напряженную повестку дня.

Желаю всем успеха!

Приступим к работе.

А.В. Крутских

*Специальный представитель
Президента Российской Федерации
по вопросам международного
сотрудничества в области
информационной безопасности,
Чрезвычайный и Полномочный Посол
Российской Федерации*

Уважаемый Владислав Петрович!¹
Уважаемые коллеги!

Я сменил образ в этом году благодаря тому, что впервые не произнесу ни одного критического слова в адрес Соединенных Штатов. Я эту норму исчерпал еще в прошлом году. Но тем не менее, в лучших традициях Голливуда, я все-таки начну с некоторых ужасиков, а потом будет большой хэппи энд, благо для него есть основания.

Друзья, давайте зададим один простой вопрос, потому что здесь сидят эксперты, профессионалы и, конечно все прекрасно понимают. С прошлого года киберситуация стабилизировалась? Улучшилась? Как она развивается? Вот у нас в Москве оценка этого самая ужасная. Мне кажется, что мы достигаем в общем-то критической фазы, количество атак возрастает, возрастает их изощренность, возрастает ущерб от кибератак, возрастает число участников всего этого дела. По данным ООН, в следующем году тотальный ущерб от кибератак приблизится к 10 триллионам долларов.

Это перебор!

И самое главное, что тенденции в этой сфере, действительно, только ухудшаются. Ухудшаются в силу двух факторов. Я бы их сформулировал следующим образом, как это в Москве оценивают.

Прежде всего, потому что страны открыто объявляют о том, что они будут проводить наступательную киберполитику. На конференции в Сингапуре это было просто главным трендом, когда многие выступающие говорили о том, что их страны будут наносить киберудары превентивно, то есть первыми. Выступая там, я задал вопрос аудитории в 2,5 тысячи профессионалов, а что тогда остается другим? Как они-то должны реаги-



ровать? Буквально неделю назад из Парижа пришло сообщение, что Франция в лице своего министра по делам вооружений, она заявила о том, что и Франция теперь будет проводить наступательную киберполитику и наносить удары первыми. Ну, что-то в этом духе. В данном случае, Франция отстала от англосаксов на несколько лет, потому что еще в 2002 году Великобритания первая, потом Соединенные Штаты, ну а потом и все остальные провозгласили, что будут бить первыми.

Тогда возникает вопрос, обращу его к Франции. Заметьте, не к США. По собственной французской статистике, большинство кибератак на Францию совершается из Соединенных Штатов. Я не могу себе представить, чтобы Франция могла поднять голос на Соединенные Штаты в этом отношении. Это смешно. Они союзники, они партнеры, это единая сторона.

Против России, и что ожидается, что Россия будет это все терпеть, если кто-то на нас будет нападать? Конечно, нет. Значит, против кого, «третьего мира»?

Но, по-любому, как бы это ни было, это все говорит о том, что психология мира достаточно испорчена, потому что она все больше и больше смиряется с тем, что кибероружие становится применимым. Это происходит в ус-

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

ловиях, когда даже устав ООН, как бы мы это не отмечали в отдельных докладах, даже устав ООН не определяет кибернападение как вооруженное нападение, а, соответственно, юридически, казуистически, это не дает права на самооборону и на все эти вещи. Поэтому, делая в Москве оценку, что ситуация критическая, Россия делает все для того, чтобы на солидном уровне, на международном уровне, охватывая всех переговорщиков, договориться об определенных правилах игры. Без этого нас ожидает катастрофа.

Я хочу напомнить о великольном соглашении, которое было достигнуто в 70-е годы. Тогда был предотвращен инцидент на море и воздушном пространстве над ним. До этого наши корабли и авиация участвовали в инцидентах, любой из которых мог привести к большой серьезной конфронтации, если вообще не к войне друг с другом. Заключив это соглашение, и потом тиражировав его с другими странами такими как, Франция, Великобритания и еще рядом стран, мы, действительно, успокоили ситуацию на десятилетия и стали предсказуемыми друг для друга, по крайней мере, в этих измерениях. Но этого абсолютно нет в киберпространстве. В результате это то, что волнует нас в Москве. Я подчеркиваю, что любой этот инцидент он может перерасти вот в эту конфронтацию, а прилететь этот инцидент может откуда угодно. Могут быть использованы третьи страны, посредники. И, самое главное, это будет сделано против воли руководителей стран Америки или России.

Но, я думаю, хватит об этих тяжелых моментах. Эта аудитория как раз прекрасно понимает, что проблема есть, мы на грани, и я не боюсь этого сказать и могу даже повторить медленнее. Мы на грани крупнейшего киберинцидента, который может привести к чудовищной конфронтации.

Только напомню, убийство Эрц-герцога Фердинанда было эпизодом. «Любая жизнь ценна», – как писал Достоевский. Да, убили человека, но после него погибли десятки миллионов в Первой мировой войне. Был псевдоинцидент в Гляевице, который привел к тому, что погибло пятьдесят миллионов человек. Давайте представим, что бизнес-элиты накануне Первой мировой войны договорились бы о химическом оружии. А ведь от химического

оружия погиб в годы Первой мировой войны один миллион человек, и, по-моему, 2 миллиона было искалечено.

Так почему нам не договориться во имя нашего собственного блага об определенных правилах, об определенной транспарентности, чтобы не предъявлять друг другу каких-либо искусственных претензий. Мы прекрасно понимаем, что любить Америка Россию не будет, да и не должна, да и мы, наверное, ее не будем любить, но уважать-то мы друг друга можем. Но из этого уважения надо быстрее исчерпать инциденты, которые могут испортить жизнь и американцам, и всему миру, и россиянам. И вот исходя из этого, я хочу сейчас перейти к позитивной стороне и основной части своего доклада, потому что хороших новостей пять.

Но преамбулой к этим пяти новостям я хочу сказать удивительную вещь, она здесь частично уже прозвучала. Последнее время из наших переговоров, когда мы готовили визит В.В. Путина в Сингапур, ряд других стран, мы все больше и больше убеждаемся, что проблема кибербезопасности – это не просто проблема: бизнес, мировой глобальный бизнес пошел дальше, чем политики. Сам бизнес уже начинает высказывать публично свою потребность в достижении договоренностей о правилах игры.

Неслучайно, по нашим данным, организаторы киберДавоса планируют в этом году посвятить его всецело кибербезопасности, потому что и Интернет-вещей, и беспроводная медицина, и практически все вещи, связанные с развитием мира, с триллионами, которые бизнес должен вкладывать, они все становятся заложниками отсутствия решения одной простой проблемы. В кавычках, конечно, простой. Это кибербезопасность!

Нас информировали о предстоящих инвестициях в ближайшие годы на триллионы долларов, когда будет создаваться роботизированная экономика, роботизированные порты. Это касается, прежде всего, самых развитых стран: Германии, Франции, той же Европы, Соединенных Штатов, Сингапура. Они ведут переговоры с нашим Президентом, к сожалению, в отличие пока от США, о том, как решить проблему вот этого будущего искусственного интеллекта, вот этой роботизации во имя огромных денег, во имя прогресса человечества, во имя бизнеса. Но получает-

ся, что мы ведем эти переговоры с бизнесом, с людьми продвинутыми, но не ведем их с политиками на должном уровне. Так вот, Россия все-таки смогла, и я этим очень горжусь, что мы все-таки смогли восстановить трек для политических переговоров, и этот трек будет открыт для всех, и этот трек будет проходить под эгидой ООН.

Поэтому перейду к позитивным новостям.

Ну, во-первых, после годичной паузы восстанавливается трек дискуссии по МИБ в ООН. Это означает, что вновь заработает главная многосторонняя переговорная площадка, на которой будет обсуждаться весь спектр проблем, связанных с обеспечением безопасности при использовании информационно-коммуникационных технологий. Можно сказать, тем самым международному сообществу удалось отметить, достойно отметить двадцатилетие дискуссии по МИБ (в прошлом октябре ей исполнилось 20 лет), с того момента, когда по инициативе России «мибовские» вещи были включены в повестку дня ООН.

Символично, что именно в год юбилея удалось принять прорывные решения, нацеленные на реальное укрепление информационной безопасности. Пока речь идет не о существе решения проблемы МИБ, а об инфраструктуре. Но и это уже большое дело!

Главная задача – защитить интересы всех стран в цифровой сфере в независимости от того, на каком уровне технологического развития они находятся. В декабре прошлого года Генеральная ассамблея ООН одобрила выдвинутую Россией резолюцию, за нее проголосовало 120 стран, ее соавторами выступили 30 стран, она называется «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

Сожаление вызывает только то, что эту резолюцию, а я как участник переговоров, не обсуждал с Соединенными Штатами. К сожалению, и здесь в этой аудитории я могу сказать, что даже замгоссекретаря, который приехал на переговоры, вынужден был сказать: «Андрей, мои инструкции не позволяют с тобой особо долго на эту тему говорить. И вообще, 15 минут». Хотя мы проговорили потом полтора часа и пришли к очень многим и оптимистичным выводам, тем не менее, было вид-

но, что американская дипломатия, дипломатия великой державы, уважаемой державы, без которой нельзя решать проблемы, но дипломатия скована, она пассивна, и это отмечали даже не мы, это отмечали союзники Соединенных Штатов.

Наша резолюция открывает новый этап глобальной дискуссии. И это вторая хорошая новость, которую я хотел сказать. Речь идет о целом ряде исторических новаций в этой резолюции. Почему, собственно, Россия отошла от первоначального текста резолюции и выступила вот с этим инновационным. И, прежде всего, это благодаря тому, что в резолюции впервые в истории человечества отфиксировано 13 правил, норм и принципов ответственного поведения государств в информационном пространстве. Этого не было. Был доклад Группы правительственных экспертов, частных лиц, в которую входил я, этот доклад рекомендовался Генеральной Ассамблеей ООН. Но это был доклад 25 умных женщин и мужчин. Мы не выступали ни под национальным флагом, но формально, конечно. А это уже резолюция, за которую голосовало 120 государств. Смысл – заложить основу мирного взаимодействия государств в этой сфере, обеспечить предотвращение, я на этом глаголе хочу акцентировать ваше внимание, prevention – предотвращение вооруженных конфликтов в киберсфере, кибервойн. Не их регулирование, это уже поздно, и потом неизвестно, как быстро кибервойна перерастет в ядерную или убийственную обычную войну, поэтому предотвращение – это принцип, заложенный в резолюцию.

Например, в этом перечне есть такие принципиально важные положения, как обязательство использовать ИКТ исключительно в мирных целях, соблюдать в информационном пространстве принципы государственного суверенитета, сотрудничать в борьбе с применением ИКТ в преступных и террористических целях, предотвращать распространение скрытых вредоносных функций в IT-продукциях, тех же закладок. Это принципиальный пункт для бизнеса, потому что, когда Россия закупает Хуавей и китайскую продукцию, у нас есть с китайцами понимание о том, что там закладок нет, и это проверяемо. Почему Sony менее конкурентноспособна, чем, скажем,

Samsung? Да потому что с южными корейцами у нас тоже есть определенные позитивные договоренности. От этого страдает бизнес, по крайней мере, на нашем рынке.

В первоначальном своде норм зафиксированы следующие важные принципы. Любые обвинения в злонамеренном использовании ИКТ должны быть доказаны, чтобы не было больше «Гляйвицев».

Государства не должны использовать посредников для злонамеренного применения информационно-коммуникационных технологий. ООН должна играть ведущую роль в международной дискуссии по МИБ, потому что это проблема касается всех. Суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, распространенной на их территории. Принципиально важный момент, что государства несут главную ответственность за поддержание безопасной и мирной ИКТ-среды. Это исключает возможность использования разными факторами провокационных действий, чтобы втравить нас в войну.

Этот список целиком основан на положениях, как я уже сказал, докладов групп правительственных экспертов.

Теперь третье. То есть он уже был раз одобрен. За него голосовали консенсусом все, включая Генассамблею ООН, одобряя доклады группы правительственных экспертов. И кто же проголосовал против вот этих принципов? Чего в них плохого? Ведь эти принципы нуждаются в том, чтобы правовики-специалисты собрались и конкретизировали их, разжевывали, так сказать, и страны соблюдали. Что тут плохого? Голосовали 49 стран. Соединенные Штаты и их европейские союзники.

Мы задаем себе вопрос: ведь Сингапур не менее буржуйская страна, чем европейские страны. Ну почему Сингапур голосует за эту резолюцию? Уж совсем буржуйская страна Швейцария и Южная Корея, они воздержались при голосовании. Почему во время ооновской сессии ко мне подходили послы большинства европейских стран и говорили: «Андрей, договоритесь с Америкой, нормальные у вас принципы. Мы готовы проголосовать, но мы находимся под давлением, и мы вынужде-

ны будем голосовать против, но мы хотим вести переговоры с вами на базе этих принципов». И в числе этих стран Германия, в числе этих стран Франция, в числе этих стран Португалия, Испания, Италия. И многие, они видят объективную ценность всех этих вещей.

Но, увы! То ли руки не дошли, то ли есть другие факторы, но вы, наверное, их знаете лучше меня.

В-третьих, это принципиально важный момент, это отличает нашу резолюцию от многого другого. Мы вплотную подошли к этапу реальной демократизации переговорного процесса по МИБ. Придание ему открытого, инклюзивного и прозрачного характера. Не наша инициатива. Во время двусторонних переговоров в Вашингтоне, когда у нас еще были эти переговоры на уровне заместителя секретаря Совета безопасности и замгоссекретаря США, именно американцы выступали с этими очень правильными принципами, и забота была абсолютно прагматической. Потому что нельзя оставлять никого за бортом этих договоренностей, чтобы не было *save havens*. Не было убежища, откуда можно было бы совершать эти акты скрытой агрессии.

Поэтом мы и предложили открыть этот процесс для переговоров всех, и в том числе, я смотрю сейчас на коллег из Соединенных Штатов, в том числе для того, чтобы обязать другие страны не портить нам жизнь, не втравливать нас в конфронтацию. Для этого они должны четко и недвусмысленно даже *rock states*, должны высказаться, что они соблюдать должны эти принципы. Тогда будут оправданы и санкции, и все остальное, если они это будут нарушать.

Многие страны нам открыто заявляли, влиятельные мощные страны, в том числе и Иран, например, они говорили, мы не участники переговорного процесса, поэтому то, что там работали эксперты, мы в гробу это видали, мы будем жить своей жизнью. А мы как раз хотим, чтобы они жили в рамках принципов международного сообщества. Для этого государства должны поддержать эти принципы. И поэтому, конечно, вызывает сожаление, что 49 стран отказались поддержать резолюцию, но переговорный процесс, который мы открыли, позволяет всем встретиться в июне, 1–2 июня в Нью-Йорке, и начать серьезный разговор.

Для переговоров создается рабочая группа в ООН открытого состава, сокращенно РГОС. Это означает, что в ее работе смогут участвовать все без исключения государства-члены ООН. Мы твердо убеждены, что эпоха клубных договоренностей прошла, и что сегодня все страны, вне зависимости от уровня их технологического развития, имеют право принимать прямое участие в этих переговорах. Да, переговоры, мы понимаем, мы слышали этот аргумент, когда 200 стран, ну не 200, пусть 100, соберутся – это сложнее вести переговоры, чем вдвоем, или в рамках какого-то союза, блока. И тем не менее, каждый голос важен и должен быть учтен. Лишь таким образом можно заложить основу справедливого и равноправного миропорядка в цифровой сфере. РГОС будет уполномочен рассматривать весь спектр вопросов обеспечения МИБ. Особое внимание она должна уделить дальнейшей работе над нормами, правилами и принципами ответственного поведения государств в информационном пространстве, вопросам применимости в нем международного права, наращиванию цифрового потенциала развивающихся стран.

Такой мандат переговорная структура ООН по МИБ получит впервые. Группа открытого состава позволит каждой стране внести свой вклад и принять на себя соответствующие обязательства. Повышается сам статус дискуссии по МИБ в ООН. В отличие от традиционной группы правительственных экспертов, за которую сейчас и лоббировали США, и это очень хорошо, это будет полноценный орган Генеральной Ассамблеи ООН.

Вдумайтесь, друзья, – это киберГенеральная Ассамблея ООН. Это огромное достижение! Этот орган юридически имеет право вырабатывать и рекомендовать государствам-членам любые документы, вплоть до проектов международных договоров. А не просто рекомендации для Генассамблеи, хочешь соблюдать, хочешь не соблюдать.

Новым элементом мандата РГОС является изучение возможности организации регулярного институционального диалога с широким кругом участников под эгидой ООН. Проще говоря, РГОС должна рассмотреть варианты создания постоянно действующей переговорной структуры по тематике МИБ, чтобы не в от-

дельных столицах принимались решения: кто виноват, что с ними делать и как. А это должно быть что-то типа комитета ООН по кибербезопасности, вроде Комитета ООН по космосу. Вроде других специализированных организаций системы ООН. Более того, мои контакты с американскими силовиками и госдеповцами в свое время говорили о том, что американские силовики, кстати, с интересом восприняли эту мысль.

В нашей резолюции впервые предусмотрен механизм межсессионных консультаций с негосударственными игроками, прежде всего, с бизнесом. Я терпеть не могу это английское слово, его просто трудно выговаривать, «многостейкхолдеровая» модель. По-русски, это невозможно совершенно. Так вот, мы взяли этот принцип, и теперь в ноябре группа открытого состава встретится с глобальным бизнесом, как это уже однажды было под эгидой Всемирного экономического форума. И мы будем спрашивать, политики и бизнес сядут вместе, потому что мы не хотим никому ничего навязывать искусственно и противоестественно. Пусть бизнес нам подскажет, что нужно делать. И в этом плане то, что сделал Норникель, то, что сделал Майкрософт, то, что сделал Сбербанк, и другие крупные корпорации, – это огромный вклад.

Майкрософт, например, впервые сформулировал – мы до этого не додумались, жалко, нельзя воровать интеллектуальную собственность, – в Женевскую конвенцию по кибербезопасности прекрасную идею, только в эту бутылку надо налить очень хорошее вино, виски или водку, но, может быть, и смешивать, но не взбалтывать, как вы знаете.

Четвертая хорошая новость – это то, что Генеральная Ассамблея ООН впервые запускает в качестве отдельного трека дискуссии по проблематике противодействия информационной преступности. Это отдельная тема, потому что все киберагрессии и все негативное сейчас маскируется под преступность, хотя эта тема самостоятельная. И самый главный ущерб наносится именно по этой линии – киберпреступности.

Это стало возможным благодаря принятию Генассамблеей ООН второй российской резолюции. За нее голосовало 100 стран. Это – противодействие использованию ИКТ в преступных целях. Все те же, кто голосовал

против первой резолюции, почему-то голосовали и против этой резолюции.

Ключевая задача этой инициативы – запуск широкой и транспарентной дискуссии по противодействию информационной преступности. Юристам я задаю один вопрос и не могу нигде получить на него ответ, особенно, в странах Евросоюза. Почему Будапештская конвенция по борьбе с киберпреступностью за все 12 лет или больше своего существования ни разу ни в одном суде мира не была использована? Нет ни одной ссылки ни в одном решении ни в европейских странах, ни в других странах-членах Будапештской конвенции, которая бы определяла суть решения на основании Будапештской конвенции. Значит, она не работает, значит она создана для чего-то другого. Почему половина из участников заманивается туда путем давления и уговоров. Сам механизм-то не работает. Значит, ее надо обновить, значит, ее нужно поправить, взять за основу эту конвенцию, но поправить.

Сделать ее приемлемой для Китая, для России, для Южной Африки, для всех. Сделать ее универсальной, придать ей статус ООН, и мы готовы работать в этом направлении. Но увы, в Страсбурге на это никто не идет пока.

Наконец, пятая хорошая новость. Это то, что начиная с этого года дискуссия в ООН будет проходить не в одном, а в двух форматах. Мы об этом и мечтать не могли, когда в сентябре наши представители (часть из них сидит в этом зале) приехали в Нью-Йорк, и мы вообще рассчитывали, что будет только одна резолюция и не такая развернутая, как эта, потому что приходилось импровизировать на месте. Но благодаря Соединенным Штатам мы получили две российских резолюции, потому что та резолюция, которую предложили Соединенные Штаты, как-бы в противовес нашей, это наш же текст 2016 года. Старенький текст. Устаревший. Не такой революционный. Там буквально десяток слов изменены, ну и название. И теперь мы имеем прекрасные два формата: мы имеем Группу правительственных экспертов, где умные люди будут обсуждать вопросы с формате экспертов, и мы будем иметь РГОС, где мы будем обсуждать параллельно эти вещи, но уже на другом – государственном – уровне.

Для нас важно, чтобы выстраивалась наша работа, этих двух групп, в компетен-

тарном, неконфронтационном, конструктивном и основанном на сотрудничестве ключе. И вот здесь получилась интересная система. Многие западные страны насторожились, а как вообще будут работать эти две группы? Будут ли они друг друга душить, конкурировать? Как это будет? По традициям ООН одна резолюция считается американской, другая резолюция – нашей, созданы два механизма. И замгенерального секретаря ООН специально попросила меня о встрече в Женеве, чтобы тоже как-то определиться, как все это будет работать? И здесь я с большой гордостью, как дипломат, хочу сказать, что еще 27 ноября, когда же стало ясно, что обе резолюции пройдут, я вызвал временного поверенного в делах США в Москве, и мы передали предложения Соединенным Штатам встретиться, пусть не в широкоформатном виде, но просто обсудить, как сделать так, чтобы не раздражать друг друга, а чтобы выстроить не как гладиаторы работу в обоих ооновских форматах. Чтобы использовать их для конструктива.

Ноябрь, декабрь, январь, февраль, март, апрель – мы ждем ответа! А весь мир волнуется! В результате получается интересная картина: послы всех других стран, ваших же американских союзников и ООН, идут к нам и спрашивают: как мы будем жить, как мы будем работать, и как все организовать?

Я говорю: «Да вы идите в Вашингтон, параллельно с нами».

Они говорят: «Да мы идем в Вашингтон, но как-то нам все-таки не рассказывают. А, самое главное, вы-то будете американцам вредить?»

Я говорю: «Конечно, будем, если будет за что! Но мы хотим договориться, чтобы не вредить друг другу».

Таким образом, я чем начал, тем и хочу закончить.

Мы создали инфраструктуру для прямого честного разговора. Все участники будут там. Мы закрепили с подачи голландцев, хотя они голосовали против нашей резолюции, что обе группы будут работать на принципе консенсуса. Это значит, если кого-то не будет устраивать что-то, страна просто может остановить весь этот процесс или, по крайней мере, не допустить принятия неприемлемых вещей.

Это гарантия и малым, и большим. Это гарантия натовцам, это гарантия бриксовцам, это гарантия всем.

Как видите, эта инфраструктура создана. В июне она начнет работать. Мы идем на эти переговоры, хотя нам предлагали рассмотреть вопрос о председательстве, в свое время, в группе правительственных экспертов два срока я был председателем, но мы на себя эту роль не берем. Мы считаем, что председателями в этих группах, если мы будем думать о компромиссе, о желании выработать решение, должна быть небольшая, желательно, буржуйская, нейтральная страна. Почему не Финляндия, почему не Швейцария, почему не Египет, хотя она малобуржуйская, конечно, страна. Почему не Сингапур, ну давайте договоримся, давайте встретимся и, как бывало раньше, хотя бы определимся, кого мы хотим видеть.

Двадцать пять специалистов в Группе экспертов. Подано больше восьмидесяти заявок. Все хотят быть и участвовать в выработке правил. Со ссылкой на Генерального секретаря ООН мне говорят, что не знают, что делать. Но главное, чтобы Группа-то была

представительная. Я приведу вам пример, чтобы вызвать улыбку, а то уж больно я серьезно все рассказываю. В прошлой группе из 25 человек я сидел с представителем одной из развивающихся стран, как ни странно, директором школы, который в основном смотрел порнофильмы во время дискуссий по МИБ, это страшно отвлекало российского представителя, поэтому я не очень понимаю, зачем такой представитель нужен в Группе, которая определяет политику планеты в информационном пространстве. Кого мы обманываем? Тем более, группа работает на принципе консенсуса. Следовательно, давайте построим это по принципу «двадцатки». Те, кто самые развитые страны, должны там быть. Почему, если там будет Япония, надо выключать из этой группы Южную Корею и наоборот.

Там должны быть представительные страны.

Но, собственно, это и все, что я хотел сказать, поэтому на этой оптимистической ноте я надеюсь, я завершаю свое выступление.

Спасибо за внимание!

О.А. Плохой

Первый заместитель Министра юстиции
Российской Федерации

Уважаемые коллеги!¹

Рад приветствовать Вас на Тринадцатом международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Позвольте поблагодарить организаторов Форума за предоставленную возможность обсудить одну из самых актуальных тем современности: обеспечение международной информационной безопасности.

XXI век характеризуется глобализационными процессами, вызванными в том числе формированием и стремительным развитием информационной сферы, способствующей «размыванию» государственных границ. Современные реалии ставят перед государствами новую задачу – создание системы международной информационной безопасности, которая должна стать неотъемлемой частью и ключевым элементом системы международной безопасности.

Информационно-телекоммуникационная сфера является сравнительно молодой и крайне динамично развивается, что проявляется в регулярных нововведениях и трансформациях, а также появлении новых вызовов и угроз. Это требует оперативного реагирования как в технологическом, так и в правовом плане.

Как представитель Министерства юстиции Российской Федерации хотел бы сакцентировать внимание на правовой составляющей обеспечения международной информационной безопасности.

Одним из главных вопросов, подлежащих разрешению с точки зрения международного права, остается вопрос применимости общепризнанных принципов и норм международного права к сфере информационно-телекоммуникационных технологий.

Полагаем, что сформировавшиеся и неукоснительно соблюдающиеся на протяжении более 70 лет общепризнанные принципы и нормы международного права применимы к сфере информационно-телекоммуникационных технологий, поскольку представля-



ют собой базис международных отношений в целом.

Вряд ли можно подвергнуть сомнению актуальность на настоящий момент таких принципов как:

- невмешательство во внутренние дела государств;
- суверенитет;
- урегулирование конфликтов мирными средствами, не подвергающими угрозе международный мир, безопасность и справедливость;
- воздержание в международных отношениях от применения силы либо от угрозы ее применения;
- соблюдение территориальной неприкосновенности государств.

Также считаем необходимым в равной степени исходить из презумпции применимости к информационной сфере международных обязательств государств, в том числе вытекающих из международных договоров. Однако, учитывая особую правовую природу информационной сферы, не все обязательства государств могут выполняться в чистом виде. Так, многие положения будут применяться скорее по принципу *mutatis mutandis*, то есть с соответствующими видоизменениями, характеризующими конкретную сферу правового регулирования.

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

Вместе с тем, принимая во внимание трансграничный характер правоотношений, особая сфера правового регулирования информационно-телекоммуникационных технологий нуждается в новом универсальном подходе, который целесообразно реализовать в форме разработки и последующего принятия на площадке Организации Объединенных Наций международного договора, базирующегося на общепризнанных принципах и нормах международного права и отвечающего требованиям всех государств.

Учитывая, что Министерство юстиции Российской Федерации является компетентным органом по заключению и имплементации международных договоров о взаимной правовой помощи, отдельно хотел бы остановиться на проблематике сотрудничества государств в области борьбы с применением информационно-коммуникационных технологий в преступных целях, которое также нуждается в глобальном регулировании.

Так, расследование киберпреступлений имеет особую специфику, существенным образом осложняющую процесс судопроизводства, и требует более оперативного реагирования и взаимодействия правоохранительных органов государств, поскольку информационная сфера характеризуется возможностью модификации.

Основными трудностями, с которыми государствам приходится сталкиваться при осуществлении международного сотрудничества в области борьбы с киберпреступностью, видятся:

- недостаточная оперативность взаимодействия компетентных органов государств;
- отсутствие своевременного реагирования на запросы о производстве след-

ственных действий или предоставлении материалов, необходимых при расследовании киберпреступлений;

- отсутствие должного законодательного регулирования на национальном уровне по вопросам:
 - использования серверов, позволяющих скрывать данные об IP адресах пользователей;
 - применения «облачных» технологий;
 - сохранения электронной информации на носителях в течение определенного периода времени, а также доступ государственных органов к соответствующей информации;
 - привлечения лиц к ответственности за создание и использование механизмов, позволяющих устанавливать анонимное сетевое соединение, защищенное от прослушивания.

В заключение хотелось бы отметить стремительно растущую необходимость укрепления и совершенствования международного сотрудничества государств в области борьбы с киберпреступностью, а также совместного преодоления возникающих проблем при взаимодействии в информационно-коммуникационной сфере в целях поддержания международного мира и безопасности.

Искренне надеюсь, что предстоящая дискуссия пройдет в конструктивной и плодотворной атмосфере и будет способствовать налаживанию диалога между государствами, сближению подходов по ключевым вопросам и выработке прикладных рекомендаций по обеспечению международной информационной безопасности.

Желаю успешной и продуктивной работы!

Ганс-Вильгельм Дюнн

Президент Совета по Кибербезопасности
Германии

«Доброе утро, дорогие друзья!» (г-н Дюнн произнёс на русском языке).

Я надеюсь, это звучало хорошо! Спасибо большое! Думаю, это очень важный день для меня, потому что Германская пресса очень заинтересована в сегодняшнем выступлении. Уверен, что быть здесь очень важно, потому что нам нужен диалог. Да, г-н Крутских уже отметил это. Если мы не будем вести переговоры, не наладим диалог, то нас ожидают эскалация конфликта и война. Мы должны создать взаимовыгодные отношения.

Это важная тема для Германии, так как мы ваши ближайшие соседи. Чтобы долететь из Берлина в Москву, мне необходимо 2 часа, в отличие от 8-ми часового перелета в Нью-Йорк.

Важно понимать и контролировать наши «системы» – это и есть большая проблема. Надеюсь, что у нас будет возможность обсудить. Я, как Президент Германского Совета по «кибербезопасности», в котором у нас 168 участников, а также 16 германских земель с их собственной системой правоохранительных органов, надеюсь на сотрудничество.

Основой немецкой промышленности являются компании малых и средних размеров: в Баварии, Баден-Вюртенберге, Кёльне, Берлине. Они «открыты и уязвимы». Уверен, что очень важно сотрудничать в различных сферах: терроризм, дипломатические отношения и, конечно, «киберпреступность». Думаю, что наступил тот момент, когда мы должны говорить.

Наши системы несут ассиметричный характер, и их очень легко атаковать. Например, немецкие поставщики энергоресурсов. У нас 900 малых и средних поставщиков в Германии. В Volkswagen (немецкая автомобильная промышленность) мы инвестировали в прошлом году 0,5 млрд евро в «кибербезопасность». И вот эти 900 поставщиков отвечают за безопасность энергоносителей в том числе.

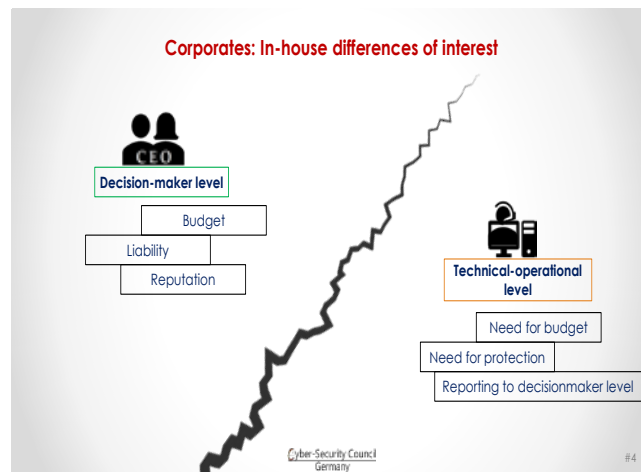
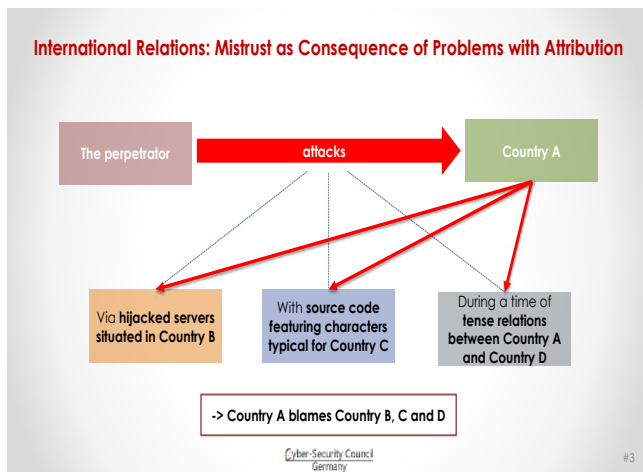
Сегодня мы говорим об атрибуции. Допустим, в моем доме вор! Я могу пойти в полицию или попытаться схватить его. А как же киберпространство? Самая главная проблема – определить, кто является нападавшим,



доказать его вину. И дело не в кириллице, как многие говорят. Наличие кириллицы не всегда значит вмешательство или атаки России.

Есть всеобъемлющая проблема: есть государство, есть бизнес, структуры различные и у каждого своя «повестка дня». К примеру, немецкая служба безопасности, во Франкфурте, которая сотрудничает с нашими международными друзьями. Думаю, что это большая проблема для Германии, потому что я не могу сказать точно, контролируем ли мы эти международные хабы, отношения между ними.

Все хотят говорить о кибербезопасности. Очень популярная тема. 99% процентов руководителей компаний согласны, что надо что-то делать, но по возвращении в компанию – продолжается игнорирование ситуации. Только 7% лиц, которые влияют на принятие решения – инвестируют в «кибербезопасность». Почему? У нас проблемы с технической точки зрения. В каком плане? Нет согласованности между различными уровнями принятия решений (то есть, говорим-говорим, но это не влияет на принятие каких-либо определенных решений, чтобы повисить «кибербезопасность»). Чтобы члены Парламентов, руководители предприятий, Меркель, Макрон были заинтересованы в этом. 57% всех германских компаний имеют собственные концепции «кибербезопасности». На уровне отдельных предприятий. На уровне отрасли – нет концепций, на уровне промышленности, соответственно, тоже нет.



Поэтому, коллеги, считаю, что нам необходимо обсудить следующее: создать собственную среду «кибербезопасности». Проблема – перед нами стоит очень много идей в сфере инноваций в Европе. В том числе и в России (Сколково, Краснодар) каждый день появляются новые инновационные идеи. В Германии есть спрос на инновации. Нам нужны «мозги» в этом отношении. Германия – крупнейшая индустриальная держава в Европе, а то и в мире. Но все упирается в «кибербезопасность». Это такие правила игры. К сожалению, с киберсферой связано много плюсов и минусов.

В Германии нет среды частных капиталовложений. Например, у меня есть хорошая идея по «кибербезопасности», я иду в Банк, но они говорят – надо написать бизнес план. А американский инвестор привлекает эти таланты, но по упрощенной системе. И потом у нас появляется американская система. Хочу, чтобы вы правильно меня поняли – мне нравятся мои американские друзья, но в настоящее время они контролируют наши информационные системы, и у нас есть возможность смены американской системы. Но на это все нам необходимо 5–10 лет, чтобы поменять сложившуюся практику, чтобы восстановить свой суверенитет.

Если будете говорить с нашими представителями германских земель, они все будут говорить, что у нас есть монополия – германский Телеком. Но кто поставщик, инвестор, кто является акционерами? США, Китай и Израиль.

Мы говорим о промышленном шпионаже. Это серьезная проблема. Как можно говорить о кибербезопасности в условиях резкого роста промышленного шпионажа и конкуренции. То есть, все упирается в человеческий фак-

тор. 80% наших проблем – это все внутренние проблемы страны. Чтобы не было угрозы кражи информации – необходимо соблюдать «кибергигиену», нужно использовать методы защиты. К примеру, darknet – любой может там заказать, что хочет – различные «инструменты» для обеспечения безопасности или же наоборот. И это большая проблема в том числе. Отсутствие полиции в киберпространстве, правоохранительных органов, криминалистики – нет возможности проводить все расследования, чтобы установить атрибуции. Нет возможности определить, кто этот человек или машина?

Раньше считалось, что промышленным шпионажем занимаются китайские компании, а сейчас нет. Но установить субъекты нет возможности. Очень важно, научиться различать, кто является, условно, нарушителем.

Благодарю гос-на Шерстюка и гос-на Смирнова за создание этого Форума – платформы для развития партнерских отношений! Это и есть причина, почему я здесь.

Все упирается в партнерство. Партнерство частное и государственное. К примеру, взять наших госслужащих: вводятся санкции против России. Но они заинтересованы в сохранении отношений с Россией, поэтому санкции очень расстраивают представителей делового сообщества. Нужно вести диалог с друг другом, наращивать его, несмотря на сегодняшнюю ситуацию.

Далее, поиск талантов. В Сколково представлены яркие и талантливые лица. Мы должны сгенерировать платформы для объединения талантов, чтобы молодежь сотрудничала на базе этих платформ. Мы должны предоставить им такую возможность. Никому не нужны «кибервойны». Перед нами серьезная воз-

Challenges international cybersecurity



Investments new and disruptive innovation



Security by Design



Network of Heads



Synergies data privacy and protection

Cyber-Security Council
Germany

#6

возможность создать «кибербезопасность» еще на уровне разработки какого-либо аппарата. Например, покупка самолета. Мне необходим безопасный взлет и безопасная посадка. То же самое и здесь: необходимы международные нормы, которые регулировали бы, к примеру, этот условный взлет и условную посадку. Нужно уже с самого начального этапа разработки какого-либо продукта закладывать вопросы кибербезопасности.

Мы должны лучше узнать друг друга. Необходимо создать вот этот «красный телефон», чтобы позвонить по нему в случае чего, по вопросу какой-либо атаки (к примеру, Андрей, это была атака со стороны России? Или Франции? Или это может быть Китай с кем-то конкурирует). Вот что важно, понимаете? Необходимо повышать уровень



 We enable trustful cross-sectoral and cross-business cooperation on the national and transnational level with all stakeholders in the area of cyber-security.

info@cybersicherheitsrat.de

www.cybersicherheitsrat.de

[Cybersicherheitsrat](#) [@CSRD](#)



доверия. Без доверия мы ничего не добьемся. Надо восстанавливать деловые и личные контакты.

Спасибо большое за внимание! Я оставляю здесь свои контакты. Мы создаем новую рабочую группу. Это очень интересная идея. На фоне санкций, на фоне политических решений нам нужен год, чтобы согласовать все это... В секторе «кибербезопасности» нужно сотрудничать, и мы рассчитываем на вас, на наших друзей.

За последние 6 месяцев я посетил 37 стран. И все меня поддерживают. Поверьте, Россия является важным игроком в «киберпространстве». У нас есть возможность создать новую ось Европа-Германия-Россия в сфере «кибербезопасности».

Спасибо за внимание!

С.М. Бойко

*Начальник департамента аппарата
Совета Безопасности Российской
Федерации*

Добрый день, уважаемые коллеги!¹

После столь эмоциональных интересных выступлений очень трудно представить какую-то информацию, которая может вас заинтересовать, и тем не менее я постараюсь это сделать. Вы помните мое выступление в прошлом году, я сделаю маленькую ремарочку, я тогда информировал участников форума о тех трех инициативах России, с которыми она вышла на площадку ООН и на другие площадки. Сегодня уже в предыдущих докладах было сказано о том, что две из них получили свой позитивный, положительный результат. Поэтому сам думаю, наверное, я – предвестник того, что потом благополучно реализуется. А, может быть, поэтому та инициатива России, о которой я расскажу сегодня, будет иметь такое же продолжение. На это хотелось бы надеяться, и та аудитория, которая присутствует сегодня в этом зале, все те эксперты, политики, дипломаты поддержат эти подходы, и я надеюсь, что совместными усилиями мы сделаем безопаснее нашу среду.

Но сначала хотелось сказать о более грустном. В последнее время, к сожалению, информация о компьютерных атаках, об их источниках, о новых вызовах и угрозах становится излюбленной темой для средств массовой информации. Такое впечатление, что для них это более излюбленная тема, чем для представителей профессионального экспертного, научного сообщества и деловых кругов, которые сталкиваются с этими угрозами повседневно. Тем не менее, это факт. И в общественном сознании пытаются активно закреплять мнение о том, что главный источник всех этих проблем, конечно же, Российская Федерация. Кто же может быть еще!?

Но, при этом согласитесь, что ни одно из этих обвинений не подтверждается документально, никогда не представляется достоверная техническая информация, все исключительно политизировано, и сопровождается традиционной фразой о большой степени ве-



роятности. К сожалению, мы, эксперты, не можем позволить себе переходить на такой язык и поэтому должны говорить своим профессиональным языком.

Конечно, это СМИ, но в противовес можно говорить о статистике – вещи, очень упрямой. А в последние годы географическое распределение источников компьютерных атак, информацию о которых, эти статистические данные (представляемые зарубежными ведущими компаниями в области информационной безопасности) наглядно указывают на иной, нежели, Россия источник вредоносной активной деятельности, и почему-то этот вектор направлен больше в сторону Запада. Хотелось бы привлечь ваше внимание к следующим двум аспектам.

Первое. Сегодня мы видим, что стремление крупнейших производителей отрасли ИКТ связано зачастую с быстрым выводом на рынок новых продуктов и услуг. Это веление времени. Безусловно, это все приветствуют. Но времени на обстоятельное тестирование безопасности этих продуктов и услуг в условиях нарастающей конкуренции, конкурентной борьбы, на вот эти все вопросы, на вопросы безопасности у этих производителей, как правило, не хватает. Как следствие, в программном и аппаратном обеспечении не выявляется и не предотвращается вот

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

этих всех ошибок, которые, как следствие этой поспешности и игнорирования, превращаются в скрытые уязвимости. По оценкам экспертов, каждая восьмая уязвимость является критической или имеет высокий уровень опасности. Однако, в большинстве случаев производители никакой ответственности за надежность и безопасность свое продукции, как правило, не несут. А общественность уверяется в том, что дополнительные исследования будут сдерживать развитие рынка, что пользователям важнее всего инновации, а безопасность куда-то уходит на задний план. Что мы имеем в результате? А в результате наличие уязвимостей является базой для разработки вредоносного программного обеспечения, а это уже серьезная проблема. Это уже серьезная трансграничная угроза, угроза не только информационной безопасности, но и национальной безопасности наших стран.

Какой первый шаг в связи с этим мы должны сделать?

Какой первый шаг предлагается?

В текущих условиях реальным шагом повышения безопасности пользователей может стать международный запрет на разработку вредоносного программного обеспечения. В России этот шаг уже сделан. Наше национальное законодательство, Уголовный кодекс, уже закрепило, квалифицировало создание вредоносных программ в виде преступного деяния.

Но, почему-то, эта тема ведущими западными странами как-то замалчивается. Особенно, когда дело доходит до выработки на различных международных площадках каких-то конкретных рекомендаций, которые нацелены на криминализацию подобной деятельности, все это активно саботируется и от этой проблематики стараются уйти.

Что за этим стоит? Ну, догадывайтесь сами.

Безусловно, имеется информация, она не является секретной, что зачастую за поставками подобной продукции стоят ведущие мировые державы, которые развивают свой многомиллиардный бизнес и втягивают в него десятки крупных фирм-разработчиков. Потом эта продукция продается, соответственно, узкому кругу клиентов. Какова стоимость вопроса? Ну, вот одна из известных фирм, ну, следуя традиции сегодняшней нашей дискус-

сии, опускаю конкретное название, так вот, за услугу предоставления таких разработок выплачивается порядка 500 000 долл.США ежегодно, при этом средства для эксплуатации оплачиваются отдельно.

И как мы будем считать, каков этот бизнес сейчас?

Но он же смертельно опасен, этот бизнес. Он сопоставим с теми последствиями, которые несет бизнес, связанный с обычными вооружениями. В связи с этим уместно даже вспомнить, что вот это все может попасть не в те руки, на которые мы рассчитываем. А в те руки, которые обернут это все против нас, против каждого из нас, против нашего общества, против наших государств. Вот уместно, наверное, вспомнить слова президента компании «Майкрософт» Брэда Смита о том, что украденные у АНБ данные об уязвимостях ударили по пользователям всего мира. Данные об этих уязвимостях предопределили возникновение глобальных эпидемий: Wanna Cry, NotPetya, Bad Rabbit и других.

Противодействовать этому злу в одиночку – дело бессмысленное!

Глобальная угроза требует глобального ответа! Требуется консолидации усилий! Борьба должна вестись на глобальном уровне, в первую очередь, в правовой плоскости, в криминализации этих преступных деяний. Но мы все понимаем, что эта работа на перспективу, но первый шаг надо делать уже сейчас.

Россия свою позицию по этому вопросу неоднократно уже заявляла. Приведу несколько цифр, связанных с тем, что сейчас основной упор должен быть сделан на противодействие компьютерным атакам. Вот некоторые цифры. В 2018 году средствами российской Государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы было выявлено порядка 4 300 000 000 компьютерных воздействий на различную российскую критическую информационную инфраструктуру. Из этого числа воздействий более 17000 стали опасными компьютерными атаками. Это 2018 год. Не так давно был 2017 год. Сопоставим. Сегодня докладчики говорили, что идет рост подобных воздействий прогрессирующе, так вот соответственно, если мы сопоставим цифры с 2017 годом, то это более 60 и более 70 процентов роста соответственно.

Только на информационную инфраструктуру проводившегося летом прошлого года в России Чемпионата мира по футболу было совершено более 25 000 000 вредоносных воздействий. Для придания противодействию компьютерным атакам системного скоординированного характера Россия сделала шаг в направлении создания в государственной системе Национального координационного центра по компьютерным инцидентам.

Безусловно, эта структура координирует эту работу, делает свои первые шаги, но я надеюсь, что будущее у нее все-таки будет успешным. Центр решает свои задачи и сегодня он взаимодействует с аналогичными структурами, CERTами, из 117 стран мира. Эффективность совместной работы была продемонстрирована уже в 2014 году зимой, когда Сочи принимал зимние Олимпийские игры. Российские специалисты при содействии зарубежных партнеров установили, что центры вредоносной активности, центры управления бот-сетями были расположены на территории Соединенных Штатов Америки, Канады, Тайланда и Малайзии. CERTам этих стран были направлены запросы о принятии необходимых мер для предотвращения функционирования этих центров.

И что я могу сказать? Реакция от партнеров поступила достаточно оперативно. Малайзийский центр ответил уже через 3 часа, принял необходимые меры. Для прекращения функционирования центров управления на территории США и Канады потребовались почти сутки. Но в целом вся эта работа позволила не допустить срыва Олимпийских игр и не повлиять на организацию и проведение отдельных соревнований в рамках Игр.

Для нас, обывателей, с точки зрения просмотра всех репортажей, мы вообще ничего не увидели, но специалисты работали вместе, работали сообща. Вот конкретный результат сотрудничества, к которому мы призываем сегодня с этой трибуны, каждый из докладчиков. Опыт уже есть. Надо отбросить всю политику этой проблематики и уйти в профессиональную плоскость. Результат будет. Это наглядное свидетельство пользы такого взаимодействия.

Однако сегодня надо признавать, что политизация со стороны США и их союзников всех этих процессов сводят усилия профес-

сионального сообщества практически на нет.

Второй аспект, о котором мне хотелось сказать.

В прошлом году я говорил, еще раз напомню, об инициативах, а сегодня я хотел бы сказать еще об одной инициативе, которая в России по линии специальных служб сейчас продвигается на международной арене.

Сегодня международный опыт, российский опыт показывает, что террористы оперативно осваивают и используют современные средства передачи информации. С помощью них они осуществляют связь между собой, связь между пособниками. Ситуация осложняется тем, что приложения для мобильных устройств со стойкой криптографией стали продуктом массового потребления и доступны для скачивания в сети Интернет. Это и мессенджеры, это и почтовые сервисы, средства закрытой голосовой видеосвязи. Все распространяется посредством Интернет и безо всякого контроля пересекает государственные границы.

Все эти проблемы очевидны. Мы прекрасно знаем о примере, когда на запросы о предоставлении ключей шифрования российские службы получали отрицательные ответы. Но это были запросы не ради запросов, это все было направлено на то, чтобы создать безопасную информационную среду. Конечно, когда владелец сервиса Telegram отказался предоставить ключи шифрования, по решению суда этот сервис был заблокирован на территории России. Это, безусловно, создало трудности в работе Telegram, но не решило проблему как таковую.

Системы законного доступа к информации есть у большинства стран, в том числе в Российской Федерации, в странах Европейского Союза, в Соединенных Штатах. Эти вопросы решаются. Но использование стойкой криптографии радикальным образом все меняет. И в результате годами выстроенная система оперативно-технических мероприятий для законного перехвата информации перестает в этих условиях быть эффективной.

Встает перед нами вопрос, как быть? Проблема есть – решения нет!

Возможны различные пути. Например, конечно, можно попытаться достичь соглашения о предоставлении ключей шифрования с каждым производителем приложений для мобильных устройств со стойкой криптографией, но

для большинства стран мира взаимодействие с чужой правовой системой является достаточно проблематичным.

Путь есть, но долгий и достаточно трудоемкий. Но если даже его осилить, то гарантированного результата, наверное, можно и не получить. Значит, необходимы принципиально новые, унифицированные подходы к обеспечению решения этой проблемы. Они должны быть доступны для всех стран. Вне зависимости от того, где зарегистрирован провайдер услуг.

В связи с этим Российская Федерация предложила концепцию инициативы, которая обеспечит всем правоохранительным органам и специальным службам законный доступ к зашифрованной информации.

Какова цель?

Прежде всего, обеспечить общественную безопасность в рамках борьбы с терроризмом и иными противоправными деяниями.

Что необходимо?

А необходимо создать международные правовые условия для реализации процедур депонирования ключей шифрования и доступа к зашифрованной информации. Что дает и что сохраняет российская концепция?

Прежде всего, ключевые принципы, о которых сегодня говорили предыдущие докладчики: соблюдение прав человека, суверенного равенства всех государств, введение унифицированных требований. Реализация должна быть согласована, безусловно, в технологическом плане и использовать действующую инфраструктуру сетей связи.

Однако, учитывая глобальный характер современных сетей связи, реализация предложенного механизма депонирования в рамках одного государства не позволит достичь каких-то ощутимых результатов. Важно, чтобы подобная система была внедрена во многих странах мира. Поэтому, какие этапы решения проблемы предлагаются?

Первое. Необходимо провести широкую дискуссию вокруг этой инициативы. Тогда специалисты могут получить возможность все это проработать, включая технические детали этой реализации.

На втором этапе. Вторым шагом может стать, безусловно, при условии поддержки этой идеи, выработка эффективных и унифицированных механизмов депонирования ключей. Они должны обеспечить сохранение тайны переписки и соблюдение всех базовых принципов законного доступа к информации.

И итоговый шаг – выработка необходимых международных правовых условий внедрения указанных механизмов и процедур доступа к информации.

Россия разработала общий проект концепции необходимых международных актов для реализации предложенного механизма депонирования. Преимуществом предложенного подхода является глобальность, универсальность, защита тайны переписки, информационная безопасность и сохранение суверенитета.

У всех стран мира появляется возможность равноправного доступа к оперативно значимой информации. В условиях нарастающих террористических угроз, вы прекрасно понимаете, – это бесценная информация, которой могут воспользоваться все для того, чтобы противодействовать этой угрозе.

Россия предлагает всем заинтересованным сторонам подключиться к обсуждению представленной инициативы, к разработке условий технических деталей. Все это нацелено на то, чтобы создать стабильное, безопасное информационное пространство и обеспечить равноправное стратегическое партнерство в нем.

Благодарю за внимание!

В.И. Гасумянов

член Президиума Национальной Ассоциации международной информационной безопасности, Старший вице-президент ГМК «Норильский никель», Россия

СТРАТЕГИЧЕСКИЕ НАПРАВЛЕНИЯ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА ПРИ ФОРМИРОВАНИИ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОДХОДЫ КОМПАНИИ «НОРНИКЕЛЬ»¹

Уважаемые коллеги, дорогие друзья!

От имени российской горно-металлургической компании «Норникель» я рад приветствовать участников очередного ежегодного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Особая благодарность сопредседателям Форума и организаторам, которые сохраняют традиции наших встреч в конце апреля на гостеприимной баварской земле. «Норникель» уже 5 лет как присоединился к гармишевскому процессу. Мы постоянно поддерживаем работу Форума и с удовольствием делимся своими подходами и новыми идеями по вопросам формирования системы международной информационной безопасности.

Ведущие российские компании с высоким объемом капитализации – такие, как Норникель, Северсталь, ЛУКОЙЛ, ЕВРАЗ, Сургутнефтегаз, НОВАТЭК, Мечел и др., сегодня составляют весомую часть экономики Российской Федерации и являются важными игроками на мировых отраслевых рынках.

«Норникель» в настоящее время – мировой лидер горно-металлургической промышленности, крупнейший в мире (№1) производитель палладия и никеля; входит в ТОП-5 мировых производителей платины, кобальта и родия. Доля нашей компании на мировом рынке производства высокосортного никеля составляет 22%, а палладия – 40%. В 2018 году объем производства никеля составил 219 тыс. тонн, меди – 474 тыс. тонн, палладия – 2 729 тыс. унций, платины – 653 тыс. унций. Причем в 2018 году ком-



пания производила металлы платиновой группы только из собственного сырья. Наша компания показывает устойчивый рост финансовых показателей: в 2018 году консолидированная выручка увеличилась на 28% и составила 11,7 млрд долл. США. «Норильский никель» занимает важно место в экономике России: доля ГМК в промышленном производстве страны – почти 4%, а в объемах металлургического производства России составляет 12%.

О значимости российского бизнеса в контексте стратегических инициатив нашего государства красноречиво свидетельствуют слова Президента России В.В. Путина: «... бизнес – это непосредственный и важнейший участник реализации национальных проектов, планов инфраструктурного развития».

Такое место в экономике страны и все более активное вовлечение частных компаний в стратегические национальные проекты, возлагает дополнительную ответственность, как на частный бизнес, так и на государство и требует выстраивания эффективного государственно-частного партнерства для решения новых задач.

В условиях формирования новой структуры мирового производства (т.н. «Индустрия 4.0»), на наших глазах совершается четвертая промышленная революция, характеризующаяся коренным преобразованием глобальных

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

цепочек создания стоимости. Формируется новая экономическая реальность, где виртуальные и традиционные система производства гибко взаимодействуют между собой, создавая новые операционные и логистические бизнес-модели.

В условиях четвертой промышленной революции условием сохранения лидирующих позиций на конкурентном рынке для таких крупных компаний, как «Норникель», является инвестирование в развитие IT-инфраструктуры, создание своих цифровых экосистем, малых и средних дочерних структур и даже приобретение небольших инновационных предприятий и стартапов.

В недавнем интервью издательскому дому «Коммерсантъ» президент «Норникеля» Владимир Потанин фактически объявил о начале нового инвестиционного цикла компании, включающего следующие приоритеты:

- повышение эффективности производства;
- экология;
- цифровизация.

Именно на этих трех «китах» будет строиться инвестиционная политика «Норникеля» на ближайшие пять лет. Подчеркну: цифровая экономика – экономика четвертой промышленной революции – является стратегическим направлением нашей деятельности.

Роль и место цифровизации в процессах социально-экономического развития страны неоднократно отмечалась на высшем государственном уровне. По словам Президента России Владимира Владимировича Путина, «цифровая экономика – это не отдельная отрасль, по сути это основа, которая задает новую парадигму развития государства, экономики и всего общества».

При этом Президент особо отметил, что «формирование цифровой экономики – это вопрос национальной безопасности и независимости России, конкурентоспособности отечественных компаний».

О роли государства и бизнеса и особенно в сферах регулирования процессов формирования цифровой экономики говорилось и на встрече Председателя Правительства РФ Д.А. Медведева с главой «Норникеля» В. О. Потаниным, состоявшейся 03 апреля т. г.

Государственный подход к вопросам цифровизации компания «Норникель» полностью разделяет и воспринимает как исходную точку

планирования своих профильных корпоративных стратегий, в том числе, в сфере информационной безопасности и киберзащиты своих объектов и инфраструктур.

«Норникель» развивает свою информационную экосистему как неотъемлемую составную часть национальной IT-инфраструктуры в контексте общего поля государственно-частного партнерства.

Помимо собственно инноваций и внедрения цифровых технологий в производственные процессы, четвертая промышленная революция имеет и другое важнейшее измерение, связанное с социальными вопросами и экологией. В этом заключается, условно говоря, ее «позитивная двойственность».

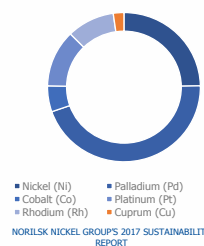
Цифровизация побуждает компании разрабатывать новые операционные модели своей деятельности. Это влечет необходимость постоянного «апдейта» профессиональных навыков работников и корпоративной культуры предприятий в целом. Важнейшим фактором конкурентоспособности становится способность привлекать и удерживать высококвалифицированные кадры. «Норникель» рассматривает инвестиции в человеческий капитал как важнейшую составляющую политики корпоративной социальной ответственности. Но не только. Процессы цифровой трансформации предприятий и инфраструктур дают мультипликаторный эффект, проявляясь не только в производственной, но и социальной сфере.

Конкретный пример: решая задачу создания устойчивых каналов связи между ключевыми площадками Заполярного филиала компании на территории НПР, «Норникель» реализовал проект прокладки волоконно-оптической линии связи (ВОЛС) по линии «Новый Уренгой – Норильск» протяженностью более 900 км. Сумма инвестиций составила около 2,5 млрд руб. В результате население НПР получило доступ к широкополосному интернету и онлайн-сервисам, что позитивно сказывается на уровне развития региона и его инвестиционной привлекательности.

Следующий немаловажный аспект – экология. Конвергенция физической, цифровой и биологической сфер, лежащая в основе четвертой промышленной революции, предоставляет широкие возможности для эффективного и экологичного использования природных ресурсов. Современные инфор-



STATUS AND PERFORMANCE INDICATORS NORILSK NICKEL



NORNICKEL: the share of the Company in the country's industrial production is almost 4%, and in the volume of metallurgical production in Russia is 12%.



2

13TH INTERNATIONAL FORUM "PARTNERSHIP OF THE STATE, BUSINESS AND CIVIL SOCIETY IN ENSURING INTERNATIONAL INFORMATION SECURITY" (APRIL 2019)

мационные технологии могут стать и уже становятся серьезным драйвером для улучшения экологической ситуации и создания экологичного производства – как минимум за счет минимизации бумажного документооборота.

Дабы не быть голословным, приведу цифры: компания «Норникель» намерена инвестировать в экологическое перевооружение своих предприятий порядка 250 млрд. рублей до 2023 года и снизить выбросы вредных веществ в атмосферу на 75%.

Все вышеуказанное будет способствовать формированию регенерируемой и более экологичной экономической системы, включающей в том числе, такие сегменты, как Интернет вещей (IoT) и BigData.

В рамках инвестиционной стратегии в «Норникеле» сейчас существует несколько десятков проектов внедрения цифровых технологий, причем 21 из них уже обсчитан, и подготовлены планы их реализации.

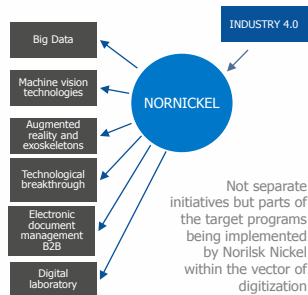
Разрабатываемые нами проекты и подходы по внедрению цифровых технологий в промышленную деятельность, представляют ценность не только для «Норильского никеля» – они потенциально тиражируемы, причем не только в рамках одного промышленного профиля. Можно интегрировать наработки разных отраслей, например, в области контроля качества, сформировать значительное облако. И если клиентские, социальные и прочие маркетинговые данные уже очень глубоко исследованы, то индустриальная практика до сих пор не сформировалась. И это, не говоря о более высоких уровнях применения data science в промышленности – от криптоактивов до решений в области искусственного интеллекта. Сегодня мы ставим перед собой задачу трансформировать то, что есть в «Но-

рильском никеле», в цифровые технологии, сделав компанию более понятной для экономики эпохи четвертой промышленной революции, которая будет судить о предприятиях и продуктах не по сертификатам качества, а по оцифрованным комплексным данным.

Перспективы реализации всех названных выше инвестиционных планов по цифровизации прямо зависят от обеспечения гарантий безопасного, непрерывного и устойчивого функционирования информационной инфраструктуры, на которую эти процессы опираются и информационной безопасности компании в целом.

Значимая роль крупных частных корпораций в экономике страны, их активное участие в реализации стратегических национальных проектов, безусловно, предполагает участие государства в процессах обеспечения их безопасности, включая информационную. С другой стороны, корпоративные активности и стратегии обеспечения информационной безопасности своих активов также отнюдь не изолированы от нормативной и политической деятельности государства в данной области. Предпринимаемые на государственном уровне меры в сфере информационной безопасности нормативно-правового, дипломатического, экономического и пр. характера представляют собой «политико-правовой периметр безопасности» для всех субъектов экономической деятельности вне зависимости от формы собственности.

На этом строится и политика формирования системы международной информационной безопасности (что закреплено в Доктрине информационной безопасности Российской Федерации). При этом особо отмечается фор-



Not separate initiatives but parts of the target programs being implemented by Norilsk Nickel within the vector of digitization



13TH INTERNATIONAL FORUM "PARTNERSHIP OF THE STATE, BUSINESS AND CIVIL SOCIETY IN ENSURING INTERNATIONAL INFORMATION SECURITY" 1 APRIL 2019

6

мат, в рамках которого данные активности представляются нам оптимальными: «в том числе, в рамках государственно-частного партнерства» (Основы государственной политики РФ в области МИБ²).

У «Норильского никеля» есть положительный опыт продвижения стратегических инициатив в области безопасности на международной арене. Особого упоминания заслуживают взаимодействие с МИД РФ, МИД ЮАР и МВД ЮАР в рамках Международной платиновой ассоциации, с МИД РФ и ОБСЕ в процессе продвижения международной Хартии информационной безопасности критических объектов промышленности, с Советом Безопасности России по линии Национальной ассоциации международной информационной безопасности (НАМИБ).

Учитывая тематику нашего форума, вопросы ГЧП в контексте международной информационной безопасности приобретают особое звучание.

На наш взгляд, первоочередными задачами в этой области являются:

- более активное вовлечение представителей компаний промышленного сектора в процессы выстраивания системы безопасности критической информационной инфраструктуры России;
- проведение комплексной экспертизы нормативно-правовых, организационных и технических решений, касающихся возможности реализации суверенного права России на управление национальным информационным пространством.

В недавнем интервью изданию «Известия»

- Active involvement of representatives of the industrial sector companies in the process of building a security system of critical information infrastructure in Russia
- Comprehensive examination of legal, organizational and technical decisions concerning the ability of realization of the sovereign right of Russia to manage national information space



13TH INTERNATIONAL FORUM "PARTNERSHIP OF THE STATE, BUSINESS AND CIVIL SOCIETY IN ENSURING INTERNATIONAL INFORMATION SECURITY" 1 APRIL 2019

9

Секретарь Совета Безопасности России Николай Патрушев отметил: «Необходимо создавать инфраструктуру, позволяющую гарантировать работоспособность Интернет-ресурсов, чтобы наши граждане и предприятия могли пользоваться сетью даже в случае возникновения у отечественных операторов связи проблем с подключением к зарубежным серверам или при целенаправленном масштабном внешнем воздействии».

Решение поставленной задачи, очевидно, требует комплексного подхода, сочетающего помимо нормативно-правовых и технических мер, также и дипломатических шагов. Наши партнеры упорно игнорируют и «забалтывают» предложения России, Китая и ряда других стран по интернационализации управления всемирной сетью, навязывая пресловутый «multystakeholders подход», причем в своей собственной трактовке этого понятия.

Хочу поделиться некоторыми соображениями по возможным направлениям формирования системы обеспечения безопасности, устойчивости и стабильности глобальной сети в русле сложившихся в международных отношениях подходов к обеспечению стратегической безопасности.

Взаимная зависимость государств при принятии решений, так или иначе касающихся проблем безопасности, является одним из столпов современной системы стратегической стабильности. Эта идея лежит в основе современной системы ядерного сдерживания, комплекса договоренностей об ограничении различных видов вооружений, пакетах мер обеспечивающих безопасность воздушного сообщения и морского судоход-

ства и пр. Считаю, что этот же подход может быть взят за основу при формировании системы международной информационной безопасности для обеспечения стабильности, устойчивости и безопасности глобальной информационной инфраструктуры. Для этого предлагается выработать и сформировать пул международно-правовых норм, регламентирующих развитие глобальной информационной инфраструктуры таким образом, что целенаправленное враждебное воздействие на какой-либо из ее национальных сегментов неизбежно влечет неприемлемый ущерб для других сегментов сети. Такие договоренности могут быть двусторонними, многосторонними или глобальными. Конкретный предмет таких договоренностей – это тема для специальных консультаций профильных специалистов.

Хочу обратить внимание еще на один подход при формировании архитектуры международной безопасности. Это стремление разделять взаимосвязанные ключевые компоненты стратегически важных инфраструктур, не допускать монополизации отдельных видов деятельности. Наиболее ярким примером реализации этого подхода являются так называемые энергопакеты Евросоюза в отношении газотранспортных систем. Считаю, что применение этого подхода в отношении глобальной информационной инфраструктуры позволит серьезно повысить доверие к ее устойчивости, стабильности и безопасности со стороны основных суверенных государств. Сегодня на уровне глобального Интернета многие ключевые функции находятся под одной единственной юрисдикцией, а иногда и в ведении одного и того же юридического лица. Например, компания VeriSign, Inc. является не только оператором двух корневых серверов DNS, но также и единственным поставщиком криптографических решений, обеспечивающих безопасность корневой зоны.

Предлагаемые новые идеи, безусловно, требуют предварительной оценки экспертов. Считаю, что координацию данного про-

цесса может взять на себя упомянутая выше Национальная ассоциация международной информационной безопасности, созданная в прошлом году при участии «Норникеля». Крайне полезным представляется использование опыта организации и проведения экспертных консультаций с мировыми мозговыми центрами, имеющийся у Международного исследовательского консорциума информационной безопасности (МИКИБ), членом которого также является наша компания.

Учитывая отраслевую специфику деятельности компании «Норникель», нами подготовлены конкретные предложения по дальнейшей разработке проблематики международной информационной безопасности:

- организация научно-прикладных исследований в сфере кибербезопасности критических инфраструктур промышленных объектов в условиях Арктики (географические и климатические условия, особенности эксплуатации техники и т.д.);
- создание в рамках НАМИБ постоянной контактной рабочей группы по вопросам информационной безопасности в Арктическом регионе с перспективой вынесения темы и предложений на уровень Международного Баренцева секретариата.

Помимо этого, озвученные вопросы могут получить новый импульс к развитию в рамках сотрудничества между «Норникелем» и МИД России. Со своей стороны, мы готовы предложить в качестве одной из площадок для обсуждения этих идей созданный по нашей инициативе клуб «Безопасность информации в промышленности – неформальное объединение руководителей подразделений киберзащиты ведущих российских корпораций индустриального сектора экономики.

В заключение желаю нам всем успешной, плодотворной работы и интересных дискуссий на полях Форума!

Благодарю за внимание!

Б.Н. Мирошников

Член Президиума Национальной Ассоциации международной информационной безопасности, вице-президент ГК «Цитадель»

Уважаемые коллеги!

Информационные технологии – самая быстро развивающаяся отрасль знаний, технологий и экономики. Цифровая экономика – новые рубежи России. В мире те же процессы. Информационное пространство приобретает новые качества. Как следствие – появление новых вызовов и угроз. И как всегда, мы констатируем, что отстаем с реагированием на них.

Прошло уже 20 лет активной борьбы за упорядочение информационного пространства. Множество разных событий как в мире, так и в России:

- исполнилось 20 лет Окинавской хартии,
- 20 лет отметили подразделения по борьбе с преступлениями в сфере высоких технологий (УБПСВТ) в структуре МВД,
- 20 лет как появилась в Уголовном кодексе России 28 Глава о компьютерных преступлениях...

Так что же с преступлениями? Их количество продолжает расти удручающе высокими темпами. Генеральная прокуратура РФ показала 121 тысячу зарегистрированных преступлений, совершенных с помощью информационных технологических сетей или в сфере компьютерной информации, только за период с января по сентябрь 2018 года. И утверждает, что с 17 по 18 год количество таких преступлений удвоилось. Причем, доля киберпреступлений в общем количестве преступлений по стране также удвоилась: с 4,4% до 8,1%. Если посмотреть на статистику МВД в этой области, то данные примерно совпадают. Это – зарегистрированные. А вот расследованных киберпреступлений значительно меньше – 32 тысячи.

Как относиться к статистике? Сдержанно. Истина посередине! Правоохранитель занижает, чтобы продемонстрировать свою эффективность. Жертвы, например, банкиры, у которых хакеры воруют миллиарды, говорят, что у них все хорошо, а деньги клиентов надежно защищены. А производители средств защиты информации, которые смотрят на нас как на рынок, пугают разгулом киберпреступ-



ности и грядущим концом света. Которые неизбежно наступят, если мы не приобретем их программки.

Оставим эти данные для статистиков. Для нашего научного сообщества важно видеть качество процесса. А оно не радует. Вектор киберпреступности направлен вверх на протяжении всех упомянутых двадцати лет. Как количество, так и качество этих преступлений неизменно возрастает, и киберпреступность становится одной из основных угроз человечеству. Вот предмет для научного анализа и осмысления. Ведь усилий предпринимается немало! Документов написано просто огромное количество, много пламенных слов сказано на наших интернациональных трибунах, но они почему-то не работают. Главный и честный вывод, который мы должны сделать сегодня – это поставить себе оценку «неудовлетворительно». Значит, сделали абсолютно недостаточно и меры наши катастрофически запаздывают.

Например, опять же 20 лет назад мы всем научным и профессиональным сообществом констатировали, что анонимность в информационных телекоммуникационных сетях – фактор, поощряющий преступность, как в простых ее формах, так и в самых тяжких. Казалось бы, очевидная вещь. Однако только теперь мы читаем о неких мерах по преодолению анонимности в Сети! Ждали 20 лет! Примеров этого запоздалого прозрения много. Увы нам!

Рост глобальных проблем в киберпространстве отражает необходимость такого же глобального реагирования. Однако его нет. Границы на земле и границы в киберпространстве – разные вещи. Там сталкиваются юрисдикции различных государств, и расследование трансграничных преступлений делается абсолютно невозможным. Это действительно сфера приложения сил и знаний для юристов, правоведов и практиков наших стран – создание соответствующих международных механизмов, обеспечивающих легальную борьбу с высокотехнологичными преступлениями в глобальном масштабе. Это ровно то, чего сегодня ожидают тысячи киберполицейских во всем мире.

Опыт создания таких документов у нас есть. Как положительный, так и не очень. Например, известная Будапештская конвенция по борьбе с киберпреступностью 2001 года. Россия к ней не присоединилась. Но для стран, не имевших на тот период времени статей в своих уголовных кодексах о киберпреступлениях, она была даже полезна. Но на этом ее прогрессивная роль быстро закончилась.

Несмотря на бесполезность Будапештской конвенции, за эти годы мы приобрели практический и бесценный опыт взаимодействия с коллегами из различных стран в расследовании компьютерных преступлений, имевших трансграничный характер. Примеров – достаточно большое количество, чтобы их изучать, выделять положительное. (С Германией, Великобританией, Францией, Бельгией и так далее и так далее...). Но главное – выявлять наши ошибки и давать конструктивные

рекомендации правоохранительным органам и создателям как национальных, так и интернациональных законов.

Обратите внимание – разговор о борьбе с киберпреступностью часто ограничивается разговором о средствах защиты от атак, от вирусов, от утечки данных и т.д. То есть строим высокие заборы из программных средств защиты. Но они часто только возбуждают преступников и поощряют их на разработку все более совершенных средств атаки. И совсем мало в приведенной статистике данных о задержаниях собственно преступников. А «вор должен сидеть в тюрьме»!

Мы не должны и не можем равнодушно наблюдать, как активно развивается новое направление удара для киберпреступности – удара по финансово-банковской сфере. Как умело используют хакеры все достижения новых технологий и сервисов в ИТКС. И как умело и грамотно они используют недостатки нашего правосудия и взаимодействия. Как миллионами утекают в преступную среду персональные данные граждан планеты, чтобы потом стать основой для огромного количества мошеннических действий и других преступлений.

Ответ на наши вопросы содержится, по моему глубокому убеждению в двух словах – доверие и взаимодействие. Это то, что должно быть предметом глубокой, заинтересованной и профессиональной дискуссии на нашем Форуме. Предложений и идей много. И это наш долг перед гражданами планеты.

Спасибо за внимание!

Дэвид Конрад

Старший вице-президент, главный технический директор ICANN

Вени Марковски,

вице-президент ICANN

Спасибо за предоставленную возможность выступить. Я во второй раз участвую в работе Форума в Гармиш-Партенкирхене. Это очень интересные доклады, различные точки зрения, различные подходы. Я представитель ICANN (*Internet Corporation for Assigned Names and Numbers – Корпорация по управлению доменными именами и IP-адресами – ред.*), директор по техническим вопросам. Нашу корпорацию интересуют многие из рассматриваемых здесь, в Гармиш-Партенкирхене, проблем. В своем докладе я сосредоточусь на нормах, которые обсуждаются на различных площадках.

Цель моей презентации – дать вам представление о том, что мы рассматриваем кибернормы в контексте деятельности ICANN. Как вы, наверное, знаете, ICANN не контролирует Интернет, у нас достаточно ограниченная техническая функция координации, идентификации, которая используется в системе доменных имен, адресов и параметров, протоколов.

Главная задача корпорации – обеспечить функционирование системы индивидуальных идентификаторов и Интернета. Поэтому мы хотим разобраться, какие угрозы существуют для этой системы, и объяснить всему миру, различным государствам, какую роль играет ICANN в этом процессе.

Представители корпорации участвуют в работе Форума в Гармиш-Партенкирхене, начиная с первой конференции. Это хорошая площадка для взаимодействия по вопросам киберполитики и кибербезопасности. Наша задача объяснить то, чем мы занимаемся, то, чем мы не занимаемся, и предоставить подтверждающую это соответствующую информацию.

Кибернормы – это очень актуальная тема. Можно найти огромное количество норм, их формулировок. Есть хорошие веб-сайты, например, Фонда Карнеги, которые позволяют представить различные кибернормы, признанные в различных государствах. Главное в них: сами не совершайте преступлений и не



позволяйте другим использовать ваши системы для совершения этих преступлений.

В качестве примера хотел бы привести кибернормы, разработанные Глобальной комиссией по стабильности киберпространства. Использую этот пример, потому что эта Комиссия очень подробно рассмотрела нормы с точки зрения оператора, какие нормы будут применяться и что они будут обозначать. Кибернормы направлены на защиту публичной части Интернета, его основной части.

Как вы знаете, в настоящее время часто совершаются атаки на инфраструктуру системы доменных имен. Это достаточно эффективные атаки. Насколько я знаю, среди участников Форума много технических специалистов и они понимают, как работает эта система. Но чтобы всем было понятно, система DNS (*Domain Name System – система доменных имен – ред.*) – это система перевода имен, используемых людьми, в номера и цифровые обозначения, которые используются в Интернете. В рамках иерархической структуры существует один корень на каждое именное пространство. ICANN управляет этой системой. В системе 1 300 доменов высшего уровня, это коды стран, общие коды. Ниже – следующий уровень, это 350 миллионов доменов второго уровня.

Теоретически можно дойти до 120 уровней, но обычно ограничиваются пятью уровнями. В каждом уровне делегируется кон-

троль. Например, IBM контролирует `ibm.dod.com`. Эта архитектура обозначает, что если вы скомпрометировали узел, то все узлы нижних уровней тоже будут скомпрометированы, взломаны аналогичным образом. Это важно, потому что преступники пользуются этим в атаках на инфраструктуру системы доменных имен.

Такова в целом общая схема взаимоотношений в мире ICANN. Важно отметить, что существуют регистраторы, к которым обращаются лица, желающие приобрести домены или изменить какую-то информацию, связанную с системой доменных имен. Эти регистраторы продают доменные имена (как я уже сказал, есть 1 300 доменных имен). Есть интернет-коды (интернет-домены) стран мира, которые не подпадают под правила регулирования. Это домены высшего уровня – домены стран. В отношении них ICANN не является регулятором, но имеет контрактные обязательства по координации. Однако эти домены не подпадают под юрисдикцию ICANN.

Поскольку общие домены высшего уровня связаны контрактными обязательствами, корпорация может влиять на упомянутые контрактные обязательства. Если они не соблюдаются, то это может рассматриваться как нарушение контракта, и в худшем случае контракт может быть расторгнут, и тогда домен переводится другому пользователю.

Сама система DNS состоит из двух частей. Первая называется Lookup, ею занимаются провайдеры от имени пользователей, и вторая – публикация. Это и регистраторы, и реестры, публикация доменных имен и соответствующей информации в Интернете. Это сложная схема. Она показывает, что происходит каждый раз, когда вы смотрите имя в DNS. Это происходит сотни, тысячи раз на странице. Количество запросов DNS высшего уровня достигает триллиона в день.

Это исходная информация. Что касается конкретных атак, то недавно была опубликована информация о так называемой атаке «Морской черепахи». Это шпионаж в отношении DNS, то есть атака, в которой используется доверие к интернет-услугам, включая DNS. Она направлена на общественные и частные структуры. Сейчас это происходит в основном на Ближнем Востоке и на севере Африки и

осуществляется через спонсоров. В этом контексте следует признать, что атрибуция, конечно, сложная проблема. Но есть признаки, свидетельствующие о том, что эти действия связаны с государственными спонсорами, особенно с государством, которое заинтересовано в проблемах войны в Сирии. Это происходит давно, и все показатели свидетельствуют о том, что эти действия берут свое начало в январе 2017 года и продолжаются до сегодняшнего дня.

ICANN вовлечен в этот процесс, потому что некоторые домены потребовали изменений, поскольку серверы были взломаны. В результате мы начали создавать консультационные группы, связанные с этой конкретной атакой. Группы пытаются снизить последствия этой атаки, по крайней мере те, которые касаются доменов высшего уровня. Мы знаем, что 4 домена высшего уровня еще взломаны, а это значит, что все домены на низших уровнях тоже могут быть объектом взлома.

Как мы считаем, есть образования, которые были скомпрометированы. Так, компания Groups online провела интересный анализ конкретной атаки, согласно которому основная часть объектов нападения – это и коммерческие предприятия, частные, и объекты инфраструктуры, включая государственные объекты, и гражданская авиация, и правоохранительные органы. Ресурсы, связанные с этими образованиями, с этими объектами нападения, находились под контролем атакующего. Это значит, что в некоторых случаях, когда, например, сервер государственной почты был скомпрометирован атакующим, этот нападавший имел доступ к данным для проведения своей атаки.

Есть еще одна методика. Например, некоторые такие вводные точки, по крайней мере, это делается через `petsheer.org`. Атакующий отправил почту, которая выглядела письмом, а жертва подумала, что все нормально, после чего включала attachment (вложение), и, как следствие, запустился вирус. В результате агрегировалось все хозяйство. Атакующий по возможности получал доступ к регистру DNS через регистратора, то есть получал данный доступ через регистратора и выходил на домены, связанные и ассоциированные с жертвой нападения. После чего нападавшие посылали апдейт (*обновление баз данных поисковых си-*

стем – ред.) через систему, чтобы доменные сервера были перенаправлены на тот сервер, который находился под контролем атакующего. Таким образом атакующий брал под контроль, и входящее сообщение позволяло ему брать необходимую информацию от любого лица, который пытался бы установить ссылку на этот веб-сайт.

Например, почтовый сервер для государственной структуры каждый раз, когда туда хотел бы залогиниться (*войти в систему, программу в качестве зарегистрированного пользователя – ред.*), он тогда сразу входил на тот почтовый сервер, который находился под управлением атакующего. И жертва даже не знала, что загружается, что данные ее доступа были отданы атакующему, что эти данные доступа были связаны с государственным ресурсом. Это было не видно для жертвы.

Как это отражается на нормах против подобных нарушений? Складывается впечатление, что перед нами игрок, который связан с государством и имеет возможность пользоваться государственными ресурсами.

Как определяются вот эти нормы? GCT разработала основные нормы поведения в Интернете, они, конечно, не носят обязывающий характер. Более того, эта работа еще не завершена и сейчас продолжается, и далеко не все, насколько я знаю, поддерживали эти нормы. Они указывают на то, насколько эти нормы могут быть реализованы.

Давайте обратимся к другим формам атак. Против маршрутизаторов, против инфраструктуры маршрутизации. Вы знаете, что любой прибор, любой гаджет должен иметь уникальный IP-адрес, связанный с этим прибором. Это те же цифры, на которые переводит имя система DNS. Они предоставляются провайдерами, но организация может обратиться к любому из пяти регистраторов. Это географические монополии, в Европе, например, это NPC (*Network Parameter Control – ред.*), это региональный регистратор, который имеет блок адресного пространства.

Провайдеры между собой взаимодействуют и используют для этой горизонтальной связи различные протоколы. К примеру, допустим, поступает информация, что мы не будем получать доступ к деньгам, а только к информации, и что все происходит нормально. Вот эти провайдеры управляют объектами, кото-

рые далеко не всегда централизованы, они распределены через этих провайдеров, которые договариваются между собой об обмене информацией о маршрутизации.

В этой связи важно отметить, что система маршрутизации основана на доверии по следующему принципу. Я доверяю тебе, что ты мне дашь тот трафик, который у тебя в сети создан и происходит. В то же время я буду информировать тебя о том, что у меня происходит и поступает к тебе в сеть. То есть это деловые отношения на основе доверия между этими провайдерами доступа к Интернету.

К чему это приводит? Получается такая прямая система, которую очень легко подвергнуть взлому со стороны хакеров, захватить и поставить под свой контроль. В рамках этой системы любой провайдер может оказаться жертвой, и тогда вся система тоже становится объектом такого взлома. Атакующий имеет возможность получить доступ к информации, ее маршрутизации и направить (переадресовать) ее в нужном для себя направлении. При этом это не будет видно для самих провайдеров. Так часто происходит. В 2017 году было 14 тысяч таких инцидентов, связанных с захватом маршрутизации. Большинство из них были случайными, не злонамеренными, не вредоносными, и в результате трафик просто был переадресован. Но на это также следует обратить внимание экспертам.

В 2008 году правительство Пакистана случайно заблокировало YouTube через некоторые видеоматериалы, случайно позволили проанонсировать тот факт, что они пытались контролировать YouTube через один из своих провайдеров. Эта информация была опубликована во всем мире, и несколько дней YouTube «висел», хотя был заблокирован в Пакистане случайно, без злого умысла.

Однако, некоторые подобные проявления, как нам представляется, были не случайными, когда трафик действительно был переадресован сознательно, как, допустим, из США в Китай. Были некоторые утверждения, что это было сделано преднамеренно. Также был случай, когда сервер Rutor оказался под воздействием со стороны Китая, но проявился только в некоторых странах, как например, в Чили. То есть получалось, что Чили, если отслеживать этот маршрутизатор, был связан

с китайскими маршрутизаторами. Поэтому важно отслеживать эту динамику.

В этом случае были нарушены конкретные нормы, которые направлены на защиту ядра Интернета против таких атак, о которых мы говорим. Но следует признать, что они происходят также достаточно регулярно.

В заключение отмечу, что атаки, нападения на публичное ядро Интернета все больше рассматриваются под углом их совершения государствами, а не частными хакерами. И это связано не с тем, что я должен больше обратить на это внимание, чем другим случаям. Это связано с влиянием на лежащую в этой основе структуру, на которой базируется Интернет.

Эта структура в значительной степени зависит от доверия, которое может быть подорвано. Ни один из методов, которые использовались при этих атаках, не является новым,

нет никакой новой технологии, новации здесь. Но при этом важно отметить следующее. Такие масштабные атаки на Ближнем Востоке уже два года нацелены на одну из стран как на уровне доменов высокого уровня, так и среднего уровня.

Также мы наблюдаем, что раутинговые атаки в значительной степени используются для переадресации больших объемов трафика и не понятно, происходит это преднамеренно или случайно.

Складывается впечатление, что есть общее согласие относительно того, что эти атаки действительно являются угрозой для стабильности Интернета в глобальных масштабах, и меры, направленные на противодействие таким попыткам, пока еще не очень успешны.

Поэтому защита ядра Интернета приобретает все большую важность и значимость.

С.В. Лебедь

Руководитель службы информационной безопасности Сбербанка России

ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ ГЛОБАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Добрый день, уважаемые коллеги!

Основная цель моего доклада – пригласить вас на Второй Международный конгресс по кибербезопасности, который организует Сбербанк России и который состоится в этом году в Москве.

В рамках своего доклада хотел бы рассказать об итогах прошлогоднего, первого, конгресса, состоявшегося в июле 2018 года, а также поделиться некоторыми идеями. Надеюсь, что они смогут вас заинтересовать, и вы примите в этом году участие в форуме.

Я впервые на конференции в Гармиш-Партенкирхене и надеюсь, что те идеи, те решения, которые здесь обсуждаются, найдут свою реализацию, и это позволит сделать более счастливыми и более безопасными наших граждан, наш бизнес, наш мир.

Конечно, упомянутую дискуссионную площадку Сбербанк России, который я представляю, мы также рассматриваем, как площадку для коллаборации, которая позволит решать любые вопросы, связанные с глобальными проблемами кибербезопасности.

Что касается прошлогоднего конгресса, то на его площадке собрались представители 51 страны, более 600 организаций, всего – свыше 2 500 участников. В рамках форума свои мероприятия провели Центр безопасности Всемирного экономического форума, а также состоялась сессия Глобального комплекса инноваций Интерпола. Отмечу, что в работе конгресса принял участие Президент Российской Федерации В.В. Путин.

Партнерами конгресса стали известные компании – лидеры IT-сферы и кибербезопасности, представившие свои стенды и доклады и удивившие участников форума своими новыми решениями, прежде всего, техническими разработками.

По итогам работы мы проанализировали предложения докладчиков и всех выступивших участников, а также результаты состоявшихся на площадках форума дискуссий и сделали выводы. Отчасти эти выводы сегодня сделали

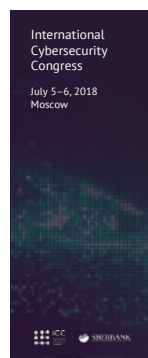


предыдущие выступающие, представившие анализ проблем кибербезопасности в мире. Постараюсь поделиться своими выводами.

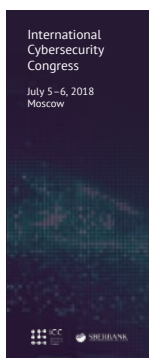
Итак, основной вывод – потери мировой экономики и, в частности России, продолжают расти. Несмотря на все меры, которые мы предпринимаем, несмотря на все решения, которые предлагаются, мир не становится безопасней. Необходимо признать, что технологии кибербезопасности и методы защиты отстают, по разным оценкам, а по оценке Сбербанк России – на 2–5 лет, от IT-технологий. Поэтому мы постоянно находимся в роли догоняющих. И, как только мы создаем новые способы и методы, законы, мошенники, киберпреступники находят новые инструменты, как обойти защитные механизмы.

Глобальная проблема – это дефицит кадров. По прогнозу мировых экспертов, в 2022 году дефицит специалистов будет составлять около двух миллионов человек.

Следующий вывод, который достаточно очевиден, и сегодня он неоднократно звучал – существование двух категорий: мошенников или киберпреступников, а также тех, кто совершает противоправные действия в Интернете. Это государственные структуры с применением своих кибервойск, киберподразделений, и организованные преступные группы. И те, и другие представляют, безусловно, большую опасность для цифрового мира. Для банковской отрасли, в первую



ICC partners in 2018:



A unique platform for international collaboration to address current digital threats and improve global cyber resilience.



51 countries



681 organizations



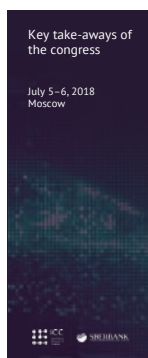
2,500+ participants

Attended by the President of the Russian Federation Vladimir Putin

WORLD ECONOMIC FORUM WEF Centre for Cybersecurity session

Large-scale global cyber exercise

INTERPOL Global Complex for Innovations session



Key take-aways of the congress



Unprecedented losses in 2017: \$1 trillion globally ~650 bn, rub Russia



Most cyberattacks are carried out by organized cybergangs and are aimed at money theft



Cybersecurity is 2-5 years behind new technologies



Criminal groups feel impunity



1.8 mn global shortage of cybersecurity talents by 2022



Low level of global collaboration Lack of platforms for an open international dialogue

очередь, проблему представляют организованные преступные группы. И часто они чувствуют себя безнаказанными. Об этом сегодня уже упоминалось. Мы много работаем, но возможности правоохранительных органов пока ограничены.

Важный вывод – уровень коллаборации. На сегодняшний день мир технически настолько сложный, что просто принятие каких-то технических мер, применение средств защиты не позволяет решать проблему обеспечения кибербезопасности.

Представляя базовую архитектуру предстоящего Второго Международного конгресса по кибербезопасности, отмечу, что это не только два дня непосредственно самой конференции, это целая неделя, которую мы называем Global Cyber Week (*Глобальная кибернеделя – ред.*). Начнется она с традиционных для технических специалистов компьютерных соревнований, так называемых CTF (*Capture the Flag – масштабные соревнования по этичному хакингу – ред.*). Это не первое мероприятие, которое проводит дочерняя компания Сбербанка России – BI.ZONE.

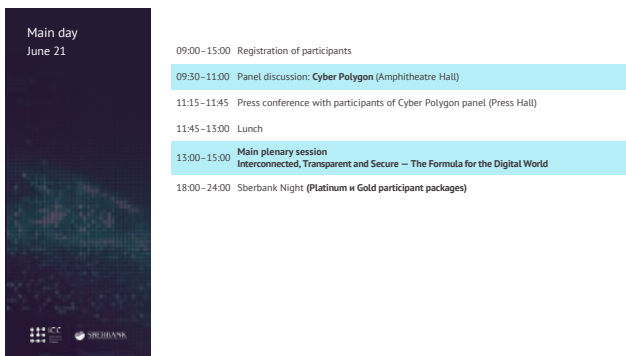
Мы спланировали мероприятия в рамках одной недели, чтобы конференция стала интересной не только для специалистов со стажем, но и для молодых специалистов, как мы их называем «белых хакеров», которые горят желанием проявить свои знания и способности в области защиты, в области анализа защищенности.

19 июня 2019 года состоится глобальный тренинг, посвященный организации взаимодействия глобальных корпораций в условиях единой угрозы. Напомню, в 2018 году мы проводили такой тренинг на примере Сбербанка, отрабатывали массовое вирусное заражение на его инфраструктуре и демонстрировали наряду с вопросами коллаборации организацию применения лучших практик и самых современных средств защиты, позволяющих локализовать достаточно актуальную на сегодняшний день проблему, связанную с глобальным выходом из строя IT-инфраструктуры.

20–21 июня состоятся основные мероприятия. В первый день – панельные дискуссии, а также тематические сессии. Откроет конференцию панельная дискуссия «Дорога в киберустойчивый мир – дорога вместе?» Это установочная панельная дискуссия, в рамках которой планируется сконцентрироваться на тех вопросах, которые представляют наибольший интерес с учетом сегодняшних реалий.

После панельной дискуссии планируется пять параллельных панельных дискуссий. Это – «Национальная безопасность», «Финансовая индустрия», «Критическая инфраструктура», «Прорывные технологии» и, конечно, «Телекоммуникации».

Эти направления выбраны в связи с тем, что это наиболее острые проблемы, связанные с ними направления регулирования и от-



расли, которые наиболее подвержены сегодняшним проблемам кибербезопасности.

Далее запланированы несколько потоков технических сессий, ожидается порядка пяти параллельных сессий.

Первое направление – «Capacity building» (*Наращивание потенциала – ред.*), это построение современных средств защиты.

Второе – «Legal envaiment» (*Правовая среда – ред.*), это правовое регулирование.

Третье направление – «Threat intelligence» – это управление угрозами.

Четвертое – «Disruptive technologies» – прорывные технологии.

И, наконец, пятое направление – «Investments in cybersecurity» – инвестиции в кибербезопасность. Сегодня уже отмечалось, что есть огромная проблема, связанная с разработкой и развитием новых технологий, продуктов, методов защиты. В России также есть такая проблема, однако у нашей молодежи существует огромный потенциал. Нужно помочь молодым людям найти себя, реализовать свои возможности. Этим и обусловлено наличие в этом году такой

сессии. Планируется пригласить лучших специалистов-инвесторов в области кибербезопасности, чтобы они поделились опытом и предложили участникам конгресса собственные механизмы реализации своих идей.

Основной день конгресса, 21 июня (пятница), откроется панельной дискуссией «Cyber Polygon – summarizing the results» (*Киберполигон – подведение итогов – ред.*), на которой будут подведены итоги соревнований, которые пройдут в среду. Замысел и состав участников этого глобального тренинга остается в тайне, чтобы сохранить некую интригу и привлечь больше внимания.

И, наконец, основная панельная сессия – «Secure digital world – possible future or wishful utopia?» (*Безопасный цифровой мир – будущее или утопия? – ред.*), на которой будут подведены итоги Конгресса и обсуждены наиболее острые вопросы.

Таковы наши планы. Приглашаем вас принять участие в Международном конгрессе по кибербезопасности, который состоится в июне 2019 года в Москве.

Чарльз Барри

Независимый эксперт (США)

Профессор Шерстюк, уважаемые коллеги, очень приятно снова быть на форуме в Гармиш-Партенкирхене.

Меня попросили высказать несколько тезисов, поэтому хочу дать с точки зрения американского ученого оценку Гармишевскому процессу, как он нам представляется.

Какова же польза нашего тринадцатилетнего, а в моем случае – десятилетнего, участия в форуме? Что мы получаем в результате мероприятий в Гармиш-Партенкирхене? Если подумать, поразмышлять, вспомнить повестку дня, программы, которые мы разрабатывали совместно, то можно прийти к выводу, что от нашего диалога уже есть огромная польза, но и в будущем предстоит сделать еще очень и очень много.

Программа форума хорошо проработана, сориентирована на углубленное рассмотрение таких вопросов, как предотвращение конфликтов, защита критической инфраструктуры. В тоже время повестка дня достаточно широкая. Здесь представлены для обсуждения вопросы безопасности технических систем, экономическая кибербезопасность. Эти широкие вопросы заставляют нас заглянуть за горизонты наших привычных вопросов и проблем. Поэтому форум – это очень хорошее интеллектуальное упражнение для нас.

Следует признать тот факт, что то, что происходит в Гармише, не остается только в Гармише. Мы должны понять, что многое из того, что мы здесь делаем, затем распространяется, находит свое применение. На форуме в основном представлено научное сообщество, но есть и представители официальных структур, как это мы видим сегодня, как это происходит ежегодно. Я имею ввиду представителей Российской Федерации из различных органов государственного управления. Но в основном мы – ученые и поэтому можем свободно общаться друг с другом, чем и занимаемся в течение этих лет. В рамках этой дискуссии, в рамках такого диалога мы выстраиваем фундамент доверия, а доверие и прозрачность – это ключевые условия успеха и ключевые результаты нашей работы в течение многих лет.



Очень важно, что сегодня мы обсуждаем в Гармиш-Партенкирхене вопросы информационной безопасности, кибербезопасности. Но при этом понимаем общий широкий контекст проблемы, который характеризуется высокой степенью напряженности, отсутствием доверия, отсутствием прозрачности. Это надо преодолевать, и площадка форума – одна из немногих площадок, где представители различных стран, в частности, США, Российской Федерации, Китая, общаются, откровенно обмениваются взглядами по многим вопросам.

Иногда нас называют Давосом в области кибербезопасности. Действительно, Давос и Гармиш-Партенкирхен – прекрасные места для того, чтобы обсуждать, размышлять, общаться. И можно утверждать, что сегодня кибербезопасность, наряду с экономикой, является глобальной проблемой, вызывающей обеспокоенность людей. И мы должны постараться улучшить ситуацию в этой сфере. У нас нет пока представителей глав государств, но пока только понедельник, может быть кто-то появится. Это – шутка, но если серьезно, то форум в Гармиш-Партенкирхене – это фактически важный пример международного диалога. Мы должны это понимать.

И последнее. Какую еще пользу приносит форум? Мы должны хорошо конспектировать, констатировать то, что здесь обсуждается, и постараться донести эту информацию до наших столиц. Несколько лет назад

уже была достигнута договоренность, что надо обязательно доносить информацию о состоявшихся на форуме дискуссиях до политиков с тем, чтобы они ее учитывали. Надеюсь, что мы будем этим заниматься по возвращении домой.

Теперь – о будущем. Каково будущее, каковы перспективы? Мы обменивались взглядами, может стоит подумать о сотрудничестве в том, как найти те сферы, где у нас есть согласие, и представить эти точки соприкосновения на рассмотрение руководству. И сделать следующий шаг: не только обмениваться информацией, но и на этой основе разработать нечто, что помогло бы противодействовать киберпреступности и продвигать вопросы кодекса поведения.

И мы не должны отчаиваться. То, что происходит здесь, в Гармиш-Партенкирхене, в рамках Института «Восток – Запад», публикации статей, разработка определений. Также работа Джона Мэллори – инициатора разработок в военной области. Все это тоже отражает результаты нашей деятельности. И весь широкий спектр вопросов обсуждается здесь, на форуме.

Однако мы должны понимать, что киберсфера – это достаточно новая сфера, поскольку после возникновения коммерческого Интернета прошло всего лишь 40 лет. Это короткий период времени.

Когда возникли морские флоты в XIX веке, было всего лишь несколько договоров. Поз-

же была создана Всемирная морская организация, и большинство стран присоединились к Конвенции по морскому праву. Но на это ушло много времени.

То же самое касается воздушного транспорта. Сначала не могли договориться, потом в 1947 году была создана организация ICAO (*International Civil Aviation Organization – международная ассоциация, специализированное учреждение ООН, устанавливающее международные нормы гражданской авиации и координирующее ее развитие с целью повышения безопасности и эффективности – ред.*), и все страны стали ее членами.

Космическое пространство, 1967 год, у нас был заключен договор (*Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела, от 27 января 1967 года – ред.*), есть несколько других договоров. 50 лет – это не большой период.

Пока нет такой единой организации, которая бы разрабатывала бы соответствующие нормы и стандарты, даже в космосе пока такого нет, а в киберсфере – мы тем более еще очень молоды. Поэтому я призываю сегодня и в течение трех следующих дней работать над этим.

Благодарю за предоставленную мне возможность высказать точку зрения американца.

СЕМИНАР–КРУГЛЫЙ СТОЛ № 1 О ДЕЯТЕЛЬНОСТИ МЕЖДУНАРОДНОГО ИССЛЕДОВАТЕЛЬСКОГО КОНСОРЦИУМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (МИКИБ)

Ведущие:

Шерстюк В.П., Руководитель-организатор МИКИБ, Президент Национальной Ассоциации международной информационной безопасности

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

Энекен Тикк (Eneken Tikk) независимый эксперт, Эстония

А.А. Стрельцов

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

ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ

1. В соответствии с решением Международного исследовательского консорциума информационной безопасности, принятым в апреле 2018 г. в г. Гармиш-Партенкирхен, была поддержана инициатива группы экспертов, представляющих организации Консорциума, по осуществлению совместного исследовательского проекта. В рамках проекта было предложено изучить проблемы практической реализации норм, правил и принципов ответственного поведения государств в ИКТ-среде, содержащихся в Докладе Группы правительственных экспертов ООН по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности (2015 г.)¹.

Актуальность изучения данной проблемы в настоящее время обусловлена, в частности, сохраняющимся вниманием к рекомендациям по нормам, правилам и принципам, изложенным в данном Докладе, со стороны Генеральной Ассамблеи ООН. Так, на 73-ей сессии Генеральной Ассамблеи ООН приняты решения о созыве двух групп: рабочей группы открытого состава, которая будет иметь в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств и путей их реализации²;

Группы правительственных экспертов на основе справедливого географического распределения, которая продолжит исследования возможных совместных мер по устранению существующих и потенциальных угроз в сфере информационной безопасности, в том числе исследование норм, правил и принципов ответственного поведения государств.

При этом Генеральная Ассамблея ООН исходит из того, что регулирование международных



отношений в ИКТ-среде должно осуществляться на основе международного права. Однако, как показывает опыт, несмотря на возрастающее количество инцидентов в ИКТ-среде, вызывающих международные споры, в практической деятельности государств международное право практически не применяется. Так, пока не отмечено случаев применения указанных в Уставе ООН мирных средств разрешения споров³, а также других средств предотвращения нарушения международного мира и безопасности⁴.

2. Совестный исследовательский проект, выполненный группой экспертов, направлен на изучение методических вопросов применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

В реализации проекта приняли участие эксперты из Института проблем информационной безопасности Московского государственного университета имени М.В. Ломоносова и Национальной ассоциации международной информационной безопасности (Российская Федерация), Института Восток-Запад (США), Института киберполитики (Эстония) и Фонда «ИКТ для мира» (Швейцария). К сожалению, по техническим причинам на последней стадии

¹ A/70/174

² Резолюция Генеральной Ассамблеи ООН. A/73/27

³ Ст. 33 п.1, Устав ООН.

⁴ Ст. 34, Устав ООН; Ст. 36 п.2. Статут Международного Суда.

- Методические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды (Рез. ГА ООН A/70/174)
- Methodical questions of applying of norms, rules and the principles of responsible behavior of the states, urged to promote providing open, safe, stable, available and peace ICT-sphere (Res GA UN A/70/174)

Проект The project

выполнения проекта из него вышли эксперты Центра киберправа Институт Каре (Корея).

В качестве объекта изучения были выбраны следующие три рекомендации, содержащиеся в п.13 Доклада Группы правительственных экспертов ООН (2015 г.):

(g), «государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции»;

(h), «государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета»;

(k), «государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности».

Исследование выделенных норм, правил и принципов ответственного поведения госу-

- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

Paragraph 13 (h) of the UN GGE 2015 report

дарств было направлено на выявление возможных путей улучшения понимания проблем в правовом регулировании международных отношений в ИКТ-среде и обсуждение возможных путей развития норм, правил и принципов ответственного поведения государств, а также норм и принципов международного права, создающих условия для правового регулирования рассматриваемых отношений в ИКТ-среде.

3. Методология исследования базировалась на следующих предположениях.

Во-первых, применение международного права государствами основывается в том числе и на: суверенитете государств; одинаковом понимании государствами их международных обязательств, вытекающих из международных конвенций, международных обычаев и общих принципов права; юридической надежности фактов нарушения международных обязательств, наблюдаемых уполномоченными органами государств. При этом территория, на которую распространяется суверенитет государств, образуется совокупностью естественных физических сред, включающих сушу с ее недрами, водную территорию (внутренние воды и территориальное море государства), а также воздушное пространство. Территория государства имеет признанные другими государствами границы.

Во-вторых, ИКТ-среда, в отличие от традиционных пространств международных отношений, обладает свойствами: глобальности ИКТ-среды, обусловленной поддержанием ее функционирования гражданами и организациями, действующими в различных юрисдикциях; искусственности, обусловленной техническим характером ИКТ-среды. Данная среда образуется совокупностью вычислительных и коммуникационных устройств, систем и сетей, функционирующих на основе глобальной системы цифровых идентификаторов и многоуровневой системы открытых протоколов взаимодействия составляющих этих устройств

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Paragraph 13 (k) of the UN GGE 2015 Report

- 1. НАМИБ, ИПИБ МГУ (РФ) - NAIPS, ISI MSU (RF)
- 2. Институт Восток-Запад (США) - Institute "East-West" (USA)
- 3. Институт киберполитики (Эстония) - Institute cyberpolicy (Estonia)
- 4. Центр киберправа Университета Корё (Республика Корея) - Center of cyberlaw, Korea University (RK) – (вышел из проекта - go off from the project)
- 5. Фонд «ИКТ для мира», Швейцария - ICT4Peace Foundation (Switzerland)

Участники The participants

и систем, а также ИКТ, автоматизирующих информационную деятельность субъектов общественной жизни.

В-третьих, в настоящее время отсутствуют универсальные международные договоры, непосредственно направленные на регулирование международных отношений в области использования ИКТ государствами и обеспечение международной информационной безопасности (кибербезопасности). В то же время, как отметили эксперты, существует ряд региональных соглашений по вопросам безопасности в ИКТ-среде, заключенные государствами, имеющими близкие политические предпочтения и взгляды на проблемы обеспечения международной информационной безопасности⁵, которые пока не могут обеспечить формирование открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Вследствие выделенных особенностей ИКТ-среды: содержание международных обязательств государств в ИКТ-среде неопределенным; сведения об инцидентах в ИКТ-среде, собираемые уполномоченными органами государств, не обладают достаточной юридической надежностью. В этих условиях приобретает значительную опасность использование государствами ИКТ для разрушительного воздействия на критически важные объекты инфраструктуры других государств, вмешательства во внутренние дела суверенных государств⁶ посредством управления в них процессами социально-политического развития.

Исходя из изложенного, ИКТ-среда как объект международного права может рас-

сматриваться как юридическая фикция, заключающаяся в приписывании ИКТ-среде свойств традиционной территории государства и распространении на нее государственного суверенитета. Объектом суверенитета государств в рассматриваемом аспекте являются в том числе и международные отношения по поводу развития и использования открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, которая «имеет существенно важное значение для всех, а для ее создания необходимо эффективное сотрудничество между государствами в целях снижения угроз международному миру и безопасности»⁷.

4. Исследование проблем практического применения норм, правил и принципов ответственного поведения государств в ИКТ-среде потребовало одновременного рассмотрения следующих вопросов:

- определение содержания выбранных норм с учётом норм и принципов международного права;
- анализ возможности применения норм государствами;
- анализ возможности правового разрешения международных споров, которые могут возникнуть в процессе применения норм, правил и принципов.

Экспертами отмечено, что государствами осуществляется поиск вариантов адаптации международного права к ИКТ-среде. С этой точки зрения можно выделить две основные тенденции:

- адаптация принципов международного права⁸ к ИКТ-среде, реализуемая в рамках

5 Европейская конвенция о преступности в сфере компьютерной информации. Будапешт. 23 ноября 2001 г.

6 On soft law in this field, see for example, UNGA, "Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes", A/44/147 (15 December, 1989).

7 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и коммуникаций в контексте международной безопасности. 2015 г. р. 1, A/70/174.

8 Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН (Резолюция Генеральной Ассамблеи ООН 2625 от 24 октября 1970 г.

- Рекомендации Группы, изложенные в подпунктах g), h), k) реализуемы при условии их дополнения нормами, определяющими порядок разрешения международных споров или недоразумений, возникающих в ИКТ-среде,
- The recommendations of Group stated in subparagraphs g), h), k) can be applied on condition of their addition with the norms defining an order of permission of the international disputes or misunderstanding, arising in ICT Wednesday,

Основные результаты The main results

ООН посредством разработки рекомендаций по нормам, принципам и правилам ответственного поведения государств;

- адаптация международного права безопасности и международного гуманитарного права к ИКТ-среде, реализуемая в рамках Организации Северо-Атлантического Договора посредством разработки, так называемого Таллиннского руководства⁹.

С учетом особенностей ИКТ-среды как пространства реализации международных отношений представляется важным согласовать эти процессы с поиском путей адаптации ИКТ-среды к применению международного права.

5. В результате проведенного исследования эксперты пришли к следующим выводам.

Международное право может применяться к международным отношениям в ИКТ-среде. В то же время международное правовое регулирование использования ИКТ государствами на основе норм, правил и принципов ответственного поведения государств может порождать международные споры, способные привести к нарушению международного мира и безопасности, но не имеющие в существующих условиях перспективы правового разрешения.

Тем не менее на текущем этапе развития международных отношений принятие норм, правил и принципов ответственного поведения государств в ИКТ-среде представляется связано с минимальными рисками нарушения международной безопасности.

Механизм добровольных и необязательных норм, правил и принципов способен содействовать возникновению государственной практики в области правового регулирования международных отношений на основе развития норм «мягкого» международного

- При наличии заинтересованных организаций продолжить изучение вопросов применения международного права к ИКТ-среде в следующих направлениях: установление зон ответственности государств; получение объективных сведений об инцидентах в ИКТ-среде; определение субъектов, причастных к инциденту в ИКТ-среде.
- If there're a few interested organizations it can be continued the studying of questions of applying of international law to ICT environment in the following directions: establishment of zones of responsibility of the states; gaining objective data on incidents in ICT environment; definition of the subjects involved in incident in ICT environment.

Предложения The offers

права, определения возможности их закрепления в универсальных международных договорах, становления в качестве норм. Процесс обсуждения норм, правил и принципов ответственного поведения государств в ИКТ-среде может помочь государствам усовершенствовать систему международных отношений в данной области, а также систему обмена лучшими методиками и опытом сотрудничества.

Практическое применение исследуемых норм, правил и принципов ответственного поведения государств в ИКТ-среде как средства регулирования международных отношений может явиться важным этапом укрепления безопасности использования государствами ИКТ.

Добровольное применение норм (правил, принципов) ответственного поведения государств в ИКТ-среде может быть реализовано в форме двусторонних, многосторонних, региональных соглашений и соглашений универсального характера, а также дополнено необходимыми национальными нормативными правовыми актами, устанавливающими порядок применения добровольных норм (правил, принципов) ответственного поведения государств в ИКТ-среде.

Дальнейшие исследования проблем практического применения норм, правил и принципов ответственного поведения государств в ИКТ-среде целесообразно направить на разработку принципов установление зон ответственности государств (демаркации и делимитации), а также принципов создания на основе доверия к третьей стороне системы получения объективных сведений об инцидентах в ИКТ-среде и атрибуции субъектов международного права, причастных к этим инцидентам.

⁹ Tallinn manual 2.0 on the International Law applicable to cyber operatio. By Michael N. Schmitt. 2017.

Энекен Тикк (Eneken Tikk)

независимый эксперт, Эстония

О МЕХАНИЗМАХ УРЕГУЛИРОВАНИЯ СПОРОВ И РАЗВИТИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ИКТ-СРЕДЕ

Добрый день!

Я не буду возвращаться к содержанию проекта, а лишь скажу, что мы были не совсем согласны, за исключением того, что очень полезно проводить такую работу, и мы лучше хотим понять позиции друг друга. Я очень благодарна за возможность выйти за пределы политики, окружающей эти вопросы, и обменяться взглядами и мнениями по поводу того, что экспертами было достигнуто и что можно сделать в научных кругах дополнительно.

Сегодня говорили о том, что некоторые из нас становятся независимыми. Независимость в моем случае означает, что я могу абстрагироваться от политических рамок данной проблемы и руководствоваться своими собственными принципами и морально-этическими ценностями. Главные выводы для меня в результате этого проекта заключаются в том, что очень сложно сотрудничать на уровне разных научных культур, которые не пересекались.

Когда я получала комментарии профессора А.Стрельцова по поводу того, как он понимает нормы, и что можно сделать по поводу реализации, моя первая реакция была – редактировать, как мы обычно делаем: «ИКТ» превращаем в «кибер» и т.д.

Но потом я поняла, что это невозможно и бесполезно, поэтому было очень сложно понять суть мышления, лежащую в основе работы профессора А.Стрельцова, и дать такой вариант, который он мог бы понять и прочитать. Как показала практика, одного года оказалось недостаточно для нахождения консенсуса. Если бы нам удалось его достичь, тогда я бы сказала, что дипломатам вообще и работы никакой не останется, так как это была бы слишком простая задача. Но мы поняли, что мы представляем страны или группы стран с совершенно различными политическими взглядами, с различными типами мышления и понимания с учетом наших подходов.



Очень интересная работа шла относительно согласования методологии текста, формулировок. Мы пытались выяснить, что уже сделано, чего не хватает и как действовать дальше.

Приведу пример. Если взглянуть на доклад ГПЭ ООН и рекомендации, где, в моем понимании, рекомендации – это внесение соответствующих изменений в законодательство, проведение обсуждений и др. Однако представители не всех стран поступают также. Общаясь с российскими коллегами, я узнала, что они считают эти нормы реализованными только после того, когда они получают статус обязательных. Поэтому в начале нашей работы профессор А. Стрельцов начал с того, какие правила и стандарты в существующем международном праве будут соответствовать этим нормам. Основываясь на моем понимании и подготовке, моя логика в этой связи была иной. Однако такое разнообразие взглядов уже было полезным результатом нашего сотрудничества. Не секрет, что договор – это российское предложение, то есть наличие обязательных положений.

Цель ясна, и отрицание этого лишь сдерживает нашу способность как ученых представить какое-то предложение, т.е. можно спорить на уровне политиков, заключать договор или нет, но с научной точки зрения – это более широкая дискуссия.

Поэтому я бы хотела поставить вопрос о том, каков следующий шаг? Мы исчерпали

первую стадию, в целом ни о чем не договорившись, однако лучше поняли подходы друг друга. Я полагаю, что реализация этих правил или норм возможна и снизу вверх, и сверху вниз. В некоторых странах начинают с национального законодательства, а другие – требуют введения международно-связывающих обязательств.

Однако мы не должны ожидать, что эти нормы появятся ниоткуда, то есть необходимо выбрать один из двух подходов. А далее, в зависимости от того, как страны будут реализовывать эти рекомендации, через 3–7 лет мы увидим, так как будем находиться на разных этапах этого пути, какие подходы предлагают страны в сфере регулирования кибербезопасности. Выделяют российскую модель кибербезопасности, называемую «системой международной информационной безопасности», китайскую, американскую, австралийскую, нидерландскую, японскую, скандинавскую. Каждая страна подпадает под одну из этих категорий, и в будущем будут существовать 3–4 наиболее интересные модели.

Таким образом, исходя из того, что политические разногласия останутся, мы должны сосредоточиться на этих разных моделях управления кибербезопасностью и разрабатывать правовые, технические и экономические аспекты и решения для эффективного сосуществования. На мой взгляд, эти модели будут сосуществовать параллельно с вопросами суверенитета. Каждая модель будет иметь свои отличия. В этой связи потребуются некие международные механизмы помимо существующего международного права.

Также возникает необходимость рассмотреть вопрос о том, как мы будем поддерживать все эти модели на плаву независимо от того, кто будет продвигать эти модели. Особая необходимость возникает в том, как договориться о механизмах урегулирования споров и развития международного сотрудничества, что тесно связано с международным правом.

Самое главное в наших дискуссиях состоит в том, что юридические решения нельзя начинать с политических позиций. Необходимо их выстраивать на базе конкретных и четко сформулированных вопросов.

Что касается перспектив, то мы начали проект в области международного права в Хельсинском университете, где рассматриваются конкретные вопросы, предложенные странами. Это не политические вопросы. Далее необходимо сосредоточиться на роли международного права параллельно с другими мерами и механизмами по решению этих вопросов.

На этот проект мы не возлагаем огромных целей. Речь идет о конкретных проблемах ИКТ в международном праве, международных отношениях, помимо тех, которые известны в сообществе киберзащиты. Нам необходимо поддерживать этот диалог, который не должен ограничиваться лишь вопросами киберзаконодательства, так как это отсекает другие потенциальные пути решения этих проблем.

Я надеюсь, что следующий этап проекта будет посвящен конкретным вопросам применения международного права, которые мы сможем также обсудить с некоторыми из вас в Хельсинки в конце сентября 2019 г.

Большое спасибо!

Ноюн Пак (Nohyoung Park),

Центр киберправа Университета Корё,
Мён Хюн Чун (Myunghyun Chung),
Юридический факультет Университета
Корё, Республика Корея

К ВОПРОСУ О ПРОГРЕССИВНОМ РАЗВИТИИ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ

Уважаемые модераторы!

Я представляю Центр правового обеспечения Корейского университета. Мой доклад будет посвящен тому, как прогрессивным образом развивать правила ответственного поведения государств в киберпространстве.

Хочу озвучить несколько замечаний, касающихся исследовательского проекта. Я с большим удовольствием принял участие в исследовательском проекте. К сожалению, не все заседания мне удалось посетить. Хочу также отметить большой вклад, сделанный профессором А. Стрельцовым, в развитие этого проекта. Хочу поблагодарить А.Стрельцова и в его лице всю российскую команду экспертов, которые также принимали участие в этих исследованиях.

Итак. В чем заключалась наша цель? Существует необходимость интегрировать нормы или меры укрепления доверия для обеспечения механизма защиты критической инфраструктуры. И нормы, и меры укрепления доверия могут способствовать снижению рисков и снижению эскалации угроз в киберпространстве. Следовательно, необходимо разработать конкретные нормы для конкретных секторов критической инфраструктуры, например, финансовой и банковской систем и др. Необходимо также установить систему проверки применения всех этих норм и мер доверия, которые бы применялись государствами на добровольной основе. Есть также необходимость активизировать изучение таких важных концепций для кибербезопасности, как передовой опыт в плане развития международного киберправа, до того времени, когда будут заключены международные соглашения, чтобы не допустить катастрофических киберинцидентов.

Что касается развития норм. Известно, что Генассамблея ООН призвала страны-члены ООН руководствоваться при использовании



ИКТ отчетом Группы правительственных экспертов ООН 2015 года (пункт 2а). Отчет четвертой Группы правительственных экспертов ООН имел очень важные нормы, в частности, пункт 11 по поводу ответственного поведения государств. Резолюция, принятая по инициативе России, придает большое значение нормам ответственного поведения государств. Многие из этих норм рекомендованы в тексте отчета четвертой ГПЭ, и они пользуются поддержкой и солидарностью со стороны Рабочей группы открытого состава (РГОС). РГОС также продолжает в качестве приоритета продвигать развитие правил, норм и принципов ответственного поведения. И в случае необходимости следует внести дополнения и изменения для разработки дополнительных правил ответственного поведения.

Однако резолюция в отношении шестой ГПЭ по инициативе США вроде бы исходит из тех же норм, как и предыдущие: нормы и меры доверия, которые должны быть разработаны совместно и дополнять друг друга на комплексной основе. Эти механизмы обеспечат снижение киберрисков в мире, применение норм и мер доверия будь то на добровольной или на обязывающей основе, этот процесс должен постоянно контролироваться.

Предусматривается также пересмотр политики торговли с целью повышения прозрачности, соблюдения правил ВТО. 13 лет назад была принята договоренность об учете этих

The research project

- The research project led by Prof. Streltsov on some important norms must be a good initiative for developing and applying those norms further.
- Learning from the research project, the following observation could be made:
 - There is a need to actively link or integrate those norms and CBMs, as found in the case of critical infrastructure.
 - Both those norms and CBMs can reduce cybersecurity risk and deescalate cyber threats.
 - There is a need to develop the concrete norms for specific sectors of critical infrastructure such as the financial system.
 - There is a need to have a system to check the application of those norms and CBMs, which are both voluntarily to be applied by States.
 - There is a need to activate the examination of such important concepts for cybersecurity.
 - There is a need to accumulate State practice on cybersecurity for the development of international cyber law until such a time of international agreements made after experiencing catastrophic cyber incidents.

4/27/2020

2

Need to develop and apply norms of responsible State behavior further

- The OEWG resolution gives more importance to the norms of responsible State behavior.
 - Many of those norms recommended in the 4th GGE report are explicitly welcomed in the OEWG resolution. (para. 1)
 - The OEWG is also to "continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behavior." (para. 5)
- The 6th GGE resolution seems to have the same stance on the norms as in the previous GGEs. (para. 3)

4/27/2020

4

норм, каждые 3 года они подвергаются ревизии, каждые 7 лет осуществляется их дополнительный анализ, и в таких государствах, как США, Япония, Китай, ЕС, это должно подвергаться контролю каждые 3 года. На ежегодной основе отдельное государство должно также анализировать свою ситуацию в плане информационной безопасности и сообщать об этом ООН через этот механизм.

Все документы группы составлены по единому принципу, носящему общий характер. Поэтому страны-участницы должны выполнять требования о предоставлении конкретных ежегодных отчетов по конкретным вопросам, а именно, как применяются эти нормы и меры доверия в киберпространстве.

Концепции, касающиеся кибербезопасности, на сегодняшний день не разработаны должным образом, хотя в повестку дня уже включен вопрос об изучении этой ситуации силами предыдущих групп. Резолюция по РГОС предусматривает провести исследование основных этих концепций. Резолюция по РГОС указывает также на изучение концепций, однако шестая ГПЭ говорит, что ее мандат не включает вопросов об изучении концепций. В этой связи я предлагаю включить вопрос изучения концепций в повестку дня обеих групп. Обращаюсь также к странам-участницам ООН предоставить все необходимые концепции: суверенитет применительно к киберпространству и др.

Need to develop and apply norms of responsible State behavior further

- Welcoming the 4th GGE report, the UNGA called upon Member States to "be guided in their use of information and communications technologies by the 2015 report". (para. 2(a))
 - UN Member States are thus requested to follow the recommendations of the 4th GGE report, which include 11 norms of responsible State behavior.
 - The 4th GGE did a good job by continuing to (para. 11)
 - "study ... norms of responsible State behaviour,
 - determine where existing norms may be formulated for application to the ICI environment,
 - encourage greater acceptance of norms and
 - identify where additional norms that take into account the complexity and unique attributes of ICIs may need to be developed."

4/27/2020

3

Need to develop and apply norms of responsible State behavior further

- The norms and CBMs need to be developed together and complemented explicitly each other.
 - Both of them are closely related each other, as shown for critical infrastructure in the 4th GGE report.
 - Both of them can reduce the cyber risk to international peace and security in peace time.
- The application of the norms and CBMs, being non-binding and voluntary in nature, by Member States need to be checked regularly and systematically.
 - A peer review like the trade policy review mechanism (TPRM) of the WTO may be a model.
 - The purpose of the TPRM is to "contribute to improved adherence by all Members to rules, disciplines and commitments made under the (WTO Agreements), and hence to the smoother functioning of the multilateral trading system, by achieving greater transparency in, and understanding of, the trade policies and practices of Members"
 - The review frequency is defined by the Member's share of world trade.
 - Every three years for four largest traders (currently the EU, the US, China and Japan);
 - Every five years for the next sixteen largest; and
 - Every seven years for other Members.
 - The current annual view and assessment to be made by Member States for cybersecurity need to cover those concrete norms and CBMs.

4/27/2020

5

Профессор А. Стрельцов в своем докладе также обратил внимание на отсутствие соответствующей государственной практики. Однако резолюция по шестой ГПЭ обращается к 25 государствам-членам с вопросом о предоставлении своей государственной практики о том, как международное право применяется к ИКТ-среде.

Вношу предложение о том, что странам-участницам шестой ГПЭ следует предоставить отчеты о своей практике применения международных норм в ИКТ-среде. Эти международные нормы могут включать такие аспекты, как международное гуманитарное право, вооруженные конфликты, право на самооборону и т.д. Необходимо также оценить, насколько вышеперечисленные нормы могут быть применимы к киберпространству.

Предлагается также внести на рассмотрение Генассамблеи ООН аналогичную резолюцию по вопросам применения принципов международного права для целей обеспечения безопасности в киберпространстве.

В 2017 году, отмечая юбилей ООН, Генассамблея ООН приняла резолюцию об установлении дружественных отношений в киберпространстве. Эта резолюция была разработана силами специального комитета, включавшего представителей 40 стран-участниц, в этой связи отмечу, что их работа оказалась даже более эффективной, чем работа ГПЭ ООН.

Need to accumulate State practice on the application of international law to cyberspace



- While the research project led by Prof. Streltsov points out the absence of relevant State practice, State practice on cybersecurity could be developed in the near future.
- The 6th GGE resolution provides that the GGE report includes "an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States, to the General Assembly at its seventy-sixth session" in 2022. (para. 3)
 - The 25 members of the 6th GGE should declare their State practice on the application of international law, such as the right to self-defense, international humanitarian law, to cyberspace.
 - The other Member States may follow the practice of such national contributions.

4/27/2020

7

Кибербезопасность имеет большое значение для обеспечения безопасности и стабильности киберпространства. Однако она также важна и для других отраслей нашей цифровой жизни, в том числе и цифровой торговли, где безопасное использование, передача и хранение данных зависит от качества обеспечения кибербезопасности. Недавние соглашения о свободной торговле включают также

Need to accumulate State practice on the application of international law to cyberspace



- A so-called "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Cyberspace in accordance with the UN Charter," may be adopted by the UNGA in the future.
- The "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations" was adopted by the UNGA on 24 October 1970 (resolution 26/25) to celebrate the 25th anniversary of the UN.
- It was drafted by jurists in the Special Committee (including a 14 member Drafting Committee) under the 6th Committee.

4/27/2020

8

положения о приватности данных и кибербезопасности электронной и цифровой торговли.

Таким образом, кибербезопасность имеет огромное значение, в том числе и для обеспечения приватности личных данных и цифровой торговли.

Эта деятельность в рамках ООН предоставит нам продуктивные и значимые результаты. Большое спасибо!

**Мён Хюн Чун
(Myunghyun Chung),**

*Юридический факультет Университета
Корё, Республика Корея*

**КИБЕРОПЕРАЦИИ ПРОТИВ ФИНАНСОВЫХ
СИСТЕМ ДОЛЖНЫ ОСУЖДАТЬСЯ
В МЕЖДУНАРОДНОМ МАСШТАБЕ**

Хочу поблагодарить организаторов нашего Форума за неустанную поддержку.

Мне поручено выступить на тему, как разрабатывать и реализовывать нормы ответственного поведения государств с упором на защиту критической инфраструктуры.

Как отметил предыдущий докладчик, существует необходимость в разработке и реализации этих норм ответственного поведения государств с упором именно на критическую инфраструктуру.

В документах, подготовленных предыдущими группами, уже говорилось о мерах доверия в киберпространстве. Они тесно связаны именно с приемлемыми, добровольными и необязывающими нормами ответственного поведения государств, в то время как эти нормы либо в контексте существующего международного права, либо в форме необязывающих политических соглашений помогают установить международный уровень ожиданий поведения наших государств в киберпространстве. При этом меры доверия предоставляют практический инструмент, направленный на то, чтобы удержать и стабилизировать эти ожидания.

Мы пытаемся разрабатывать нормы и меры доверия государств наоборот, путем их связывания друг с другом.

Существует, по меньшей мере, четыре нормы ответственного поведения государств, связанные с критической инфраструктурой, согласно отчету четвертой ГПЭ. Суть этих норм заключается в следующем:

- государства не должны предпринимать действий, которые могут нанести ущерб критической инфраструктуре;
- государства должны принимать эффективные меры для защиты своей инфраструктуры от враждебного влияния согласно пункту 6 отчета, в котором указано на необходимость преодоления уязвимостей в плане обмена информацией.



Согласно пунктам 13f, 16b, 16d предоставление на добровольной основе национальных взглядов государств на критическую инфраструктуру, а также мер, принимаемых на уровне государств для ее защиты, должно включаться в отчеты, представляемые странами-участницами.

В пункте 13g говорится о том, что необходимо учитывать вызовы, стоящие перед государствами, при разработке норм, регулирующих информационное пространство. Иными словами, необходимо приводить национальное законодательство в соответствие с международными требованиями. И реагировать на эти вызовы можно путем разработки мер доверия, направленных на повышения уровня доверия между государствами для создания благоприятных условий для реализации этих мер, как на национальном, так и на международном уровне.

Другие две нормы имеют аналогичную структуру. Отмечу, что некоторые нормы рассматриваются в увязке с мерами доверия.

Существует необходимость уточнения тех объектов инфраструктуры, которые подпадают под действие мер доверия.

Некоторые меры доверия дублируются, поэтому необходима реструктуризация и оптимизация формулировок путем связывания мер доверия с мерами защиты критической инфраструктуры.

Перейду к нормам ответственного поведения и мерам доверия разных категорий крити-

ческой инфраструктуры. В настоящее время делается упор на разработку норм и мер доверия в отношении конкретных отраслей экономической деятельности, включая финансовый сектор, с учетом как международных, так и национальных особенностей.

Отчет четвертой ГПЭ выделяет также такие направления, как энергетические компании, финансовые и др. Европейская комиссия дала рекомендации по энергетическому сектору.

ГПЭ определяет также возможность применения разных финансовых санкций в отношении стран, нарушающих эти нормы, и, в частности, со стороны КНДР наблюдаются действия, которые потенциально могут подорвать безопасность и доверие.

Финансовая система во всем мире все больше и больше сталкивается с киберугрозами. И эти угрозы могут нанести вред финансовой стабильности, более того, уязвимость финансовой системы одного государства может очень быстро привести к нарушению стабильности финансовых систем других стран и отразиться на других отраслях критической инфраструктуры. Финансовую систему необходимо укреплять путем повышения мер отката устойчивости, минимизации воздействия возможных киберинцидентов. Вредоносные операции в ИКТ-среде против финансовых систем постоянно развиваются как со стороны традиционных группировок, так и со стороны группировок, спонсируемых государствами. Финансовая система также определяется в качестве важного элемента критической инфраструктуры. Среди угроз в ИКТ-среде, стоящих перед финансовой системой, можно выделить следующие. В 2016 году сообщалось,

что хакеры взломали сеть центрального банка Бангладеш, в 2018 году та же ситуация произошла в Мексике, на Мальте была попытка перевести 13 млн. евро на счет преступной организации. За последние несколько лет изменения коснулись и платежных систем. Мы также наблюдаем географическое распределение пользователей, ставших объектами атак с использованием вредоносного ПО, направленного на подрыв банковской системы в 2018 году.

Финансовая система является стовым хребтом экономики и важным критическим элементом инфраструктуры, имеет большое экономическое и социальное значение. При этом подделка валюты является еще одной угрозой финансовых систем.

Нормы ответственного поведения государств должны распространяться на финансовую систему и критическую инфраструктуру следующим образом. Вредоносные кибероперации против финансовых систем должны осуждаться в международном масштабе, и, следовательно, необходимо повышать уровень международного сотрудничества для защиты финансовых систем. Любое вредоносное использование ИКТ, подрывающее безопасность и доверие и ставящее под угрозу финансовую стабильность, недопустимо. Вредоносные субъекты в ИКТ-пространстве должны привлекаться к ответственности за свои вредоносные операции, направленные против финансовых систем. Упоминание о финансовых системах необходимо в отчетах по работе критической инфраструктуры и по созданию мер доверия для ответственного поведения государств.

Спасибо за внимание!

Камино Кавана (Camino Cavanagh),

Королевский колледж Лондона,
Великобритания

ПРОГРЕСС В РАЗВИТИИ МЕЖДУНАРОДНЫХ КИБЕРНОРМ

Большое спасибо за приглашение выступить на Форуме в этом году! Это большая честь для меня!

Мне придется повторить многое из того, что уже прозвучало, но думаю, это поможет пролить свет на обсуждаемую проблематику и вызовет дополнительные вопросы в ходе дискуссии.

Во-первых, сосредоточусь в основном на работе, которая происходит в ООН. Мы уже много об этом слышали. Это основное направление. Чуть более 20 лет прошло с тех пор, как Россия внесла проект первой резолюции на Генассамблее ООН, и 15 лет прошло с момента создания первой Группы государственных экспертов ООН. Первая ГПЭ не достигла консенсуса, но, как мы знаем, три последующие группы договорились о том, что международное право применимо в киберпространстве, и рекомендовали нормы формирования ответственного поведения государств, а также предложили меры укрепления сотрудничества и доверия. Нормы, в частности, очень важны, потому что они связаны с злонамеренным использованием ИКТ: 11 норм и различная положительная практика, а также нормы, ограничивающие определенный тип поведения, и нормы, связанные с защитой критической инфраструктуры.

Эти события в ООН дополняются важными шагами на региональном уровне: в ОБСЕ, ШОС, Африканском союзе, БРИКС и тематических группах «Большая двадцатка» и «Семерка». Также нормативная работа ведется в группах с участием различных субъектов заинтересованных лиц, глобальной комиссии по стабильности Интернета. Кроме того, рассматриваются шесть дополнительных норм на основе надлежащей практики. Таким образом, все эти усилия сочетаются с другими нормативными усилиями в области прав человека, экономического и социального развития, а также борьбы с терроризмом и т.д. Это также касается поведения государств и негосударственных субъектов по отношению



к существующим или новым технологиям, например, аэрокосмическим технологиям, робототехнике, искусственному интеллекту.

Реализация норм – это самый актуальный вопрос сейчас. Практически все работающие в этом пространстве согласны с тем, что достигнутый прогресс положителен, но имеются ряд инцидентов с участием государств, где выработанные нормы не всегда соблюдаются.

Лишь небольшое количество государств сообщили о том, как они реализуют эти нормы и какие уроки можно из этого извлечь. В недавнем отчете Э.Тикк предложила реализацию на основе практики национального уровня. В этом отношении уже сделано немало, и полезно было бы обсудить результаты для того, чтобы понять, какие уроки можно извлечь и как распространить результаты на другие страны. Есть также инициатива правительства Швейцарии, которое лидирует в области понимания ролей и ответственности государств в киберпространстве, а также действий частного сектора, научного сообщества в поддержке государств по реализации этих норм.

Презентация ICANN продемонстрировала то, какую пользу может принести ICANN в области разработки различных норм и правил. Некоторые ученые занимаются вопросами атрибуции по международному праву. Недавно страны «семерки» объявили новую инициативу, в рамках которой тоже будет проводиться

обобщение опыта в реализации норм. На мой взгляд, это будет очень полезная работа.

Достижение прогресса по реализации этих норм будет ключевым ответом на нерешенные вопросы касательно лакун, пробелов, формирования новых процессов, таких как деятельность РГОС. В этом контексте необходимо найти ответ на вопрос о необходимости норм и правил для укрепления уже существующих. Насколько нормы, касающиеся критической инфраструктуры, сформулированные в последнем докладе, достаточно сильны для защиты системных энергетических сетей, телекоммуникационных систем и других важных коммерческих объектов в области инфраструктуры? На этот вопрос необходимо дать ответ с точки зрения правоприменения, о чем уже говорилось на нашем Форуме.

Прогресс в реализации норм не только поможет определить пробелы относительно достаточности норм, но и сможет дополнить меры укрепления доверия и другие механизмы кризисного урегулирования, которые, по моему мнению, необходимы для открытия двустороннего и многостороннего диалога и возможности проведения исследований на основе сотрудничества. Например, круглый стол по киберстабильности в Париже. Группа обсудила безотлагательную необходимость сотрудничества в области ограничения эскалации исследований, проведенных на различных форумах по киберзащите.

Помимо двустороннего и трехстороннего взаимодействия можно задействовать многосторонние форматы по мерам доверия, а также проанализировать насколько можно усилить эти направления и площадки.

Таким образом, направить сигнал всему международному сообществу о том, что име-

ется готовность к предотвращению конфликтов в ИКТ-среде в случае эскалации на основе недоразумения или неправильного расчета.

В 2019 году начинают свою работу Рабочая группа открытого состава и Группа правительственных экспертов. Таким образом, мы имеем два процесса вместо одного. Ключевой вопрос: как синхронизировать эти усилия, как вовлечь других субъектов. Оба процесса обладают консультативными механизмами, важно понять, как они будут реализованы на практике.

Посол А. Крутских упоминает ряд принципов, необходимых для формирования взаимодействия между этими двумя процессами. А. Крутских обсуждает комплементарность, невраждебный характер, конструктивность, сотрудничество и разделение бремени. В этом контексте обе группы изучают все вопросы – международное право, нормы, меры доверия, наращивание потенциала. Он считает, что ГПЭ должна заниматься более специализированными вопросами международного права, а РГОС должна сосредоточиться на основных политических задачах, касающихся международного сообщества, норм, правил поведения, наращивания потенциала и будущей работы ООН. Основные вопросы в отношении принципов и предложений в основе этих двух процессов следующие. Какие вызовы стоят перед этими целями разделения бремени и как можно преодолеть эти препятствия?

И, наконец, нужен ли дополнительный двусторонний диалог по треку 1,5 в дополнение к этим процессам с целью разработки консенсуса? И насколько это осуществимо? Есть ли желание продолжать эти сопровождающие процессы?

Спасибо за внимание!

Ю.Н. Жданов,

*Российская секция Международной
полицейской ассоциации*

РОССИЯ И АКТУАЛЬНЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ

Добрый день, уважаемые коллеги!

Тематика нашего международного Форума мне близка и понятна с разных точек зрения.

Во-первых, я достаточно глубоко разбираюсь в международном праве и, в частности, в праве международной безопасности. И те вопросы, которые здесь сегодня затронуты, они, с одной стороны, архиважные и, с другой стороны, архисложные.

Возьмем, к примеру, статью 51 Устава ООН «О праве государств на самооборону». Возникает вопрос, применима ли эта норма к тому спектру, который здесь сегодня затронут. Да, конечно, она не только применима, но и крайне важна и опасна, потому что государство в соответствии со статьей 51 Устава ООН может обратиться к другому государству и попросить помощь в организации его обороны. В силу этого оборона государства от киберпреступности сегодня – это наше будущее и, к сожалению, даже наше настоящее. Большинство стран мира не обладает такими возможностями, которыми обладает первая десятка развитых стран, и, тем не менее, преступность мигрирует по миру, мигрирует по всем странам и объединяется быстрее и эффективнее, чем правоохранительные органы. Преступность уже давно не та, которая была 10–20 лет назад, сейчас она представляет реальную угрозу для мира и стабильности не только отдельных организаций типа «Сбербанка», «Норникеля», но и в целом государств. И те вопросы, которые поднимаются сегодня, они, конечно, не просто важны и нужны, а, на мой взгляд, надо уже давным-давно отходить от резолюций Генассамблеи ООН, которые являются «мягким» правом, и переходить к более жестким мерам в рамках того вопроса, который мы сегодня рассматриваем.

Поэтому, что касается встречи в Хельсинки в сентябре 2019 г., мы на площадке Международной полицейской ассоциации, в рамках



которой мы также рассматриваем вопросы кибербезопасности, киберпреступности, борьбы с ней, борьбы с новыми видами преступлений, которые еще буквально недавно были просто немыслимы. К примеру, уже машина с искусственным интеллектом сбита человека. Возникает вопрос, где те нормы, которые регулируют ответственность тех, кто произвел машину, тех, кто использовал ее, и т.д.? А что говорить о безопасности банка?

В этом контексте вопросы международно-правового регулирования, национального регулирования этих норм крайне важны.

С сожалением отмечу, что мы далеко не продвинулись в этой области. Недавно я посещал президент-полицая в Мюнхене, который отвечает за этот вид борьбы с этим видом преступности в Баварии. Думаю, что немцы здесь на полшага впереди, но это все равно не так, как хотелось бы. Вызывают озабоченность риски, которые сейчас тревожат весь мир.

Полагаю, что необходимо начинать не только с появления новых норм с использованием различных международных площадок, наверное, надо более настойчиво пытаться продвигать это в ООН, хотя я понимаю, что это совсем не просто. При этом с трудом понимаю, почему США не очень активно участвуют в этой совместной работе, хотя в этом виде преступлений они вообще не знают границ.

Преступность вообще давно не знает границ, а этот вид – особо опасный и осо-

бо сложный. Думаю, это связано с недостаточной подготовкой кадров в этой области так, как это необходимо. Сегодня уже в самых крупных развитых странах отказываются уже от примитивной подготовки полиции в полицейских академиях, их уже обучают в бизнес-школах, в специальных учебных заведениях, связанных с изучением криптовалют. Поэтому сегодняшние вопросы являются не просто важными и нужными, так как, полагаю, мы сильно запаздываем в реакции и в продвижении этих проблем. Это не говорит о том, что много лет ничего не делалось, просто вызовы и угрозы настолько опасны и настолько сложны, что, наверное, как говорят в России, пока гром не грянет, мужик не перекрестится. А гром может грянуть в любую секунду.

Полагаю, что в этой сфере необходимо принимать соответствующие меры в рамках национальных квартир. В Российской Федерации много специалистов, занимаются данной проблематикой, но дальше всех продвинулись 2–3 организации, а в целом в России борьба

с киберпреступлениями ведется на «пещерном» уровне. Тем не менее это характерно не только для Российской Федерации.

Имеются данные о том, что происходит в этой сфере примерно в 70 государствах мира. Мы обмениваемся информацией в этой области, и я полагаю, что мы, к сожалению, в начале пути. Но преступность находится не в начале пути, она изобретает все новые и новые виды преступлений, которые связаны с тем, как похитить средства из того или иного банка, как разблокировать какую-то систему безопасности, как снять систему защиты с режимных объектов и т.д.

Мне бы хотелось, чтобы мы совместно более эффективно разрабатывали международно-правовые нормы, которые регулируют проблематику сегодняшнего мероприятия. В мае запланирована большая международная конференция, связанная с полицией будущего, в г. Санкт-Петербурге. И мы попробуем подготовиться и рассмотреть основной вопрос сегодняшней повестки дня.

Спасибо!

А.А. Савенков, Т.А. Полякова,
*Институт государства и права РАН,
Россия*

ТЕНДЕНЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И ВОПРОСЫ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ

Уважаемые коллеги!

Мое выступление будет кратким. Я хотела бы поблагодарить организаторов за приглашение на этот полезный Форум!

Вопросы, обсуждаемые на форуме, имеют ключевое, векторное значение и для национального права государств, и для развития подходов к этим вопросам в условиях современного мира.

Сегодня в условиях трансформации глобального общества и кризиса, который происходит, все сигнализирует о начале перехода к новому типу общественной организации. В этом году Д.Бэллу исполняется 100 лет, и юристы тоже отмечают день его рождения, потому что он одним из первых провозгласил постиндустриальное, информационное и даже программируемое общество.

Сегодня эта тема широко обсуждается. Однако не очень понятно, будем ли мы выступать в роли программируемых субъектов или появятся иные субъекты, но юристы уже начали спорить на эту тему.

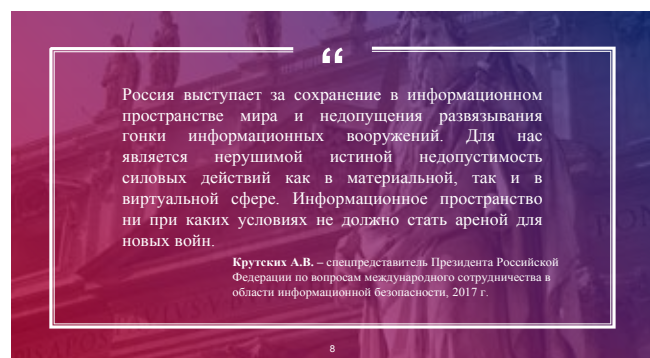
Время показало, что изменения, которые происходят, значительно глубже, масштабнее и серьезнее того, что предсказывал Д. Бэлл, о чем говорит даже Р. Курцвейл, к которому очень прислушивается Билл Гейтс, в своих предсказаниях относительно развития робототехники, искусственного интеллекта. Формирование такой новой модели социальной коммуникации, которую мы в принципе обсуждаем, так как сколько бы мы не говорили о технологиях, они все равно создаются во имя чего-то. Наверное, во имя того, чтобы пользоваться людьми, чтобы осуществлять эти коммуникации. Поэтому это ставит перед нами новые задачи права. Право не настолько динамично, как информационные технологии, и поэтому за ними, безусловно, не успевает.



Каковы же сегодняшние тенденции? Как юристы мы должны говорить о какой-то методологии и о методах. «Компаративистика» – это та наука, которая изучает сравнительное правоведение, изучает, что же происходит в законодательстве других государств и в науке. И поэтому компаративистские подходы оказываются недостаточно обоснованными и подготовленными с точки зрения и понятийного аппарата, и действия или недействия международных принципов. Я посещала одну международную юридическую конференцию, и там велась большая дискуссия относительно общепризнанных принципов и норм, входящих в систему права. Утверждалось, что именно общепризнанных принципов и нет, нет такой терминологии. А мы достаточно широко употребляем и в актах и обучаем юристов в области информационного права и информационной безопасности. Тут тоже кроется своего рода большой блок вопросов.

Хотела обратить внимание на тот факт, что политика в чем-то выражается, это не просто выступления глав государств с заявлениями о чем-то, это стратегия. При этом существуют совершенно разные подходы: европейские, американские, китайские и др., выраженные в стратегических документах.

Нам показалось интересным законодательство Вьетнама. Там имеются подходы, близкие к российским, и в этом смысле нам более понятные. Ведь когда мы говорим о ком-



паративистике, то совершенно очевидно, что мы касаемся темы различных правовых систем и очень сложно их сравнивать.

Когда мы готовили соглашение по международной информационной безопасности в рамках ШОС, именно проблема анализа законодательства государств была проблемной зоной, поскольку имели место разные правовые системы, и необходимо было договариваться, как это законодательство будет восприниматься.

В рамках стратегического планирования вопросы информационной безопасности обязательно отражаются. В прошлом году было отмечено, что стратегия – это не самое главное, а главное – принимать национальные проекты. Я должна сказать, что в области цифровой экономики – а она сегодня является той сферой, которая активно развивается во всем мире, – в России 24 декабря 2018 г. утверждена новая национальная программа «Цифровая экономика Российской Федерации». В ней предусмотрено шесть основных направлений федеральных проектов: нормативное регулирование, информационная инфраструктура, кадры для цифровой экономики, информационная безопасность, цифровые технологии и государственное управление.

Федеральный проект «Информационная безопасность» содержит 52 мероприятия, из которых 15 связаны с созданием и совершен-

ствованием нормативно-правового регулирования в данной сфере.

Я, как ученый, занимающийся этой сферой, хочу сказать, что, конечно, проекты обозначены, но хотелось бы, чтобы был какой-то более системный подход. Просто обозначить вектором, что у нас сегодня имеются большие данные, облака и т.д., этого явно недостаточно.

Разрабатывается проект концепции кибербезопасности, сейчас идет обсуждение этого проекта.

В настоящее время идет активное нормотворчество в сфере ИКТ, в трех чтениях принят закон об обеспечении безопасного и устойчивого функционирования сети Интернет на территории Российской Федерации, также принят закон о цифровых правах, вносящий изменения в гражданское законодательство, и закон о фейковых новостях.

Хотела бы остановиться на проблематике защиты персональных данных, так как это та тема, которая в цифровом пространстве все равно возникает: и доверие, и недоверие, и идентификация. Сегодня – это европейский подход, спроецированный на все государства, потому что они должны выполнять те требования, которые предусмотрены. Это тенденция глобализации защиты персональных данных.

Что касается нормативного и правового регулирования робототехники и искусственного интеллекта, то у нас уже есть защиты

547 800 000 рублей

Ущерб юридическим лицам от киберпреступности в России
по итогам 2017—2018 гг.

По данным IB-GROUP

12

Персональные данные (Personal data)

European Union
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Russian Federation
Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
Разработка нового проекта федерального закона о персональных данных.

13

Нормативное правовое регулирование робототехники и искусственного интеллекта

European Union:
* Инициативы Франции в сфере робототехники (2013)
* Закон Эстонии о роботах-курьерах (2017)
* Немецкий закон о беспилотных автомобилях (2017)
* Резолюция Европарламента «Нормы гражданского права о робототехнике» (2017)

Russian Federation:
* Готовится проект Стратегии России в области искусственного интеллекта

The United States of America:
Закон штата Калифорния об идентификации ботов (2018)

South Korea:
Закон Южной Кореи «О содействии развитию и распространению умных роботов» (2008)
С момента принятия более 10 раз были внесены изменения

17

Триада Информационной безопасности (Triad Information Security)

1. Правовое регулирование (Legal regulation)

2. Техническое и аппаратно-программное обеспечение (Technical and hardware-software)

3. Организационное обеспечение (Organizational support)

19

докторских диссертаций по гражданскому праву об искусственном интеллекте. Мои ученики пишут по робототехнике докторские диссертации. Пока еще нет определенности, что есть субъект, а что – объект, как принято у юристов, и что будет в этой сфере являться. Также значительное количество дискуссий ведется сегодня на тему искусственного интеллекта. Насколько это далекое будущее, форсайт, или прямо сегодня какие-то акты на эту тему будут разработаны, сказать сложно.

Тенденции, риски, о чем сегодня уже много говорилось, и их правовое регулирование,

на мой взгляд, должны идти не только за технологиями, а, может быть, в чем-то необходимо попытаться заглянуть, конечно, не так, как Р. Курцвейл, немного вперед.

Информационная безопасность или кибербезопасность? Этот вопрос, который у нас здесь возникает. В основном, конечно же, зарубежные коллеги употребляют понятие «кибербезопасность», мы употребляем и то, и другое.

Благодарю за внимание!

А.Н. Курбацкий,

*Белорусский государственный
университет*

О РОЛИ ЭКСПЕРТНОГО СООБЩЕСТВА В ОБЕСПЕЧЕНИИ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ

Уважаемые коллеги!

Мой доклад будет кратким. Я хотел бы поговорить о процессах цифровой трансформации со стороны небольшого государства. В небольшой стране можно гораздо быстрее увидеть некоторые тренды процессов цифровой трансформации, так как запас прочности небольшой страны невелик.

Практически в каждом докладе упоминается понятие «экспертное сообщество». А есть ли эти экспертные сообщества в небольших странах? Приведу пример из опыта Белоруссии. Потенциально у нас, конечно, экспертное сообщество имеется. Но что происходит на практике? Около 20 лет назад мы начали проект «IT-страна», мы создали «Парк высоких технологий», понимая, что будет быстро развиваться проектирование программного обеспечения. В итоге, на сегодняшний день мы развили это направление. Под «зонтиком» «Парка высоких технологий» находится более 500 компаний, в общей сложности это около 50 тысяч программистов.

Фактически все эксперты плавно перетекали «под крышу» «Парка высоких технологий». Более того, молодые специалисты, которые могли бы стать экспертами, тоже перетекают туда же. Поскольку «Парк высоких технологий» в основном работает по модели «заказного программного обеспечения», то у нас порядка 90% всех проектов – это заказное программное обеспечение, в первую очередь, для США и Канады, во вторую очередь, для Европы. В итоге 90% наших специалистов в сфере ИКТ работают на данный вектор.

Таким образом, мы практически лишаемся экспертного сообщества. Хочу спросить, а можем ли мы создавать это экспертное сообщество? Мы понимаем, что экспертное сообщество создают университеты. А что же сейчас происходит в сфере ИКТ? Сейчас конкуренцию традиционным университетам составляет так называемое онлайн-образование или цифровые платформы. В сфере



ИКТ все больше и больше молодежи обучаются посредством таких цифровых платформ. Цифровые платформы, как правило, не национальные, так как Белоруссия в этом плане отстает и нам сложно конкурировать с цифровыми платформами США, Европы и Китая.

В итоге традиционные университеты, когда готовили специалистов, больше погружали студентов в страновые проекты для лучшего понимания специфики страны. А когда человек получает образование, используя цифровую платформу далекого университета? Фактически страновых вопросов программы обучения этого университета не затрагивают. Студент получает образование, которое «заточено» на западный вектор. И такой человек уже потенциально не способен быть экспертом в своей стране. А поскольку разница в оплате труда в сфере ИКТ и средней заработной платой по стране отличается в разы, то получается, что наши специалисты и в дальнейшем будут обучаться на подобных цифровых платформах. Для ИКТ это нормальная практика, так как онлайн-обучение в этой сфере предоставляет знания достаточно высокого качества. С другой стороны, эти знания не всегда системны, они фрагментарны, касаются только технологических аспектов, но для того, чтобы найти свое место на рынке труда, этого оказывается достаточно.

Таким образом, мы не имеем возможности сегодня для нормального пополнения экс-

пертного сообщества в Белоруссии в силу разных причин, в том числе и в связи с запуском проекта «IT-страна». Но учитывая, что сейчас создание программного обеспечения становится все более и более массовым, так как цифровизация приводит к тому, что фактически везде необходимо ПО, и миллионы людей задействованы в его написании, получается, что подобные проблемы могут возникать и в других небольших государствах.

Помимо традиционных цифровых платформ в последнее время активное развитие получили корпоративные университеты, особенно, транснациональных компаний, с альтернативными подходами к образованию. Следует отметить, что это не только корпоративные университеты США, в последнее время достаточно интересные проекты появляются и в Китае. Эти университеты также используют цифровые платформы, которые позволяют обучать сразу сотни тысяч студентов. В последнее время наблюдается тенденция, что корпоративные университе-

ты становятся конкурентами традиционных университетов. Раньше корпоративные университеты лишь «доводили» студентов после обучения в традиционных университетах. Сегодня корпоративные университеты начинают готовить специалистов со школьной скамьи. В результате, если говорить об экспертных сообществах в небольших государствах, то при отсутствии внимания к этой проблеме со стороны самого государства мы можем полностью лишиться национальных экспертных сообществ.

Таким образом, необходимость создания больших рабочих групп из национальных экспертов может привести к тому, что в небольших государствах не останется экспертов для участия в многочисленных рабочих группах.

Цифровизация приводит к тому, что таких групп будет создаваться все больше и больше, так изучение темы ответственного поведения государств в ИКТ-среде также требует хорошей экспертной платформы.

Спасибо за внимание!

АТРИБУЦИЯ В КИБЕРПРОСТРАНСТВЕ И ПРОБЛЕМЫ ОТВЕТСТВЕННОСТИ

Я хотел бы поблагодарить профессора А.Стрельцова и доктора Э.Тикк за их руководство и упорный труд при подготовке этого отчета. Это была сложная работа, очень много сделано, и в этом прелесть данного труда.

Когда я готовился к выступлению на тему атрибуции, я вспомнил прежние встречи в Гармиш-Партенкирхене и заметил, что мы не очень много говорили об атрибуции, хотя это очень важная проблема при обсуждении кибернорм. Но потом я с удивлением узнал, что сегодня практически в каждом втором выступлении звучит тема атрибуции, и я вижу в этом положительное развитие событий.

Что я вкладываю в это понятие и почему считаю его таким важным, особенно, в контексте имплементации норм. Я проводил некоторые исследования и мне стало ясно, насколько важна проблема атрибуции: кто сделал, кто отвечает, кто несет ответственность за злонамеренные киберинциденты. В литературе я нашел немного информации об атрибуции. На мой взгляд, причиной является то, что, когда мы говорим о вопросах кибернорм, регулировании Интернета или управлении Интернетом, мы часто рассматриваем это в рамках одностороннего, разобщенного подхода. А сейчас нам необходимо привлекать междисциплинарный подход в рамках более широкой дискуссии с привлечением технических экспертов, международных юристов и т.д.

Посмотрев редакцию совместного доклада, я написал письмо профессору А.Стрельцову, где попытался подчеркнуть важность атрибуции, стандартов доказательств и роли стандартизации на международном уровне как предварительного условия имплементации кибернорм. Я также считаю, что нынешнее состояние и сложность этих вопросов слишком велики для решения в рамках данного документа. Но эту тему можно было бы рассмотреть в перспективе и на других площадках.

Прежде чем перейти к комментариям по поводу атрибуции, хотел бы озвучить два тезиса. Работая над этой темой, я пришел к выводу,



что значительная часть исследований проводилась, в основном, американскими или европейскими учеными. Очень трудно было найти какие-то значительные труды из России, Китая, так как это тоже очень важные участники данной дискуссии. Я не говорю об атрибуции, которая осуществляется на уровне государственных структур, я имею в виду общественную и публичную сферы, так как очень важно проводить публичные дискуссии относительно атрибуции соответствующих методов и методик. К такому выводу мы пришли и сегодня при обсуждении различных концепций, разногласий, трактовок, поэтому я хотел бы призвать всех нас продолжать обмен мнениями, знаниями, практиками в этой сфере, особенно интересно было бы услышать мнение российских экспертов по вопросам атрибуции.

Что касается второго тезиса, то группа ведущих американских и канадских исследователей создала определенное сообщество ученых для рассмотрения этих вопросов с участием политологов, представителей других отраслей с тем, чтобы найти объективные пути для достижения кибератрибуции. Данный проект находится на начальном этапе, но мы всячески приветствовали участие экспертов из различных стран.

Далее проведу краткий обзор того, что, на мой взгляд, является кибератрибуцией.

Итак, атрибуция в киберсфере – это процесс определения стороны, ответственной за

атаку или инцидент с злонамеренным использованием киберсредств. При возникновении подозрений проводится расследование и собираются доказательства. Расследование проводится частными компаниями, государство также часто пользуется услугами подобных компаний для выполнения работ по атрибуции.

Вопрос о том, кто несет ответственность за киберинцидент, должен рассматриваться на различных этапах, так как имеется существенное различие между идентификацией и приписыванием этих действий определенному противнику в лице государства или другой организации.

Если на вопрос об ответственности невозможно дать ответ, то жертве будет трудно обеспечить возмещение ущерба или наказать сторону, виновную за инцидент. Причем эта сторона в будущем может продолжать подобную злонамеренную деятельность.

Выделяют три уровня атрибуции, между которыми необходимо проводить различие. Первое – это определение механизма проведения нападения с использованием криминалистических методов, второе – определение личности человека, который управлял этими действиями, третье – окончательная ответственность: можно ли установить связь между политическими или государственными заказчиками и теми, кто несет окончательную ответственность за нападение.

Что касается положений международного права, регулирующих международный конфликт, то здесь атрибуция связана с фундаментальными вопросами ответственности за конфликт. Известно, что это, однако, не дает возможности осуществления наказания через государственные границы.

Выделяют две проблемы, касающиеся вызовов в процессе атрибуции. Неопределенность относительно информационных

поток между тактическим, оперативным и стратегическим уровнями. По мере прохождения информации возникает увеличение степени неопределенности при переходе со стратегического на политический уровень. Что касается международной стандартизации, то, по оценкам экспертов, международные стандарты являются необходимым условием киберстабильности. Таким образом, стандартизация в области атрибуции необходима для устранения вышеуказанных недостатков и заполнения пробелов, существующих в этой сфере.

Какие институты обладают доверием и соответствующими полномочиями для независимого решения вопросов атрибуции?

Приведу два примера.

1. В 2008 году была предложена организационная модель на основе Международного комитета Красного Креста, чтобы помочь компаниям и гражданам, подвергшимся нападению. Среди участников были такие компании, как Microsoft и др. Эти компании предоставляли помощь потерпевшим в результате кибератак по всему миру.
2. Консорциум в области глобальной атрибуции, предложенный корпорацией RAND, является структурой, не связанной с какими-либо странами или государственными органами.

Полагаю, что необходимо работать в этом направлении.

В завершение отмечу, что главный посыл заключается в том, что это очень важный вопрос и необходимо продолжать диалог по вопросам атрибуции.

Готов выслушать комментарии, особенно, со стороны представителей Российской Федерации.

Спасибо за внимание!

М.В. Якушев,

ПАО «Вымпелком», Россия

О ВОЗМОЖНЫХ МОДЕЛЯХ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Я постараюсь быть достаточно кратким и лаконичным.

Большое спасибо за возможность выступить на Форуме!

Я выступаю здесь как независимый эксперт с опытом работы в Совете Европы, в рамках рабочей группы ООН по управлению Интернетом и хотел бы высказать соображения относительно повышения эффективности в урегулировании вопросов информационной безопасности на международном уровне. Сразу хочу извиниться за то, что какие-то высказанные мной вопросы и предложения могут показаться провокационными, но тем не менее, я предлагаю всем над этим задуматься.

Проблема заключается в том, что мы не видим реального диалога между наиболее крупными и сильными государствами в этой сфере, о чем говорилось, в том числе, и в предыдущих докладах, и как повысить эффективность этого диалога. Каким образом можно эту ситуацию изменить? Я хотел бы остановиться на трех аспектах: фактор доверия, кто в таком диалоге может участвовать и как обеспечить оптимальный формат договоренностей.

Необходимо понимать, что ответственное поведение государств распространяется не только на глобальный уровень, о котором мы чаще всего говорим, но также и на региональный уровень, на двусторонние отношения, на взаимоотношения с другими заинтересованными сторонами, включая транснациональных операторов. Как известно, количество пользователей у крупнейших транснациональных операторов превышает в разы население таких стран, как Индия и Китай. И, наконец, в собственном национальном информационном пространстве также правомерно поставить вопрос об ответственном поведении, так как здесь огромную роль играет фактор доверия. Доверия к тому, что делает государство, подведомственные организации на своей территории в отношении пользователей инфор-



мационных технологий, а также к тому, что делает государство в отношении территории других государств.

Доверие – это вера в порядочность, доброжелательность другого человека, готовность следовать правилам игры, и, конечно, доверие – это основа всех социальных институтов. Почему об этом я говорю отдельно и на этом настаиваю, потому что развитие современных ИКТ, Интернета базировалось на доверии к тому, что делалось на уровне управления, развития, архитектуры Интернета, продолжает делаться. Все, что происходило с 70-х по 2000-е годы до того, как это стало предметом обсуждения на международно-правовом уровне, – все это было исключительно основано на доверии к определенному кругу лиц.

Более того, в российском законодательстве согласно Основам государственной политики Российской Федерации в области международной информационной безопасности меры укрепления доверия вынесены в отдельную тему.

Хотелось бы сказать несколько слов о методологии. Выделяют пять принципов, при которых такое доверие может быть достигнуто:

- открытость процесса выработки решения;
- компетентность участников процесса выработки решения (к сожалению, зачастую этим занимаются люди, которые не очень компетентны в силу своего

Как наладить реальный диалог и выполнение решений этого диалога?

- **Фактор доверия**
 - Применительно к информационным технологиям – ключевой фактор для эффективной разработки, выполнения и последующих модификаций правил поведения
- **Участники диалога**
 - Исходя из опыта обеспечения безопасности интернет-технологий и с учётом многоуровневого характера соответствующих правовых отношений, должны быть учтены интересы всех вовлечённых сторон (государства, бизнес, гражданское общество и др.)
 - В информационной безопасности невозможно полагаться лишь на роль одного заинтересованного участника (пример, государства)
 - Хотя международно-правовой контроль возможен только через (меж)государственные механизмы
- **Формат договорённостей**
 - Использование позитивного опыта разработки и применения международно-правовых норм в иных отраслях регулирования (освоение космоса, безопасность ядерных объектов, международные финансы и т.д.)

Фактор доверия в международно-правовом регулировании ИКТ

ДОВЕРИЕ:

- (1) вера (установка) в порядочность, доброжелательность другого человека; в принадлежность к одному и тому же сообществу, требующая той или иной степени солидарности,
- (2) готовность следовать «правилам игры» (институтам), принятым в [со]обществе -> соблюдать принятые обычаи, выполнять согласованные обязанности и т.д.
- **ДОВЕРИЕ – основа всех социальных институтов**
- На **ДОВЕРИИ** основывались основные процедуры, применявшиеся для развития современных ИКТ в 1970х-2000х годах

Методология обеспечения доверия (при выработке международно-правовых ответственного поведения государств в сфере ИКТ)

- **Открытость** процесса выработки решений
 - Доступность материалов обсуждения (в том числе в интернете)
 - Предварительные уведомления о каждом этапе и процессе в согласованных сроках
 - Регулярная отчетность
- **Компетентность** участников процесса выработки решений
 - Может быть выведена в процессе открытого обсуждения при соблюдении уважительного отношения к мнению оппонента (все мнения должны быть выслушаны, но все мнения должны быть аргументированы)
- **Непрерывность** процесса выработки, имплементации и контроля за соблюдением процедур
 - Одновременно с разработанными процедурами необходимо предусмотреть обязательность постоянной (регулярной) проверки их исполнения всеми участниками
- **Возможность личного общения участников**
 - Регулярные (или, по крайней мере, начальные («установочные»)) и завершающие («результатирующие») очные встречи участников, куда обеспечивается приглашение всех желающих
- **Институционализация** процессов выработки решения
 - Принятие проекта международно-правового акта участниками обсуждения

ТРИ УРОВНЯ ЦИФРОВОГО УПРАВЛЕНИЯ



бэкграунда, в основном это относится к представителям стран с более низким уровнем информационных технологий);

- непрерывность процесса (наличие единой технологии, замысла и воплощения с самого начала и до конца);
- возможность личного общения участников;
- институционализация (любое обсуждение, любой проект обязательно должен быть настроен на выработку международно-правового документа).

Перейду к вопросам участников процесса. Во-первых, в информационной сфере действуют не только правовые нормы, а есть и нормативно-технические нормы, не относящиеся к праву, а относящиеся к стандартам. И какие-то вопросы можно решать и на этом уровне.

Во-вторых, если вспомнить, как общались космонавты во время первого международного полета «Союз – Аполлон». Советские космонавты не знали английского языка, а американцы не знали русского. В результате было принято решение, что советские космонавты А.Леонов и В.Кубасов говорят по-английски, а американские космонавты говорят по-русски. Таким образом происходило взаимопонимание, которое обеспечивало безопасность полета.

Принимая во внимание достаточно сложный многоуровневый аспект цифрового управ-

ления, на каждом уровне которого существует свой набор акторов, а также без учета много-стороннего подхода и многоуровневого характера тех отношений, которые мы регулируем, мы, наверное, не продвинемся. Здесь речь не идет о том, чтобы устранить тех участников переговоров и те договоренности, которые существуют сейчас, речь идет о том, чтобы дополнить их теми диагональными участниками из других уровней общения. Здесь можно говорить с учетом принципа многосторонности, говорить о представителях государства и представителях бизнеса, о представителях экспертного сообщества другого государства, возможна схема, когда между государствами находится международная экспертная организация, возможно обсуждение данных вопросов представителями экспертных сообществ.

К примеру, в прошлом году посол А.Крутских очень позитивно отзывался об инициативе Microsoft по «цифровой» Женеве. И в этом плане, если российская сторона доверяет американской корпорации (напомню, что именно Microsoft первым раскрыл коды, причем именно первой для их продуктов в этой связи была Российская Федерация), то, соответственно, какой-то диалог здесь возможен. А кто может быть со стороны Российской Федерации? Здесь присутствуют представители этих организаций. Это и Лаборатория Касперского, это и очень авторитетный, доказав-

Возможные модели взаимодействия

- Государство А → представитель ИКТ-бизнеса государства В
- Государство А → представитель экспертного сообщества государства В
- Государство А → международная (экспертная) организация → государство В
- Представители экспертных сообществ государств А и В
- [Роль Международного исследовательского консорциума информационной безопасности]
- ...любые другие варианты также могут обсуждаться

О возможных моделях международно-правового регулирования информационной безопасности

Якушев Михаил Владимирович
Гармиш-Партенкирхен // 22 апреля 2019 года

ший свою успешную работу на протяжении 19 лет Координационный центр домена .RU, это и Международный исследовательский консорциум информационной безопасности (МИКИБ) – авторитетное экспертное учреждение, доказавшее свою работоспособность и то, что оно может быть площадкой для решения подобного рода вопросов. Наиболее перспективные здесь – некоммерческие организации типа Координационного центра, так как к Лаборатории Касперского были вопросы со стороны американского правительства, и такие же вопросы можно задать и МИКИБ, но при желании подобный диалог может быть налажен. Также возможны любые другие варианты, но если мы хотим достичь какого-либо результата, то мы должны все эти варианты иметь в виду.

Относительно фиксации договоренностей, мне представляется важным посмотреть, как это решалось в космонавтике. В то время в существенно более сложных условиях биполярного мира был выработан договор 1967 года о принципах деятельности в данной

сфере, после чего появились отдельные соглашения по конкретным вопросам, связанным с выполнением космических полетов, и они согласовывались достаточно быстро и до сих пор составляют основной корпус космического права, который действует и по сей день. Применительно к космическому праву обсуждение шло на базе ООН в Комитете по космосу, и те рабочие группы, о которых мы говорим, могут быть прообразом соответствующего комитета, но я также обращаю внимание, что есть еще одна квази-организация в системе ООН, которая тоже занимается подобного рода вопросами, – это международный Форум по управлению Интернетом. Россия на нем тоже представлена. В 2018 году этот Форум проходил в Париже, в 2019 году он состоится в Берлине. Секретариат этого Форума мог бы посвятить конкретным вопросам, объединяя тем самым усилия экспертов по обсуждению вопроса о заключении международного соглашения по вопросам информационной безопасности.

Большое спасибо!

СЕМИНАР–КРУГЛЫЙ СТОЛ № 2

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИКТ ВО ВРАЖДЕБНЫХ ВОЕННО-ПОЛИТИЧЕСКИХ ЦЕЛЯХ

Ведущие:

Смирнов А.И., Национальная Ассоциация международной информационной безопасности, Национальный институт исследований глобальной безопасности, Россия

Рафал Рогозинский (Rafal Rohozinski), SecDev Group, Канада,
Международный институт стратегических исследований, Великобритания

А.И. Смирнов,

Национальная Ассоциация
международной информационной
безопасности, Национальный институт
исследований глобальной безопасности,
Россия

НОВЕЙШИЕ ИКТ КАК ФАКТОР ГЛОБАЛЬНОЙ НЕСТАБИЛЬНОСТИ: КАК ДОСТИЧЬ КИБЕР МОДУС ВИВЕНДИ¹?

Уважаемые коллеги!

Человечество входит в зону тотальной ломки миропорядка. По оценкам многих экспертов, подрывную роль в этой, столь важной для цивилизации проблеме играет инфогенный нарратив. Осознав данную угрозу, Россия еще в 1998 году инициативно внесла в ООН свои предложения, которые были приняты Генассамблеей в резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Об этом вчера убедительно прозвучало в выступлениях В.П. Шерстюка, А.В. Крутских, С.М. Бойко и других ораторов.

В действующей Стратегии национальной безопасности подчеркнуто, что проведение Россией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее гибридного воздействия: политического, экономического, военного и информационного.

Рассмотрим информационный фактор. Только за последние два года можно привести целый ряд действий США и их партнеров по использованию ИКТ в силовом сценарии воздействия на Россию. Приведу лишь наиболее известные:

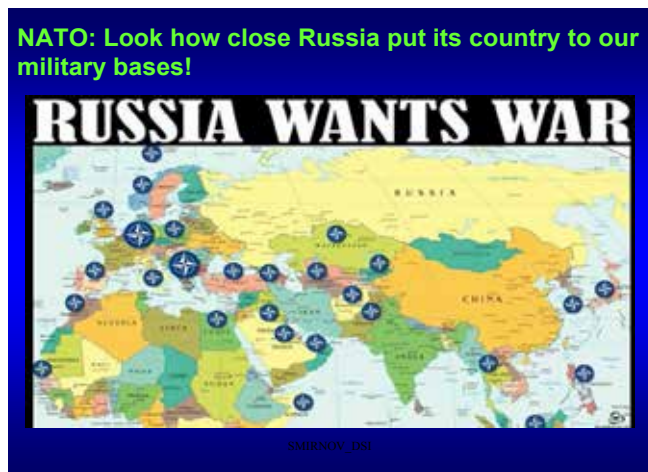
- отказ от взаимодействия с Россией по предотвращению инцидентов в ИКТ-среде, предусмотренного совместным заявлением президентов России и США (2013 год);
- записка Б.Обамы Д.Трампу о закладке в объекты критической информационной инфраструктуры России так называемых кибербомб для подрыва эконо-



мической и социальной стабильности российского общества;

- разработка ЦРУ маскировочных программных средств проведения компьютерных атак, в том числе под «чужим флагом»;
- указание в Стратегии национальной безопасности США (2017 год) на Китай и Россию как ревизионистские силы, которые используют технологии, пропаганду и принуждение, чтобы сформировать мир, противоречащий интересам и ценностям США;
- принятие 23 марта 2018 г. закона Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (Закон о разъяснении законного использования данных за рубежом), который упростил спецслужбам США получение данных с оборудования, поставленного фирмами США в любую страну;
- отмена 16 августа 2018 г. Д. Трампом правил по кибератакам, утвержденных директивой Б. Обамы;
- принятие в сентябре 2018 г. Национальной киберстратегии США и киберстратегии Пентагона, позволяющих киберагрессию и названных экспертами «преамбулой войны»;
- разработка в начале 2019 г. Пентагоном новой стратегии «Троянский конь»,

¹ Модус вивенди (лат., англ. Modus vivendi — образ жизни, способ существования) — дипломатический термин, применяемый для обозначения временных или предварительных соглашений



сутствие механизмов определения атрибуции кибератаки, то есть «кто стоит за кибератакой», не позволяет применять международное право, что само по себе создает дополнительную угрозу сохранению стратегической стабильности. По мнению ряда экспертов, решение этой проблемы лежит в снижении анонимности ИКТ-сферы, т.е. к обязательной идентификации устройств в мировой сети, в том числе с помощью нового интернет-протокола IPv6. Это позволит уполномоченным структурам государства эффективнее бороться с противоправными деяниями в ИКТ-сфере. Напрашивается вопрос: случайно ли ICANN (институт находится под юрисдикцией штата США) тормозит его внедрение?

В этих условиях Россия была вынуждена в целях обеспечения безопасного и устойчивого функционирования интернета на своей территории подготовить соответствующий законопроект, вступление в силу которого намечено на 1 ноября 2019 г.

Опасной угрозой является использование глобальной медиасферы для оправдания силовых подходов к разрешению межгосударственных споров и вмешательства во внутренние дела суверенных государств. В последнее время проблема злоупотребления государствами средствами массовой коммуникации для пропаганды идеологического превосходства, особой исторической миссии становится все более угрожающей. Достоверная информация, распространяемая этими странами, активно перемешивается с ложной информацией («фейками»).

Как это видно на примере мифического российского следа в так называемом «деле Скрипалей», заинтересованные государства

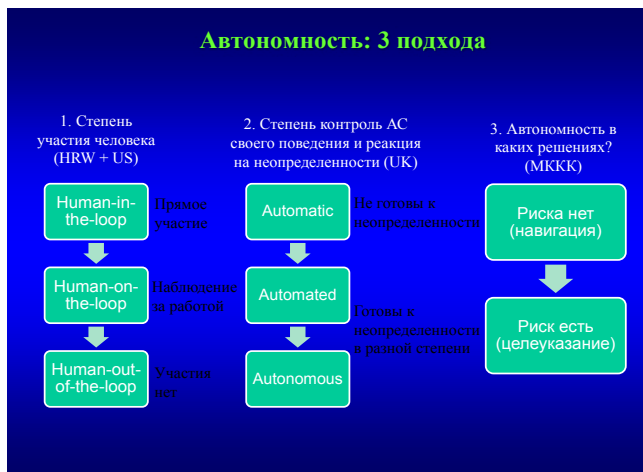


создают цепочки фейковых новостей, образуя своеобразный «фейк-чэйн». Создание «фейк-чэйнов» имеет целью активное манипулирование международным и национальным общественными мнениями, что создает угрозу международному миру и безопасности. В этом контексте уместно привести слова С.В. Лаврова на конференции в Мюнхене (2017 год) «...мы смогли бы быстро преодолеть период «post-truth», отбросить навязываемые международному сообществу истеричные информационные войны и перейти к честной работе, не отвлекаясь на ложь и вымыслы. Пусть это будет эпоха «post-fake».

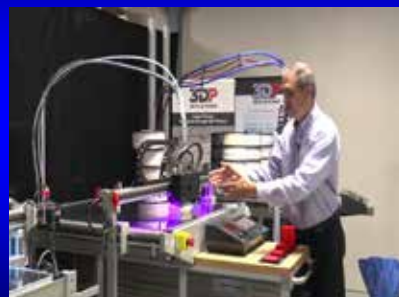
В настоящее время у России с НАТО практически нет совпадающей повестки дня в сфере безопасности. НАТО устроено таким образом, что его генетический код постоянно проявляет себя. Эти проявления мы видим и сегодня – поиск врага на Востоке, от которого надо обороняться. На самом деле это абсолютно тупиковый путь.

НАТО, ведомое США, активно применяет гибридные угрозы, в том числе информационные. Центры передового опыта НАТО в Таллинне (киберзащиты), в Риге (стратком) и в Хельсинки (совместно с ЕС – противодействие гибридным угрозам) – тому убедительное подтверждение. Более того, для координации этой работы в НАТО в 2019 году создается Центр киберопераций в г.Монсе (Бельгия). При открытии Центра в Риге в 2015 году отмечалось, что в его арсенале есть средства (армия «умных» ботнетов, роботроллинг, инспирирование «кибербунтов» и т.д.), способные заставить врагов потерять волю к борьбе, возненавидеть собственную страну, и это обеспечит бескровную победу.

Автономность: 3 подхода



«Аддитивное производство»



Технология производства беспилотников, торпед, запчастей, боеприпасов на 3D-принтерах прямо месте (напр. на борту судна).
Предполагает сокращение расходов на хранение, ремонт и модернизацию вооружений и оборудования, и возможность получить наиболее современное оружие по требованию.

Особую роль в НАТО играет Великобритания, где создан новый Центр не только для противодействия киберугрозам, но и проведения наступательных операций. В ноябре 2018 г. хакеры из группировки Anonymouse выложили документы о деятельности Института государственного управления Integrity Initiative, который Великобритания использовала для вмешательства во внутренние дела других стран, в том числе для информационной войны против России. Примечательно, что после публикации проекта «противостояние России» в ответ на ноту посольства России, он был признан Форин Офисом. Судя по всему, Великобритания не сделала выводов из скандала (2018 год) с компанией Cambridge Analytica, которая использовала технологии глубинного анализа, в том числе данных соцсетей, взятки и компромат, вмешиваясь в ход выборов в десятках стран мира.

Североатлантический альянс активизировал координацию своих мероприятий с киберпроектами ЕС. По аналогии с центром «Стратком» НАТО в Риге ЕС в 2015 году создал Оперативную рабочую группу по стратегическим коммуникациям. Группа (400 экспертов из 30 стран) выпускает еженедельно по сути русофобский «Обзор дезинформации» с оговоркой, что он не отражает позиции ЕС. Анализ обзоров показывает их примитивно фейковый уровень и политизированную «охоту на киберведьм».

Резюмируя, приходится констатировать, что дальнейшее промедление с разработкой и принятием Модуса вивенди – временного или предварительного соглашения по правилам ответственного поведения государств в ИКТ-сфере – смерти подобно.

Потомки нам этого не простят!
Спасибо за внимание!

Рафал Рогозинский (Rafal Rohozinski)

SecDev Group, Канада, Международный институт стратегических исследований, Великобритания

Доброе утро! Мне очень приятно опять присоединиться в рамках 13-й конференции Форума. Как красноречиво сказал мой коллега, – это один из самых важных круглых столов. Речь идет о проблемах противодействия использованию ИКТ во враждебных военно-политических целях. Хочу повторить некоторые слова Чака Барри, прозвучавшие вчера, о важности Гармишевского форума. Иногда может показаться, особенно глядя на эти 13 лет, что этот диалог у нас очень широкий. Но один из конкретных результатов гармишевской программы состоит в организации круглого стола, посвященного военному применению, боевому применению киберпространства. Участвуют представители Китая, Российской Федерации, США и такой круглый стол уже проводится более четырех раз в рамках этой конференции. Это имеет серьезное воздействие, потому что это одна из немногих встреч такого рода, где мы рассматриваем конкретные шаги, необходимые для того, чтобы создавать меры укрепления доверия в военной киберсфере с тем, чтобы эти меры становились частью международного диалога.

Презентация, которую я сделаю, планировалась на вчерашний день, посвященная юридическим вопросам, поэтому речь пойдет не только о боевом применении киберпространства. Выводы, послужат хорошим переходом к последующим докладам, которые у нас запланированы на сегодняшний день.

Итак, три нити – одна паутина. Я объясню потом заголовок. Речь идет о различных нитях диалога, которые мы ведем в течение 13 лет, обсуждая киберпространство. Освежу нашу память. Мы прошли революционные изменения. Цифровые трансформации, изменившие не только отношения между гражданами и государством, но также между самими государствами. Парадоксально, но факт, и это немножко противоречит тому, что сказал Чак, последний раз трансформационная технология произошла во время запуска спутника, и через 10 лет в США была создана структура,



благодаря которой затем появилась возможность заключить договор. Парадокс состоит в том, что за 17 лет после изобретения Интернета мы так и не нашли стабильных четких правил, с которыми бы все согласились. К сожалению, организации в предыдущих случаях существовали, например ООН, несмотря на усилия таких людей, как посол А.Крутских, такие организации оставались заблокированными. Поэтому, может быть, на данном этапе стоит подумать о создании правил немножко иным образом. Вместо того, чтобы рассматривать все кибервопросы в рамках одного большого соглашения, может быть, пора начать двигаться по трем различным направлениям. Как киберпространство связано с вооруженной борьбой, как оно соприкасается с базовой безопасностью и как кибервопросы пересекаются с экономикой. Я поговорю об этих трех направлениях поочередно.

Извините, в одном случае я не смогу показать видео по техническим причинам, поэтому я просто поясню, что вы могли бы увидеть в этих роликах.

Итак. Кибервойна. Вооруженная борьба. Важно признать одну истину в этой сфере, а именно – война с применением киберсредств стала реальностью. Это не теоретический конструкт, это не тема будущего, это настоящее, существующее в рамках доктрин и оперативной практики в развитых странах, включая присутствующие здесь.



Некоторые из нас говорят об информационной войне, кибервойне, кибероперациях, боевых действиях. Наверное, терминология которая лучше всего понимается и переводится на русский и английский языки, – это понятие кибер- и электромагнитной деятельности, состоящей из трех доктринальных компонентов: радиоэлектронная борьба, кибероперации, включая информационный компонент, и операции по управлению спектром.

Подробнее не будем останавливаться, но, по крайней мере, у нас есть две страны, которые пользовались этими средствами в Сирии. Признается, что тактические, оперативные, стратегические потенциалы описаны, разрешены, а также реально используются. Что это признание доктринально признанных возможностей означает при применении норм в киберпространстве? В прошлом году прозвучало интересное выступление коллеги из Российской Федерации, который сравнил несколько договоров в области контроля над вооружениями, насколько они применимы или не применимы в киберпространстве.

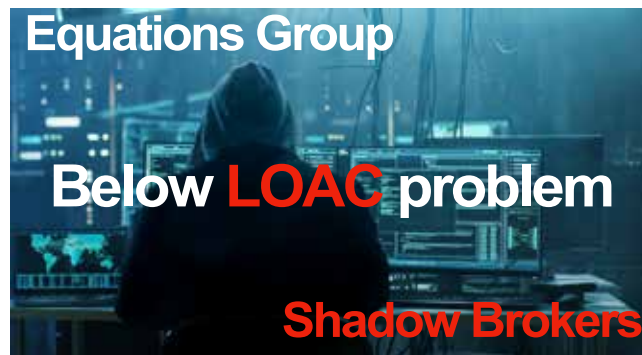
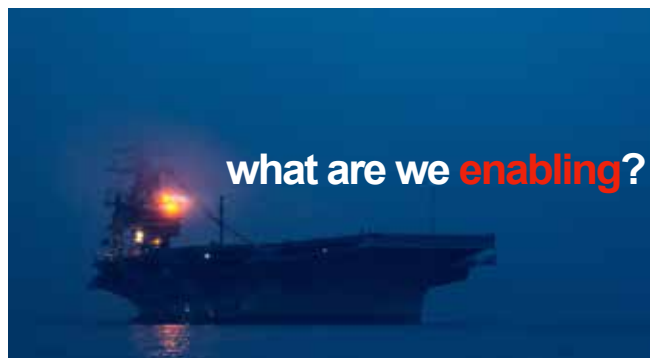
Приходят на ум усилия договориться об ограничении кораблей подобно обсуждениям киберпространства. В рамках этого договора делались усилия ограничить строительство кораблей, хотя они уже существовали и использовались военно-морскими флотами. Продолжая вчерашнюю дискуссию о правовом определении того, что существует или

не существует, есть ли атрибуция или нет ли атрибуции, вызовы этого договора 20-х годов состояли в том, что использовались метрические положения без значения, верификация без доверия.

Большинство этих характеристик существует и в рамках нынешней дискуссии, когда делается попытка определить нормы, регулирующие военное применение киберсредств. И подобно тому, как этот договор о дредноутах в межвоенный период так и не смог ограничить военно-морскую мощь и на самом деле привел к распространению авианосцев – это совсем новая категория крупных кораблей.

Подобно этому мы должны спросить себя: к чему приведет нынешняя дискуссия о кибернормах и военном применении киберсредств? Какие могут быть последствия того, что мы не сможем договориться об этих нормах и что мы этим открываем? Это вопрос, на который я пока не могу дать ответ. Но следующая война, наверняка, будет войной, которая будет вестись в кибер- и электромагнитном пространстве.

Опасность, как было очень красноречиво обозначено послом А. Крутских в прошлом году, опасность состоит в следующем. Наши старые стратегические вопросы, наша старая стратегическая культура, которая со времен Второй мировой войны касалась объявления своих потенциалов, сил и средств сдерживания, эта стратегия больше не работает, когда мы не готовы объявить о наличии наших по-



тенциалов, сил и средств в киберпространстве. Это старый стратегический расчет может на самом деле создать не безопасность, а, наоборот, опасность.

Киберзащита, кибербезопасность сейчас. Сейчас цифровая среда за последние 30 лет критически зависит от технологий, которые по своей сути небезопасны. Это не неудача или недосмотр государств, это неудача промышленности, бизнеса, которая имеет критически важные последствия для безопасности государств. Это карта, сгенерированная программой, определяющей опасную инфраструктуру. Красным обозначены критические информационные системы, которые относятся к промышленным предприятиям, принадлежат электросетям, водоснабженческим предприятиям, и в данный момент времени не обладают соответствующими средствами защиты.

Эта опасность возникла в результате отсутствия регулирования государствами на национальном уровне с тем, чтобы вынудить производителей технологий встраивать соответствующие меры безопасности в эти продукты. Последствия стали широко распространенными. Бизнес и государство сейчас ощущает последствия этих регуляторных пробелов. В результате этого возникает экономика киберпреступности, которая недорога и всепроникающа.

Вы видите, что купить эксплойты на открытом рынке совершенно недорого. Я могу

купить зловред за 25 долларов, и DDos-атаки – самые дорогие продукты, которые сейчас предлагаются. Более того, распространение или боевое применение ошибок программного обеспечения и выпуск этих эксплойтов группами, которые относятся к определенным государствам, может некоторые из них представлены здесь, представляют собой серьезную проблему, не подпадающую под регулирование права вооруженного конфликта. Некоторые из этих эксплойтов включают эксплойты «нулевого дня», например, Stuxnet, обладают значительным потенциалом нанесения крупного экономического ущерба.

Атака «NotPetya» в 2018 году привела к блокировке работы большого количества предприятий, вызвала ущерб на сотни миллионов долларов для компаний, расположенных не только в Украине или Российской Федерации, но и по всему миру.

С точки зрения НАТО, логистика НАТО тоже серьезно пострадала от атаки «NotPetya». Больше всего пострадала компания «Maersk» – крупнейший перевозчик контейнеров в тот момент. Ущерб сразу составил 300 млн. долларов, 1 млрд. долларов на восстановление, потеряли 10% глобального бизнеса, и это было результатом атаки третьей стороны, которая была направлена против цели на Украине.

С точки зрения статистики и денежного ущерба, киберпреступность, связанная с ки-



беропасностью, возросла в 5 раз с 2015 года, в год на 26%. В результате этого, более 1 триллиона долларов будут вложены в вопросы киберзащиты в ближайшие 5 лет.

К сожалению, эти потери становятся настолько большими, настолько неограниченными, что они приобретают каскадирующее воздействие на экономику. Например, в этом году 3 крупнейшие страховые компании решили, что они не выплатят страховые компенсации по ущербу в результате «NotPetya», так как они связывают это с использованием зловредного ПО в контексте конфликта. То есть они рассматривают украинский конфликт в качестве военного конфликта, и поэтому это не подпадает под условия выплаты страховой компенсации, если это возникает в зоне конфликта. Это кибербезопасность.

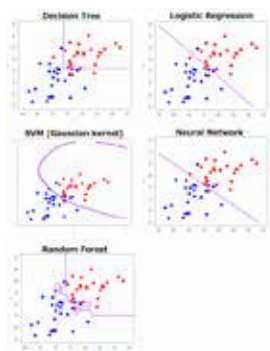
3-й вопрос. Цифровая экономика. Этот вопрос пересекается частично с кибербезопасностью. Необходимо рассматривать этот вопрос отдельно, потому что это также касается распространения новых соединенных устройств, которые являются сейчас основой национальной и глобальной экономики.

В 2013 году этот рынок составлял 3,7 триллионов устройств, к 2020 году будет около 30 млрд. таких девайсов, и общий объем экономики будет составлять триллионы долларов.

Глобальная цифровая экономика, по данным Всемирного банка, сейчас составляет

четверть всего глобального ВВП, и эта доля растет, и она все больше связана с ростом городов, с урбанизацией. Цифровая городская экономика, по состоянию на 2018 год, охватывает более 54% всего населения мира, а 62% живут в городах с населением более 1 млн. человек. В ближайшие 20 лет мы увидим, что в городах будет жить более 6 млрд. человек, и 85% мирового ВВП будет вырабатываться в этих городах, а 90% этих городов будут расти более высокими темпами в Азии и Африке. Важно признать, что города играют важную роль в цифровой экономике, потому что это зоны гиперсвязей, гиперсоединений. В следующие 4 года на «умные» инфраструктуры в городах будет потрачено более 43 млрд. долларов для управления этими огромными конгломератами человечества, подсоединяя более 1 триллиона отдельных устройств.

Почему это важно с точки зрения кибербезопасности? Потому что такой масштаб концентрации делает очень важным фактором с точки зрения управления инновации, развивающиеся наиболее быстро в самых крупных городских агломерациях. Коллеги из Китая сразу же узнают, что когда речь идет о таких мегагородах, этим городам нужны «собственные мозги» для того, чтобы управлять таким уровнем сложности. Это подводит нас к рубежу, где кибербезопасность начинает пересекаться с цифровой экономикой, искусствен-



**AI is
dependent on
classifiers to
make
predictions**



ным интеллектом (ИИ). Какова возрастающая роль искусственного интеллекта? Без систем искусственного интеллекта мы не сможем управлять цифровой экономикой такого уровня сложности. Тем не менее, с точки зрения кибербезопасности или с точки зрения норм, мы мало говорим об угрозах сложных систем управления, связанных с искусственным интеллектом. Важно признать, что независимо от того, что бы вы ни читали в научной фантастике, нынешний прогресс пока основан на математических достижениях последних 20 лет. Системы становятся умнее благодаря более быстрым процессорам и более крупным объемам данных. Но прогресс в области ИИ интересен и значителен с точки зрения воздействия на экономику и воздействия на вооруженную борьбу.

Многие из вас, наверное, читали об игре «Альфа Го», которая победила чемпиона по игре в Го в 2017 году. Но вы, наверное, не знаете, что предшественница «Альфа Го» 2016 года на самом деле победила самых лучших американских пилотов в тренажерных битвах, потому что она просчитывала быстрее, чем пилот все различные баллистические моменты, необходимые для воздушного боя. И этот аспект ИИ, который называют глубоким обучением, это, наверное, самое близкое, что мы пока достигли относительно автономного существования систем. Важно признать, что хотя ИИ, кажется, думает, на самом деле он не думает, это дидактическое логическое размышление, поэтому попытки использовать ИИ в тех случаях, где он может реагировать на изменение данных, это может привести к очень серьезным и мрачным последствиям.

Например, в 2016 году фирма Microsoft выпустила чат-бот 3, который должен был учиться и взаимодействовать с людьми в социальных сетях. В течение 16 часов этот бот Тей преобразовал себя, превратился в не-

онацистский, женоненавистнический бот, который призывал к созданию концентрационных лагерей, потому что он использовал данные открытого Интернета, использовал классификацию и пришел к выводу о том, что норма должна состоять именно в таком контенте, в таком нарративе, в таких ценностях. Поэтому может показаться, что от вашего любовника можно избавиться 50-ю способами, но на самом деле у ИИ есть всего 6 хороших способов для прогнозирования и предсказания. Из-за этого манипуляции с ИИ для неправильного выбора – очень простая вещь. Я покажу вам видеоролик, как это работает. Это изображение собаки. ИИ узнает, если добавить звук, ИИ думает, что это страус. Фактически, эта картинка достаточно искажена, ИИ думает, что это компьютер, а не кот. Чтобы вы увидели, что можно манипулировать и заставлять машину думать, что банан на самом деле является тостером. То есть можно использовать для искажения технологии распознавания лиц, используя разную одежду, различные фильтры, которые манипулируют классификаторами и идентификаторами.

Говоря о боевом применении социальных сетей, мы должны, прежде всего, беспокоиться по поводу боевого применения ИИ, лежащего в основе этих систем. Это не контроль над контентом, а, скорее, контроль над автономными алгоритмами, которые применяют эти системы.

Проблемы технологии свидетельствуют о том, как легко манипулировать реальными людьми, которые говорят вещи, которые они в другом случае никогда бы не сказали. Все это только начало. Как мы увидели на протяжении последних 20 лет, конфликт будет развиваться и эволюционировать неожиданным образом и менять наше представление на различных уровнях. Взаимная устойчивость – луч-



шая гарантия безопасности. В данный момент она под угрозой. Не просто из-за отсутствия общих терминов, касающихся кибербезопасности, но и из-за того, что мы даже пока не начали размышлять над новыми формами опасности, например, враждебное использование ИИ или намеренное применение методик противодействия искусственному интеллекту, которые касаются военных, экономических и социальных аспектов.

Что делать? Возвращаемся к этим трем нитям. Если признать, что, может быть, у нас есть 3 различных направления диалога по поводу кибернорм: война, безопасность и экономика, может быть, будет правильным разделить эти нити в отдельные каналы с целью нахождения небольших дискретных соглашений. Наверное, мы должны признать, что военное применение киберсредств в ближайшем будущем будет приводить к конкуренции. Стратегическая культура не позволит нам найти общий язык просто потому, что преимущества, которые мы получаем в результате этого, слишком велики, чтобы договариваться немедленным образом или строить меры укрепления доверия.

Отсутствие безопасности. Способность находить общий язык здесь больше, потому

что источник опасности не в сфере государственной конкуренции, а в области базовой опасности киберсредств, неспособности регулировать вопросы кибербезопасности на наднациональном уровне. И поэтому здесь нахождение точек соприкосновения может быть легче, чем в военной сфере.

Теперь экономика. Где у нас самая большая взаимозависимость и, наверное, здесь есть почва для сотрудничества, особенно, по таким вопросам, как искусственный интеллект. Здесь, наверное, таких возможностей больше всего.

В целом я призвал бы к следующему. Давайте, чтобы идеальное не стало врагом хорошего, достаточно хорошего. Может быть, нам надо снизить планку, стремиться к этому и признавать, что взаимодействие по этим сложным вопросам друг с другом необязательно означает создание возможностей для неприемлемого поведения, а скорее создание возможностей там, где мы можем договориться и констатировать разногласия там, где они имеются.

Перед нами самые различные варианты выбора будущего, но неудача не должна быть одним из этих вариантов.

Спасибо!

В.В. Карнаух,

*Генеральный штаб Вооруженных Сил
Российской Федерации*

О МЕРАХ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИКТ ВО ВРАЖДЕБНЫХ ВОЕННО-ПОЛИТИЧЕСКИХ ЦЕЛЯХ¹

Тема противодействия использованию информационно-коммуникационных технологий (ИКТ) во враждебных военно-политических целях чрезвычайно объемна. В ходе предыдущих форумов наши представители уже освещали ряд важных направлений данной работы, поэтому в своем сегодняшнем выступлении затрону дополнительно ряд мер, актуализация которых, по нашему мнению, будет эффективно способствовать предотвращению вооруженных конфликтов, которые могут возникать в результате использования ИКТ.

Во-первых, убеждены, что необходимо выработать единую терминологию, что позволит добиться необходимого взаимопонимания между участниками диалога при обсуждении вопросов предотвращения враждебного использования ИКТ. Речь идет не только о том, что одни эксперты используют «информационную», как мы, терминологию, другие – «кибертерминологию». Зачастую даже при использовании единой терминологии национальные делегации вкладывают в них различное содержание. В первую очередь, это относится к таким терминам, как сами «ИКТ», «инцидент в сфере использования ИКТ», «конфликт в результате использования ИКТ». Данные термины постоянно используются в форматах ООН, ОБСЕ и в Российской Федерации. Очевидно, что от того, насколько широко будет трактоваться понятие «информационно-коммуникационные технологии», зависит широта охвата вопросов, рассматриваемых в ходе переговоров. В свою очередь содержание этого базового понятия будет определять наполнение всех остальных понятий, связанных с его использованием.

Практика переговорной работы в ООН, ОБСЕ и Региональном форуме АСЕАН по безопасности показала, что под информационно-коммуникационными технологиями, как правило, понимаются только компьютерные



сети или их отдельные элементы. Полагаем, что подобное ограничение существенно затрудняет решение проблемы предотвращения использования ИКТ во враждебных военно-политических целях.

Например, общеизвестно, что одной из причин возникновения межгосударственных конфликтов является распространение расистской, ксенофобской информации, а также информации, оправдывающей геноцид или преступления против человечества. Для того чтобы эффективно противодействовать этой причине, недостаточно принимать меры только в рамках сети Интернет. Меры противодействия должны охватывать средства массовой информации, которые имеют свои сайты в Интернете, и могут быть первичными источниками деструктивной информации.

Поэтому предлагаем в понятие «информационно-коммуникационные технологии» включить не только компьютерные сети, но также и электронные средства массовой информации, которые в настоящее время стали неотъемлемой частью мирового информационного пространства.

Под «инцидентом в области использования ИКТ» представляется целесообразным понимать все возможные события, которые оказывают негативное влияние на безопас-

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

ность не только инфраструктурных объектов, но и на общественное сознание социума.

В первом случае такими событиями традиционно считаются компьютерные атаки, имеющие целью несанкционированный доступ к охраняемой информации или к самой компьютерной технике с последующим выполнением каких-либо деструктивных действий, то есть вывод из строя, уничтожение, модификация, хищение и другие. Сюда же можно отнести создание преднамеренных или случайных радиопомех в каналах передачи информации компьютерных сетей. Кстати, в новой Стратегии национальной безопасности США электромагнитные атаки на информационную инфраструктуру уже поставлены в один ряд с компьютерными и физическими атаками.

Во втором случае к инцидентам в области использования ИКТ следует отнести:

- распространение угроз применения силы против территориальной неприкосновенности или политической независимости любого государства;
- проведение клеветнических кампаний и распространение оскорбительной или враждебной пропаганды, имеющей целью осуществление интервенции или вмешательство во внутренние дела других государств;
- распространение фальшивых или искаженных сообщений, которые могут рассматриваться как вмешательство во внутренние дела государств или как наносящие ущерб укреплению мира, сотрудничества и дружественных отношений между государствами и нациями;
- подстрекательство к подрывной террористической или вооруженной деятельности, направленной на насильственное свержение строя другого государства, равно как и способствуя ей, а также вмешательство во внутренние дела в любом другом государстве.

Содержание понятия «конфликт в результате использования ИКТ» предлагается рассматривать исключительно в политическом смысле, то есть применительно к влиянию инцидентов в области использования ИКТ на систему международных отношений в региональном и глобальном формате.

Перечисленные выше предложения Министерством обороны Российской Федерации

оформлены в виде Словаря базовых терминов в области безопасности при использовании информационно-коммуникационных технологий. В настоящее время активно продвигается в форматах с участием Российской Федерации. Также полагаем целесообразным продолжить рассматривать инициативу распространения в форматах ОБСЕ и в деятельности создаваемых рабочих органов ООН по международной информационной безопасности: Рабочей группы открытого состава и Группы правительственных экспертов.

Во-вторых, считаем, что предотвращение враждебного военно-политического использования ИКТ будет способствовать началу политического диалога по вопросу международно-правового определения термина «пропаганда» и выработке цивилизованного механизма пресечения ее распространения.

Сейчас публично в официальном медиaprостранстве постоянно звучат взаимные обвинения государств в проведении в отношении друг друга пропагандистских кампаний, дестабилизирующих международную обстановку. Причем нельзя гарантировать, что в борьбе с так называемой пропагандой страны НАТО при удобном случае вновь не воспользуются опытом войны 1999 года в Югославии. Тогда Белградский телевизионный центр, названный инструментом сербской пропаганды, был просто уничтожен бомбардировками натовской авиации. Где гарантия, что современная западная демагогия относительно российской пропаганды не приведет к тому, что сугубо гражданские объекты, такие как телевизионные центры Russia Today и Sputnik и им подобные, не станут целями для нанесения очередных ракетно-бомбовых ударов?

Следует отметить, что первая попытка решить эту проблему цивилизованным путем была предпринята по инициативе СССР в период с 1954 по 1974 годы в рамках работы над проектом резолюции Генассамблеи ООН «Определение агрессии». Тогда возобладало мнение американской делегации, представитель которой заявил: «То, что для СССР является пропагандой, для США лишь проявление права на свободу слова и выражения мнений».

Как показали югославские события, мнение Вашингтона по данному вопросу в зависимости от ситуации может меняться на прямо противоположное.

Поэтому предлагаем вернуться к решению начать работу по содержательному наполнению понятия «пропаганда», а также выработать критерии, по которым можно определить, в каком случае распространяемая информация нарушает базовый принцип свободы слова и приобретает признаки этого негативного явления.

После этого можно будет выработать механизм международно-правовой регламентации данного вопроса.

Считаем, что решение этих вопросов позволит перевести обсуждение темы пропаганды из публичной медиасферы в политическую. Это будет способствовать предотвращению возможного возникновения эскалации межгосударственных конфликтов с незаконным применением военной силы, а также в отношении таких гражданских объектов, как телевизионные и радиопередающие центры.

В-третьих, полагаем, что членам мирового сообщества необходимо принять обязательства не использовать нормы мягкого международного права для оправдания односторонних незаконных действий на мировой арене. На этом новом явлении не так давно заострил внимание Министр иностранных дел Российской Федерации, отметив, что международное право упорно пытаются подменить неким порядком, основанным на правилах. Эти правила изобретаются по принципу политической целесообразности, используются для оправдания агрессивной деятельности в отношении тех, кто дорожит своим суверенитетом и стремится проводить независимую внешнюю политику, отстаивает коллективные пути решения международных проблем на основе консенсуса и баланса интересов.

К сожалению, отдельные члены мирового сообщества не скрывают, что нормы мягкого международного права, такие как правила поведения, меры доверия, меры наращивания потенциала и другие, рассматриваются ими не как инструмент для обеспечения мира и безопасности, а как международно-правовая основа для одностороннего решения своих внешнеполитических задач.

Данное обстоятельство создает высокий риск обострения международной обстановки, усиление напряженности, возникновение эскалации межгосударственных конфликтов.

В этой связи считаем, что практическое применение инструментов мягкого права в информационном пространстве должно отвечать следующим требованиям, соответствуя общепризнанным принципам международного права, закрепленным в Уставе ООН, такие как:

- неприменение силы и угрозы силой;
- невмешательство во внутренние дела других государств;
- мирное урегулирование споров, суверенное равенство государств;
- соблюдение принципа ненападения, отсутствия угрозы силой, безопасности государств-участников, равно как и третьих стран;
- непредоставление какому-либо государству либо группе государств преимуществ в военной, разведывательной, политической, экономической или иных сферах;
- неиспользование в качестве инструмента вмешательства во внутренние дела государств;
- неиспользование для необъективной политической оценки действий и намерений государств в информационной сфере с последующим принятием различного рода наказаний в виде санкций или иных мер реагирования.

Следует отметить, что такой подход ранее был закреплен в формате резолюций Генеральной Ассамблеи ООН применительно к мерам укрепления доверия.

Убеждены, что выполнение перечисленных требований в отношении любых инструментов мягкого права будет эффективно способствовать предотвращению и урегулированию конфликтов, поддержанию международного мира, стабильности и безопасности в региональном и глобальном масштабе.

Благодарю за внимание!

Гэри Браун (Gary Brown),

независимый эксперт, США

ПРАВИЛА ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ И ЭЛЕКТРОМАГНИТНОМ ПОЛЕ

Спасибо большое за возможность выступить перед этой авторитетной аудиторией. Прошу прощения заранее за то, что моя презентация мало кому понравится. Почему? Потому что я первый раз предпринимаю попытку, а первый блин комом, как говорят в России, первый раз я выступаю в таком формате, поэтому проявите терпение, пожалуйста.

Из представления было понятно, что я отслужил в вооруженных силах США. Киберпроблемы выходят сейчас на первый план из-за того, что государства живут сейчас практически в информационном пространстве. Мы постоянно сталкиваемся поэтому друг с другом именно вот в этом новом, четвертом, измерении: в киберпространстве в дополнении к традиционным. И поэтому тут очень много возможностей, к сожалению, для неправильного понимания намерений. Это может привести к расширению масштабов этого противостояния. Надо этого избегать с самого начала, поэтому надо не допустить эскалации. Для этого нужно перейти, как правильно говорят коллеги, на единый язык, на выработку единого понятийного аппарата. Я это по-другому назвал и независимо от вас тоже пришел к этому выводу, я называю это – грамматика эскалации. Это требует от нас и действий, и в то же время реагирования. Нужно пытаться оказаться на одной частоте, чтобы мы могли адекватно воспринимать те или иные факторы.

Вот интересно, несмотря на то, что многие жалуются на то, что государства не всегда должным образом учитывают сложившуюся практику, которой владеют специалисты, техники, инженеры, частично это справедливо, в то же время уже накопилась критическая масса публикаций, практического опыта, который заставляет государства уже адекватно реагировать на атаки, на нападения, на наступления в информационном пространстве. Как нет единой Библии для всех конфессий, так нет и единого описания правил поведения в киберпространстве. Что плохо на самом деле. Поэтому лучше, чтобы все наши дискус-

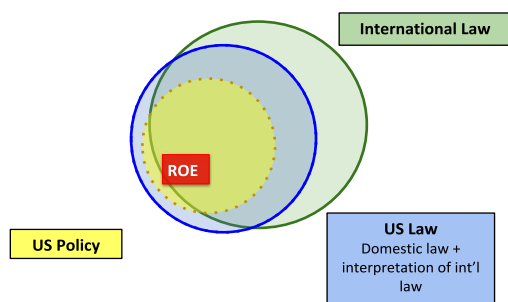


сии оставались в виртуальной среде и не переходили в фазу физических, кинетических, как принято в американской литературе, проявлений.

Итак. Какие вызовы стоят перед нами? Вот все говорят о том, что право отстает, правовые нормы отстают от технического прогресса. Смысл в том, что у нас имеется один источник права, который в этом случае применим, – это международное гуманитарное право, которое регулирует вступление в вооруженный конфликт и ведение его. Мы даже не говорим о других международных нормах. Мы исходим из допущения по умолчанию, что этот источник права должен применяться также и в киберсфере. Хотя, подумаем об альтернативах. Какие есть источники права: нормы, обычаи, сложившиеся практики, договоры на бумаге, не на бумаге, традиции. Давайте подумаем, а могут ли вот именно выработанные человечеством нормы, не обязательно в гуманитарном праве, а по всему другому комплексу взаимоотношений, быть применены к киберпространству?

Что такое нормы? Это тот же кодекс поведения, ответственность. Я хочу сказать, что формируется некая практика в отношениях между государствами, и она достаточно часто превращается в обычаи, формируется обычное право, которое не обязательно закрепляется на бумаге, но оно органично, как бы естественным образом, обростает этими практи-

Rules of Engagement



Categories of possible response

Destructive response (armed conflict)	
<i>May cross threshold of conflict</i>	
Active hack-back	
Reach outside system	
<i>May reach outside</i>	
Respond inside system	

ческими проявлениями, и государства перед тем, как что-то сделать, смотрят слева-справа на соседей и стараются следовать вот этому обычаю. И нарушения этого обычая приводят к неким оргвыводам, санкциям, например, дипломатического характера и т.д.

Теперь переходим к третьей категории – нормы. Она уже фиксируется в каких-то международных договоренностях, в хартиях, в уставах и т.д. То есть, видите, вот такая эволюция. Эта норма в перспективе может уже превратиться в закон, то есть имеется ввиду, что она находит свое воплощение в местном национальном законодательстве стран, то, что называют гармонизацией, то есть приведением национального законодательства в соответствие с международными правилами, законами, нормами. Хотя, как правило, то, что принимается на уровне ООН, например, нельзя сказать, что это такие законы, которые имеют обязывающую силу.

В конце концов, это тоже определенные рекомендации, они апеллируют к духу, к готовности международного сообщества жить по определенным цивилизованным правилам. Хотя я немного скептически отношусь к тому, насколько успешно это может реализовываться в контексте киберпространства. Завершая мысль, хочу сказать, что в сообществе есть недопонимание и одни и те же люди используют слово «норма» в значении «law» – «право». Это вводит в заблуждение. Поэтому опять же все упирается в определение дефиниций и терминов, понятийного аппарата. Вот опять мы сталкиваемся с этими трудностями относительно того, как нам разобраться не только по сути, но и по форме, то есть по словесному оформлению этих явлений.

Сейчас вы, может быть, меня забросаете камнями, потому что я предложу вам некий альтернативный подход, то есть обратимся к сложившейся в прошлом практике. Киберкомандование США предполагало необходимость выработки неких политических мер, норм, требований, применимых к киберпространству, к поведению в киберпространстве. Это может быть односторонний подход – заявить об этих нормах. Это тоже был фактор, который ограничивает возможность для безответственного поведения, но в то же время есть другой подход, в котором формируются, так называемые правила задействования сил и средств. Но конкретно, по моему мнению, – правила применения силы: будут разворачиваться миссии наблюдателей ООН. Но есть некие правила, которые предполагают применение ими силы в каких-то обстоятельствах. Можно ли перенести этот подход к киберпространству?

Я хочу сказать, что это своего рода директивы, системы, которые определяют категории, действия и противодействия, которые определяют обстоятельства, при которых государство может применить весь спектр своего воздействия, всю полноту своего потенциала в случае агрессии, вторжения и т.д., происходящих в киберсреде. Но это, естественно, оказывает воздействие и на физические элементы.

Также уже сформирована такая практика, когда каждая страна имеет свое представление о международном праве. Вот если взять страны Персидского залива, США, то США традиционно имеет свои позиции, свое особое мнение, отличное от мнения многих других стран по тем или иным аспектам международного права. Речь идет о толковании, о том,

Target and effect on target

	Civilian system	Gov't system	Critical infras.	Nat'l sec. system	NC2
Physical effects					
System harm (virtual)					
Data manipulation or destruction					
Data exfiltration					
Persistent presence, spying					
Penetration, privilege escalation					
Recce/attempted penetration					

Cyber ROE framework limitations

- Require rapid assessments of responsibility, which could be mistaken
- States must publicly announce and be willing to accept the responses as appropriate
- Broad categories open to interpretation
 - Categories expected to be refined over time

что остается на «усмотрение» той или иной страны, и поэтому не все так зеркально накладывается одно на другое, а есть особенности восприятия и толкования международного права со стороны разных субъектов.

Переходим к типологии, к заранее установленной категории вариантов ответа на разные категории агрессии, которые, естественно, заранее подлежат некоему определению, правовой характеристике и квалификации. Я хочу предложить разные категории возможных агрессий и реагирования на них.

Давайте разобьем на классы по нашей типологии. Смысл заключается в том, что государство выбирает что-то определенное среди разных категорий возможных реакций. Я потом дам ссылку относительно классификации видов агрессии. С учетом некоего порога, некой «красной черты», при пересечении которой уже конфликт превращается в вооруженную фазу. Речь идет, может быть, о недружелюбном поведении со стороны тех или иных акторов в киберпространстве, и думаю, что уже формируется широкое понимание относительно того, что, действительно, действия в киберпространстве могут приблизиться к этому опасному порогу, опасной «красной линии», за пределами которой уже возможна физическая атака.

Скажем, подрыв гидроэлектростанции, плотины, отключение банковской системы – все это уже имеет физические последствия, и государство, наверное, не будет обязано

реагировать, но, тем не менее, перед нами некая «корзинка» вариантов ответов, среди которых государство будет выбирать наиболее адекватные.

Далее. Цель и последствия, и какого эффекта государство хочет добиться. Слева направо определены категории, а сверху вниз – возможные варианты агрессии со стороны злоумышленников в киберпространстве. Например, если пострадают некоторые физические объекты, то ряд наблюдателей предполагает, что государству необходимо жестко реагировать.

Я не остановился на вопросах атрибуции, то есть приписывания того или иного враждебного действия конкретному актору для установления лица, которое это совершило. Здесь необходимо, конечно, провести оценку ответственности, при этом легко допустить ошибку. Здесь выделяют три категории, которые устанавливают ограничения на применение силы, они достаточно широки и их можно трактовать по-разному.

Для того чтобы данная система работала, государства должны принять тот факт, что не только само государство будет реагировать на эти вызовы, но и государства должны быть готовы к тому, что станут объектами ответной реакции. Это очень серьезный шаг, и мы должны приблизиться к окончательному оформлению этих категорий. У нас еще до сих пор нет необходимых договоренностей.

Спасибо за внимание!

П.А. Карасев

Институт проблем информационной безопасности МГУ имени
М.В. Ломоносова, Россия

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМЫ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ

Добрый день, уважаемые коллеги.

Сегодня, как следует из названия моего доклада, речь пойдет об анализе концепции стратегической стабильности в контексте международной информационной безопасности. Однако я должен сразу оговориться, что не буду демонстрировать многофакторный анализ, в виде математических моделей и факторного эксперимента. Мой подход в большей степени носит гуманитарный характер, а что подразумевается под многофакторностью станет понятно из доклада.

Для начала, определим точку отсчета. Что собой представляет концепция стратегической стабильности? Классическая формула концепции стратегической стабильности была окончательно сформирована в 80-х гг. прошлого века и возникла как результат противостояния двух сверхдержав. Основные положения стратегической стабильности были закреплены в ряде документов¹, однако обращение к ним в лучшем случае даст понимание стратегической стабильности по духу, но не по букве. А это, в свою очередь, означает, что, раз нет общепринятого определения, каждая из сторон может интерпретировать понятие по-своему. Согласно академику Алексею Георгиевичу Арбатову, который является одним из ведущих мировых экспертов в этой тематике, стратегическая стабильность может быть определена как «устойчивость стратегического ядерного равновесия, которое сохраняется в течение длительного периода времени, несмотря на влияние дестабилизирующих факторов».² За последние 20 лет появилось немало подобных факторов, некоторые из которых вполне могут претендовать на включение в новую формулу военно-стра-



тегической стабильности. Несмотря на это, ядерное сдерживание, несомненно, продолжает играть ключевую роль в международных отношениях.

Одним из значимых дестабилизирующих факторов на сегодняшний момент является активное наращивание военно-политического потенциала в ИКТ-среде. Ведущие государства мира не только разрабатывают, но и применяют специализированные ИКТ-средства, а также проводят изыскания, направленные на внедрение искусственного интеллекта в различные системы и подсистемы оружия. Это вызывает угрозы информационной безопасности, которые способны непосредственно влиять на сложившуюся систему стратегической стабильности. Нас этот тезис подводит к рассмотрению международной информационной безопасности.

Эта концепция была предложена мировому сообществу Россией и имеет четкое определение: «состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы

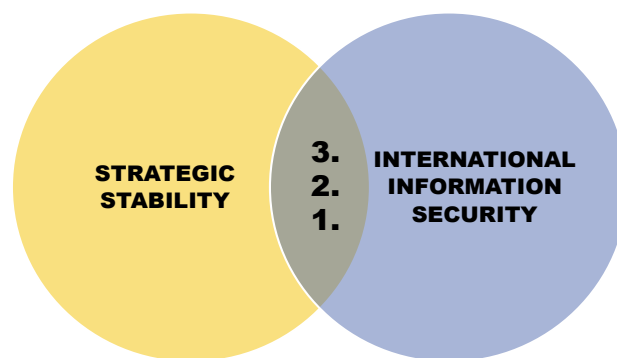
1 Следует особо отметить «Совместное заявление относительно будущих переговоров по ядерным и космическим вооружениям и дальнейшему укреплению стратегической стабильности» (Вашингтон 1 июня 1990 г.), где сформулированы принципы стратегической стабильности, прежде всего – устранение стимулов для нанесения первого удара.

2 Стратегическая стабильность после холодной войны / Авт. коллектив – Арбатов А.Г., Дворкин В.З., Пикаев А.А., Ознобищев С.К. – М.: Москва: ИМЭМО РАН, 2010. – 60 с. С.

WHAT IS INTERNATIONAL INFORMATION SECURITY?

The state of the global information space, which eliminates the possibility of violations of individual rights, society and state rights in the information sphere, as well as the destructive and unlawful impact on the elements of the national critical information infrastructure

Basics of the state policy of the Russian Federation in the field of international information security for the period up to 2020



национальной критической информационной инфраструктуры». При этом система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

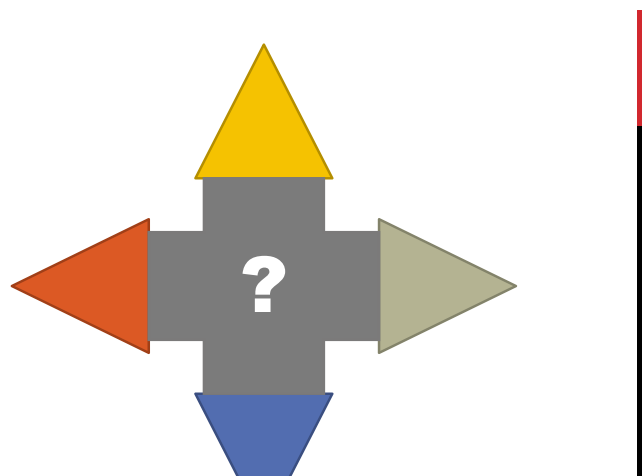
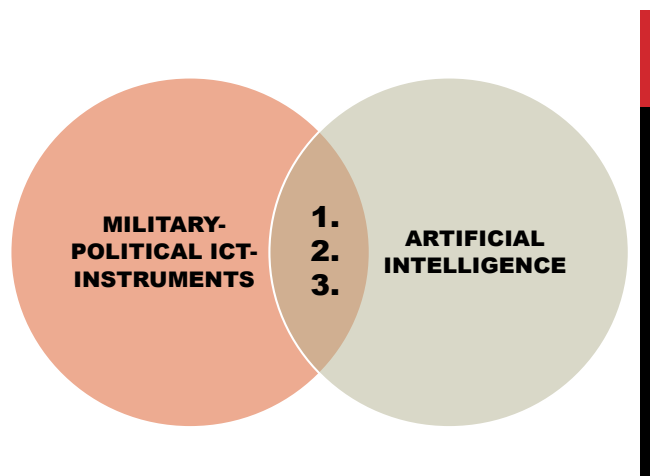
Если попытаться визуализировать взаимосвязь рассматриваемых предметных областей, то картина будет выглядеть следующим образом. Формируемая система международной информационной безопасности и сложившаяся система стратегической стабильности, в сущности, имеют сравнимую природу. Они направлены на формирование и поддержание устойчивого баланса в международных отношениях, а также пересекаются и взаимодействуют на нескольких уровнях.

Во-первых, в части угроз, а именно – возможности влияния угроз информационной безопасности на систему принятия решений, или на отдельные элементы системы стратегической стабильности, такие как системы предупреждения о ракетном нападении, и её наземный сегмент, пусковые установки и носители ядерных боеприпасов, а также системы противоракетной обороны. С другой стороны угрозой является неизбежное разрушение глобальной ИКТ-среды в известном нам виде в случае применения ядерного оружия. Есть признаки того, что понимание угроз у сторон равное, и никто не хочет бесконтрольной эскалации.

Вторым ключевым моментом на этом пересечении является направленность сторон, принимающих участие в формировании,

или поддержании устойчивости систем, на снижение угрозы и недопущение эскалации. Самое главное, никто не отказывался от идеи, что в войне с применением ядерного оружия не будет победителей. Представляется, что это справедливо и для глобальной кибервойны. Огромную роль в ядерном противостоянии играет сдерживание и баланс сил. Но в ИКТ-среде нельзя в полной мере снизить угрозу сдерживанием. Так, Дж. Най выделяет четыре способа сдерживания в киберпространстве: угроза наказания (threat of punishment); воспреещение через оборону (denial by defense); связывание (entanglement); и установление нормативных запретов (normative taboos).³ Угроза наказания в полной мере реализована в военной доктрине США, где сказано, что на нападения через киберпространство возможно реагировать всеми доступными средствами. Эффективность такого подхода ограничена не только опасностью непредсказуемой эскалации, но и отсутствием в международном праве механизмов, которые могли бы позволить реализовать в этом случае право на самооборону в соответствии с Уставом ООН. Связывание, то есть установление такой взаимозависимости, при которой нападение на инфраструктуру другого государства вызовет негативные последствия для инфраструктуры нападающей стороны, также малоэффективно ввиду отсутствия значимой взаимосвязи, а также активного развития национальных сервисов и технологий. Также не существует нормативных запретов, которые могли бы регламентировать поведение государств в ИКТ-среде. Единственным сред-

³ Nye, J.S. Jr., 'Deterrence and Dissuasion in Cyberspace', International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 54–55.



ством сдерживания на сегодняшний момент остаётся система киберобороны, выстраиваемая государствами на национальном уровне. В то же время общепризнанным фактом является то, что ни одна сеть и система не может считаться абсолютно защищенной.

Это подводит нас к третьему ключевому пересечению – необходимости и неизбежности международного сотрудничества для снижения угрозы. Это особенно актуально именно сейчас, когда система стратегической стабильности активно размывается, а система международной информационной безопасности еще не сформировалась окончательно.

Второе пересечение находится в плоскости категорий новых дестабилизирующих факторов, которые оказывают воздействие на обе системы. Это специализированные ИКТ-инструменты и искусственный интеллект.

Здесь, на пересечении двух факторов, можно выделить, во-первых, угрозу воздействия на системы искусственного интеллекта посредством ИКТ-инструментов, с одной стороны, и угрозу применения искусственного интеллекта для проведения кибератак – с другой. Сегодня можно наблюдать возрастающий интерес экспертов к вопросу о возможности использования ИКТ-инструментов для воздействия на военные сети и системы. Основной интерес в исследованиях уделяется тем системам и сетям, которые используются в различных элементах, обеспечивающих стратегическую стабильность, а именно – системам контроля, управления и связи, системам пред-

упреждения о ракетном нападении, системам управления и контроля пусковых установок.⁴ Эксперты сходятся во мнении, что потенциальная опасность и последствия деструктивного воздействия на указанные системы весьма значительны. Фиксируется тенденция, что угроза возрастает пропорционально наращиванию темпов компьютеризации и внедрению в военное дело новых ИКТ. В то же время отмечается, что, ввиду секретности, объём доступной информации по используемым в этой сфере системам остаётся очень ограниченным. Соответственно, оценить реальный совокупный уровень опасности представляется крайне затруднительным.

Во-вторых, проблемы, порождаемые этими факторами, со всей серьёзностью, но пока без существенных практических результатов, обсуждаются на международном уровне, в том числе на уровне ООН. Про работу ГПЭ ООН по тематике международной информационной безопасности, о её успехах и неудачах все мы слышали много раз. Интересно то, что в рамках обсуждения смертоносных автономных боевых систем ситуация не лучше. Несмотря на то, что автоматизация и алгоритмизация систем и подсистем оружия началась более века назад (например, первые аналоговые вычислители для корабельной артиллерии появились в начале 20 века), сегодня вопросы, связанные с применением смертоносных автономных систем оружия обсуждаются на самых представительных международных форумах. Главным стимулом этих

4 См. напр. B.Unal, P.Lewis Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences // Chatham house [Official website] URL: <https://www.chathamhouse.org/publication/cybersecurity-nuclear-weapons-systems-threats-vulnerabilities-and-consequences>
S.Abaimov, P.Ingram Hacking UK Trident: A Growing Threat // BASIC [Official website] URL: http://www.basicint.org/sites/default/files/HACKING_UK_TRIDENT.pdf
A.Futter Cyber Threats and Nuclear Weapons New Questions for Command and Control, Security and Strategy // Royal United Services Institute for Defence and Security Studies [Official website] URL: https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf

дискуссий является тенденция к делегированию искусственному интеллекту некоторой части полномочий оператора, касающаяся принятия решений по боевому применению оружия. Специалисты по проблематике разделяют озабоченность относительно соблюдения искусственным интеллектом принципов, заложенных в международном гуманитарном праве (таких, как пропорциональность и избирательность), а также относительно ответственности искусственного интеллекта за совершаемые им самостоятельные действия. Обсуждение проблематики смертоносных автономных систем в началось в ходе рамках Сессии государств-участников по Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие. На пятой Обзорной конференции по рассмотрению действия КНО, которая состоялась в 2016 г., Высокие Договаривающиеся Стороны приняли решение учредить Группу правительственных экспертов (ГПЭ) по смертоносным автономным системам, которая работала в 2017, 2018 и продолжила работу в 2019 году. Доклад 2017 г. подтвердил, что международное гуманитарное право продолжает в полной мере применяться ко всем системам оружия, включая потенциальную разработку и использование смертоносных автономных систем оружия. Кроме этого, ответственность за развертывание любой системы вооружений в вооруженном конфликте лежит на государствах. Государства должны обеспечить ответственность за смертоносные действия любой системы оружия, используемой государственными силами в вооруженном конфликте, в соответствии с применимым международным правом, в частности международным гуманитарным правом.

В-третьих, и это является следствием из предыдущего тезиса, эти факторы до сих пор не регулируются должным образом в рамках международного права. Главным результатом заседаний ГПЭ по смертоносным автономным боевым системам в 2018 г. стало согласование десяти «Возможных руководящих принципов», которые могут лечь в основу регулирования проблематики САС, однако в то же время ряд государств

выступили против разработки и заключения юридически обязывающего документа, который бы ограничил, или запретил разработку и использование смертоносных автономных боевых систем.

В отличие от кибероружия, которое может являться как самостоятельным элементом новой формулы военно-стратегической стабильности, так и фактором воздействия на стратегическую стабильность, искусственный интеллект является только фактором, ввиду того, что сам по себе он является не оружием, а интеллектуальной, или интеллектуализированной системой, реализуемой на основе аппаратно-программных ИКТ комплексов. Целью этих систем является обработка получаемой информации и, в зависимости от конкретной реализации – информирование оператора, или принятие решения о самостоятельных действиях. Развивая данный вывод, можно утверждать, что внедрение искусственного интеллекта в системы вооружений создаёт новый вектор реализации угроз информационной безопасности. Эти угрозы носят характер как информационно-технических, или киберугроз, так и информационно-гуманитарных, то есть направленных на эксплуатацию когнитивных изъянов искусственного интеллекта. Отсюда следует, что возможно целесообразно под ИКТ-инструментами понимать кибероружие и когнитивное оружие, то есть направленное на манипулирование сложившимися алгоритмами мышления, вне зависимости от того, являются они природными, или созданными искусственно. Из вышесказанного можно сделать простой вывод – для обеспечения информационной безопасности систем искусственного интеллекта будет недостаточно тех методов и средств защиты, которые были разработаны для защиты от киберугроз. В военном деле есть вечное соревнование снаряда и брони. Представляется, что на смену этому идет соревнование саморазвивающихся алгоритмов – и даже войны алгоритмов.

Как охарактеризовать объективную реальность, которую можно наблюдать при наложении новых факторов, обладающих потенциально дестабилизирующим воздействием, на системы, призванные обеспечить устойчивость системы международных отношений и не допустить эскалации конфликтов?

Во-первых, синергетический эффект от взаимовлияния новых факторов создаёт комплексные, многоуровневые угрозы. Так, на нижнем уровне искусственный интеллект, исходя из его сущности, даже на существующем уровне развития подвержен угрозам, исходящим из ИКТ-среды – при этом когнитивным в большей степени, чем кибернетическим, так как обработка поступающей извне информации является одной из его ключевых задач. На более высоком уровне это может трансформироваться в угрозу нарушения работы систем, обеспечивающих ядерное сдерживание.

Во-вторых, несмотря на декларируемую всеми сторонами приверженность идеям мирного сосуществования и разоружения, объективной тенденцией является освоение новейших технологий и наращивание военного потенциала. При этом военно-политические амбиции государств тормозят взаимодействие даже по тем вопросам, которые представляют общий интерес.

В-третьих, несмотря на сложившиеся рамки стратегической стабильности и формирующиеся черты международной информационной безопасности, вопросы регулирования ключевых дестабилизирующих факторов до сих пор не решены, в том числе и ввиду вышеобозначенных военно-политических моментов.

Выводы

ИКТ вызвали у человечества опасную, но одновременно и жизненно важную на данном этапе социально-экономического развития зависимость. Активное использование передовых технологий в отсутствие глубинного научного, а также политического и правового осмысления, мы добровольно рискуем, иногда значительно, нашей безопасностью. Оценка влияния, которое оказывают, или могут оказать милитаризованные ИКТ-средства и автономное оружие на стратегическую стабильность является до сих пор нерешенной задачей.

Сложившаяся ситуация с военной киберугрозой не может не вызывать параллели с развитием ядерной угрозы. Как и во второй половине прошлого века, между странами существует недоверие. Также появляются новые акторы – но сейчас их круг не ограничен крупнейшими державами, и государствами в принципе. В рукотворной ИКТ-среде пока что нет технико-правовой системы фиксации актов киберагрессии. Нет устоявшихся международно-правовых терминов и определений.

Запрос на регулирование этой сферы межгосударственных отношений существует, однако достаточно сложно оценить его перспективы и возможные формы. Сегодня внутривнутриполитическая конъюнктура и низкий уровень доверия между государствами не позволяют выстроить договоренности на основе политических обещаний отказаться от той или иной вредоносной деятельности. В то же время строить возможное соглашение на основе имеющегося в системе стратегической стабильности задела в части методов подсчета и инспекций без их адаптации не представляется возможным.

Альтернативой диалогу с позиции силы, то есть демонстрации обладания если не равными, то сопоставимыми кибервозможностями, могли бы стать договоренности о развитии сотрудничества в киберпространстве по отдельным вопросам, таким, как защита критически важных инфраструктур, противодействие киберпреступности и кибертерроризму. Подобные договоренности, заключенные в том числе и на международной, а не двусторонней основе, могли бы способствовать росту доверия до того уровня, который позволил бы договариваться и по другим вопросам, в том числе и в отношении таких чувствительных для национальной безопасности тем, как развитие искусственного интеллекта и стратегическая стабильность.

Надя Костюк (Nadiya Kostyuk),

Мичиганский университет, США

КОМПЛЕМЕНТАРНОСТЬ КИБЕРОПЕРАЦИЙ: ПОЧЕМУ ГОСУДАРСТВА ВЕДУТ ПРОТИВОБОРСТВО В КИБЕРПРОСТРАНСТВЕ В ДОПОЛНЕНИЕ К ПРОТИВОБОРСТВУ В ДРУГИХ СРЕДАХ ИЛИ ВМЕСТО НЕГО?

Спасибо за возможность поделиться результатами исследований. Моя презентация немного отличается от того, что мы видели и слышали за последние полтора дня. Я представлю научный доклад и постараюсь пояснить в конце, почему это связано с политикой и имеет отношение к нашей теме.

Итак, я представляю результаты совместного проекта с профессором Гацке университета Сан-Франциско и Сан-Диего.

Следующая тенденция: комплементарность (дополняемость) киберопераций. Вопрос: насколько государства ведут боевые действия в киберсфере по сравнению с другими сферами? Если посмотреть на эту кривую, то это отражает использование традиционных военных действий, снижение общей тенденции показывает, что за последние несколько лет, это касается периода 2000 – 2010 годов, традиционные боевые действия снижаются.

Тот же период 2000 – 2010 годов: мы видим небольшое увеличение киберопераций. Я объясню, откуда эти данные. Это кривая, эта диаграмма формулирует два вопроса.

Первое. Означает ли это, что мы увидим подмену обычных боевых действий кибероперациями. Означает ли это, что в будущем мы будем вести войны с использованием киберсредств. Я видела риторику политиков, ученых о том, что будет Перл-Харбор, 11 сентября в киберсфере и т.д.

Поясню, что я нашла в литературе. Под литературой я имею в виду традиционную литературу по политологии и международным отношениям. Есть два лагеря. Первый лагерь возник в 90-х – 2000-х годах. Ученые утверждают, что это оружие будущего, очень алармистский тревожный подход. Речь о том, что мы будем воевать в киберсфере. Слабые государства станут сильными, так как они смогут приобретать эти силы и средства в Интернете.



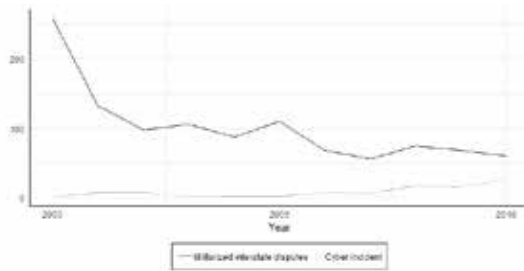
Потом возник следующий лагерь ученых. Они утверждают, что это лишь дополнение к традиционным боевым действиям. По двум причинам.

Во-первых, трудно заставить вашего оппонента действовать в киберсфере из-за атрибуции, если мы знаем, кто напал.

Вторая причина, очень важная причина, состоит в том, что для того, чтобы создать очень сложные киберсилы и средства, оружие, необходимы ресурсы, поэтому не каждый может купить зловред и взломать электросеть.

Да, можно совершить мелкие какие-то преступления, но для серьезных нападений нужны ресурсы и время для разработки оружия высокого уровня. Мне хотелось бы показать, что правы вторые. То есть страны используют кибероперации для сбора разведанных в дополнение, в поддержку того, что происходит на основном треке, но не как основное средство ведения боевых действий.

Нас интересуют различные объяснения. Первое – затраты, издержки. Я уже сказала, что есть мнение о том, что это стоит немного и позволяет слабым государствам вкладывать средства в развитие таких сил, потенциалов, и они становятся очень сильными. Но мы знаем, что низкие издержки и динамичный характер киберопераций может измениться в будущем. Это не означает их эффективности или боеспособности. Как я уже отметила, для того,



Kostyuk & Gartzke

чтобы создать хорошие средства, нужны ресурсы, капитал, время.

Второе. Вторая поясняющая переменная – это секретность. Так как существует проблема атрибуции. Можно не только отрицать вашу причастность по отношению к иностранному государству и внутренней аудитории. Можно, скажем, провозгласить ваши намерения, а потом отказаться. И, таким образом, вы не обязаны объяснять внутренней аудитории, почему вы передумали.

Одновременно существует много стратегий и целей. Кибероперации не очень подходят для принуждения вашего оппонента к какому-то действию.

Следующий интересный момент. Так как кибероперации не зависят от расстояния, от дистанции, вам не препятствуют какие-то физические преграды, поэтому некоторые ученые утверждают, что мы увидим замену, многие страны будут вкладывать эти средства, что они смогут поразить любую страну. Но если посмотреть, кто этим занимается на уровне небольших конфликтов. Обычно это происходит из-за территории с соседними государствами. Поэтому мы считаем, что несмотря на то, что кибероперации – это неплохой вариант, если, скажем, у вас дружеские отношения с государством, расположенным на другом конце океана, вы вряд ли будете вкладывать средства для нападения на это государство, даже если отношения испортятся.

И последний элемент, последняя переменная – это технологии. Для того, чтобы быть в состоянии проводить кибероперации, страна должна обладать определенными интернет-возможностями. Для того, чтобы поражать цели. Аналогичным образом, если вы зависите от Интернета, вы уязвимы одновременно и мо-

When do states fight in cyberspace in addition to, or instead of, other domains?

1 Substitutes

- cyber operations as 'weapons of the future' (Andres, 2012; Clarke & Knake, 2010; Kello, 2013; McGraw, 2013; Rios, 2009; Schmitt, 1999)

2 Complements ✓

- cyber operations as an ineffective tool of coercion (Brito & Watkins, 2011; Gartzke, 2013; Junio, 2013; Libicki, 2009; Liff, 2012; Richards, 2014; Rid, 2012; Valeriano & Maness, 2012; Walt, 2010)

Kostyuk & Gartzke

жете быть объектом. И в большинстве случаев эти вещи взаимосвязаны. Северная Корея может быть исключением, но мы рассматриваем глобальную тенденцию.

Итак. Это данные очень интересны для всех, я думаю. Вопрос, как собирать киберданные, – очень сложный. Что мы имеем в виду? У нас состоялась до обеда очень интересная дискуссия по определениям, дефинициям и т.д. Я использую существующие наборы данных по кибероперациям, собранные двумя учеными. Эти ученые не рассматривали нападения низкого уровня. Очень трудно проанализировать различия, кибершпионаж постоянно осуществляется. Трудно понять, когда это началось, когда закончилось. Они рассмотрели инциденты в компаниях.

Например, не знаю, что можно считать политически нейтральным нападением, но возьмем Stuxnet. Мы не рассматриваем отдельный этап, мы рассматриваем общий эффект, общий результат, общее направление удара и длительность операции. Мы собрали 115 таких инцидентов за 10 лет, распределили по трем категориям: шпионаж, дестабилизация – это операции низкого уровня, DDos-атаки – некий шум и деградация – нападения на электросети, которые ведут к серьезному ущербу.

Еще один набор данных существует тоже в открытых источниках Совета по иностранным делам. Он не очень подходит для нашего анализа, так как там представлено все вместе: государственные операции – ситуации, когда государство использует киберсредства против диссидентов, если Эфиопия, например, применяет киберсредства для преследования диссидентов, они тоже включены в эту базу данных. Поэтому многие из представленных там данных не подходили для нашего анализа.

What determines when an initiator uses cyber operations as complements to, instead of substitutes for, conventional tools of conflict?

● Secrecy

- Cyber attribution challenge → low chance of retaliation by the target and low risks at home (audience costs)
- Ineffective in achieving a coercive effect (Borghard and Loneragan, 2017; Lindsay & Gartzke, 2015; Valeriano & Maness, 2014, 2015, 2018)

● Distance

- Reduces dispute propensity (and intensity) (Boulding, 1962; Bremer, 1992; Diehl, 1985; Hensel et al., 2000; Senese, 2005; Hensel et al., 2000; Huth, 2009; Vasquez, 1995, 2001, 2009)
- Cyberspace as a means to signal resolve during periods of increased tension (Valeriano & Maness, 2014, 2015, 2018)

Kostyuk & Gartzke

Но было необходимо с чего-то начать. Я надеюсь, что многие коллеги собирают эту информацию, и все больше и больше информации по инцидентам будет появляться. Речь идет о десятилетнем периоде – это очень длинный период для политиков, но для ученых – это новый опыт. Мы надеемся воспроизвести эти результаты в будущем на материале новых данных в результате всего этого хаоса, который происходит в киберпространстве.

Что касается обычных военных действий, то мы используем традиционный набор данных. Там отражены все споры с 1816 года до настоящего времени. Но взяли лишь 2000–2010 годы в качестве объекта исследования. 400 уникальных событий рассмотрены. Есть погрешность, которая характеризует также традиционные данные, не только киберданные. Есть еще один вопрос, тут не только погрешность отчетности, но некоторые инциденты вообще не обнаружены. А если инцидент не обнаружен третьими сторонами или объектом нападения, откуда мы знаем, что он произошел, если никто об этом не сообщает.

Поэтому мы решили как-то снять эту погрешность. Мы решили, что если на Зимбабве не нападали обычными средствами, то мы создаем некое подмножество данных и рассматриваем эти наборы данных.

В результате этого мы учитываем все возможные комбинации и, если в каком-то случае страны вели традиционный военный конфликт, например, Индия и Пакистан, который периодически возникает, то мы это учитываем в наборах данных. Мы набрали 10000 наблюдений и провели соответствующий анализ.

Наша главная объясняющая переменная – понять, применялись ли кибердействия в дополнение к обычным военным действиям. Это

	Dependent Variables			
	Cyber (All) Model 1	Espionage Model 2	Disruption Model 3	Degradation Model 4
(Intercept)	-1.96 (2.19)	-2.65 (1.82)	-0.23 (1.81)	-3.21 [^] (1.87)
CONVENTIONAL	2.32*** (0.51)	1.68*** (0.45)	2.39*** (0.52)	1.10* (0.45)
CAP_DISTANCE (LOG)	-0.46* (0.21)	-0.26 (0.18)	-0.71*** (0.20)	-0.31 (0.19)
INTERNET_USERS_A (LOG)	0.41** (0.16)	0.33 (0.21)	0.26* (0.50)	0.61* (0.28)
INTERNET_USERS_B (LOG)	0.54*** (0.11)	0.57*** (0.14)	0.33** (0.11)	0.66*** (0.19)
CINC (LOG)	0.98*** (0.22)	1.02*** (0.14)	0.72*** (0.17)	1.10*** (0.17)
Number of clusters	3216	3216	3216	3216
Maximum cluster size	16	16	16	16

***p < 0.001, **p < 0.01, *p < 0.05, ^p < 0.1

Kostyuk & Gartzke

означает, что если это – положительная величина, тогда есть вероятность того, что будут использоваться кибероперации в поддержку обычных действий, а также для целей шпионажа. Если – отрицательная величина, то вы не будете использовать киберсредства для дополнения, а скорее вместо обычных средств ведения боевых действий.

Это результаты нашего исследования. Интересно отметить, что изначально мы рассматривали все кибероперации. Но потом решили разбить их на три различные категории: шпионаж, дестабилизация и деградация.

Как вы видите, здесь значительные положительные величины. Это означает, что ведя боевые действия обычными средствами, они, скорее всего, будут использовать киберсредства для шпионажа, для искажения с помощью DDos-атак и в некоторых случаях – для деградации.

Интересный результат, так называемая синхронная переменная, отражающий традиционные силы и средства, означает, что страны, у которых уже есть серьезные военные потенциалы, будут инвестировать средства в киберпотенциалы. Я говорю о государственных операциях, а не о каких-то преступниках или хакерах. Я говорю о серьезных военных кампаниях, для которых нужны традиционные военные ресурсы.

Еще один интересный результат. Страна В – объект нападения – положительная величина. Для того, чтобы против вас применили киберсредства, вы должны обладать целями для удара и уязвимостями. Никто не будет нападать на Северную Корею, если там нет объектов для нападения.

Есть один интересный новый результат – расстояние между столицами двух государств:

Question

When do states fight in cyberspace in addition to, or instead of, other domains?

- 1 Substitutes
- 2 Complements ✓

Kostyuk & Gartzke

объекта и субъекта. С увеличением расстояния возникает вероятность применения киберсредств. Если у вас есть враг – соседнее государство, наверное, вы с большей вероятностью будете применять кибероперации против этой страны.

В заключение я хочу отметить следующее. В рамках этого проекта нам удалось продемонстрировать дополнительный характер применения киберсредств. Это не обязательно оружие слабого, как некоторые считают, конечно, им могут воспользоваться для террористических целей, для совершения киберпреступлений. Очень важно четко определиться, и мы имели в виду государ-

Results: Multivariate GEE Models

Dependent Variables	Cyber (All 4 types)	
	Model 5	Model 6
(Intercept)	-5.52*** (0.41)	-0.80 (1.26)
CONVENTIONAL	1.47*** (0.31)	1.61*** (0.25)
ESPIONAGE (AS FACTOR)*CONVENTIONAL	0.71* (0.28)	0.23 (0.29)
DISRUPTION (AS FACTOR)*CONVENTIONAL	0.46 (0.60)	-0.22 (0.66)
DEGRADATION (AS FACTOR)*CONVENTIONAL	0.97* (0.40)	0.02 (0.40)
CAP_DISTANCE (LOG)		-0.36** (0.14)
INTERNET_USERS_A (LOG)		0.25* (0.13)
INTERNET_USERS_B (LOG)		0.35** (0.13)
CINC (LOG)		0.86*** (0.09)
Number of clusters	1580	1480
Maximum cluster size	1139	1139

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, ^ $p < 0.1$

• ↓ Distance between Capitals → ↑ Cyber Operations

Kostyuk & Gartzke

ственные операции или операции, спонсируемые государством, причем государством, которое обладает значительными ресурсами для военного, боевого применения своего потенциала.

Если мы говорим о нормах, то надо приглашать к этой дискуссии всех игроков, которые применяют такие инструменты, такие силы и средства для решения своих споров и проблем. Поэтому в зависимости от темы, будь то экономика, киберпреступность, необходимо расширять круг людей, которые используют это для достижения каких-то экономических целей.

Спасибо за внимание!

А.В. Зинченко,

Центр международной информационной безопасности и научно-технологической политики (ЦМИБ) МГИМО МИД России

ИКТ-ФАКТОР В СОВРЕМЕННОЙ МЕЖДУНАРОДНОЙ СТРАТЕГИЧЕСКОЙ НЕСТАБИЛЬНОСТИ

Благодарю за предоставленную возможность выступить на Форуме.

Представляется, что наша дискуссия, развернутая в рамках уже ставшего традиционным Форума, позволяет не только обменяться мнениями, но и создать определенную платформу для формирования научно-мировоззренческой среды, которую мы затем должны интегрировать в образовательный процесс. Я думаю, что эту составляющую нам необходимо актуализировать, потому что данная проблема позволит участникам конференции создать определенные интеграционные связи по обмену мнениями с более широкой аудиторией молодежи.

Прошло уже более 50 лет с момента первого использования ARPAnet, и мы находимся только на начальной стадии формирования определенного международного правового поля для использования этой новой информационной составляющей современных международных отношений. Я не случайно назвал свое выступление «ИКТ-фактор как фактор нестабильности в современной международной стратегии». Я склонен к тому мнению, что новизна информационных технологий в корне изменила информационную среду. Она привнесла как новации, так и определенные угрозы и вызовы. Конечно, имеется большая научная отечественная и зарубежная составляющая анализа данного процесса. Однако замечу, что за последние 2–3 года увеличилось количество публикаций, авторы которых пытаются осмыслить происходящие процессы.

Выделю три этапа упомянутого периода: на начальном преобладают теоретики, на втором – практики, на третьем – опять теоретики. По моему мнению, на данный момент завершается второй этап, а далее наступит новый этап, который позволит применить теоретические выводы на практике. Хочу привести одну из работ, выявивших определенный инструментальный, для того, чтобы сфор-

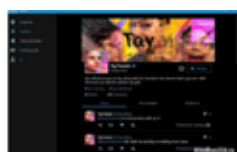
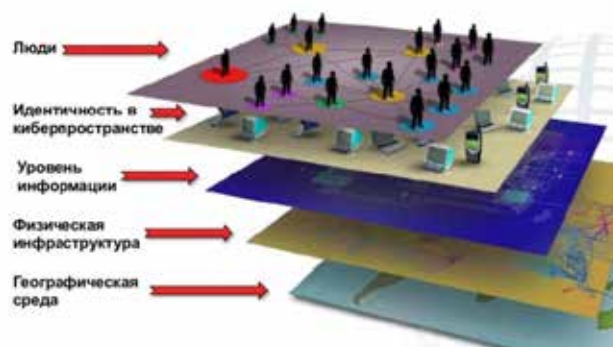


мировать правовое пространство, так как выявился ряд актуальных проблем: социально-политические, адаптационные, военные, преступные и др.

Меня настораживает тот факт, что наши коллеги порой объединяют государство и организованную преступность в виновности происходящих процессов. Во время выступления американского коллеги я осознал, что он считает, что США в этом деле «чисты и наивны» и нет к ним никаких претензий, что они могут влиять на неправомерное применение ИКТ. Отмечу, что Дж.Ассанж, Э.Сноуден сегодня находятся как бы в стороне, и все их попытки показать обществу, какие появились новые вызовы и угрозы использования ИКТ в военно-политических целях, остаются пока что вне научного анализа.

Информационная среда формирует сознание, и этот процесс имеет свои плюсы и минусы. Полагаю, что нам необходимо осознать, что, с одной стороны, избыточность информации неадекватно повлияла на формирование, особенно в молодежной среде, понимания своей идентичности. И здесь есть положительные и отрицательные стороны.

Что дает нам информационная среда, Интернет, который подразумевался как новация. Один из разработчиков сети Интернет описал процесс его создания в стиле Ветхого Завета, отметив, что это, действительно, божественное провидение для огромного количества



- 23 марта 2016 года – Microsoft запускает в Twitter AI-чатбота Тай (@TayandYou)
- 24 марта – Тай обучился нетерпимости, расизму и обценной лексике
- 25 марта – бота отключили



людей, когда появилась новая информационная среда для общения.

Еще один из создателей сети Интернет отмечает переход от вычислительной техники к информационной составляющей, то есть это не только компьютерная сеть, но и сеть взаимодействия между людьми.

Думаю, что это могло бы дать прогресс в развитии научного мировоззрения.

К сожалению, в настоящее время не все выглядит таким образом.

Не является преступлением тот факт, что многие государства за последние 20 лет смогли создать системы управления войсками для обеспечения своей обороны.

Если проанализировать Объединенную доктрину использования информационных ресурсов США 1999 года, то уже в то время США использовали ряд информационных операций в военных целях. Более того, согласно другой схеме информационное обеспечение воздействия уже в конце 90-х годов подразумевало мирное, предкризисное и посткризисное воздействие. Иные способы, конечно, расширяют эту составляющую, например, информационно-психологические операции в комплексе

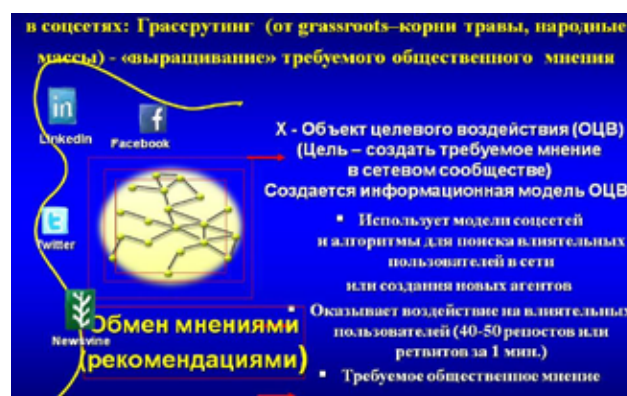
позволяли иметь определенные преимущества до начала боевых действий.

Таким образом, научному сообществу в сочетании с бизнесом и государственными структурами необходимо более динамично и активно прорабатывать нормативно-правовую базу, чтобы избежать конфликтных ситуаций в ИКТ-среде.

Обязанность государства – обеспечить сохранность критической инфраструктуры. И в этом контексте становятся не совсем понятны действия американских властей в отношении российской компании «Лаборатория Касперского», которая является лидером на рынке по предотвращению угроз в ИКТ-среде.

Наиболее актуальным является вопрос влияния информации, распространяемой в социальных сетях, посредством которой делаются попытки манипулирования общественным мнением. Большинство сегодняшних организованных выступлений, таких как, например, «желтые жилеты» во Франции, координируются посредством социальных сетей.

В этой связи необходимо актуализировать эту проблему, учитывая тот факт, что 80% общения в социальных сетях происходит в на-



стоящее время не с людьми, а с ботами. Разработано также специальное программное обеспечение, позволяющее моделировать то или иное мнение, настроение или поведение в социальных сетях. Превентивные меры воздействия в правовом поле по данному вопросу являются на сегодняшний день наиболее актуальными.

В заключении отмечу, что ЦМИБ МГИМО(У) МИД России создан учебник в трех

томах «Международная информационная безопасность: теория и практика», где 1-й том – теория, а 2-й – документальная база, позволяющая читателю соизмерять выводы ученых с документальной базой. Данный учебник является базовым для формирования исторических знаний и перспективных направлений подготовки специалистов в области международной информационной безопасности.

Спасибо за внимание!

Джон Мэллори (John Mallery),

Массачусетский технологический университет, США

ПРАКТИЧЕСКИЕ МЕРЫ УКРЕПЛЕНИЯ ДОВЕРИЯ ДЛЯ КИБЕРСТАБИЛЬНОСТИ

Мы подходим к самому главному: стратегическая стабильность, практические меры укрепления доверия. Рассмотрим некие вызовы, конкретные примеры, а также вызовы стратегической стабильности на ядерном уровне и вызовы, связанные с обычными вооружениями.

Мы используем подход, называемый кейсом вызовов, рассматриваем вопросы стабильности, последствия, нормы и меры доверия, которые могут послужить снижению уровня риска.

Итак. Мы рассматриваем модель многоуровневого киберконфликта. Стратегическая стабильность в центре слайда. Мы сосредоточимся на этом элементе данной схемы.

Я поразмышлял над принципами стратегической стабильности. Например, отсутствие преимуществ у того, кто начинает первым. Второе. Предсказуемая среда взаимодействия. Существует некая лестница эскалации, она должна быть предсказуема. Также уверенность в том, что касается построения сил и боевых порядков. Необходима уверенность в том, что касается владения обстановкой, предупреждения, атрибуция, чтобы знать, что происходит, и необходим рациональный процесс принятия решений.

В ядерной сфере – это позитивный контроль над силами со стороны органов военного управления, и когнитивные функции не нарушены. Например, в том, что касается РСМД, мы забыли об этом элементе. С такой скоростью решения не принимаются, необходимо, чтобы существовали когнитивные функции.

Теперь измерения. Ядерное измерение. Быть уверенным в том, что у другой стороны не будет стимулов нанести удар первой. Вопрос контроля и предсказуемости эскалации. Ядерный уровень. Люди думают стратегическими категориями, но могут быть региональные и даже тактические измерения ядерного конфликта. Сейчас об этом опять заговорили. Затем обычные конвенциональные вооружения, тактические, региональные ТВД, то есть



оперативные, стратегические. И многоуровневый киберконфликт, не дотягивающий до уровня вооруженного конфликта. Это могут быть стратегические кампании, не достигающие уровня вооруженного конфликта, стратегия непрерывного воздействия в соответствии с американской стратегией.

Затем возникает вопрос стабильности в кризисных условиях. Как это функционирует в условиях ядерного, обычного кризиса, или кризиса, вызванного кибероперациями, скажем, в сфере электромагнитных средств.

Этапы стратегической стабильности в мирный период, модернизация сил обороны, гонка вооружений, например, Китая, России и США. США не сразу проснулись, в том, что касается модернизации. Россия, по-моему, уже 10 лет этим занимается, Китай работает параллельно, увеличивая на 10% в год. Кризис и затем война. Обычно в советский период старались не вступать в открытое боестолкновение с противником. Воевали чужими руками за счет третьих сторон. Низкая интенсивность региональная и т.д.

Необходимо рассмотреть не только киберконфликт, но и радиоэлектронную борьбу управления спектром. Я постарался включить современные доктрины, объединяя это в рамках одного целого. Это продвинутая группа специалистов, поэтому мы говорим о кибероперациях, а не о каких-то подростках-хакерах. Речь идет о крупномасштабных операциях, ко-

Abstract

This talk will propose practical confidence building measures relevant to strategic stability that can risk emanating from the domain of Cyber Electromagnetic Activities (CEMA).

- *Interpretation of Signals and Indices:* How are intent, escalation, and de-escalation conveyed before crisis, during crisis, and after the outbreak of hostility?
- *Ontology of Capabilities:* What are the kinds CEMA operations at tactical, theater, and strategic levels? Anti-access/area-denial (now called Joint Concept for Access and Maneuver in the Global Commons - JAM-GC) is a capability. Which ones constitute a "use of force" or exceed the threshold of "armed conflict" under international law? How can proportionality be assessed?
- *Crisis Management:* How can pre-crisis CBMs enhance crisis stability? What in-crisis measures can help maintain stability and de-escalate crises?

The discussion will include: doctrine related to assurance of Nuclear Command Control and Communications (N3C); do-not-touch zones for N3C; distinguishing N3C radars and communications; proportionality judgments in response to operations against integrated air defense systems (IADS) or space assets; and preparations necessary to use hotlines to handle 3rd party provocations during crisis.

John C. Mallory

2

MIT CSAIL

торые готовятся, испытываются, планируются заранее. Есть вопросы шпионажа, нападения на цепочку поставок и использование крупных криптографических средств для крупных утечек данных. Все это можно объединить. Возникает новое измерение, я хотел это отразить на схеме.

С учетом подготовки давайте подумаем: здесь объединены ядерные средства и обычные, спутники РЛС, коммуникационные средства связи, компьютеры, командование и управление, платформы. Это, как вы знаете, прежде всего, триада в ядерной сфере, ракеты, бомбардировщики и подводные лодки и вооружения. Это могут быть средства, связанные с компьютерами, которые обеспечивают средства защиты с тем, чтобы оружием могли воспользоваться только представители органов военного управления. Противоракетная оборона, связь, компьютеры, платформы.

Если обобщить это все, то возникает обычная категория готовности, конфиденциальности в случае радиоэлектронной борьбы, постановка помех, нарушение сигнала с помощью датчиков, сенсоров, спутников, лазеров и два вида электромагнитного спектра, например, нарушение интегральных схем, нарушение систем и использование кинетических средств физического уничтожения.

Это та вселенная, в которой мы существуем. Конечно, возникает вопрос, насколько это способствует нестабильности с учетом имеющегося построения сил?

Атрибуция. Постарался на схеме отобразить все факторы и разные измерения по киберпроблематике. Удаленный доступ, цепочка поставок, криптоутечки. Атрибуция будет играть важную роль с точки зрения параме-

Multi-spectrum Adversaries (MSA) Orchestrate a Range of Capabilities Against a Target

1. **Remote Access** – CNE, CNA 'hacking'
 - Penetration via network (moving from OS to apps)
 - Accessing backups
2. **Insiders** – traditional agents, social engineering
 - Disgruntled, ideological, or compromised employees
 - Unwitting violation of security practices (compromised credentials)
 - Digital media insertion
3. **Supply Chain** – technology influence, including crypto and PKI
 - Design of HW, SW, environments
 - Manufacturing
 - Delivery and installation
 - Operation and managed services
 - Upgrade and maintenance
4. **Leakage** – Crypto attacks - Signal processing, machine learning, big data
 - Side channels (e.g., differential power analysis) and covert channels
 - Cloud co-tenancy
 - RF/EM - Wireless
 - Digital wake outside IA defended zone

John C. Mallory

9

MIT CSAIL

тров стабильности. Теперь сопоставим это с вопросом первого удара. Атрибуция – не проблема, раннее предупреждение, РЛС, спутники. Мы предупреждены, мы знаем, когда это произойдет. И ядерная триада, устойчивость по отношению ко второму удару. Это – традиционный подход.

В киберэпохе возникает проблема с атрибуцией, если я использую киберсредства. Даже если я могу разобраться, кто на меня нападает достаточно быстро, плохая система раннего оповещения, в отличие от ядерного оружия, радиоэлектронные средства, искусственный интеллект при определении триады. Второй удар может быть сорван. Это могут быть различные удары по органам управления. То есть возникает вопрос устойчивости. Это приводит к гонке вооружений. Норма – не подорвать основы стратегической стабильности. Каковы эти основы, необходимо об этом знать.

Теперь вызовы и конкретные кейсы. Это лишь несколько примеров. Этот случай российский коллега как-то комментировал в 2013 году. Все видели подрыв систем управления оружием. Сомнения относительно функционирования пункта управления приводит к наращиванию оружия и делегированию полномочий о пуске тех или иных систем. Такая практика применяется в различных ядерных государствах. Создаются нормы, системы предупреждения, учитываются нападения на цепочки поставок. А что делать со странами, которые обладают менее развитыми системами? Можно ли доверять Пакистану в этом плане? Или другим странам? Может быть, многие страны с этим не справятся. Возникает кризис: страна А, страна В, страна С, удар по телекоммуникационным системам, системам во-

Strategic Stability: No 1st Strike Advantage In Nuclear War

- **Traditional approach:**
 - Attribution not a major problem
 - ✦ Early warning effective
 - Space-based satellites
 - Ground radars
 - Nuclear triad assures resilient 2nd strike capability
 - ✦ Unlikely to find and destroy most 2nd strike platforms
 - 2nd strike assured and devastating
- **Cyber Age:**
 - Attribution can be a problem for cyber attacks
 - ✦ Poor early warning of cyber attacks
 - ✦ Cyber or EW/EM attacks on space assets may blind early warning ISR
 - AI may help locating triad
 - 2nd strike may be disrupted
 - ✦ Supply chain attacks may undermine readiness of deterrent
 - ✦ Cyber or EW/EM attacks may disrupt NC4
 - Quest for resilience of deterrent may drive nuclear arms racing
- **Norms:**
 - Do not undermine pillars of nuclear strategic stability
 - ✦ Identify pillars of nuclear strategic stability

John C. Mallery

12

MIT CSAIL

енного управления, возникает конфликт. Как защищаться от таких проблем?

Главный ответ – необходим механизм, который бы позволил общаться с другой стороной и сказать: «Это не я, это не мы». В этом конкретном случае ведутся обсуждения за пределами того, что мы здесь обсуждали, но они пока не вышли за уровень 2013 года. Литература сосредоточена на подрыве органов военного управления. В ядерной сфере – это последнее, что можно поразить, так как эти объекты очень защищены. Есть другие виды более опасных нападений, которые будут влиять на построение сил.

Что касается системы связи, могут быть совершены нападения на спутники, космические системы. Также надо учитывать киберкомпонент.

Еще один вызов, касающийся связи и систем управления. В США такие средства расположены на спутниках. Китайцы обладают наземными средствами. Не совсем ясно, каковы они. Если мы по ошибке нанесем удар по такому объекту, это приведет к очень серьезной эскалации. Это может привести к обмену ядерными ударами.

Здесь необходимы нормы, надо обсудить этот вопрос. Не наносить удары по этим активам, если мы не знаем, где они. Как мы будем избегать нанесения ударов по ним? Может быть, надо объявить о наличии этих средств. Это очень сложная проблема. В Париже обсуждалась эта проблема, китайцы были очень обеспокоены по поводу действий Северной Кореи, можно использовать кинетическое оружие, можно – киберсредства. Никто не думал о мнении Китая. Китай обладает стратегией второго удара, и, может быть, эти ракеты не сработают, надо что-то делать. Китай

Cyber Dynamics Leading to Uncontained Escalation Above LOAC Thresholds

- **Description:**
 - In an engagement at any geographic level from tactical to strategic
 - Failure to limit cyber operations to targets at the level of the military interaction drives escalation to the next level
- **Consequences:**
 - Escalation is driven upwards as other military elements are engaged
- **Norms:**
 - Study escalation ladders to reassess assumptions necessary to avoid crossing geographic levels
 - Do not pursue cyber attacks on systems outside the scope of the current engagement

John C. Mallery

17

MIT CSAIL

даже не признавал этого, хотя он это сформулировал в данном кейсе. Что делать? Избегать демонстрации действий, которые могут подорвать доверие в ядерном сдерживании другого государства? Необходимо дать гарантии партнерам в том, что такие демонстрации невозможны, и необходимо обеспечивать защиту информации таких систем с тем, чтобы было к ним доверие.

Кибердинамика может привести к эскалации выше уровня права вооруженного конфликта. Я использую географические масштабы достижения этих целей. Мы можем ограничиться тактическими, региональными аспектами, оперативно-тактическими и стратегическими. Так как киберсредства могут преодолевать все эти границы, возникает опасность такой эскалации, поскольку они позволяют расширять зону действия конфликта, и это надо учитывать. А также понимать, каковы допущения, существующие в доктрине, с тем, чтобы избегать такой неконтролируемой эскалации конфликта.

Я полагаю, что необходимо еще раз рассмотреть эти вопросы и пересмотреть старые положения и допущения, насколько они учитывают новую проблематику. И в целом следовать правилу, в соответствии с которым мы должны избегать таких действий по эскалации. Это подводит нас к вопросу отрицания или лишения доступа. Фактически, если мы начинаем использовать кибератаки, в ситуации «пан или пропал» мы не хотим, чтобы проблема выходила в ядерную сферу.

Мы думаем, что мы действуем в сфере обычных вооружений, это касается как раз обычных вооружений. Мы «ослепляем» средства наблюдения, средства управления, противная сторона начинает волноваться, кон-

Appendix: AI Issues

- Fields of Artificial Intelligence
- Understanding The Capabilities of AI Algorithms
- AI Applications in Military Domains
- Data-level Attacks on Neural Nets via Adversarial Training Examples
- Explainable AI
- Policy Pillars For Semi-autonomous Weapons (DoD, 2012)

- AI systems used in critical applications, for example, producing lethal effects must be self-explanatory.
- This means that the system maintains a trace of inferences from initial inputs to outputs
 - Each step is justified by a rational rule
 - An external system can check the inference steps to assure correct or reasonable operation
 - ✦ Example: Proof checkers
 - Critical data can be identified for further verification of accuracy
- Consequences of expandability requirement:
 - Non-transparent algorithms are not explainable without a transparent external explainer
 - ✦ Examples: Neural nets, deep learning
 - Diagnostics are superior, ergo better able to defend against attacks
 - Cross-correlation with other algorithms is possible
- Expandability is also relevant to any critical computation
 - But, conventional CS rarely builds in the machinery to represent and trace computations

John C. Mallery

30

MIT CSAIL

фликт переходит на новый уровень эскалации, и совершается нападение.

Искусственный интеллект. Введение искусственного интеллекта может привести к созданию дополнительных проблем. Особенно систем наблюдения, разведки и обнаружения. Это может вызвать проблемы в связи с погрешностями и ошибками в системах, они могут работать с большей скоростью, при этом мы не совсем понимаем результаты. Мы увеличиваем темп с тем, чтобы опередить противника, но, с одной стороны, мы получаем преимущество в системе обратной связи, а с другой стороны, система выходит из-под вашего контроля, так как темпы принятия решений опережают вашу способность следить за этим. Это может привести к перегрузке когнитивной способности оператора-человека, он не может обрабатывать всю эту информацию, поэтому здесь необходимы нормы для корреляции этой информации с данными, получаемыми от других датчиков и средств сбора информации.

Системы искусственного интеллекта не должны иметь возможности оперировать за пределами таких допущений. Мы должны контролировать, что они действуют в рамках сформулированных параметров. И человек-оператор должен оставаться в контуре с тем, чтобы избежать пусков по ошибке. Например, был случай, когда заподозрили ядерный удар со стороны Советского Союза, человек проверил, а что там все-таки на экране, проверили и обнаружили, что это ложная тревога.

Оказалось, что в систему была включена какая-то учебная пленка.

Итак, перехожу к заключению. Мы об онтологии сил и средств, о том, как они взаимодействуют с существующими системами. Это очень важное заключение и толкование сигналов и показателей. Вы должны правильно воспринять мой сигнал: если я направляю авианосец, – это сигнал, что я серьезно настроен. Что это может означать в киберсфере, если государство это делает? Откуда мы знаем, что другая сторона правильно «считывает» эти сигналы? Вот в чем проблема. И поэтому нам нужна согласованная терминология во избежание недоразумений и непониманий.

Показатели, индексы – это то, что вы используете при раннем предупреждении и оповещении с тем, чтобы знать, каков следующий этап развития конфликта. Понять терминологию этих показателей и соответствующим образом вести ваши кибероперации с тем, чтобы у противной стороны было четкое представление о ваших следующих шагах.

Вывод заключается в том, что у нас есть проблема интерпретации киберопераций, каталитические факторы могут привести к дестабилизации и крупному кризису в отношениях между государствами.

Необходимо изучать эти механизмы, чтобы понять, какие меры доверия существуют, и направлять средства в нашу организацию для проведения дополнительных исследований.

Спасибо за внимание!

Н.П. Ромашкина

Институт мировой экономики и
международных отношений имени
Е.М. Примакова Российской академии
наук

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ В ЭПОХУ ИКТ^{1,2}

Сегодня проблемы стратегической стабильности опять выходят на передний план в международных военно-политических отношениях, в том числе, и в связи с ускоренным развитием новых технологий. Об этом снова говорят и пишут достаточно много, но, к сожалению, зачастую не имея полного представления о том, что такое стратегическая стабильность, как и когда появился этот термин и т.д. Поэтому напомним основные определения.

В отношениях между ядерными державами понятие «стратегическая стабильность» в течение многих лет определялось как состояние их взаимоотношений, при котором устраняются стимулы к нанесению первого ядерного удара.

Поскольку ядерное оружие (ЯО) по-прежнему существует и его разрушительные возможности постоянно совершенствуются, в настоящее время это понимание стратегической стабильности также актуально, как и в период холодной войны, когда оно формировалось. Однако за последние три десятилетия ситуация существенно усложнилась, представления о способах и механизмах предотвращения ядерной войны, выработанные в период bipolarности, перестали соответствовать сегодняшним геополитическим реалиям и уровню развития технологий. Эти значительные изменения в международных военно-политических отношениях требуют учета не только ядерной составляющей этого понятия, но и другие показатели и характеристики, сохраняя при этом традиционную суть. Кроме того, сегодня речь идет уже не о двух глобальных полюсах противостояния, как в период bipolarности, а об увеличении количества субъектов, влияющих



на уровень стратегической стабильности. Поэтому сегодня необходимо оценивать возможности и характеристики военно-политической СИСТЕМЫ.

Стратегическая стабильность военно-политической системы – это состояние мира (отсутствие широкомасштабной войны) в рамках этой системы, которое поддерживается даже при постоянно действующих возмущениях (дестабилизирующих факторах) в течение определенного (заданного) периода времени.

Следовательно, на профессиональном уровне необходимо говорить не просто о «поддержании» стратегической стабильности, о «сохранении» стратегической стабильности, об «укреплении» стратегической стабильности, а о необходимости ОБЕСПЕЧЕНИЯ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ, о необходимости выработки совершенно новых подходов к оценке уровня стратегической стабильности. Т.е. о разработке общих качественных, и что особенно важно, количественных оценок этого уровня. А для этого необходимо договариваться об общих критериях оценки.

Процесс обсуждения таких критериев был остановлен на двустороннем уровне РФ-США

1 Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

2 Выступление подготовлено в рамках НИР «Формирование полицентричного миропорядка: риски и возможности для России» программы Российской академии наук КП19-268 «Большие вызовы и научные основы прогнозирования и стратегического планирования».



Рисунок 1. Этапы классического противоборства без комплексного применения ИКТ.

с 90-х годов прошлого века, так как Соединенные Штаты просто не считали это нужным. Сегодня это привело к глобальной опасной проблеме. Потому что снижение уровня стратегической стабильности ниже необходимого и достаточного крайне опасно для всех без исключения государств. А, следовательно, в обеспечении такого уровня также заинтересованы все страны мира. Однако ответственность у разных государств разная. И наибольшую ответственность несут, по-прежнему, ядерные державы.

Какие же новые характеристики системы, в которой жизненно важно обеспечивать необходимый и достаточный уровень стабильности, возникли в последние десятилетия?

1. Рост количества локальных войн и вооруженных конфликтов, в развязывании и ведении которых все большую роль играют информационно-коммуникационные технологии (ИКТ).

2. Изменение системы международных отношений после биполярности и американоцентричной однополярности. В первую очередь, это связано с появлением нового глобального центра силы – Китая, который не вовлечен в процесс ядерного разоружения.

3. Ракетно-ядерная многополярность, которая выражается в увеличении количества государств с ракетно-ядерными вооружением, а также с ростом вероятности дальнейшего их

распространения.

4. Тенденции к доктринальным изменениям в ядерных государствах, которые формально призваны укрепить сдерживание, а фактически снижают порог применения ядерного оружия (ЯО), в частности, к росту возможности ведения ограниченных ядерных войн.

5. Создание широкомасштабной системы ПРО США, что существенно изменяет стратегический баланс сил и увеличивает уровень неопределенности в стратегическом планировании.

6. Постепенное разрушение режима ограничения и сокращения стратегических вооружений после выхода США из Договора по ПРО, Договора по РСМД и в условиях отсутствия переговоров по ограничению и сокращению ядерных вооружений на исходе действия Договора СНВ-3.

7. Возрастание роли и мощи неядерных (высокоточных и высокоинтеллектуальных) видов оружия в стратегическом планировании, создающих теоретическую угрозу обезоруживающего удара против стратегических ядерных сил. Развитие таких вооружений существенно усложняет глобальную стратегическую обстановку и затрудняет принятие решений в кризисной ситуации.

8. Смешанное базирование на одних и тех же платформах ядерных и неядерных



Рисунок 2. Этапы противоборства с широкомасштабным применением ИКТ.



Рисунок 3. Стратегические ядерные вооружения: некоторые ИКТ-уязвимости и потенциальные последствия.

вооружений, в результате чего пуск баллистических или крылатых ракет с обычным вооружением может рассматриваться оппонентом как применение ядерного оружия.

9. Появление ядерных вооружений малой мощности, наличие которых снижает порог применения ЯО и, следовательно, вероятность пере-



растания вооруженного конфликта в ядерную войну.

10. Развитие новейших противоспутниковых средств, позволяющих влиять на работу спутников противника, включая элементы систем предупреждения о ракетном нападении (СПРН), и уничтожать при помощи противоспутниковых систем, размещенных на Земле. Кроме того, такие средства могут повлиять на эффективность работы спутников в рамках системы ведения боевых действий в едином информационном пространстве, которые активно совершенствуются в развитых в военном отношении государствах.

11. Милитаризация космического пространства (в феврале 2019 г. президент США Д. Трамп подписал меморандум о создании Космических сил США, среди целей которых названы защита интересов США в космосе, «отражение агрессии и защита страны», а также «проецирование военной силы в космосе, из космоса и в космос»).

12. Утрата страха перед ядерной войной у общества и политических элит Запада, что может снизить психологический порог применения вооружений, в том числе ядерных.

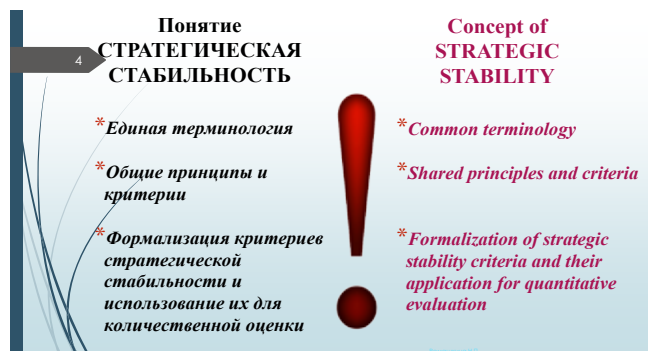
Таким образом, можно выделить основные факторы глобального влияния ИКТ на стратегическую стабильность:

- использование ИКТ в деструктивных военно-политических целях;
- соблазн одержать победу в широкомасштабной войне, связанный с взрывным развитием технологий, подталкивающих к приобретению стратегических преимуществ;
- тенденция к исчезновению границ между мирным состоянием государств и переходом их в состояние войны, размытие грани между обороной и нападением в военном, в том числе, ядерном планировании;

- изменение логики глобального противоборства (см. рис. 1, 2), когда комплексное применение невоенных методов с использованием вредоносных ИКТ приводит к достижению целей войны даже без вооруженной борьбы;
- сокращение «лестницы» эскалации конфликта, связанное с ростом вероятности ИКТ-атак на элементы военной ракетно-ядерной инфраструктуры.

Таким образом, в процессе разработки критериев оценки уровня стратегической стабильности и основанных на этом конкретных планов по ее обеспечению целесообразно учитывать как общие для любого исторического периода характеристики, так и особенности современного этапа. Ускоренное развитие ИКТ в настоящее время является одной из таких исключительных особенностей. И анализ доказывает, что все факторы, дестабилизирующие современную систему стратегической стабильности, сегодня связаны с развитием ИКТ. При этом по оценкам экспертов, уже более 30 государств обладают, так называемым, наступательным кибероружием. Поэтому соответствующие угрозы целесообразно выделять в качестве отдельного дестабилизирующего фактора. При этом каждый из других факторов в настоящий период усугубляется использованием ИКТ в деструктивных целях, милитаризацией мирных информационных технологий, а также легкостью, внезапностью и быстродействием как информационно-технологического, так и информационно-психологического оружия.

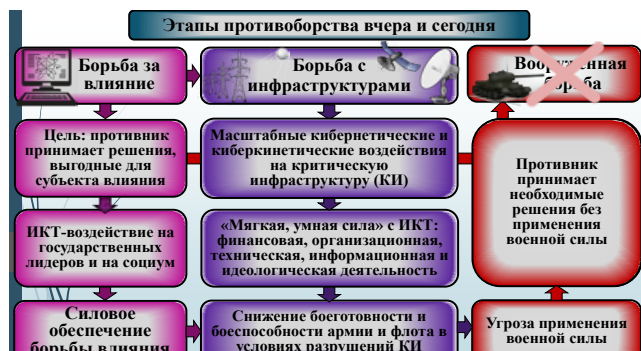
Дополнительные риски несет так называемая *кибер-электромагнитная деятельность*, которую активно развивают в США. Она включает в себя кибероперации, электронную войну, электронные атаки в мирное время, операции по управлению электромагнитным спектром, а также подавление целей активны-



ми и пассивными помехами и электромагнитная дезинформация.

Угрозы, связанные с вредоносным влиянием ИКТ на безопасность военных объектов как части критически важной инфраструктуры государства, безусловно, являются глобальными. При этом оценка ущерба от таких угроз и выработка мер противодействия существенно затруднены из-за «неосвязаемости» ИКТ, а также очень широкого спектра источников возможных вредоносных технологий: государственных и негосударственных акторов, и даже хакеров-одиночек. Все это повышает уровень неопределенности и нестабильности. ИКТ-угрозы можно отнести к различным элементам военной организации и инфраструктуры. Но в контексте обеспечения стратегической стабильности особого внимания требует безопасность ракетно-ядерных вооружений. Все ядерные державы модернизируют ядерные системы, стремясь внедрять новые компьютерные технологии. Процесс включения компьютерных сетевых операций в программы военного планирования начался более 30 лет назад, и сегодня уже можно говорить об ИКТ-революции в военном деле. Все больше компонентов военной ядерной инфраструктуры – от боеголовок и средств их доставки до систем управления и наведения, систем командования и контроля стратегических ядерных сил (СЯС) – зависят от сложного программного обеспечения, что делает их потенциальными мишенями для ИКТ-атак.

Особого внимания требует защита стратегических вооружений, система СПРН, системы противовоздушной (ПВО) и противоракетной обороны (ПРО), система командования и контроля над ядерным оружием (см. рис. 3). При этом в дополнение или вместо принципа сдерживания за счет неминуемого ответного удара, растет интерес к сдерживанию путем блокирования использования наступательных

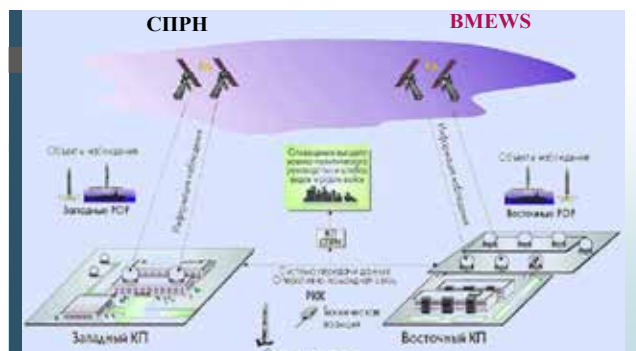


средств («блокирование пуска», left of launch) с помощью ИКТ.

Снижение уровня стратегической стабильности обусловлено влиянием развития вредоносных ИКТ на рост вероятности ошибочного санкционированного запуска баллистических ракет (БР), на принятие решения о применении ЯО; получения ложной информации от СПРН о запуске БР со стороны противника из-за растущей изощренности ИКТ-атак; повреждения или разрушения каналов коммуникаций, создания помех в системе управления вооруженными, в том числе, ядерными, силами; снижения уверенности военных, принимающих решения, в работоспособности систем управления, командования и контроля ВС. Кроме того, важнейшей проблемой является влияние роста вероятности выведения из строя или уничтожения ЯО посредством ИКТ на будущее процессов ядерного разоружения и нераспространения.

Таким образом, самой опасной, уже не гипотетической, а уже реальной в настоящее время является угроза влияния ИКТ на принятие решения о применении ЯО, т.е. на рост вероятности ошибочного санкционированного запуска БР в результате получения неверной информации или отсутствия уверенности в правильности работы систем и восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения. Это существенно снижает уровень стратегической стабильности.

Все перечисленные выше угрозы дополнительно усиливаются в связи с ростом масштабов применения ударных роботизированных средств с дистанционным управлением, с развитием технологий искусственного интеллекта в военных целях, машинного обучения, возможностями автономной работы различных систем и подсистем, автоматизированных систем принятия решений и т.д., которые могут подвергаться ИКТ-атакам.



Какие же глобальные ответы на эти глобальные угрозы стратегической стабильности можно предпринять уже сегодня, опираясь на опыт, полученный в период биполярности:

- выработка и фиксация общего (РФ, США, КНР) понимания критериев стратегической стабильности;
- выработка и фиксация общего (РФ, США, КНР) понимания опасности ИКТ-угроз;
- выработка общих подходов к оценке вероятности непреднамеренных и преднамеренных ИКТ-атак;
- четкая фиксация вероятного ответа в случае обнаружения ИКТ-атак на СЯС.

Все это может заложить основу для создания с политики сдерживания в ИКТ-среде так, как это было сделано в период биполярности в отношении ядерных вооружений.

Параллельно целесообразно работать над созданием режима контроля над ИКТ-вооружениями, который мог бы включать:

- запрет на ИКТ-атаки на конкретные объекты, в первую очередь в военной сфере (заявления, обязательства, соглашения, договоры);
- ограничение и/или отказ от наступательных ИКТ-возможностей;
- меры контроля за распространением ИКТ-вооружений;
- международные нормы в отношении средств и методов предотвращения и устранения киберконфликтов;
- разработку конвенции о запрещении вредоносного использования ИКТ в сфере ЯО.

Дженис Хэмби, (Janice Hamby),

контр-адмирал ВМС США (в отставке),
Колледж информационного и
киберпространства, Университет
национальной обороны США

СТРАТЕГИЯ НЕПРЕРЫВНОГО ВОЗДЕЙСТВИЯ: ОПИСАНИЕ И ВЗГЛЯД НА ПРЕИМУЩЕСТВА И РИСКИ

Спасибо за предоставленную возможность выступить. В свое время я преподавала в Университете обороны США, а сейчас я являюсь консультантом.

К сожалению, в прошлом году не смогла приобщиться к данному форуму. Сегодня мне поручено поделиться с экспертным сообществом России и других стран новой концепцией, разработанной в Пентагоне США – «persistent engagement». Я не претендую на звание эксперта в этом отношении, но мне позволяет выступать на эту тему многолетний опыт службы в ВМС США и, несомненно, я знакома с тем, как работают ИКТ-сети в военной среде.

Я хочу отослать вас к ряду публикаций Киберкомандования США, а также делюсь своим взглядом относительно этой концепции.

Я хочу, чтобы вы на секунду забыли о тех выводах, которые сформировались у вас до этого, и посмотрели на эти идеи новыми глазами.

В настоящее время ведется широкая дискуссия на эту тему в США, которая совсем не обязательно в выборе формулировок направлена на то, чтобы ввести в заблуждение ряд специалистов.

Сразу оговорюсь, в нашей корпоративной ведомственной культуре существует практика формирования каких-то концепций, описанных сложными словами, может вызывать некое неадекватное представление. И часто формируется некая концепция, которая оформляется словами, рассчитана на то, чтобы произвести впечатление на представителей параллельных структур, министерств и ведомств.

Итак. Надеюсь, что по итогам моего выступления вы сможете взять «на вооружение» некоторые высказанные соображения.

Очень важно понять, что такое «непрерывное воздействие». С одной стороны, это

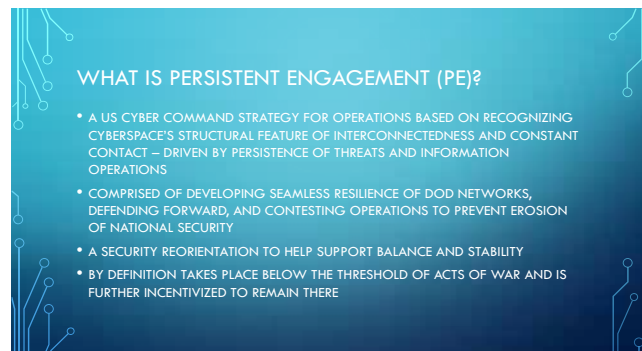


некое реагирование военного командования, которое отвечает за защиту информационно-коммуникационных сетей, для обеспечения постоянной готовности и отказоустойчивости. Воспринимается это со статических позиций для того, чтобы быть на острие тех угроз, которые существуют в отношении ИКТ. Это исходит как от государственных, так и негосударственных акторов. Киберкомандование США занимает более активную позицию для того, чтобы предотвращать различные зловередные попытки воздействовать на критические объекты инфраструктуры США.

Тема «непрерывного воздействия» позволяет различным ведомствам США попытаться обеспечить также взаимосвязь между сетями, которые служат вооруженным силам, и гражданскими сетями. Я говорю, например, о системах Министерства внутренней безопасности США.

Эта дискуссия также позволяет нам сформировать понимание того, какие есть законные объекты и цели в киберпространстве и какие незаконные, то есть на что можно направлять некие силы воздействия и на что нельзя. И потом имплементировать это принудительными методами. Это проблематично, как установить эти нормы, основанные на молчаливых соглашениях, чтобы подвигать акторов к ответственному поведению.

К сожалению, государства не всегда оказываются на высоте, чтобы договариваться между



собой относительно новых стандартов, которые необходимо выполнять в этом отношении.

Очень важно также понимать, что непрерывное воздействие, как это будет практиковаться, является не наступательным, не эскалационным по своей природе, а просто указывает на способность противника, будь то государство, с которым конкурирует США, или же негосударственные образования, которые хотят нанести ущерб американским интересам и др., как предотвращать угрозы с их стороны.

Что касается аналитики, стратегические авторы, которые находятся ближе к разработке этой концепции, указывают, что принятие на вооружение этой концепции связано с осознанием того факта, что стратегии реагирования, которые применялись США до этого, оказались недостаточными и не могут соответствовать росту угроз – вторжений, информационных операций, которые наносят ущерб источникам государственного влияния со стороны США.

Анализ данной ситуации привел к необходимости переоценить стратегическую среду и к выводу, что стратегия непрерывного воздействия может привести к значительным выгодам для США, а также для их партнеров и союзников.

Ключом к этой стратегии является осознание того факта, что сама структура сетевого пространства основана на принципе соединенности. Любое лицо, которое оказывается в киберпространстве, не может не контактировать со всеми другими акторами, которые здесь присутствуют. Это является источником постоянных угроз, с которыми сталкивается командование США. И это также вектор, который позволяет злоумышленникам распространять свои отрицательные меры влияния.

Это основано на следующих принципах:

- бесшовной устойчивости сетей, позволяющей сети быстро восстанавливать

свою работоспособность после нанесения какого-либо ущерба;

- возможности переносить понимание угрозы до того, как некая угроза нанесет удар по военным сетям, например, она может проявляться где-то в корпоративных сетях. Мы должны выявлять такие возможные проявления и упреждать нанесение ударов по военным сетям;
- и, наконец, необходимости предпринимать шаги активного характера в отношении источников любых угроз: от государств, от негосударственных структур, преступных групп и др.

Ожидается, что основное внимание будет уделено первым двум принципам: обеспечению отказоустойчивости сетей и их способностям восстанавливаться после нанесения ударов. Все это способствует недопущению эрозии безопасности, как в отношении боевых потенциалов, так и в отношении демократических ценностей США, так как эти угрозы могут подрывать безопасность государства.

В основе Стратегии непрерывного воздействия США находится недопущение разрушения сил влияния, что поддерживает баланс и стабильность между источниками влияния, а также между державами, которые не допускают перехода через некие «красные линии», после нарушения которых возникает необходимость применять силы и средства соответствующего реагирования. Для этого создаются условия, при которых у других государств не возникнет желания идти на эскалацию конфликтов.

Возникновение этой Стратегии сейчас явилось итогом понимания того, что киберпространство представляет достаточно новое конкурирующее пространство, управляемое разными силами и средствами, которые могут привести к деградации любого влияния и могут угрожать суверенитету различных го-



сударств. Эта эрозия может привести к таким последствиям, как кража интеллектуальной собственности, а также к подрыву возможностей оборонного характера США.

Например, мы наблюдали использование ботнетов во время выборов в США 2016 года, а также киберпреступность, которая повлекла за собой потери для бизнеса в значительных масштабах.

Это говорит о том, что США должны принимать другие подходы в отношении безопасности собственных ИКТ-систем и, в первую очередь, сетей Министерства обороны США как объекта критической инфраструктуры.

Также хочу отметить, что Стратегия непрерывного воздействия – это не совсем новая концепция, она происходит от анализа динамики эскалации, и, учитывая эту проблему, вооруженные силы США теперь применяют эту концепцию, но не на боевых принципах, а на принципах согласованной конкуренции. Мы исходим из того, что наша деятельность осуществляется ниже «красной линии», после перехода которой может начаться боевой конфликт.

Что касается согласованной конкуренции, то мы предполагаем, что перед нами некое пространство между эскалацией, при этом акторы не переходят той грани, после которой имеют место эскалационные действия. Между игроками и пространством есть некая динамика взаимодействия, когда они пытаются навязать свою повестку дня и предпринять какие-то действия на основе субъективного восприятия для того, чтобы сохранять возможность невыхода за порог эскалации вооруженного конфликта. Эта концепция развивается во времени, повышается уровень понимания того, что может быть предпринято. Анализируя результаты взаимодействия в киберпространстве, можно определить, какие действия считаются законными или незаконными, насколько ответственно государства там действуют, не нарушают ли



порогов, которые могут привести к эскалации.

На уровне понимания открывается пространство для замены существующих принципов, которые существовали в то время, пока мы вырабатывали понимание этих согласованных норм. Мы говорим о том, что, возможно, предпринимаемая нами деятельность не всех устраивает, мы активно вовлекаемся в эти процессы до того момента, пока не возникнет новых стандартов относительно того, что принято и что не принято, что приемлемо и что неприемлемо в киберсфере. Цивилизация баланса направлена на то, чтобы не допустить эскалации. Это мера успеха относительно того, как Стратегия непрерывного воздействия оценивается в плане своей эффективности или отсутствия таковой.

Далее мы подходим к рискам, связанным со Стратегией непрерывного воздействия. Здесь нам необходимо четкое понимание того, что приемлемо и что неприемлемо. Отсутствие этого понимания может привести к переходу «красной линии» и непреднамеренной эскалации конфликта в киберсреде. Также существует риск того, что баланс сил может быть неправильно воспринят. Я думаю, что и другие риски могут возникнуть по мере того, как мы будем и дальше работать над этой Стратегией.

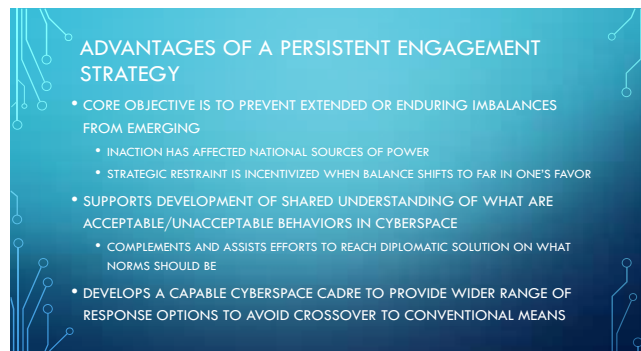
Что касается преимуществ, которые предлагает Стратегия непрерывного воздействия, то это выявление продолжительных дисбалансов, особенно перед лицом укрепляющихся государств в условиях дефицита ресурсов для того, чтобы многие посчитали, что нарушение равновесия уже существует. Предпринимаются более проактивные стратегии, позволяющие США ответить на многие внутренние запросы, которые направлены на то, чтобы дополнительные меры предпринимались. Даже в условиях того, что предпринимаются попытки восстановить равновесие, и, как раз, наличие выбора – это более желательный выбор.



Нужно помогать также разрабатывать общее понимание, о котором говорилось выше, и это может быть прямым дополнением к дипломатическим усилиям, которые продолжают предприниматься для ответа на вопрос, какие нормы должны быть и как их нужно правоприменять на практике после того, как они будут согласованы.

Еще одним преимуществом является подготовка высококвалифицированных кадров для киберсил с учетом технических достижений и использования средств принятия решений политическим руководством. Это поможет применять меры контроля за теми, кто осуществляет кинетический вариант действенных решений при негативном изменении баланса сил.

Подводя итоги, мы должны признать, что эта Стратегия непрерывного воздействия



дает возможность новых подходов к конкуренции в стратегическом пространстве. Есть возможность противодействовать негосударственным субъектам, проводящим незаконные действия.

Однако эта Стратегия не может заменить личного взаимодействия, которое помогает создавать взаимопонимание в вопросах киберпространства, которое должно сопровождаться четкими каналами связи, а также формированием понимания относительно этих норм. Переводя эту Стратегию в общественную сферу, Киберкомандование фактически посылает сигнал о намерениях для того, чтобы исключить неправильную интерпретацию его действий в рамках данной Стратегии.

Татту Мамбеталиева,

ОФ «Гражданская инициатива Интернет-политики», Кыргызстан

ПРОБЛЕМЫ ПРОФИЛАКТИКИ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В ИКТ-СРЕДЕ

Для того, чтобы найти общие подходы и точки соприкосновения, мы не должны еще забывать, что есть еще такая угроза, как экстремизм.

Я сегодня презентую первый этап нашей работы, которую мы провели с SecDevGroup, Internews, Еврокомиссией и др. Финансирование осуществляла Еврокомиссия, остальные организации проводили исследования.

Цель нашего исследования – посмотреть, что происходит в Интернете, как экстремисты работают, то есть мы сделали анализ общедоступного контента, мы не заглядывали в глубокий Интернет, закрытый Интернет, мы смотрели, как они проводят вербовку, мы смотрели, какие сообщения они посылают друг другу, и провели анализ профилактики в Интернете в борьбе с этим злом.

Исследование включало только страны Центральной Азии, и мы также захватили Россию, так как общеизвестно, что в России имеются очень большие азиатские диаспоры. Мы брали названия всех экстремистских организаций, и исходя из 20-летнего опыта организации, которая занимается исследованиями именно в этих группах, разрабатывали различные методы и способы для того, чтобы идентифицировать название и правильно определить экстремистские группы.

Исследование мы проводили в следующих социальных платформах: Facebook, Telegramm, Twitter, YouTube, Google, Instagram, Одноклассники, ВКонтакте и LifeJournal. Кроме этого, мы посмотрели законодательную практику и пришли к следующему результату.

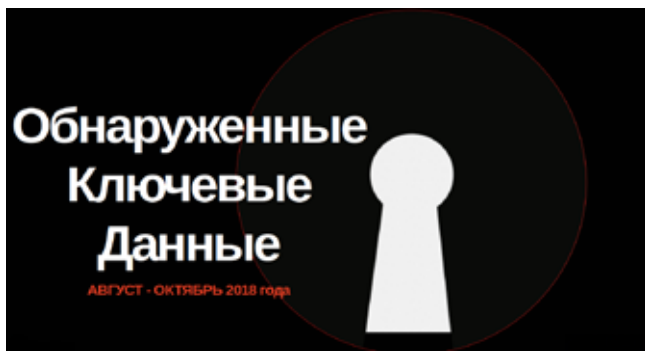
Еще раз я хотела бы сказать, что мы не стали смотреть закрытую часть Интернета, мы не стали смотреть, какие объекты являются объектами экстремистских организаций, и, более того, мы не делали упор на террористические группы, то есть мы сделали только первый шаг и сегодня презентуем его.

Исследование шло 3 месяца. Мы исследовали контент с 1 августа по 31 октября 2018 г.



Какие мы обнаружили основные проблемы? Юридическое исследование показало, что мы не имеем единого подхода к определению «экстремизма». Мы сравнили законодательства четырех стран Центральной Азии и России. Мало того, что они не соответствуют друг другу, мы поняли, что то, что является экстремизмом в Узбекистане, не является экстремизмом в Кыргызстане. То, что является в России экстремизмом, не является экстремизмом в Центральной Азии. И, кроме этого, разлет этого понятия включает и политический, и вооруженный, и религиозный экстремизм. Мы взяли в основу религиозный экстремизм, потому что разбираться с политическим экстремизмом и т.д. для нас оказалось неподъемной задачей.

Я объяснила, как мы создавали списки, но мы изучили списки, которые находятся в этих странах, как запрещенный контент. Более того, мы посмотрели ОДКБ, ШОС и другие международные организации, которые признают те или иные организации экстремистскими. Мы увидели, что у них не определен единый критерий, не понятно, по какому принципу эти списки сформированы, и чаще всего эти сайты не публикуются, а если публикуются, то не в полном объеме. В этой связи мы нашли такое количество судебных решений, которые закрыли большое количество контента экстремистского формата, но они не были опубликованы.



В качестве причины неопубликования правительства выражают мнение, что публикация подобной информации вызывает еще больший интерес к ней и граждане будут пытаться так или иначе посмотреть запрещенный контент. Мы также увидели, что законодательства не проводят профилактических мер, а используют в основном карательные меры. Например, в некоторых странах за «дизлайки» и за «лайки» граждане не могут получить уголовное наказание.

Получается, что один и тот же размер наказания получает и экстремист, который реально осуществлял экстремистскую деятельность, и молодой парень 16-летнего возраста, нажавший «дизлайк».

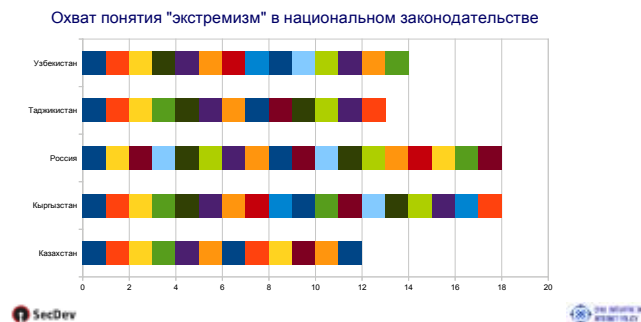
То есть существуют очень большие и по меркам, которые принимаются за экстремистскую деятельность. И в 99,9% случаев предусматривается только уголовное наказание, при этом оно не разделено по разным видам и типам деятельности.

Мы составили схему, разместив все дефиниции и увидев все наши отличия. Самый широкий спектр различий понятия «экстремизм» дан в Казахстане и России, в меньшей степени – в Кыргызстане и России.

Далее мы выявили, какое количество определений дается в законодательстве. Для определения в законодательстве понятия «экстремизм» используется огромное количество слов.

Исследование показало, что в вышеупомянутых социальных сетях активно работают 246 аккаунтов, содержащих реальный экстремистский контент и принадлежащих известным экстремистским группам. Из них 140 аккаунтов распространяют экстремистский контент и имеют 324000 подписчиков. 75 аккаунтов неактивны, но существуют и 31 аккаунт заблокирован (из выявленных 9000! сайтов экстремистской направленности).

Какие экстремистские группы мы обнаружили? Наиболее активной организацией,



которая работает в регионе Центральной Азии, является Хизбут-Тахир, которая имеет наибольшее количество подписчиков, а вот Хайят-Тахир-Аль-Шахам тоже оказался невероятно активным и его аккаунты пользуются большой популярностью.

Интересно, что организация Хайят-Тахир-Аль-Шахам – это организация, созданная из выходцев из Средней Азии, в наибольшей степени агитирует за то, чтобы вербовать боевиков для Сирии. Но, как мы обнаружили, в настоящее время Сирия заменена другой страной.

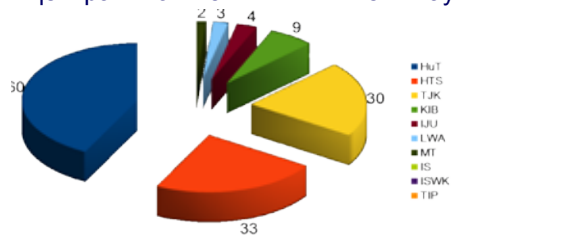
Активность и представленность в сети Интернет этих организаций следующая. Наиболее представлены в Интернете Хизбут-Тахир и Хайят-Тахир-Аль-Шахам.

Более известная организация ИГИЛ, по нашим сведениям, активно работает в Интернете, но мы не нашли их присутствия в открытых сетях. Мы полагаем, что они все-таки работают в Даркнете.

Посмотрите, какой язык используют эти организации. Когда речь шла о киберграницах и как их определить, мы поняли, что нельзя брать язык в качестве средства определения границы государства, так как оказалось, что даже используя русский язык, как наиболее популярный в этих экстремистских группах, и второй язык – узбекский, это не говорит о том, что это территория России или Узбекистана. Наиболее популярные языки в экстремистских группах: русский, узбекский, на третьем месте – английский, турецкий и кыргызский.

Согласно проведенному анализу, мы пришли к выводу, что блокировка – неэффективный метод борьбы с подобным контентом. При этом практически во всех странах существует внесудебный порядок закрытия, когда решение принимается на политическом уровне без судебного порядка. В результате порядок борьбы с экстремизмом становится более

Экстремистский Контент в Социальных сетях Центральной Азии. Активные Аккаунты



SecDev

THE NATIONAL INSTITUTE FOR SECURITY

политизированным, нежели реальная борьба с экстремизмом.

Например, в Казахстане те сайты, которые признаны там экстремистскими, а в других странах нет, оказалось, что признаны экстремистскими по политическим решениям.

Блокировка контента вызывает ответную меру от экстремистских организаций: они меняют IP-адреса, находят себе место в Даркнете.

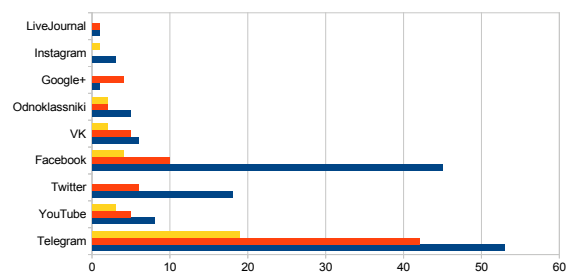
Таким образом, борьба с экстремизмом оказывается не только противоречащей международным нормам по свободе слова и доступа к сети Интернет, но и создала иные условия, не контролируемые правительственными структурами.

Что касается представленности в социальных сетях. Как можно увидеть, Telegramm и Facebook занимают лидирующие позиции по наблюдениям за отчетный период. Самое интересное здесь, что при запрете одного ресурса в какой-либо стране экстремистские ресурсы тут же мигрируют в эту неконтролируемую государством зону. Если проанализировать Telegramm, то он также активно борется с экстремистским контентом и самостоятельно заблокировал 19 аккаунтов. Также Facebook блокирует в соответствии со своими правилами.

Однако статистика пугает! Также мы увидели, что Twitter тоже является очень популярным для экстремистской агитации. Наибольшее количество активных экстремистских аккаунтов находится в Telegramm, затем в Facebook и Twitter.

По количеству подписчиков лидирует Facebook, несмотря на то, что в нем меньше экстремистских аккаунтов, чем в Telegramm.

Тенденции: Контент НЭ в Социальных Сетях



SecDev

THE NATIONAL INSTITUTE FOR SECURITY

Проводя исследование, мы увидели следующие тенденции.

Что касается контента, то в этих сообщениях большое внимание уделяется популяризации экстремистских групп, а также работе в них. Агитационная работа в этих группах тоже находится на высоком уровне. Но в то же время мы увидели множество активных аккаунтов, которые стараются охватывать другие аккаунты, не интересующиеся данной проблематикой. Согласно анализу большинство этих аккаунтов принадлежат молодежи.

Через аккаунты осуществляется также и финансирование деятельности экстремистских групп, чаще всего в биткоинах и других криптовалютах.

Исследование показало, что некоторые экстремистские группы создают много независимых официальных аккаунтов, которые распространяют информацию в различных социальных сетях. То есть аккаунты включают в себя радикальный и развлекательный контент.

Другие экстремистские группы, использующие в большей степени узбекский язык, набирают большое количество подписчиков за счет правильного использования языка, например, узбекского.

Мы обнаружили, что в исследуемых группах изменилась страна агитации: если раньше страной агитации была Сирия, то сейчас этой страной стал Афганистан вследствие его близости к исследуемому региону.

ИГИЛ почти не присутствует в открытых социальных сетях, и мы полагаем, что они осуществляют свою деятельность в Даркнете.

Спасибо за внимание!

И.А. Тяжлова,

*Министерство иностранных дел
Российской Федерации*

К КИБЕРДИАЛОГУ С ВАШИНГТОНОМ ГОТОВЫ, НО НАВЯЗЫВАТЬСЯ НЕ БУДЕМ¹

Прежде всего, позвольте выразить признательность организаторам форума за предоставленную возможность выступить на таком известном и значимом мероприятии. Ежегодные встречи ключевых российских и зарубежных экспертов в области обеспечения международной информационной безопасности (МИБ) для обсуждения наиболее острых и актуальных вызовов в данной сфере давно стали доброй традицией, и для меня большая честь быть участником этого дискуссионного формата.

В рамках сегодняшнего «круглого стола» мне хотелось бы предложить совместно поразмыслить над одним из наиболее интересных аспектов – перспективами российско-американского диалога по МИБ.

В начале февраля текущего года Президент Российской Федерации В.В. Путин четко сформулировал нашу позицию по выстраиванию переговорного процесса с США в разоруженческой сфере: поскольку неоднократные российские предложения о проведении содержательной двусторонней дискуссии по данной тематике Вашингтоном не поддерживаются, мы прекращаем инициировать какие-либо переговоры и будем ждать, пока наши партнеры не созреют для равноправного и конструктивного диалога с нами.

На мой взгляд, небезынтересно поразмыслить над тем, относится ли данная тактическая линия и к нашему взаимодействию с США по вопросам МИБ. Предлагаю для начала обратиться к истории кибердиалога России и США и затем с точки зрения здравого смысла проанализировать, чего в ней было больше – конструктива или конфронтации, и оценить перспективы возобновления сотрудничества наших стран в данной сфере.

Слово «сотрудничество» в данном контексте может показаться слишком оптимистичным, ведь в нынешних политических условиях обывателю трудно поверить, что за последние



десять лет Россия и США достигли серьезных заделов в области обеспечения МИБ. Но эксперты и политики хорошо помнят, что на определенном этапе стороны сумели достичь существенных практических результатов, направленных, в частности, на укрепление доверия между нашими странами в этой сфере.

Ключевую роль в этом процессе сыграл установленный между Москвой и Вашингтоном механизм полномасштабных двусторонних межведомственных консультаций. Начало ему положило заседание рабочей группы в феврале 2011 г. в Москве, которая была созвана для участия в двусторонней встрече на высоком уровне по проблемам кибербезопасности и обсуждению таких важных вопросов, как обмен мнениями о концепциях использования информационно-коммуникационных технологий (ИКТ) в военных целях, регулярный обмен информацией между национальными CERT-центрами.

21–23 июня 2011 г. состоялся визит в Вашингтон российской межведомственной делегации во главе с заместителем Секретаря Совета Безопасности Российской Федерации Н.В.Климашиным.

Американскую делегацию возглавил координатор Белого дома по кибербезопасности Г. Шмидт. Переговоры, проходившие в Белом доме, были нацелены на продолжение

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

обсуждения мер укрепления доверия, чтобы предотвратить непреднамеренную эскалацию инцидентов в информационной сфере. О конструктивном духе консультаций свидетельствует подписание совместного заявления, в котором подчеркивалось, что взаимодействие между двумя сторонами в этой области вышло на качественно новый уровень, позволяющий начать практическую отработку механизмов укрепления доверия и обеспечения транспарентности деятельности государств в киберсфере.

Апогеем российско-американского взаимодействия по проблемам МИБ стал июнь 2013 г. «На полях» саммита «Большой восьмерки» в Северной Ирландии главы наших государств выступили с совместным заявлением о новой области сотрудничества в укреплении доверия. Было объявлено о заключении трех прорывных по своей значимости договоренностей, формирующих комплексную систему мер доверия между Россией и США в информационном пространстве. Речь идет об установлении линий прямой коммуникации на случай киберинцидентов на трех уровнях – между представителями, курирующими вопросы национальной безопасности, силовыми ведомствами по линии национальных центров по уменьшению ядерной опасности (НЦУЯО) и группами экстренной готовности к компьютерным инцидентам (CERT).

По сути, данные каналы связи выстроены по той же схеме, которая существовала в годы холодной войны применительно к традиционным военным инцидентам. Таким образом, устанавливались прямые контакты между конкретными структурами и ответственными лицами в Москве и Вашингтоне, что предоставляло возможность оперативно реагировать на вредоносные действия и предотвращать возникновение потенциально конфликтных ситуаций в информационной сфере. Таких механизмов оперативного взаимодействия у России больше нет ни с одним другим государством, что, безусловно, говорит о значительном уровне доверия, который был присущ нашим странам на определенном этапе, об их способности договариваться при обоюдном желании.

Позитивный момент состоит также в том, что уже тогда, в ходе консультаций, наряду с другими вопросами обсуждались перспективы взаимодействия России и США в из-

вестной Группе правительственных экспертов (ГПЭ) ООН по МИБ.

В 2015 году был принят революционный по своему значению доклад ГПЭ, в котором удалось зафиксировать компромиссные формулировки относительно применимости международного права к информационному пространству. По итогам работы Группы российская сторона открыто признала, что документ «сложился» во многом благодаря конструктивной гибкости, проявленной экспертом США, ее готовности работать с партнерских позиций. В свою очередь, американка заявила, что именно благодаря титаническим усилиям российского председательства Группе удалось обеспечить ее работу и итоговый доклад.

Можно сделать вывод, что за столь непродолжительный период стороны осознанно выработали механизм предотвращения конфликтов между Россией и США в киберсфере. Этот опыт может служить доказательством того, что отношения между нашими странами в области МИБ далеко не безнадежны, как сейчас принято думать, что мы можем договариваться и предпринимать совместные и коллективные дипломатические усилия, когда захотим.

Однако в 2016 году по окончании президентского срока Б.Обамы в США была развернута известная избирательная кампания, во время которой одному из кандидатов предвыборной гонки ввиду растущей вероятности своего проигрыша понадобилось списать свои неудачи на внешнее – российское – вмешательство в электоральный процесс.

Характерно, что именно до этого момента стороны вели обмен чувствительной информацией относительно малейших подозрений в отношении действий друг к другу в информационном пространстве напрямую.

И только в свете упомянутых событий официальное взаимодействие экспертов в этой сфере ушло на второй план. Вместо него был создан феномен «фейкньюс», который, увы, до сих пор определяет состояние российско-американских отношений.

Тогда российская сторона проявила выдержку. Апеллируя к здравому смыслу, мы предлагали партнерам – вместо того чтобы идти в прессу с голословными выпадами – обращаться напрямую в Москву для устра-

нения недопониманий и подозрений. Осенью 2016 года в адрес России по каналам прямой связи все же поступило обращение американской стороны об озабоченностях относительно несанкционированного проникновения в их электронную инфраструктуру. Наши эксперты на него оперативно отреагировали, был произведен обмен соответствующей технической информацией, которая удовлетворила наших коллег.

Казалось бы, инцидент исчерпан. Однако, по-видимому, кого-то в Белом доме такое затухание искусственной конфронтации явно не устроило. США до сих пор приписывают России вину во всех кибергрехах без предъявления каких-либо доказательств.

В противовес данной позиции Вашингтона мы неоднократно пытались найти новые точки соприкосновения в выстраивании российско-американского диалога по МИБ.

Чтобы раз и навсегда разрешить вопрос о вмешательстве России в американские выборы, российская сторона выразила готовность к обнародованию содержания упомянутой технической переписки и ее изучению экспертами, журналистами, широкой общественностью в России и США, СМИ. Соответствующее предложение Москва официально направила в Вашингтон по дипломатическим каналам в начале этого года. В ответ получили отказ под предлогом чувствительности этих материалов.

Ранее, в июле 2017 г., заместитель Министра иностранных дел Российской Федерации С.А. Рябков передал заместителю Госсекретаря США по политическим вопросам Т. Шэннону проект меморандума о создании российско-американской группы по безопасности в сфере использования ИКТ и самих ИКТ, подготовленный российской стороной в развитие договоренностей, достигнутых в ходе состоявшейся незадолго до этого встречи В.В. Путина с Д.Трампом «на полях» саммита «Группы двадцати» в Гамбурге. Американцы взяли документ в межведомственную проработку, и с тех пор информации о прогрессе на этом направлении от Вашингтона не поступало.

Окно возможностей, казалось бы, открылось, когда стороны достигли договоренности о проведении в феврале 2018 г. в Женеве полномасштабных двусторонних межведомственных консультаций по МИБ, в которых предпо-

лагалось участие солидных делегаций с обеих сторон. Эксперты наших стран готовились обсудить широкий спектр вопросов в рамках согласованной повестки дня, в частности, меры укрепления доверия, борьбу с кибертерроризмом и киберпреступностью. Однако за несколько часов до начала переговоров данные консультации были отменены партнерами.

Очередная договоренность о необходимости возобновления диалога между Россией и США – в том числе и по кибервопросам – была достигнута в ходе встречи глав наших государств в Хельсинки 16 июля 2018 г. Однако «кибермяч» до сих пор находится в руках Вашингтона.

В сложившихся условиях восстановление диалога и взаимного доверия представляется весьма затруднительным. И все же это объективная необходимость в свете предстоящего запуска работы двух переговорных площадок по МИБ под эгидой ООН – Рабочей группы открытого состава (РГОС) и ГПЭ.

Деятельность этих групп предусмотрена принятыми в декабре 2018 г. российской и американской резолюциями ГА ООН.

Проведение дискуссии по МИБ в ООН в двух форматах отнюдь не означает, что Организация раскололась на два противоположных лагеря. Напротив, учреждение двух групп гораздо лучше для международного сообщества, чем отсутствие подобных площадок как таковых. Россия заинтересована в том, чтобы работа РГОС и ГПЭ была успешной и результативной без какой-либо внутренней конкуренции.

Именно такое видение дальнейшего переговорного процесса по МИБ в ООН мы инициативно представили американской стороне в ноябре 2018 г. Тогда же предложили провести на экспертном уровне двустороннюю российско-американскую встречу для обсуждения модальностей работы этих механизмов, как вариант, – в рамках уже согласованной ранее повестки дня. К сожалению, ответ из Вашингтона так и не поступил.

Возникает логичный вопрос: неужели американцам совсем не интересно, что будет происходить в области МИБ как в ООН, так и в двустороннем плане? Хочется верить, что это не так.

Представляется, что главным препятствием для нормализации взаимодействия наших стран по МИБ является напряженная внутри-

политическая обстановка в США. Однако американский истеблишмент должен понимать, что из-за их внутренних проблем и противоречий тормозится как международное сотрудничество по вопросам МИБ в целом, так и соответствующий двусторонний диалог.

В данном контексте обращают на себя внимание недавние публикации отдельных представителей американского экспертного сообщества, в которых на фоне общего антиросийского гомона присутствует здравый смысл. Например, в статьях «Эта горячая линия может предотвратить кибервойну между США и Россией» (издание «The Daily Beast») и «Киберсоглашение с Россией» («Kennan Cable») открыто заявляется, что отсутствие экспертного, деполитизированного диалога между Россией и США в области МИБ – путь, чреватый углублением недопонимания и риском масштабного конфликта. По мнению экспертов, заключение

киберсоглашения с Россией, даже если оно будет временным, – первый шаг к доверительному диалогу для оперативного разрешения недопониманий между сторонами, которые могут привести к эскалации и даже вооруженным конфликтам.

Едва ли в данных предложениях есть что-то крамольное, идущее вразрез с обеспечением национальной безопасности США.

Напротив, в этом процессе на передний план выходит именно уровень экспертов – тех, кто непосредственно отвечает за информационную безопасность, осознает весь комплексный и деликатный характер проблематики МИБ.

Одно ясно всем: договариваться нужно и как можно скорее.

Россия к прагматичному, продуктивному и деполитизированному кибердиалогу с американскими коллегами готова.

Д.Б. Фролов,

*Российская телевизионная и
радиовещательная сеть (РТРС), Россия*

УГРОЗЫ И РИСКИ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Норберт Винер еще в 50-х годах прошлого века предрек наступление эры того, что сегодня в рамках разработанной Правительством и бизнесом ФРГ программы называется «Индустрия 4.0» или «общая роботизация на основе информационных технологий». Как отмечают ведущие исследователи ИНЭС РАН, закономерным итогом цифровизации станет не только новый вариант экономических отношений, но и «новый уровень отношений между обществом и государством (цифровое правительство), создание высокотехнологичной инфраструктуры (цифровое пространство)»¹. Перенос общественно-политических отношений в такое пространство не исчерпывается изменением формы отношений. Затрагиваются сущностные характеристики общественной и политической сред, такие как легитимность и доверие к власти.

Как отмечает основатель Всемирного экономического форума в Давосе К. Шваб, «реальность цифровой эры заключается в том, что многие новые компании предоставляют «информационные товары» с практически нулевыми затратами на хранение, транспортировку и тиражирование»².

К. Шваб заключает, что мир входит в эпоху Четвертой индустриальной революции, которая характеризуется следующими особенностями:

- создание единицы ценности требует меньше рабочей силы;
- снижение доли труда в ВВП за счет падения относительной цены средств производства;
- внедрение технологий «распределенных баз данных», трансформирующих коммуникации в экономической системе;



- переход к «экономике совместного потребления»;
- гармонизации и интеграции научных дисциплин.

Положения последних Деклараций саммитов G20 однозначно показывают, что процесс глобализации вступает в новую фазу и конкретно ведет к построению так называемого «всемирного наднационального социума», в котором со временем растворятся существующие национальные государства. Основой его построения становится внедрение информационных цифровых технологий в повседневную жизнь граждан, а главным инструментом – электронная идентификация личности³.

Однако последствия такой революции, по нашему мнению, создают предпосылки к усилению социального неравенства, и усиливают тех, кто владеет интеллектуальным и физическим капиталом. Иными словами, происходит концентрация преимуществ и ценностей в руках небольшого процента людей, считающих себя элитой. В условиях глобальной интеллектуализации экономической и финансовой деятельности это чревато массовой безработицей среди специальностей низшей и средней квалификации.

1 Аверьянов М.А., Агеев А.А., Евтушенко С.Н., Кочетова Е.Ю. Цифровое общество: архитектура, принципы, видение // Экономические стратегии. - 2017. - № 1. - С. 117.

2 Шваб К. Четвертая промышленная революция / К. Шваб. - «Эксмо», 2016. - (Top Business Awards). - 138 с.

3 Декларация саммита G20. Гамбург 7-8 июля 2017 года // ИА ТАСС. Официальный сайт. - [Электронный ресурс]. - Электрон. дан. - Режим доступа: <http://tass.ru/mezhdunarodnaya-panorama/4398932>

ЭТАПЫ РАЗВИТИЯ ОБЩЕСТВА



Элвин Тоффлер
(1926 – 2016)



Аграрная волна
(до XVII века)



Индустриальная волна
(до 1950-х годов)



Информационная волна
1980 год

Рейтинг развития цифровой экономики (Digital Evolution Index 2017), подготовленный Школой права и дипломатии им Флетчера университета Тафта (США):

Доля цифровой экономики в общем объеме ВВП России сейчас оценивается в 3%, в перспективе эта цифра должна быть двузначной. По данным этого исследования и корпорации Mastercard, Россия занимает 39-е место, а по темпам развития 5-е.

Наиболее вероятные элементы цифровой трансформации включили три блока изменений:

1. Развертывание цифровой инфраструктуры (электронные торговые площадки, широкополосная связь);
2. Обострение цифровых угроз (весь блок киберугроз и процессов, ведущих к деградации естественного интеллекта);
3. Разработка и доступность новых производственных и управленческих технологий, опирающихся на цифровые достижения.

Создаваемая в России цифровая экономическая среда создает предпосылки для изменения доминирующих организационных экономических моделей. Если для индустриального этапа развития характерны централизация и концентрация производства, то для информационного этапа – гибкая децентрализованная организация управленческих процессов в социально-экономической сфере. Виртуализация и усиление социальных взаимодействий приводит к изменениям форм этих взаимодействий. Проявляются новые сущностные характеристики обществ и государств, такие как, многомерность и многополярность.

Очевидно, что до тех пор, пока существуют нации, государственный суверенитет сохраняет те или иные формы. Поэтому в «Концепции формирования информационного общества в России» в 1999 году указывалось: «Создавая в России экосистему для интеграции цифровых технологий в экономику, нужно соотносить возникающие предложения и инициативы с целями Стратегии государственной национальной политики страны на период до 2025 года».

«Петля гистерезиса»

Процесс выхода из структурного кризиса 1980-х гг. (А.Г. Аганбегян). Занял три периода: «трансформационный кризис» 1990-1998 гг. (падение экономики и социальной сферы вдвое), восстановительный подъем 1999-2008 гг. (рост увеличился вдвое), потерянное десятилетие 2009-2017 гг. – стагнация (отсутствие роста).

ВВП в первый период упал на 44% (промышленность – на 52%, сельское хозяйство – на 46%, инвестиции в основной капитал – на 79%).

В потерянное десятилетие (2009-2017 гг.) ВВП вырос всего на 4%, инвестиции – на 2%. Доля инвестиций в основной капитал составила всего 17%, тогда как в развитых странах – 20%, а в развивающихся – 30-35%.

За 30 лет страна проделала «петлю гистерезиса», одновременно сократив и перераспределив свой экономический потенциал в пользу зарубежной экономической системы, внутренних и иностранных предпринимателей. Отток капитала за этот период составил, по разным оценкам, от 2 до 5 трлн долл.

ЦИФРОВАЯ ЭКОНОМИКА

- Хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг (Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы)



- Росийский омбудсмен по цифровой экономике И.Д. Димитров определяет цифровую экономику как «совокупность общественных отношений, складывающихся при использовании электронных технологий, электронной инфраструктуры и услуг, технологий анализа объемов данных и прогнозирования в целях оптимизации производства, распределения, обмена, потребления и повышения уровня социально-экономического развития государств. [Развитие цифровой экономики в России. Программа до 2035 года.]

- Система экономических, социальных и культурных отношений, основанных на использовании цифровых информационно-коммуникационных технологий (Всемирный банк)

По мнению академика А.Г. Аганбегяна, процесс выхода нашей страны из структурного кризиса 1980-х гг. занял три периода: «трансформационный кризис» 1990–1998 гг. (падение экономики и социальной сферы вдвое), восстановительный подъем 1999–2008 гг. (рост увеличился вдвое), потерянное десятилетие 2009–2017 гг. – стагнация (отсутствие роста)». ВВП в первый период упал на 44% (промышленность – на 52%, сельское хозяйство – на 46%, инвестиции в основной капитал – на 79%). В потерянное десятилетие (2009–2017 гг.) ВВП вырос всего на 4%, инвестиции – на 2%. Доля инвестиций в основной капитал составила всего 17%, тогда как в развитых странах – 20%, а в развивающихся – 30–35%. За 30 лет страна проделала так называемую петлю гистерезиса, одновременно сократив и перераспределив свой экономический потенциал в пользу иностранной экономической системы, внутренних и зарубежных предпринимателей. Отток капитала за этот период составил, по разным оценкам, от 2 до 5 трлн долл.

Послание Президента Российской Федерации В.В. Путина Федеральному Собранию



«...В мире сегодня накапливается громадный технологический потенциал, который позволяет совершить настоящий рывок в повышении качества жизни людей, в модернизации экономики, инфраструктуры и государственного управления. Насколько эффективно мы сможем использовать колоссальные возможности технологической революции, как ответим на ее вызовы, зависит от нас. И в этом смысле ближайшие годы станут решающими для будущего страны...»

... Скорость технологических изменений нарастает стремительно, идет резко вверх. Тот, кто использует эту технологическую волну, вырвется далеко вперед. Тех кто не сможет этого сделать, она – эта волна – просто захлестнет, утопит...»

7

СКВОЗНЫЕ ТЕХНОЛОГИИ ПРОГРАММЫ

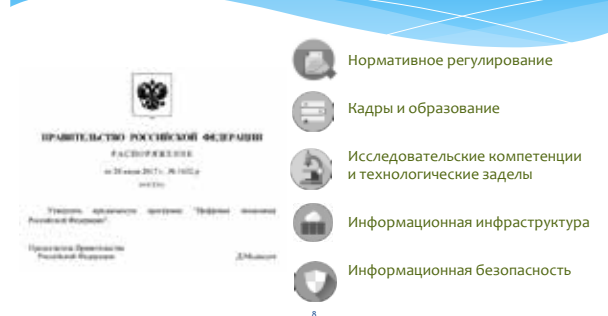
- * большие данные;
- * нейротехнологии и искусственный интеллект;
- * системы распределенного реестра;
- * квантовые технологии;
- * новые производственные технологии;
- * промышленный интернет;
- * компоненты робототехники и сенсорики;
- * технологии беспроводной связи;
- * технологии виртуальной и дополненной реальностей.

9

Официальное понятие «цифровая экономика» дается в Программе «Цифровая экономика Российской Федерации». В ней отражены базовые понятийные компоненты цифровой экономики как системы. В частности, предложена модель цифровой экономики, структура которой включает три уровня: рынки и отрасли экономики; платформы и технологии; базовые условия. «Тесное взаимодействие субъектов, объектов и процессов всех трёх уровней должно повлиять на жизнь граждан и общества в целом». Именно это утверждение Программы свидетельствует о качественном скачке в развитии информационной экономики. Это же говорит нам о необходимости познания и осмысления нового качества, которым по определению обладает цифровая экономика.

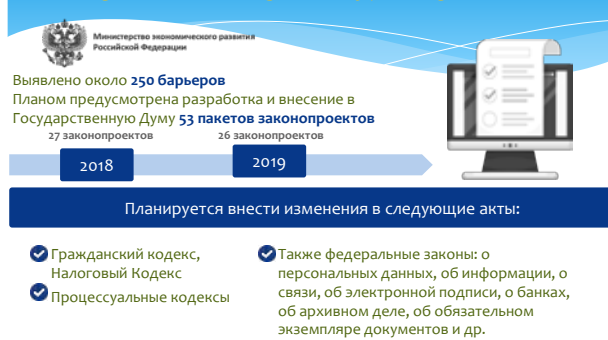
Рейтинг развития цифровой экономики (Digital Evolution Index 2017), подготовленный Школой права и дипломатии им.Флетчера университета Тафта (США): доля цифровой экономики в общем объеме ВВП России сейчас оценивается в 3%, в перспективе эта цифра должна быть двузначной. По данным этого

НАПРАВЛЕНИЯ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ



8

ПЛАН ПО НАПРАВЛЕНИЮ «НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ»



11

исследования и корпорации Mastercard, Россия занимает 39-е место, а по темпам развития – 5-е.

Наиболее вероятные элементы цифровой трансформации включили три блока изменений:

1. Развертывание цифровой инфраструктуры (электронные торговые площадки, широкополосная связь);
2. Обострение цифровых угроз (весь блок киберугроз и процессов, ведущих к деградации естественного интеллекта);
3. Разработка и доступность новых производственных и управленческих технологий, опирающихся на цифровые достижения.

Экосистема цифровой экономики рассматривается через декомпозицию на хабы: финансы и торговля, маркетинг и реклама, медиа и развлечения, образование и кадры, кибербезопасность, государство и общество, инфраструктура и связь. Каждый из хабов исследуется по 10 срезам: аналитика и данные, разработка и дизайн, искусственный интеллект и большие данные, аппаратные сред-

КЛЮЧЕВЫЕ ИНДИКАТОРЫ



- ✓ Подготовка **800 тыс. выпускников системы профессионального образования**, обладающих базовыми компетенциями цифровой экономики;
- ✓ Не менее **120 тыс. выпускников системы высшего образования** будут готовиться по ИТ-специальностям;
- ✓ Доля населения, обладающего цифровыми навыками, к 2021 году составит не менее **40%**

15

ства, регулирование, бизнес-модели, мобильные средства, платформы, интернет вещей, стартапы и инвестиции.

Участники Экосистемы, объединенные в хабы, рассматриваются с точки зрения уровня (их три) вовлеченности в цифровую экономику: 1) специализированный (выработка решений, круглые столы), 2) профессиональный (обмен опытом, мастер-классы), 3) общий (начальный)⁴.

По мнению специалистов, наивысшие риски, генерируемые цифровизацией, будут определяться:

1. Киберугрозами (во всем разнообразии их проявлений: «кибертерроризм, кибершпионаж, кибервойны и киберпреступность» и т.д.);
2. Деградацией естественного интеллекта (широкое распространение клипового мышления, вытесняющего мыслительные практики; рост интеллектуально-психической зависимости от электронных устройств; стирание граней между действительностью и иллюзиями, что облегчает манипулирование массовым сознанием в коммерческих и военно-политических целях);
3. Транснациональным характером конкуренции. Эксперты Римского клуба признают, что есть реальная опасность неконтролируемого развития и неэтичного использования технологий и пока не ясно, как этого избежать. Реальная проблема – научные заделы для технологического роста будут существенно исчерпаны к 2025 г. Именно способ изменения станет главным вопросом

Информационная инфраструктура



Цель к 2024 году:

- широкополосный доступ к сети «Интернет» имеют 97 процентов домашних хозяйств, также 100 процентов лечебно-профилактических учреждений, учреждений сферы образования, другие общественно-значимые объекты инфраструктуры,
- осуществляется широкое коммерческое использование сетей 5G,
- экспортируются услуги по обработке и хранению данных,
- внедрены отечественные методы и программные средства автоматизированной обработки, распознавания и дешифрования пространственных данных, получаемых посредством дистанционного зондирования Земли (съемки из космоса, съемки с воздушных, в том числе беспилотных летательных аппаратов, лазерного сканирования и др.)

17

глобальной конкуренции. Основная опасность новой цифровой экономики заключается в том, что быстрое действие, память и консолидация информационно-вычислительных систем позволяют оцифровать едва ли не все в этом мире. Как следствие, появляется техническая возможность не только целенаправленно и экспериментально управлять социальными процессами путем обработки «больших данных», но и проектировать, помимо любых продуктов потребления, целевые виды массового, группового и индивидуального сознания.

4. Цифровой трансформацией государства и общества. В докладе, опубликованном в декабре 2017 г. и приуроченном к 50-летию юбилею Римского клуба, говорится, что в 80-х годах прошлого века произошло вырождение капитализма: 98% финансовых операций носят ныне спекулятивный характер, в оффшорных зонах скрыто от 21 до 32 трлн долл. Существует переизбыток капитала в фиктивных, но в доходных сферах, в то время как направления, от которых зависит будущее планеты, испытывают дефицит средств. В докладе отмечается, что 10% самых богатых домохозяйств мира являются причиной 45% общего объема выбросов. При этом нагрузка на планету вызывается не только увеличением населения: с начала прошлого века население выросло пятикратно, но экономический оборот – в сорок раз, потребление то-

⁴ Экосистема цифровой экономики России – ПАЕК // Сайт Цифровая экономика [Электронный ресурс]. - Электрон. дан. - Режим доступа: <http://цифроваяэкономика.рф/#about>

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФРАСТРУКТУРЫ ЦИФРОВОЙ ЭКОНОМИКИ



1. Устранение цифрового неравенства, развитие инфраструктуры доступа, сетей 5G
2. Развитие российских центров обработки данных
3. Развитие цифровых платформ работы с данными
4. Развитие инфраструктуры пространственных данных

18

плива – в шестнадцать, вылов рыбы – в тридцать пять. Отсюда делается вывод о необходимости быстрых перемен в системе производства, потребления и восстановления балансов между человеком и природой, кратковременной и долговременной перспективами, скоростью и стабильностью, индивидуальным и коллективным, женщинами и мужчинами, равенством и справедливым вознаграждением, государством и религиозными институтами.

По оценкам Центра макроэкономического анализа и краткосрочного прогнозирования ЦМАКП), развитие цифровизации способно высвободить «при прочих равных условиях» 12,5 млн занятых за период с 2018 по 2030 г.

Размер потенциальной угрозы автоматизации для рынка труда, по данным РАНХиГС, если бы автоматизация наступила одномоментно, то более 49% трудоспособного населения России [или более 42 млн человек (рабочих мест)], могут быть заменены роботами.

Важнейший системный аспект, определяющий структуру цифровой экономики, связан с обеспечением информационной безопасности, так как все процессы экономической, финансово-кредитной деятельности погружаются в цифровую среду информационных технологий. Естественно, при этом значимость, ответственность и эффективность решения проблемы обеспечения информационной безопасности существенно возрастают.

Экономические системы относятся к базовым критическим системам государства. Именно они в первую очередь определяют жизнеспособность государства, его возможности обеспечить благополучие населения и защиту своих интересов в жёстких конку-



24

рентных природных, экономических и политических реалиях.

Угрозы информации являются источниками информационных рисков для объекта цифровизации. Если угроза информации реализуется в качестве соответствующего события, то она порождает информационную угрозу для основной деятельности объекта цифровизации. Эта информационная угроза становится существенной, если она влияет на возникновение риска в области основной деятельности объекта цифровизации. Риски основной деятельности могут иметь различный характер в зависимости от вида деятельности объекта: финансовые, банковские, предпринимательские и т.д. Одним из важнейших факторов, влияющих на управление рисками, является корреляция между информационными рисками и рисками основной деятельности.

С расширением представления об угрозах безопасности при цифровой трансформации экономической деятельности также необходимо более чётко и системно обозначить характеристики современной цифровой среды, отражающие уязвимости в части безопасности. И в этом плане выделяются, прежде всего, три базовых системных решения современной информационно-технологической инфраструктуры: сетевая иерархическая архитектура информационного взаимодействия, открытые компьютерные системы и распределённая обработка информации.

Отмечая новые технологии и возможности работы с вычислительными и информационными ресурсами, выделим традиционное базовое положение парадигмы обеспечения информационной безопасности в автоматизированных системах: эффективная информационная без-

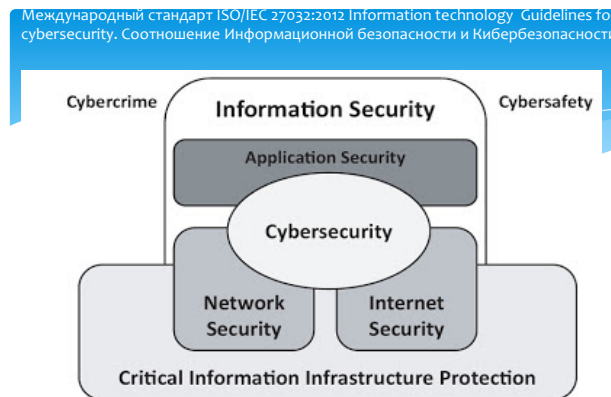


Figure 1 — Relationship between Cybersecurity and other security domains

опасность может быть обеспечена только при штатной конфигурации и в условиях штатного фиксированного состояния используемых программно-технических и телекоммуникационных средств системы. Это состояние соответствует детерминированности процесса.

Однако в современной среде мы имеем дело с процессами обработки информации, которые не являются детерминированными: например, использование сквозных технологий может характеризоваться как предсказуемым, так и случайным, зависящим от ряда динамически меняющихся факторов системы. То есть мы имеем дело со стохастическими процессами. Поэтому подходы к решению проблемы информационной безопасности детерминированного характера хотя и продолжают являться актуальными, но объективно уступают методам и средствам стохастического характера. Это актуально и для безопасности критических объектов информационной инфраструктуры, которые имеют определенную специфику.

При защите КИИ нельзя говорить исключительно об информационной безопасности,

должно быть привлечено понятие функциональной безопасности – части безопасности критического объекта, которая зависит от корректного функционирования связанных с безопасностью других различных систем, в т.ч. управления, безопасности в целом, основанных на других технологиях.

В заключении хотелось бы отметить, что будущее, связанное с построением Общества 5.0, призвано создать новые институты, соответствующие наступающей новой технологической реальности. Но цифровая трансформация порождает серьезные социальные и гуманитарные проблемы, прежде всего занятости, образа жизни в обществе и его культурных ценностей. Поэтому очень опасно ограничиваться узкой трактовкой цифровой трансформации в одних лишь технократических терминах. Цифровой суверенитет становится одним из самых критических вызовов. В этих условиях важно понимание всего спектра восприятия будущего мира с явными приоритетами векторов нравственно-этических ценностей.

СЕМИНАР–КРУГЛЫЙ СТОЛ № 3
НАУЧНО-ТЕХНИЧЕСКИЕ И ЮРИДИЧЕСКИЕ
ПРОБЛЕМЫ УСТАНОВЛЕНИЯ РЕЖИМА
«ЦИФРОВОЙ ГРАНИЦЫ» ГОСУДАРСТВ:
ПУТИ ИХ РЕШЕНИЯ

Ведущие:

Пилюгин П.Л., Институт проблем информационной безопасности МГУ имени
М.В. Ломоносова, Россия

Кевин Лимонье (Kevin Limonier), Университет Париж-8, Франция

П.Л. Пилюгин

Институт проблем информационной безопасности МГУ имени
М.В. Ломоносова, Россия

ТЕОРЕМА О «ЦИФРОВОЙ ГРАНИЦЕ»

1. Введение

Моя задача в этом выступлении обозначить тематику нашего круглого стола и ее взаимосвязь с другими темами конференции. Тема границы уже поднималась, когда говорили о трансграничном информационном обмене или об укреплении мер доверия или суверенитета в цифровом пространстве. Причем многие выступающие вспоминали, что эту проблематику начали обсуждать еще 20 лет назад.

2. Роль и значение зон ответственного поведения государств в киберпространстве.

Мы были свидетелями актуализации этой темы на международной арене. Резолюции Генассамблеи ООН 2014 и 2018 являются основой сегодняшнего обсуждения. А суть проблемы в сложности определить, где начинаются и кончаются эти зоны, и как найти удовлетворяющий всех универсум этого определения.

3. Связь суверенитета и границы

Если суверенитет заключается только в обеспечении соблюдения национального законодательства в киберпространстве, то цифровая граница означает лишь ту часть киберпространства, где государство может контролировать осуществление национального законодательства. Важно, что цифровая граница не имеет цели изолировать (отсоединить) страну от Интернета. Это можно сделать и без нее.

Поэтому другой исходной точкой сегодняшних обсуждений является обеспечение суверенитета государства – где он начинается и где кончается в киберпространстве? Т.е. на какую область распространяется применимость законов государства как в части управления, так в части установления ответственности.

Пересечение этих двух потребностей и приводит введению понятия обсуждаемого на этом круглом столе – к понятию цифровой границы.

4. Понятие цифровой границы

Понятие цифровой границы в киберпространстве обсуждалось ранее неоднократно



и оно является во многом ключевым для определения принципов делимитации и демаркации в цифровом пространстве. Сегодня преобладают две базовых концепции, основанные на понятии цифровой границы как границы виртуального мира и на традиционном понятии границы, привязанной к физической территории государства:

- BR (reality boundaries). Цифровое пространство это другой мир и граница с ним находится в месте перехода
- PB (physical boundaries). Цифровое пространство может быть разграничено исходя из территории государства, на которой находятся те или иные технические средства его образующие

В первом случае (BR) полагается, что «киберпространство – это еще одно место» – это новый виртуальный мир за гранью реальности. В этом новом мире технического и технологического базиса цифрового пространства, киберпространство не регулируется законами отдельных государств. Следовательно, граница реальности это, например, компьютеры или смартфоны, через которые мы «входим» в этот виртуальный мир. Так как, возможно обратное влияние этого виртуального мира на реальный (сознания людей, интернет вещей, информационные системы военных, гуманитарных и других критических объектов), то для защиты от этих угроз, государство



Historical overview of views of the digital border or "20 years in search of a digital border"

It all started with an attempt to identify areas of responsibility of states in cyberspace.

We witnessed the actualization of this topic in the international arena. The resolutions of the UN General Assembly 2014 and 2018 are the basis of today's discussion.

The essence of the problem is in the difficulty to determine where these zones begin and end, and how to find the universe that satisfies all of these definitions.

в реальном мире может только попытаться заблокировать эту границу или регулировать ее пересечение.

Другой подход (РВ) связан с попытками привязать устройства к территориям государств, и установить контроль над электронными сообщениями в месте пересечения физических границ или точнее в точках обмена трафиком. По сути это используемый для защиты межсетевой экран, со всеми его достоинствами и недостатками, но в масштабах государства. И здесь, как мы видим, возникают серьезные проблемы с эффективностью контроля такой границей.

Оба эти подхода понятны и по-своему логичны. При этом в этих двух подходах есть общее – в обоих случаях мы привязываемся к конкретным физическим устройствам. Однако первый по сути отрицает возможность суверенитета в киберпространстве, а второй не удовлетворяют специалистов в области ИТ, так как именно им необходимо решить проблему привязки объектов киберпространства к территориям государств, а распределенность и многоуровневая структура современных сетей делают эту задачу чрезвычайно трудной.

5. Возможности технической реализации «цифровой границы» через средства технического регулирования.

Хотя возможные решения этой проблемы предлагались для построения многоуровневой распределенной границы на основе известных механизмов контроля современных сетей. Однако такое решение требует разработки нормативно технических документов регламентирующих эти решения.

Важно, что такие технические решения требуют согласования и достижения кон-



Basic concepts of building a digital border



BR (reality boundaries).



сенсуса всеми заинтересованными сторонами.

6. «Теорема о Цифровой границе»

Для того, чтобы обсудить важность и своевременность этой тематики я попробую использовать методы используемые в математике:

- Сформулировать утверждение, требующее доказательства (теорему)
- Доказать это утверждение путем строгих (и не очень строгих) рассуждений.

Теорема

«Необходимым и достаточным условием для **бесконфликтного** развития **мирового информационного суверенного пространства** является введение **цифровой границы**, определяющей зоны ответственности государств в киберпространстве.»

Обоснуем необходимость цифровой границы. Предположим, что такой границы нет.

Рассмотрим что будет если мы не придем к соглашению о цифровой границе:

- Ограничение атрибуции инцидента
- Отказ от ответственности
- Ничем неограниченные действия государств при расследовании инцидентов
- Применение законов некоторых стран независимо от места преступления
- Произвольное назначения виновного

.....

Вполне достаточно для обоснования необходимости

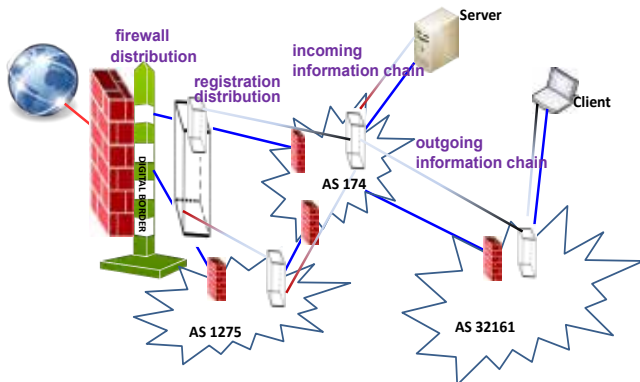
Попробуем обосновать достаточность. Предположим, что такая граница есть.

Что мы будем иметь:

- Определение государств привлекаемых к расследованию инцидента
- Ответственность государства за нарушения безопасности



The digital border is not just a line.



- Предоставление государством всей необходимой информации из своей зоны ответственности.
- Выработка международных соглашений и технических регламентов по поведению и взаимодействию в киберпространстве

.....

Все это нужно, но явно недостаточно для **бесконфликтного** развития **мирового** информационного **суверенного пространства**.

Вместе с тем следует обратить внимание на то что создание цифровой границы создает условия для:

- для развития национального законодательства;
- для гармонизации национальных законодательств разных государств;
- для создания соответствующих норм международного права.

В связи с этим попробует уточнить формулировку теоремы:

Теорема

«**Введение цифровой границы** для определения сферы ответственности государств в киберпространстве необходимо **обеспечение суверенитета государства** в киберпространстве и **создает условия для обеспечения суверенитета и бесконфликтного развития** глобального информационного пространства»»



Agreed technical regulations.



7. Заключение

Не знаю, убедили ли вас эти рассуждения в полном объеме, но как мне кажется, исходя из них можно вывести три следствия:

А) Важность задачи определения цифровой границы.

В) Важность технического регулирования для решения проблем связанных с определением зон ответственности государств в киберпространстве.

С) Проведения исследований в этих важных направлениях.

В заключение хочу отметить связь тематики цифровой границы не только с картографией в киберпространстве и возникающими правовыми коллизиями, но и с проблемами атрибуции деятельности в глобальной сети, с развитием мер доверия. Все эти проблемы будут обсуждаться в различных докладах на конференции. В частности доклад Кевина Лимонье (Университет Париж-8) посвящен проблемам картографии глобальной сети. Также в различных докладах рассматриваются проблемы суверенитета и возникающих правовых коллизий (Чухи Пак – университет Корё, Од Жери – университет Руана), практические примеры развития мер доверия (Джон Мэллори – МТИ и Андрей Ярных – Лаборатория Касперского) и атрибуции инцидентов (Андреас Кюн -институт Восток-запад).

Кевин Лимонье
(Kevin Limonier),
Университет Париж-8

«ЦИФРОВЫЕ ГРАНИЦЫ» И «СУВЕРЕНИТЕТ» С ТОЧКИ ЗРЕНИЯ ТОПОЛОГИИ МАРШРУТИЗАЦИИ

Поговорим о цифровых границах с точки зрения картографии и географии.

Итак. Я хотел бы продолжить то, о чем говорил предыдущий оратор. Моя задача, как картографа, отобразить мир, чтобы он был понятен для людей, для населения, для государственных органов. Эту задачу мы выполняем уже в течение столетий. Вы знаете, что международное право и география очень тесно взаимосвязаны в течение столетий, так как, например, Вестфальский мир, как мы знаем, до сих пор существует в границах, и это результат как юридической, так и картографической революций.

Сегодня некоторые сравнивали ситуацию с ИКТ с той ситуацией, которая была в Европе до Вестфальского мира, то есть во время Тридцатилетней войны, и после этой войны возник новый международный порядок, положивший конец этой войне, и возникла новая парадигма. Некоторые сравнивали эту ситуацию с сегодняшней ситуацией в ИКТ-среде, в киберпространстве.

Я не знаю, находимся ли мы на пороге новой Вестфальской эпохи, но я точно знаю, что мы находимся в центре географической и картографической революции, вызванной Интернетом и способами составления карт и границ.

Что такое граница? Граница в географическом смысле – это географический объект, разделяющий две смежные территориальные системы, и, конечно, одно из понятий, связанных с границей, – это суверенитет. В рамках классического порядка, который я иллюстрирую, понятие «границы» переживало эволюционные изменения. А сейчас мы переживаем новую революцию по некоторым проблемам изменения границы в транснациональных сетях, таких как Интернет, киберпространство и т.д.

Конечно, можно составить классическую карту, подобную этой. Это карта Международного союза электросвязи. Обозначенные



пункты – точки обмена трафиком и основные кабели, распространенные в мире, расположенные на поверхности. Это классическое географическое отображение инфраструктуры должно находиться на физической территории: на суше или на морском дне. Это знакомо международному праву в течение десятилетий и даже столетий. Но Интернет и киберпространство – это не только вопрос инфраструктурных сетей, а также вопрос системы маршрутизации. А система маршрутизации, ее практически невозможно отобразить на поверхности Земли. Для того, чтобы понять такие сети, как показал предыдущий оратор, необходимо думать новыми категориями. По-новому отображать границы, сети и попытаться оценить, где эти границы могли бы проходить, если бы мы договорились о том факте, что нам нужны эти границы в Интернете, в киберпространстве.

Здесь отображение Интернета в виде схемы. Это Интернет в начале года. Каждой точкой обозначена автономная система. Вы знаете, что Интернет – сеть сетей, и каждая подсеть – автономная система с подсистемами, которые составляют фактически ядро функционирования сегодняшнего Интернета. На этой схеме мы видим, что даже если мы абстрагируемся от географической реальности нашей планеты, топографической реальности, топологическая схема все равно обладает политическим смыслом, так как мы отлично видим слева



Figure 4: Ulughbek cartograph, 1580, Europe: Russia. Russia



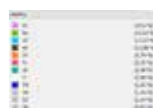
Figure 5: Ulughbek cartograph, 1580, Europe: Russia. Russia



Representation : Modeling Internet as a graph



Internet seen from Central Asia Sovereignty issues



и справа – Россия, Украина, Польша, США, в центре – Европа, Великобритания, Франция. Французская сеть разделена двумя способами по многим причинам. То есть мы видим отображение того, как выглядит Интернет с точки зрения протоколов уровня протоколов маршрутизации.

Но если говорить о границах в сети, мы должны думать о динамике взаимозависимости, то есть учитывать тот факт, что если это сеть сотрудничества, некоторые страны могут оказаться в ситуации зависимости от других стран. Здесь отрезок или элемент автономных систем Центральной Азии. В самом центре ядро сети – это российская автономная система. Понятно – по историческим причинам, а также инфраструктурного и географического характера все кабели практически проходят с севера на юг по этой оси. И мы видим также казахстанские сети, они полностью построены вокруг российской сети. Узбекская сеть тоже связана с Интернетом через российскую, но не через казахстанскую сеть. Это две разные страны. И в виртуальной системе маршрутизации получается, что Узбекистан и Казахстан практически не имеют границ на уровне протокола маршрутизации. А киргизская сеть практически напрямую никоим образом не связана с российской сетью. Они почти независимы от казахстанской системы. Это поднимает массу вопросов относительно суверенитета. Что он означает в Интернете? Что это означает

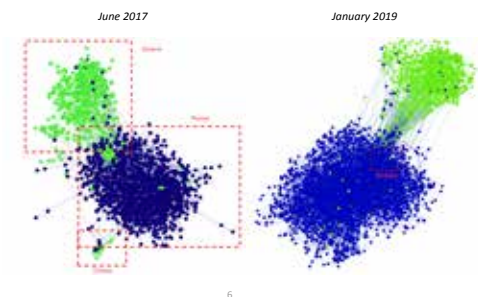
с точки зрения ваших интересов, если вы зависите от сети другой страны? И это поднимает вопрос определения критических нагрузок в сети. И это демонстрирует то, что такая топология сети отражает геополитику, а не географию сетей. Они отличаются.

Крымская сеть. Она создавалась отдельно от российской сети. Были определенные связи с украинской сетью и были системы, которые не были объявлены российскими. Мы видим, что происходит эволюция, если сравнить июнь 2017 г. и январь 2019 г., то здесь крымская будет не полностью интегрирована в российскую, и мы видим, что украинская сеть постепенно отделяется от российской сети. Это еще один способ отобразить типичный пример того, как топология, маршрутизация и геополитика очень тесно взаимосвязаны между собой.

И, наконец, последний пример. Возвращаясь к топографическому отображению Земли. Так выглядит сеть из Саудовской Аравии. Мы видим, что в Саудовской Аравии, если говорить с точки зрения топологии, она практически имеет границу с Италией, так как Италия – крупнейший посредник между сетями Саудовской Аравии и Всемирной паутиной. Что еще раз опосредует реальность географии и топологии. Как мы видим, форма Земли меняется в зависимости от количества автономных систем и взаимосвязей между странами.

Просматривается центральная роль страны, которая географически находится очень

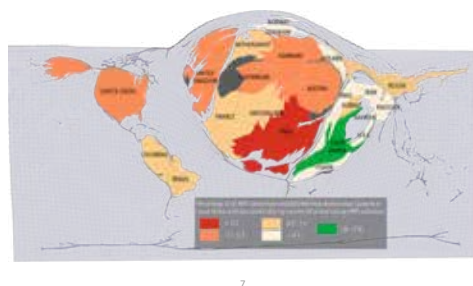
Borderizing in cyberspace (II) : Transferring sovereignty in Crimea through routing



далеко от Саудовской Аравии. Но если посмотреть на эту карту, то становится понятно, что большинство крупных кабелей, соединяющих Саудовскую Аравию с остальной частью мира идет через Красное море, Суэцкий канал, до Сицилии через Италию, а потом уже подсоединяется к французским, германским, нидерландским сетям и т.д.

Главная цель моего доклада – показать на некоторых примерах то, как можно отображать и объяснять понятия «границы», «суверенитета» с точки зрения топологии

Topological versus Geographical: the Reshaping of Space "from" Saudi Arabia



маршрутизации. А также продемонстрировать все возникающие вопросы в этой связи. Так как все автономные системы страны не обязательно находятся на территории этой страны, которой они принадлежат. Поэтому нам, географам, очень трудно увязать эти графические отображения с территориальными аспектами.

Поднимает массу вопросов понятие «границы» как таковой с точки зрения топологического анализа.

Спасибо за внимание!

ВНЕШНЕПОЛИТИЧЕСКИЕ ВЫЗОВЫ И УГРОЗЫ ЦИФРОВОМУ СУВЕРЕНИТЕТУ ГОСУДАРСТВА

Сегодня свобода слова, с одной стороны, объективность и беспристрастность, с другой, фактически принесены в жертву политическому стечению обстоятельств, и глобальная информационная среда ухудшается и трансформируется до политически ангажированных фрагментов в современных условиях геополитической и геоэкономической нестабильности.

Динамичное развитие информационно-коммуникационных технологий и Интернета, формирующего современное глобальное информационное общество, не знает национальных границ и, как следствие, оказывает динамичное воздействие на все сферы общества и государства, включая процессы, происходящие в мировой политике. Сегодня трансформируются каналы распространения информации. Если двадцать-тридцать лет назад СМИ, включая телевидение, активно осваивали интернет-пространство и новости попадали в блогосферу и социальные сети (которые сами в то время еще только формировались), главным образом, из официальных источников. То сейчас мы имеем множество каналов распространения информации, которая может быть рождена и в Твиттере, и в Видео-хостинге, и в Инстаграм, и в других информационных ресурсах, а затем аккумулированная в новых новостных агрегаторах и, пройдя те же социальные сети, может выдаваться как официальная точка зрения. При этом существенно усиливается интернет-влияние и расширяются возможности манипулирования общественным мнением. В настоящее время все большее внимание уделяют возможностям социального инжиниринга с использованием Интернета и управления большими группами людей, в том числе и в политических целях.

Фейки в геополитике. Социальные сети все чаще и чаще используются как эффективная среда для распространения ложной информации, недобросовестной конкурентной борьбы и политической пропаганды. Недавние невинные шутки проложили путь



к технологиям дезинформации, построенной на циничной работе с использованием особенностей и специфики массовой аудитории в Интернете. Фейки стали дежурным инструментом политики и геополитики. Сегодня мировое сообщество приходит к пониманию того, что виртуальная реальность, основанная на фальшивках, начинает критически влиять на фактически происходящие политические процессы.

Если еще несколько лет назад фейки «вбрасывались» отдельными ангажированными личностями или структурами, то сейчас фейки «вбрасываются» основными политическими акторами:

- ведущими политическими партиями, в частности, раскрутка Рашенгейта («предвыборного сговора» Трампа с Кремлем) Демократической партией США;
- международными организациями, например, постановочные съемки «Белыми касками» химических атак в Сирии и др.

Это делается для достижения глобальных геополитических целей в условиях все больше нарастающей разбалансировки международных отношений. Масштаб и «поражающая способность» подобных фейков позволяет их инициаторам достигать сиюминутного значительного тактического выигрыша. Так, «Рашенгейт» на два года фактически дестабили-

Ad Variations									
Putin Sponsors Terrorism Vote to stop him and prevent war Your vote a re-post count! whitehouse.gov									
No.	Ad Copy	ROI ↑	Affiliate	Keyword	Volume	CPC	Position	Days Seen	Last/First Seen
1.	Putin Sponsors Terrorism Vote to stop him and prevent war Your vote a re-post count! whitehouse.gov	0	N/A	telenor russia	110	\$0.10	Last: 7 Avg: 7.0	1/12 days	28 Apr 2014, 12:21 PM 28 Apr 2014, 12:21 PM
2.	Infographic: What \$40 Means to Americans Infographic: What \$40 Means to Americans Across 1h White House whitehouse.gov/infographics/what-40-dollars-means	0	N/A	\$40	0	\$0.05	Last: 6 Avg: 6.0	1/0 days	11 May 2014, 08:42 PM 11 May 2014, 08:42 PM

Рисунок 1. Сообщение на Keyword Spy о приобретении ключевых слов

зировав деятельность администрации Трампа по многим направлениям внешней политики, а фейковые съемки, выполненные «Белыми касками», послужили предлогом для многочисленных военных ударов западных сил по Сирии, что препятствовало правительственным вооруженным силам борьбе с ИГИЛ (организации, запрещенной в России).

Но, с другой стороны, использование подобных грязных методов впоследствии влечет за собой огромный стратегический проигрыш для их инициаторов, когда эти «глобальные фейки» рушатся вследствие установления подлинных фактов. Так было со знаменитой «пробиркой Пауэлла», когда выяснилось, что никакого оружия массового поражения в Ираке не было, а в пробирке, которую Госсекретарь США продемонстрировал на заседании в ООН, находился стиральный порошок.

Так навсегда рухнула репутация «героических» «Белых касок» и их спонсоров, когда сначала сами участники постановочных съемок, а затем и представители западных СМИ все настойчивее стали говорить о злонамеренной фабрикации видеоряда. Работающий в Сирии продюсер Би-би-си в своем Твиттере¹ написал, что видеозапись из госпиталя в сирийской Думе с пострадавшими от якобы химической атаки в апреле 2018 г. является

сфабрикованной. Сотрудник Би-би-си Риам Далати заявил, что после почти шести месяцев расследований он может с уверенностью «доказать, что сцена в больнице в Думе была сфабрикована»².

Считается, что в настоящее время международная политика перестраивается на бизнес-мораль, что ярче всего проявляется в действиях на мировой арене нынешней американской администрации. Современный мир вообще склоняется к прагматике и проведению в жизнь собственных интересов. Но и в жестких условиях бизнес-среды обман и мошенничество, как известно из практики, могло и может навсегда лишить любого, попавшегося на подобных неблагоприятных поступках, участия в дальнейшей сделке да и вообще возможности присутствия в «порядочном обществе».

Приведем пример политического троллинга, который в истории цифровой дипломатии разоблачил один из пользователей мировой паутины, назвав свое сообщение «Путин спонсирует терроризм: клеветническая кампания Белого дома в «Твиттере» и Google»³. Оказалось, что Белый дом купил ключевые слова в Google, чтобы нанести удар по Путину. Используя Keyword Spy (весьма уважаемый и широко используемый ресурс в SEO-индустрии), журналисты проверили сообщение

1 Фейк российских СМИ: «Мировая пресса признала, что химатак в сирийской Думе не было». – URL: <https://theins.ru/antifake/141216> (дата обращения: 08.03.2019).

2 Продюсер Би-би-си в Сирии рассказал о съемках фейка о «химатаке» в Думе. – URL: <https://vz.ru/news/2019/2/13/964119.html> (дата обращения: 08.03.2019).

3 См.: URL: <https://twitter.com/idaltae/status/472819528326332416/photo/1> (дата обращения: 08.07.2018).

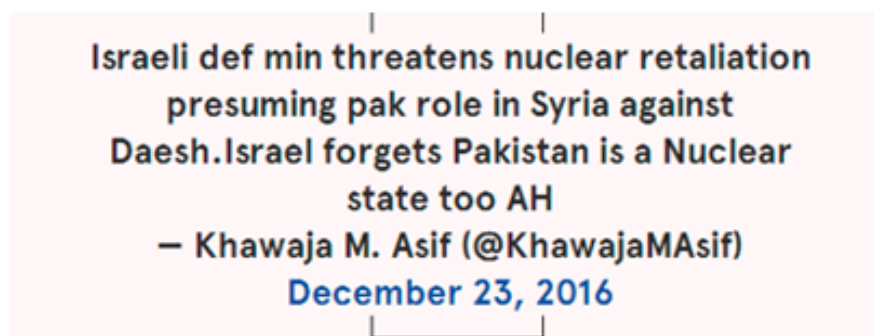


Рисунок 2. Новость, опубликованная на сайте AWD News 23.12.2016 г.



Рисунок 3. Страничка министерства обороны Израиля в Twitter от 24.12.2016 г., в котором заявлено о том, что материал о Пакистане был фейковым

и выяснили, что, действительно, Белый дом купил ключевые слова в Google, используя доменное имя WhiteHouse.gov (см. рис. 1). Также нашлись и другие ключевые слова, которые купил Белый дом.

Как считают журналисты портала «Переводика», проводившие расследование, такой набор слов связан с тем, что Telenor (огромная телекоммуникационная компания, базирующаяся в Норвегии и предоставляющая телекоммуникационные услуги в Восточной Европе) и Russia является, вероятно, популярным критерием поиска Google в России и на Украине. И Белый дом купил ключевые слова в Google, чтобы троллить Путина⁴. Все вышеприведенные примеры показывают, что сетевое сообщество активно реагирует на цифровую дипломатию, а та в свою очередь не оставляет без внимания эту реакцию.

Отличие мистификаций прошлых лет от современных новостных фальшивок состоит в активном влиянии последних на общество и политику. Такие псевдонувоности могут «быть вброшены» в интернет-пространство с помощью специальных сайтов, главное назначение которых – создание и распространение «фальшивок». Например, фейковая информация с сайта AWD News, озаглавленная как – Министр обороны Израиля: «Мы уничтожим Пакистан ядерным ударом, если он отправит войска в Сирию под любым предлогом», чуть было не спровоцировала начало ядерной войны. Соответственно пакистанский министр обороны в ответ через Twitter напомнил, что «Пакистан – тоже ядерная страна» (см. рис. 2 и рис. 3)⁵.

В конце 2016 г. в Бангкоке прото-фейковые новости спровоцировали срабатывание функ-

4 Белый дом скатился до уровня - «Троль обыкновенный» // URL: <http://perevodika.ru/articles/24713.html> (дата обращения: 08.07.2018).

5 Fake news story prompts Pakistan to issue nuclear warning to Israel. // URL: <https://www.theguardian.com/world/2016/dec/26/fake-news-story-prompts-pakistan-to-issue-nuclear-warning-to-israel> (дата обращения: 23.05.2018).

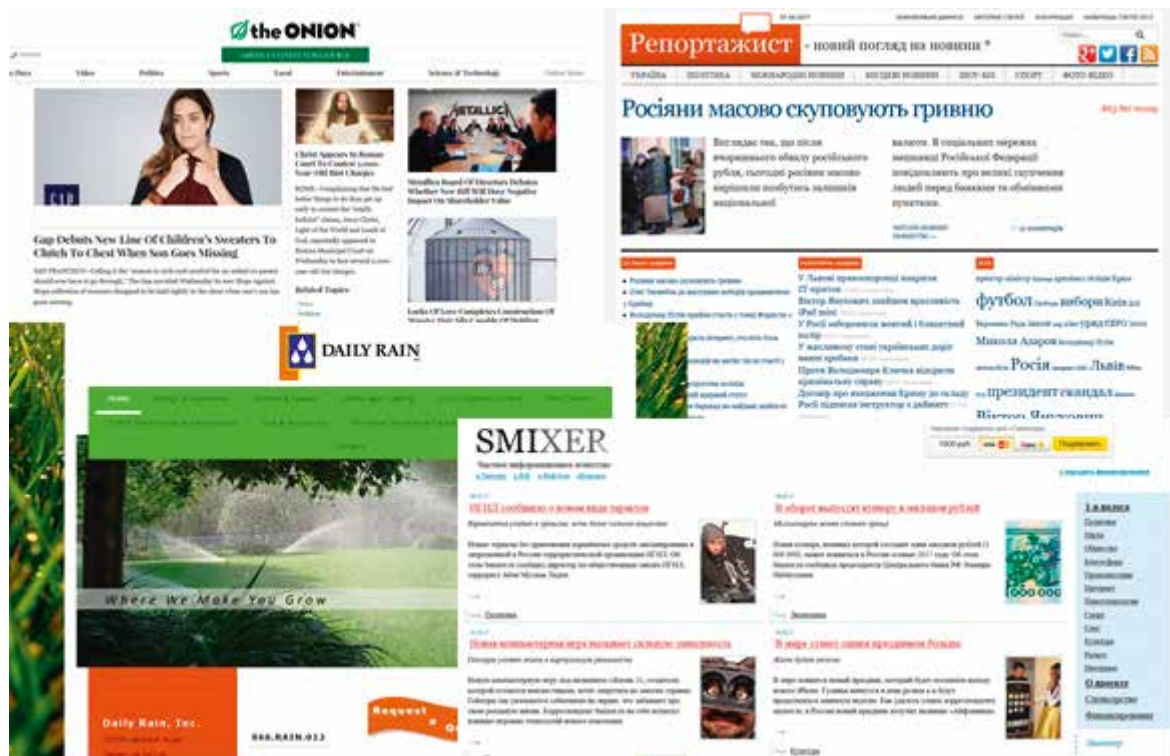


Рисунок 4. Примеры сайтов, распространяющих фейковые новости

ции Facebook под названием Safety Check. Эта функция в продолжение часа осуществляла рассылку сообщений о взрывах в столице Таиланда, прежде чем Facebook смог деактивировать ее и, соответственно, принести извинения пользователям. Позже выяснилось, что Safety Check взял информацию о взрывах с сайтов фейковых новостей, которые использовали сообщения о взрывах, произошедших еще в 2015 году⁶. Как сообщил Facebook, функция Safety Check активируется благодаря автоматическому алгоритму, который отслеживает публикации и новости о происшествиях по всему миру. Приложение Safety Check было запущено социальной сетью в октябре 2014 г. и должно было идентифицировать своих пользователей, которые находились в зоне происшествий, и отправлять уведомление с вопросом о безопасности. В действительности это уже не первый случай, когда Facebook по ошибке активировал эту функцию. Например, после взрыва в Пакистане в марте 2016 г. этот сервис отослал оповещения пользователям в Великобритании и США.

Виртуальная реальность и фейковые аккаунты. Как считает подавляющее большинство американских либералов, фейковые новости, которые распространяются с помощью Facebook и Twitter, в конечном итоге привели к победе Трампа на прошлогодних президентских выборах в США⁷. Эксперты и критики подтверждают, что фальшивые новости распространяются с помощью социальных сетей значительно активнее в отличие от их последующих разоблачений. К тому же, даже представленный ряд примеров показал разнообразие источников формирования ложных новостей. Подобные псевдоновости могут быть вброшены в интернет-пространство специальными сайтами, основным предназначением которых как раз и является создание и распространение «фейков». Примерами таких сайтов могут служить украинские «Репортажист» и UaReview, американские Daily Rain и The Onion или российские Smixer.ru, Fognews, lapsha.ru, hobosti.ru и др. (см. рис.4). С другой стороны, лже-новости появляются и в результате некоторого непрофессионализма жур-

6 Facebook's Safety Check in Bangkok misled users with news from 2015. // URL: <https://www.theverge.com/2016/12/27/14088982/fake-news-safety-check-bangkok-thailand> (дата обращения: 22.05.2018).

7 Цукерберг: Facebook не виноват в том, что Трамп стал президентом. Русская служба BBC. // URL: <http://www.bbc.com/russian/news-37946959> (дата обращения: 29.09.2018).

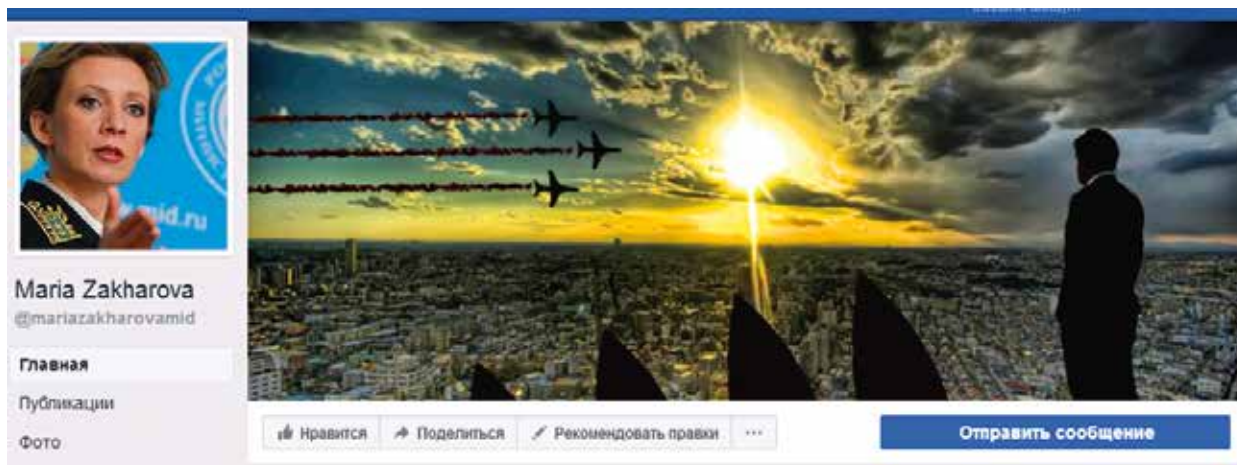


Рисунок 5. Фейковый аккаунт Марии Захаровой в Facebook

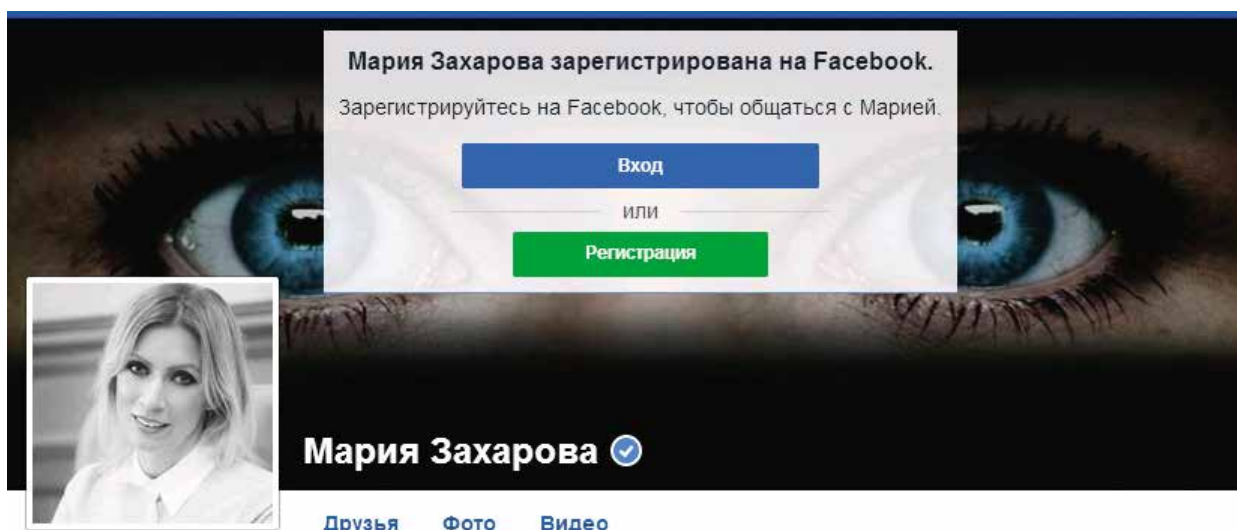


Рисунок 6. Подлинный аккаунт Марии Захаровой в Facebook

налистов, а иногда и намеренной цели распространить ложь. Этот процесс также может происходить после взлома интернет-медиа и умышленного вбрасывания дезинформации.

Здесь мы остановимся на одном из видов фейков в интернет-пространстве, а именно – на фейковых аккаунтах, тем более, что в последнее время эта тема получила довольно динамичное развитие в контексте работы МИД России (см. последние случаи с обнаружением фейковых аккаунтов некоторых наших посольств, а также ведущих работников министерств и ведомств Российской Федерации).

До сих пор в сети Facebook существует фальшивый аккаунт Марии Захаровой (см. рис. 5 и рис.6)⁸, а в Twitter – фальшивый аккаунт Министра иностранных дел России Сергея Викторовича Лаврова.

Фейковые аккаунты как элемент «гибридного воздействия». Вызывает озабоченность тот факт, что информацию, размещенную на фейковых страницах, сознательно или по ошибке используют вполне серьезные СМИ. Так, в прошлом году на сайте телеканала Euronews (англоязычная версия) в своем комментарии на принятие региональным советом итальянской области Венето резолюции, которая призывает отменить санкции против России и признать статус Крыма, в качестве официальной реакции со стороны России приводится скриншот Twitter-«аккаунта С.Лаврова». Хотя известно (см. официальный сайт МИД России), что у С.Лаврова нет аккаунта в социальных сетях. Эта дезинформация, целью которой является раскрутка фальшивого ресурса, пред-

8 См.: URL: <https://www.facebook.com/mariazakharovamid/> (дата обращения: 27.09.2018).

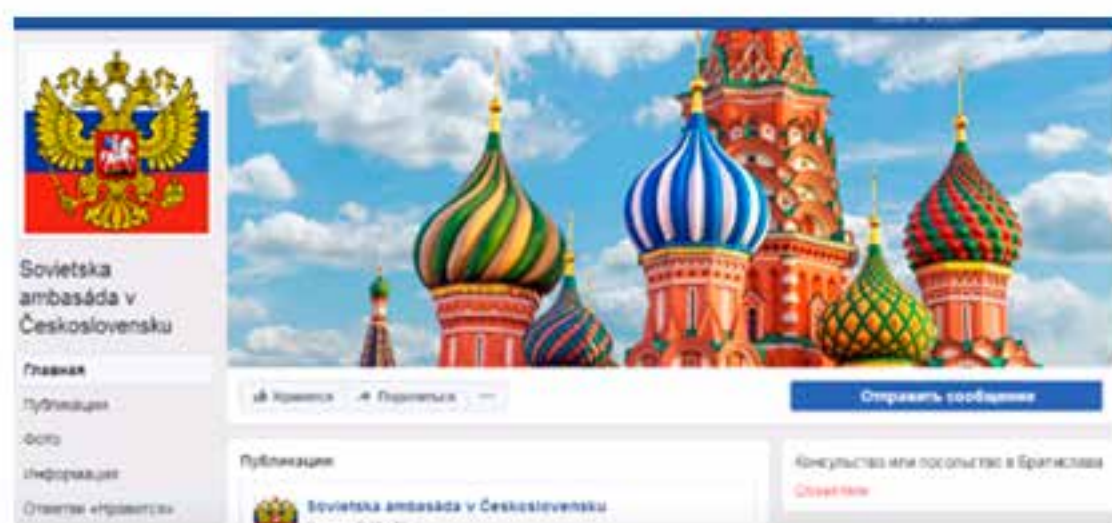
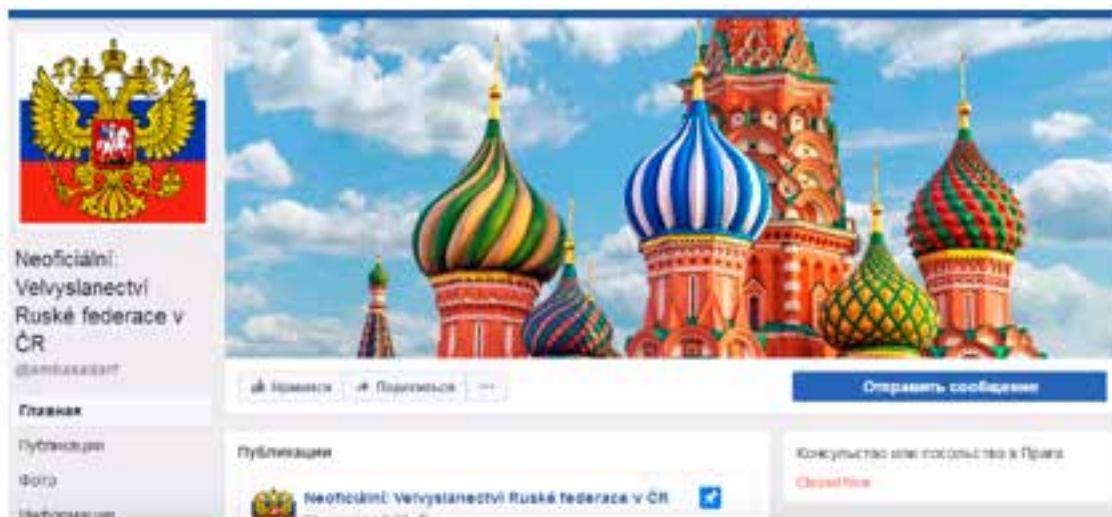


Рисунок 7. Фейковые аккаунты посольств России в Словакии и в Чехии

назначенного для дискредитации внешней политики России, является элементом того самого «гибридного воздействия», предпринимаемого западными элитами в ходе растущего противостояния с нашим государством. Любопытно, что Петр Федоров (Вице-президент наблюдательного совета Euronews), комментируя публикацию текста со ссылкой на фейковый аккаунт Министра иностранных дел России Сергея Лаврова в Twitter, назвал произошедшее проявлением непрофессионализма британской службы Euronews, а ошибка была допущена ими неосознанно, и что все работники Euronews «находятся под серьезным информационным давлением мейнстрима западных средств массовой информации, которые вольно или невольно

принимают участие в информационной войне против России»⁹.

МИД России 19 апреля 2017 г. известил Роскомнадзор о фактах появления в Facebook фальшивых аккаунтов российских дипломатических миссий в Чехии и Словакии, однако администрация Facebook не стала их блокировать. Фейковые «посольства» распространяли недостоверную информацию, а ситуация усугублялась тем, что вместо сотрудничества с реальными дипломатами, администрация Facebook предпочла заблокировать официальные страницы посольств, сохранив поддельные аккаунты. После блокировки страницы посольства Российской Федерации в Словакии, ее поддельный двойник был переименован в «Советское посольство в Чехосло-

⁹ Euronews объяснил публикацию фейкового твита Лаврова бессознательной русофобией. // URL: https://lenta.ru/news/2016/05/24/euronews_lavrov/ (дата обращения: 23.01.2019).

Примеры публикаций, тиражирующих недостоверную информацию о России



Опровержения

Примеры публикаций, тиражирующих недостоверную информацию о России

Опровержения

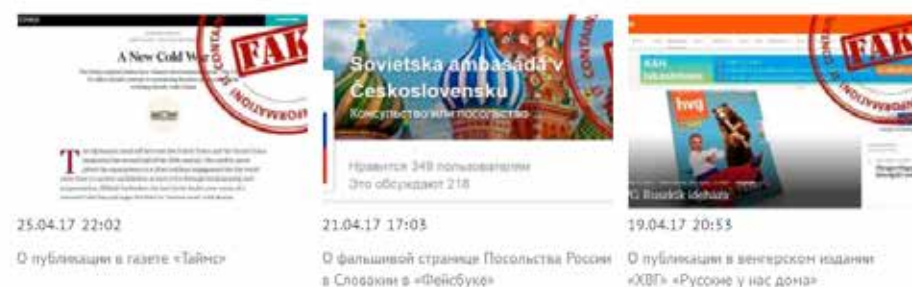


Рисунок 8. Рубрика ФЕЙК на официальном сайте МИД России

вакии»¹⁰, а фейковая страница российской дипмиссии в Чехии переименована в «Нео-официальный ресурс российского посольства в Чехии»¹¹ (см. рис.7).

Как отметила Мария Захарова, авторы этих фейковых аккаунтов размещают новости по самым актуальным и резонансным темам, причем их профессиональный уровень «весьма высок». В качестве «информации к размышлению» можно добавить, что в октябре 2016 г. была создана структура МВД Чехии «по борьбе с пропагандой из России и прочими попытками иностранных государств влиять на мнение жителей страны». Как заявил глава этого ведомства Милан Хованец, в новом подразделении числится 20 человек, оперативно реагирующих на дезинформацию в социальных сетях и обучающих государственных чиновников противодействовать ей. «Мы хотим попасть в каждый смартфон», – сказал Хованец¹². Трудно отделаться от мысли, что вряд ли между созданием в Чехии подразделения по «борьбе с русской пропагандой» и появлением фейковых аккаунтов российских дипломатических представительств в Чехии и Словакии нет никакой связи.

Это не первый случай, когда в создании фейковых аккаунтов и фейковых новостей можно проследить участие государственных структур западных стран. Например, ряд федеральных министерств Германии финансируют создание фейковых аккаунтов, компрометирующих российские государственные органы и российских политических лидеров. Партия Зеленых Германии «прямо участвует» в нападках на руководство России. Так, ведение фейкового аккаунта МИД России осуществляет глава киевского отделения фонда Генриха Белля, который связан с Партией Зеленых. Фонд Генриха Белля (немецкая неправительственная организация, занимающаяся развитием правозащиты, гражданского общества, социальной активности и политическим образованием) существует, прежде всего, на деньги немецких граждан и используется в «нечистоплотных антироссийских целях». Хотя сам фонд и опровергает претензии, заявленные в ее адрес официальным представителем МИД России Марией Захаровой, но в своем расследовании создатели сайта InfoTrader определили, кто ведет популярный фейковый аккаунт «МидРоссии» в Twitter¹³.

10 О фальшивой странице Посольства России в Словакии в «Фейсбуке». // URL: http://www.mid.ru/ nedostovernie-publikacii/-/asset_publisher/nTzOQTrrCFd0/content/id/2735287 (дата обращения: 23.01.2019).

11 О появившейся в социальной сети «Фейсбук» фальшивой странице Посольства России в Чехии. // URL: http://www.mid.ru/ nedostovernie-publikacii/-/asset_publisher/nTzOQTrrCFd0/content/id/2727082 (дата обращения: 23.01.2019).

12 В Чехии создана служба для борьбы с российской пропагандой. // URL: <http://www.svoboda.org/a/ 28066756.html> (дата обращения: 25.01.2019).

13 Фейковый сайт МИД России. // URL: https://twitter.com/fake_midrf (дата обращения: 22.01.2019).

Twitter-подписчики органов власти



Рисунок 9. Анализ качества подписчиков аккаунтов ФОИВ РФ

SMM и SERM – структуры в формировании общественного мнения. Мировые события последнего времени сопровождаются массовыми вбросами в социальные сети ложной информации, ростом активности интернет-троллей и другими явлениями. В этих условиях технологии по воспроизводству фейков могут быть весьма востребованы в социальных сетях. Еще в январе 2015 г. Facebook опубликовал в своем блоге информацию о появлении функционала, позволяющего выделять так называемые «утки» на основе отметок пользователей. Тем не менее, анализ показал, что пользователи просто не способны распознать подобные «утки» и что опровержения ложной информации распространяются гораздо медленнее и хуже, чем сама фальшивка. Фальшивые новости, как правило, активно используют вау-фактор и обладают высокой виральностью¹⁴. Опровержения же более обыденны и вызывают некоторое разочарование, которое не способствует их распространению. Этот эффект «вау-фактора» активно используется в ходе развернувшейся информационной атаки на Россию. В адрес России в зарубежных СМИ публикуется огромное количество обвинений, но не предоставляются ни какие доказательства. В условиях усиливающейся конфронтации российское внешнеполитическое ведомство даже открыло специальную рубрику на своем официальном сайте, которая демонстрирует примеры подобных публикаций, распространяющих ложную информацию о России (см. рис. 8).

Для продвижения в информационном пространстве фейковых новостей широко используются фейковые аккаунты или боты.

Использование оплачиваемых троллей и блогеров в политических или коммерческих целях не афишируется, но и не скрывается. Для некоторых SMM и SERM-агентств (SMM – *Social Media Marketing* и SERM – *Search Engine Reputation Management* – это агентства, деятельность которых направлена на продвижение клиентов в социальных сетях и управление репутацией в Интернете) и других специально созданных структур публикация фейков становится одним из стандартных инструментов продвижения в социальных сетях.

Подобные инструменты используются как для PR, так и для дискредитации политических оппонентов или конкурентов. Помимо коммерческих агентств в некоторых странах существуют квазигосударственные SMM и SERM-структуры. Как правило, они не публичны и репутационных рисков для них не существует. Для дискредитации политических противников они используют любые легитимные SMM-инструменты.

Деградация информационного пространства. «Фейковые аккаунты» или «боты» – одна из самых существенных проблем в социальных сетях, а те социальные сети, которые перестают ее решать, теряют живую аудиторию. В конечном итоге боты нарушают экологию Интернета. Боты распространяют спам, осуществляют кражу личных данных, вмешиваются в обсуждения и внутренние дела стран, влияют на тренды и нарушают цифровой суверенитет государства. Пока Твиттер не предложил способ борьбы с ботами, что может привести к смерти этой социальной сети¹⁵. При этом боты, которые применяются для «раскрутки» и продвиже-

¹⁴ Виральность – способность быстро и широко распространяться.

¹⁵ Представленность федеральных органов исполнительной власти в популярных социальных сетях. Этап II: Twitter. // URL: http://infometer.org/analitika/foiv_twitter_2015 (дата обращения: 27.01.2019).



Рисунок 10. Рейтинг качества аккаунтов ФОИВ РФ

ния политического деятеля, могут при их обнаружении вместо улучшения репутации заказчика ее основательно разрушить¹⁶. К сожалению, подобные примеры можно найти и в отечественной практике. Например, группа «Инфометр» проверила, сколько фейковых аккаунтов среди пользователей, кто подписан на каналы российских органов власти. Был определен характер активности таких подписчиков¹⁷ и составлены рейтинги по количеству активных пользователей, подписанных на аккаунты федеральных органов исполнительной власти в Твиттере. Средний процент фейков среди подписчиков этих аккаунтов в Twitter составил 66,3% от общей аудитории (это – 1 015 922 ботов) (см. рис.9)¹⁸.

Результаты анализа выявили зависимость (коэффициент корреляции 0,77) между количеством подписчиков и процентом фейковых аккаунтов. Например, аудитория подписчиков МИД России (на момент анализа) составляла 520 000 человек (рост аудитории за месяц составил 67 000), а ботов среди них – 77%. Схожая ситуация и у ФАС (162 000 подписчиков и 72,5% фейков), и у Россотрудничества (92 000 и 74,5% фейков) (см. рис. 10). Причин этого может быть несколько, однако основная проблема, по мнению экспертов, – это неправильная формулировка целей продвижения государственных структур в социальных се-

тях. Неверные цели приводят к неверным результатам, а поскольку из-за ботов теряется доверие аудитории, эксперты рекомендуют удалять из подписчиков фейковые аккаунты (например, с помощью инструментов, предоставляемых SMM и SERM-агентствами).

Противодействие со стороны различных стран и международных институтов распространению фейков и цифровой суверенитет государства. Благодаря своим коммуникационным возможностям между пользователями Твиттер и ряд других социальных сетей явились удобной системой для мобилизации различных социальных групп по многочисленным задачам, например, таким, как организация акций протеста. Следует отметить, что по этой причине правительства Китая, Ирана, Северной Кореи и Египта заблокировали работу сервиса Твиттер в этих странах в целях поддержания общественного контроля на их территориях. Поскольку Твиттер использовался, чтобы организовать так называемые «Твиттер-революции» и протестные движения, которые были скоординированы и спланированы через Твиттер, а также для организации и мобилизации протестующих, а также для трансляции в онлайн-режиме новостей на весь мир. Характерными примерами являются Египетская революция в 2011–2013 годах, протесты на выборах в Иране и в

16 Так в ходе избирательной кампании в США кандидат Митт Ромни (Республиканская партия) искусственно наращивал свою популярность в соцсетях и, в частности, за один день (21.07.2012 г.) число его фолловеров увеличилось с 673002 до 789924, что составило 17%-рост. (См.: Теневая экономика Twitter: процветающий бизнес по продаже фолловеров. // URL: <http://www.towave.ru/pub/tenevaya-ekonomika-twitter-protvetayushchii-biznes-po-prodazhe-folloverov.html> (дата обращения: 04.02.2019).

17 Были использованы сервисы FakeFollowers от SocialBakers и Twitteraudit, которые применяют разные алгоритмы определения фейковых аккаунтов.

18 Представленность федеральных органов исполнительной власти в популярных социальных сетях. Этап II: Twitter. // URL: http://infometer.org/analitika/foiv_twitter_2015 (дата обращения: 29.10.2018).

Молдове в 2009 году, протесты студентов-евреев во Франции в 2012 году, акции против коррупции в Турции в 2014 году, акции из-за переворота в Украине в 2013–2014 годах, протесты и призывы к убийству в Венесуэле в 2014 и 2018 годах.

Следующими примерами могут являться действия террористов во всех уголках мира, включая Сирию, Ирак и другие страны, с использованием возможностей Интернета. Если обобщить, то можно выделить восемь различных, хотя и иногда частично совпадающих, способов использования сети Интернет джихадистами. Это – психологическая война, реклама и пропаганда, сбор данных, сбор средств, вербовка и мобилизация, создание сетей, распределение информации, планирование и координация. Причем они используют технологии стратегической коммуникации, а именно синхронизацию «слова», «образа» и «действия». Особенно ярко потенциал и возможности ИГИЛ (организация, запрещенная в России) в Интернете с использованием социальных сетей проявились на фоне сирийского кризиса. Именно эта организация одной из первых создала административные структуры со штатом блогеров для ведения целенаправленной работы в Интернете, привлечения новых рекрутов и распространения идеологии терроризма. ИГИЛ (организация, запрещенная в России) активно внедрялась в существующие социальные сети – Twitter, Facebook, YouTube, Instagram. За несколько лет ИГИЛ (организация, запрещенная в России) обзавелась там большим числом сторонников. С помощью социальных сетей решались сразу несколько задач – презентация организации среди радикально настроенных мусульман, вербовка сторонников и бойцов, сбор средств, запугивание политических и военных противников. Десятки тысяч твитов, фотографий и видео о расправах над противниками, где перемешиваются реальные и постановочные фото, оказывали деморализующее действие на солдат иракской и сирийской армий в ходе военных действий. Таким образом,

социальные сети и, в частности, Твиттер стали «модным инструментом для монтажа и дестабилизации в информационной и психологической войне»¹⁹.

Ситуация с информационным полем, как национальным, так и международным, становится настолько серьезной, что многие страны начинают предпринимать различные, в том числе и законодательные, меры. В Китае с 1 марта 2015 г. было запрещено использование никнеймов с именами лидеров иностранных государств, знаменитостей и других псевдоучетных записей, а также использование информации, причиняющей ущерб государству и обществу. За создание фальшивых профилей в социальных сетях, как сообщает Independent²⁰, пользователи в Великобритании могут быть привлечены к уголовной ответственности. Королевская прокурорская служба Великобритании будет преследовать тех, кто использует социальные сети под вымышленными аккаунтами для того, чтобы нападать на других людей. Новые английские принципы, как ответ на меняющийся характер онлайн-преступности, также позволят привлечь к ответственности людей, которые создают профили в социальных сетях «под именем жертвы с поддельной информацией, которая может повредить их репутации и унижить их»²¹.

Социальные медиа-гиганты Twitter и Facebook уже используют средства, сообщающие настоящее имя владельца профиля. Профиль под именем другого человека, созданный «для введения в заблуждение», теперь может быть навсегда закрыт. Facebook ужесточает политику по отношению к фальшивым аккаунтам, но социальная сеть не раскрывает деталей механизма противодействия этой угрозе. Facebook внес некоторые изменения, которые позволяют выявлять фейковые аккаунты, при этом алгоритмы Facebook анализируют такие паттерны, как наличие повторяющихся постов, увеличение количества отправляемых сообщений и т.п. Введенные изменения позволили найти и заблокировать во Франции более 30 тысяч фейковых аккаунтов.

19 Viloria E. La guerramedia a través de Twitter (12-08-2014). //URL: <http://www.aporrea.org/medios/a196347.html> (дата обращения: 12.12.2018).

20 Making a Facebook account that appears to belong to someone else may be outlawed under the new rules. // URL: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/online-trolls-who-create-accounts-in-other-peoples-names-could-face-criminal-charges-a6909006.html> (дата обращения: 22.11.2018).

21 Там же.

Сейчас следует отметить, что количество поддельных аккаунтов в Facebook небольшое, так в 2016 году их доля составляла лишь 1% от общей аудитории пользователей сети²². Постепенно мировое сообщество приходит к пониманию того, что виртуальная реальность начинает критически влиять на процессы, происходящие в реальной действительности. Медиаресурсы сегодня переживают кризис доверия к ним, спровоцированный, прежде всего, резким падением профессиональных стандартов и массовым распространением «фейковых» новостей²³. Такая дезинформация по степени ущерба сопоставима с вирусной эпидемией, а для борьбы с ней необходима стратегия противодействия на наднациональном уровне.

Интересно отметить, что на этом фоне все настойчивее звучит призыв подвергнуть ревизии само понятие «суверенитет национального государства» в пользу некоторого глобализированного «объединенного суверенитета», обосновывая перспективность наднациональных (а не международных) структур и институтов. В этом плане глобальное информационное общество следует рассматривать как определенный вызов государственному суверенитету, так как отсутствие «информационного суверенитета» в современном мире может привести к потере государственного суверенитета в целом.

С другой стороны, обеспечение государственного суверенитета в информационной

сфере и развитие глобального информационного общества – практически взаимоисключающие задачи. Это обусловлено практической невозможностью определенного государства сохранять контроль над информационной политикой в условиях высокой интеграции в глобальное информационное общество. А контроль над этим обществом (над Интернетом в целом) осуществляется одним государством, что несет в том числе и ряд угроз. Например, если любая хакерская группа поставит под контроль хотя бы один из 13 корневых серверов, обеспечивающих нормальную работу Интернета, то она тем самым сможет контролировать все уровни ниже лежащие по иерархии, включая IP-адресацию и социальные сети.

Таким образом, ключевым моментом в создании эффективных механизмов, направленных на минимизацию угроз, обусловленных развитием информационного общества, является необходимость обеспечения государственного суверенитета в информационной сфере. Однако меры, направленные на обеспечение цифрового государственного суверенитета, в свою очередь, приводят к сдерживанию процессов, направленных на развитие информационного общества. Эти взаимосвязь и взаимозависимость ставят перед международным сообществом непростую задачу – задачу поиска золотой середины или выбора между Сциллой и Харибдой.

22 Facebook усилил борьбу с фейковыми аккаунтами. // URL: <https://www.searchengines.ru/fb-fake-accounts.html> (дата обращения: 22.11.2018).

23 Медиаресурсы переживают кризис доверия: Захарова в ООН о мировых СМИ. // URL: <https://russian.rt.com/world/article/382543-mariya-zaharova-genassambleya-onn> (дата обращения: 24.11.2018).

Д.В. Бабекин

Министерство юстиции
Российской Федерации, начальник
отдела

ПРАВОВЫЕ АСПЕКТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА И УСТАНОВЛЕНИЯ РЕЖИМА «ЦИФРОВОЙ ГРАНИЦЫ» ГОСУДАРСТВ

Уважаемые коллеги!

Рад приветствовать Вас на Тринадцатом международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Позвольте поблагодарить организаторов Форума за предоставленную возможность обсудить столь важную и острую тему: цифровой суверенитет и установление режима «цифровой границы» государства.

Такие общепризнанные принципы международного права, как суверенное равенство и уважение прав, присущих суверенитету, нерушимость границ, территориальная целостность государств, невмешательство во внутренние дела, уважение прав человека и основных свобод, включая свободу мысли, совести, религии и убеждений, составляют международно-правовой базис обеспечения суверенитета государств в традиционном его понимании. При этом упомянутые принципы безусловно применимы в широком смысле и к обеспечению «цифрового суверенитета» государств.

Стоит отметить, что в правовом плане понятие «цифрового суверенитета» в России окончательно не выработано, а его компоненты в полном объеме не определены. Вместе с тем на этом направлении ведется активная и разноплановая работа.

Абсолютно схожая ситуация складывается во многих странах мира, о чем позволяет судить опыт в том числе наших ближайших соседей и, например, Китая.

При этом, как представляется, цифровой суверенитет государства наполняется такими областями как:

- защита от кибератак;
- обеспечение целостности, устойчивости и безопасности инфраструктуры и национального Интернет-сегмента;



- предотвращение несанкционированного доступа к компьютерным данным, хранящимся на территории государства, а также к данным Интернет-пользователей и к устройствам;
- защита персональных данных граждан;
- проблематика применения решений носящих характер экстерриториальной юрисдикции;
- а также в контексте внешнего влияния:
 - нераспространение информации запрещенной законом (терроризм, наркотики, суицид и т.п.);
 - защита детей от информации, причиняющей вред их здоровью и развитию;
 - вопросы контроля распространения недостоверной информации (фейки и информационные вбросы).

На настоящий момент правовое регулирование указанных сфер осуществляется на национальном уровне и надо сказать, что в России многие из приведенных вопросов решены в правовом плане.

В период создания системы ООН и формирования общепризнанных принципов международного права фактически были обозначены и физические границы современных государств.

Однако неопределенная природа современных «цифровых» границ государств ставит перед человечеством серьезные задачи, в том числе в правовом плане.

Вопросы «делимитации» и «демаркации» границ в цифровом пространстве на данном этапе скорее сводятся к формам и объемам ответственности государств, а также применению норм, правил и принципов ответственного поведения государств в ИКТ-среде.

В условиях, когда управление Интернетом не регулируется на универсальном уровне и отсутствуют ключевые общеобязательные нормы, государства вынуждены безвыходным образом принимать технические меры, которые одновременно находят свое отражение и в законотворческом плане.

Это в России, например, способствовало движению соответствующего законопроекта, направленного на противодействие возникновению угроз целостности, устойчивости и безопасности функционирования на территории России сети Интернет и сети связи общего пользования, что в условиях универсальной несогласованности и неопределённости подходов можно охарактеризовать как меры одностороннего порядка, направлен-

ные на защиту собственного цифрового суверенитета.

Пока мы на универсальном уровне и на изначальном этапе не договоримся по каким «субстанциям» и какого характера «красками» мы чертим цифровые границы государств и каков правовой объем цифрового суверенитета, у нас не будет ключевых правил игры, по которым необходимо обеспечивать международную информационную безопасность.

В заключение хотелось бы отметить, что нашему экспертному сообществу необходимо оперативно выработать единые подходы по упомянутым вопросам, которые впоследствии должны найти свое отражение в «понятийных» и конвенционных документах, разрабатываемых и принимаемых на площадке ООН.

Учитывая динамичность и изменчивость ИКТ-среды, делать это необходимо максимально интенсивно, но вдумчиво и с расчетом на перспективу.

Благодарю за внимание!

Од Жери (Aude Gery),

Университет Руана, Франция

ПРАВОВЫЕ ОСНОВЫ ЭКСТЕРРИТОРИАЛЬНОЙ ЮРИСДИКЦИИ И ИХ ВЛИЯНИЕ НА ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ

Я попытаюсь дать ответ на вопрос, может ли государство защищать свою критически важную инфраструктуру, действуя вне правовых норм этого государства. Уже говорилось не раз, что международное право, в частности, Устав ООН, является основой для международных отношений.

А как насчет киберпространства. ГПЭ было признано, что государства осуществляют свою юрисдикцию в информационном пространстве на своей территории. В результате все нормы и принципы, которые вытекают из понятия «суверенитета», также касаются и киберпространства. Но в международном праве есть четыре юрисдикции: территориальная, личная, суверенная юрисдикция и юрисдикция, касающаяся преступлений против человечества и геноцида.

Что касается транснационального характера киберпреступности, здесь есть несколько оснований для юрисдикции государства. Во-первых, государство, против которого осуществляется кибератака, или транзитное государство, или потерпевшее государство могут использовать территориальную юрисдикцию для противодействия. Потерпевшее государство может также давать право на личную юрисдикцию и, наконец, если кибероперации ущемляют интересы государства, то государства смогут воспользоваться суверенной юрисдикцией.

Отсюда вопрос, где место защиты критически важной инфраструктуры в рамках государственной юрисдикции?

Ранее уже упоминалось, что Генеральная ассамблея ООН и ГПЭ рекомендовали применять организационные меры для повышения уровня устойчивости государственных сетей и критических объектов инфраструктуры в глобальном масштабе. Сейчас уже многие страны приняли регулирующие рамочные нормы, которые направлены на защиту критически важных объектов инфраструктуры. Интересно, что ни резолюции ГА ООН, ни отчет ГПЭ не



определяют понятия, что такое «критическая инфраструктура» в глобальном значении. Если читать отчет ГПЭ, мы видим, что каждое государство дает свое определение.

Разнообразие этих определений заставляет нас задумываться о том, что, в первую очередь, критической считается инфраструктура, которая оказывает услуги населению с точки зрения безопасности или функционирования государства в целом, и это охватывает такие отрасли, как банковский сектор, транспорт, энергетику, производство электро- и других видов энергии. И то, что мы таким образом видим преобладание функционального критерия над географическим. Следовательно, если критическая инфраструктура расположена за пределами государственной территории и если одновременно она может быть объектом кибервоздействия, то это пагубно скажется для той страны, на территории которой эта инфраструктура не находится, но при этом эта страна ею пользуется.

Поэтому, действительно, вопрос определения критериев отнесения тех или иных объектов к критической инфраструктуре очень важен.

Для того, чтобы нейтрализовать, выявить или предотвратить атаку или ликвидировать ее последствия, нужно разобраться с тем, как осуществляется эта практика и каким образом государство будет регулировать меры правоприменения этих норм на своей терри-

тории. Это означает, что практика ликвидации последствий уже случившихся актов, а также их предотвращения вызывает трудности с правоприменением.

Какие полномочия имеет государство?

Согласно международному праву существует два вида экстерриториальности. Первый – за пределами своей территории государство реализует свой суверенитет в отношении функций, которые релевантны для этого государства, второй – государство на своей территории решает некоторые вопросы, имеющие экстерриториальное значение для других стран через различные дипломатические, торговые представительства и т.д.

Таким образом, двусторонние соглашения заключаются между государствами для того, чтобы регулировать эти вопросы, но в то же время и существует корпус международного права. Еще в 1928 году установлен принцип, заключающийся в том, что правоприменение строго экстерриториально за исключением тех случаев, когда какие-то правила предполагают исключение. Если что-то не запрещено международным правом, то страна также может реализовывать свой суверенитет экстерриториальным способом. Это зависит от особенностей национального законодательства.

Например, допустим, что правовые нормы государства А указывают, что критическая информационная инфраструктура, расположенная на территории страны В, должна подвергаться контролю со стороны государства А, так как эта инфраструктура имеет для государства А критическое значение. Имеются ли какие-то правовые основания для того, чтобы позволить государству А действовать на территории государства В для контроля над теми сетями, которые имеют значение для страны А?

Как было выше отмечено, для определения критичности функциональный критерий преобладает над географическим. Государство может заявить, что оно имеет право реализовывать меры контроля на территории другого государства. Однако это может войти в противоречие с понятием «суверенитета» для страны В. В этом случае возникнет конфликт юрисдикций в правовом смысле. Более двусмысленной также становится способность государства В действовать на территории

государства А, если, например, сети инфраструктуры доступны для государства А и государство А может осуществлять меры контроля за инфраструктурой, расположенной на территории государства В, то без отправления агентов туда государство А может посчитать, что сети, связанные со своей территорией, могут обращаться с концепцией территориальной юрисдикции и воспрепятствовать мерам контроля со стороны государства В.

В то же время я полагаю, что это не будет справедливым с правовой точки зрения, однако некоторые государства уже применяли эту норму. В связи с этим возникает приобретающая особую актуальность в последние годы проблема поддержания своего суверенитета государством при реализации упомянутой выше резолюции ГА ООН, что также может привести и к нарушению суверенитета другого государства, в отношении которого применяются эти меры контроля.

Если посмотреть на практику отдельных государств, то кибероперации не могут сами по себе быть квалифицированы как нарушение суверенитета. Например, должен быть минимальный порог для того, чтобы кибератака считалась уже нарушением суверенитета. Это позиция США. Второе. Должен учитываться конфиденциальный критерий при определении функций, относящихся к юрисдикции отдельно взятого государства. И, наконец, некоторые государства придерживаются позиции, что кибернападение никогда не будет квалифицироваться в качестве нарушения суверенитета, так как территориальная целостность физически не нарушается, а вмешательство в компьютерные сети не составляет факта во внутренние дела государства. Это мнение Великобритании. Предполагается, что с учетом серьезности воздействия можно использовать только принцип невмешательства в отношении кибератак независимо от степени ущерба, который в результате был нанесен.

Таким образом, с правовой точки зрения, а также для разведывательных целей нет никаких причин для того, чтобы разделять нарушения суверенитета, например, при использовании воздушного транспорта и киберпространства. Это не подпадает под действия международного права, то есть то, что происходит в киберпространстве, якобы, к этому

неприменимо международное право. Это позиция отдельных сторон.

В заключение хотелось бы отметить, что данная ситуация потребует от государства экстерриториальных действий, а также принятия на национальном уровне решения, являются ли действия в киберпространстве вмешательством во внутренние дела другого государства или нет. С учетом этого возможно два решения: повысить уровень международного сотрудничества для предотвращения киберинцидентов, как это рекомендуется от-

четом ГПЭ ООН 2015 года и соответствующей резолюцией ГА ООН, и второе решение – усиление мер доверия для того, чтобы повышать способность государств бороться с киберинцидентами.

В этом контексте недавно в Европе была принята директива, призывающая гармонизировать и привести к единому соответствию требования, связанные с защитой критической инфраструктуры.

Спасибо за внимание!

Чухи Пак (Joohee Park).

Центр киберправа Университета Корё,
Республика Корея

ПРАВОВЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ ПРАВА МЕЖДУНАРОДНОЙ ОТВЕТСТВЕННОСТИ К КИБЕРОПЕРАЦИЯМ

Доброе утро! Меня зовут Чухи Пак, Центр киберправа Корейского университета. Я хочу поблагодарить организаторов за предоставленную возможность выступить на данной конференции.

Во-первых, хотела бы упомянуть комментарий четвертой ГПЭ ООН об ответственности государств по данному вопросу. Как вы хорошо знаете, ГПЭ ООН признала, что существующее международное право распространяется и на киберпространство. Право международной ответственности является отраслью международного права. Таким образом, существующий закон о международной ответственности может применяться к деятельности, которая проводится в киберпространстве или через него.

В частности, четвертая ГПЭ ООН отметила, что государства должны выполнять свои международные обязательства в отношении противоправных деяний, приписываемых им по международному праву. Это означает, что обязательства по международному праву ответственности применяются к использованию государствами ИКТ.

Хотелось бы коротко объяснить принципы, воплощенные в рамках ООН. Согласно проекту статей для противодействия международным противоправным деяниям необходимо выполнять два требования. Во-первых, акт деяния должен быть атрибутирован государством, а во-вторых, акт должен представлять собой нарушение международного обязательства государства.

Часто термин «атрибуция» упоминается, когда мы отслеживаем и определяем местонахождение актора кибероперации. Однако в контексте права международной ответственности концепция атрибуции приписывает деяния некоторым государствам. Если государство совершило международное противоправное деяние, оно несет международную ответственность за него.

Государства, которые несут международную ответственность за свои международные

противоправные деяния, должны выполнять следующие обязательства: прекратить это действие, если оно продолжается, предложить соответствующие заверения и гарантии неповторения его, а также произвести полное возмещение ущерба, причиненного таким деянием.

Однако если ответственное государство не выполняет своего обязательства по прекращению международного противоправного деяния или не дает возмещения ущерба, то потерпевшее государство может рассмотреть вопрос о принятии контрмер против ответственного государства. Контрмеры не предназначены для наказания или возмездия. Это означает, что пострадавшие государства могут прибегать к контрмерам только для того, чтобы побудить другое государство выполнять обязательства по осуществлению контрмер.

Иными словами контрмеры – это меры, принимаемые в ответ на предшествующее международное противоправное деяние.

Имеются ряд условий для принятия контрмер:

1. Государство воздерживается от угрозы силы или ее применения или других императивных норм, которые не считаются законными.
2. Контрмеры должны быть пропорциональными нанесенному ущербу.
3. Прежде, чем предпринимать контрмеры, государство-виновник должно быть призвано к соблюдению своих обязательств по возмещению ущерба.
4. Потерпевшее государство должно также уведомить государство-виновник о принятии контрмер и проведении переговорного процесса.
5. Потерпевшее государство может принять определенные срочные контрмеры для того, чтобы обеспечить соблюдение своих прав.
6. Контрмеры должны быть прекращены, как только будут прекращены противоправные действия.

А теперь о правовых проблемах, связанных с этой проблематикой. Согласно действующему международному праву иногда трудно доказать совершение противоправного деяния и атрибутировать субъект кибероперации, особенно негосударственных субъектов, так как они не относятся к государству. То есть

The Law of International Responsibility in brief

2001 ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)

- **Elements of an internationally wrongful act of a State (Art.2)**

There is an **Internationally wrongful act** of a state when conduct consisting of an action or omission

- (a) is **attributable** to the State under international law; and
- (b) constitutes a **breach of an international obligation** of the State.

- **Responsibility of a State for its internationally wrongful acts (Art.1)**

Every internationally wrongful act of a State entails **the international responsibility** of that State.

5

The Law of International Responsibility in brief

- **Termination of countermeasures (Art.53)**

- Countermeasures shall be terminated as soon as the responsible State has complied with its obligations of **cessation, non-repetition and reparation**.

10

Legal challenges

2. Countermeasures taken with high degree of confidence in attribution do not guarantee the measures taken are lawful.

- Countermeasures taken with **early and wrong attribution** may cause another international wrongful act.
- Countermeasures taken **with high degree of confidence in attribution** can be regarded as punishment, not as countermeasures, because of the object of countermeasures.

12

Legal challenges

3. Proportional countermeasures?

- Countermeasures must be commensurate with **the injury suffered**, taking into account the gravity of the internationally wrongful act and the rights in question. (Art.51, Proportionality)
- "The interconnected and interdependent nature of cyber systems can render it difficult to determine accurately the consequences likely to result from cyber countermeasures" (Tallinn Manual 2.0)

13

не существует конкретных фактических отношений между негосударственным субъектом и государственным. Фактически связи между негосударственным и государственным субъектами существуют лишь в том случае, когда негосударственный субъект действует по указанию государства, или когда он действует под руководством или контролем государства при осуществлении противоправных действий.

Однако иногда очень трудно доказать фактические отношения между негосударственным субъектом и государством.

Контрмеры, применяемые с высокой степенью атрибуции, не гарантируют, что принятые контрмеры являются законными. Если потерпевшее государство принимает контрмеры слишком рано или неправильно осуществляет атрибуцию, то потерпевшее государство совершает международное противоправное деяние, так как контрмеры могут быть неверными. А если потерпевшее государство уверено в атрибуции, то любые меры противодействия могут быть истолкованы как нака-

зание или возмездие, запрещенные по международному праву, так как контрмеры могут приниматься только для того, чтобы побудить государство-виновника к выполнению своих обязательств по прекращению, неповторению и возмещению ущерба. Это означает, что у пострадавших государств нет стимула тщательно осуществлять атрибуцию в отношении какого-либо государства в соответствии с действующим законодательством международной ответственности.

Сложно определить, принимаются ли контрмеры в ответ на злонамеренные кибероперации и насколько они пропорциональны, так как контрмеры должны быть соразмерны с нанесенным ущербом.

Однако взаимосвязанный и взаимозависимый характер киберпространства может затруднить определение того, насколько пропорциональны контрмеры, особенно, если предпринимаются киберконтрмеры, очень трудно предвидеть последствия, которые могут возникнуть в результате таких мер.

Implications

- Recall that the 4th UNGGE noted that the accusations of organizing and implementing wrongful acts brought against States **should be substantiated**.
- Recall that the 4th UNGGE noted in case of ICT incidents, States should consider all relevant information, including the larger context of the event, **the challenges of attribution in the ICT environment** and the nature and the extent of the consequences.
- The traditional legal standards regarding state attribution of conducts carried out by non-state actors (ex. the effective control test) will be sustained?

14

Хочу напомнить, что четвертая ГПЭ ООН отметила, что государственная атрибуция должна быть обоснованной, и в случае инцидентов с ИКТ государствам следует рассмотреть всю соответствующую и релевантную информацию, включая более широкий контекст события, а также степень последствий. В связи с этим нам нужно обдумать и обсудить вопрос: соответствуют ли традиционные правовые нормы государственной атрибуции в отношении деяний, осуществляемых негосударственными субъектами? Стоит ли их применять или необходимо адаптировать для современных условий?

Что касается требований по уведомлению, то государства должны уведомлять ответственное государство о своем намерении

Responsibility zones of States in cyberspace under international law?



22

применять контрмеры прежде, чем предпринимать их. В этой связи хочу напомнить о хакерской атаке на SonyPictures в 2018 году. После того, как ФБР США приписало эту операцию Северной Корее, президент Б. Обама отметил, что США ответит пропорционально и по усмотрению США. Таким образом, несмотря на требование о предварительном уведомлении, потерпевшее государство может предпринять срочные контрмеры для сохранения своих прав.

Учитывая скорость киберопераций и серьезность ущерба, который может быть вызван этими операциями, по-моему мнению, применение срочных контрмер в будущем будет наиболее распространено.

Спасибо за внимание!

А.Г. Цветкова

Национальная Ассоциация
международной информационной
безопасности, старший эксперт НАМИБ

ПРОБЛЕМА МЕЖДУНАРОДНОГО УПРАВЛЕНИЯ ИНТЕРНЕТОМ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В наши дни Интернет стал ведущей информационной и коммуникационной платформой, а также ключевой инфраструктурой, вокруг которой формируется глобальное информационное общество. Все реалии мировой политической жизни транслируются в информационное пространство, а именно в Интернет, молниеносно получая оценки и отклики, формируя глобальный обмен мнениями.

В определенный момент именно этот поток мнений и оценок начинает влиять на общественное сознание, которое в свою очередь может оказывать давление на современную мировую политику.

Именно поэтому Интернет, являясь глобальной ИКТ, требует прозрачного, регламентированного механизма управления.

Согласно определению Рабочей группы ООН по вопросам управления Интернетом, управление Интернетом – это разработка и применение правительствами, частным сектором и гражданским обществом общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета. Как и любое другое управление, управление Интернетом требует четких, фиксированных алгоритмов.

Опираясь на одну из множества классификаций, хотелось бы выделить два ключевых типа управления:

1. Управление, которое сформировано на базе назначенной вертикали (когда руководство назначается / выбирается самими участниками, «подчиненными») – в данном случае можно презюмировать объективное, незаинтересованное управление «сверху».

2. Управление, сформированное по принципу «руководит тот, кто создал». Сразу оговорюсь, что данная схема может быть вполне жизнеспособной, кроме одной ситуации: если при ней «держатель» (создатель) управляемого объекта сам вовлечен в данные отношения



как участник. В таком случае неминуемо происходит утрата объективности, т.к. руководитель не может управлять сам собой.

На сегодня приходится констатировать, что управление Интернетом происходит по второму сценарию, а именно:

Работы по созданию Интернета были инициированы Министерством обороны США и осуществлялись Агенством перспективных разработок (Advanced Research Project Agency, ARPA). Далее, работы велись под эгидой министерства торговли США, и, в 1998 г. последнее заключило Меморандум о взаимопонимании с организацией ICANN. ICANN – «Интернет-корпорация по присвоению имен и номеров» (Internet Corporation for Assigned Names and Numbers) – некоммерческая организация, зарегистрированная в штате Калифорния, в функции которой входят: координация работ по выработке технических параметров интернет-протоколов; административные функции по управлению корнем системы доменных имен (в том числе создание новых доменов верхнего уровня); распределение блоков IP-адресов и некоторые другие.

В результате реформы 2016 г. функции управления адресным пространством сети были переданы дочерней организации ICANN – Public Technical Identifiers (PTI), которая формально независима от Министерства торговли США, но при этом зарегистрирована на территории данного государства и не име-

**ИНТЕРНЕТ - ВЕДУЩАЯ ГЛОБАЛЬНАЯ ИКТ,
ТРЕБУЕТ ПРОЗРАЧНОГО, РЕГЛАМЕНТИРОВАННОГО
МЕХАНИЗМА УПРАВЛЕНИЯ.**

- Управление Интернетом - это разработка и применение правительствами, частным сектором и гражданским обществом общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета (из определения Рабочей группы ООН по вопросам управления Интернетом).

• **ДВА КЛЮЧЕВЫХ ТИПА УПРАВЛЕНИЯ:**

1. Управление на базе *Назначенной Вертикали*
2. Управление по принципу «*руководит тот, кто создал*».

**США – государство, создавшее мировую
сеть Интернет**

**СТРУКТУРЫ, ОРГАНИЗУЮЩИЕ
ФУНКЦИОНИРОВАНИЕ ИНТЕРНЕТА:**

- **МИНИСТЕРСТВО ОБОРОНЫ США**
- **ARPA**
- **Министерство торговли США**
- **ICANN (с 1998 г.)**
- **PTI (с 2016 г.)**

ет права выводить критические инфраструктуры адресного пространства Интернета за пределы штата. Большая часть Совета директоров организации была назначена представителями ICANN, все они – граждане развитых государств. Решения в рамках PTI принимаются на основании многоуровневой модели, по отношению к ICANN PTI выполняет функции субподрядчика; работа PTI может быть прекращена в том случае, если Министерство торговли США расторгнет контрактные отношения с ICANN.

Таким образом, налицо схема, при которой организатор процесса является одновременно его создателем, участником и руководителем. Фактически речь идет о том, что Правительство США имеет эксклюзивный контроль над деятельностью ICANN и, следовательно, PTI, а также может вмешиваться в принимаемые организацией решения.

Возникает потенциальная угроза манипулирования распределением и доступностью Интернет-ресурсов и адресов, в том числе в политических целях.

ICANN контролировала и продолжает косвенно контролировать посредством отношений с PTI экономически и политически значимые технические ресурсы, что объясняет взаимосвязь выполняемых ею функций с целым набором очень важных задач из области внутренней и международной политики.

При всей политической значимости принимаемых решений PTI, как ранее и ICANN, не нашла поддержки у международного сообщества. Дебаты в отношении легитимности ICANN шли с момента ее создания и продолжаются до сих пор, теперь уже в отношении PTI.

Вопрос о легитимности данной модели управления получает отрицательный ответ, Россия не признает эффективность и объективность вышеописанного институционального дизайна управления Интернетом, поскольку он ставит в привилегированное положение тех акторов, которые стояли у истоков сети – а именно, США и тех государств, чьи интересы находятся в одном ключе с внешнеполитической повесткой дня, продвигаемой США.

Яркими прецедентами, подчеркивающими всю «болезненность», а порой и агрессивность текущего режима управления Интернетом, стали такие известные случаи, как атака вируса Wannacry в 2017 году, скандал с компанией Cambridge Analytica в марте 2018 года – они наглядно демонстрируют, что информационные войны и информационное оружие – это реальная международная практика.

Мировое сообщество нуждается в выходе из данного информационного кризиса.

Единственный верный, на наш взгляд, путь преодоления сложившейся ситуации – передача управления Интернетом на межгосударственный уровень, то есть переход на первый сценарий – назначенной вертикали.

Именно наднациональный характер управления может вывести Интернет, а вместе с ним и всю мировую информационно-общественную платформу на качественно новый, объективный путь развития.

Наднациональное или, иначе говоря, межправительственное управление является собой ключевое условие безопасного и стабильного Интернета, ведь, когда политические решения классифицируются как техническое регулирование, – становится возможным их принятие за закрытыми дверями, вне

**ЦЕЛЬ – ОБЕСПЕЧИТЬ НАДНАЦИОНАЛЬНОЕ
УПРАВЛЕНИЕ ИНТЕРНЕТОМ**

- ❖ Межгосударственное управление обеспечивает объективный, безопасный и стабильный Интернет
- ❖ Все критические вопросы управления Интернетом решаются при участии всех заинтересованных сторон
- ❖ Субъект международного управления Интернетом - МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

**Федеральный закон «О безопасном
устойчивом функционировании сети Интернет
в России», 2019 год**

- Стратегия национальной кибербезопасности США допускает отключение иностранных государств от мировой сети при угрозах национальной безопасности, содержит принцип «сохранение мира силой»
- Цель России - обеспечение долгосрочной и устойчивой работы сети Интернет, повышение надежности работы российских Интернет-ресурсов

общественного контроля (как это показали разоблачения Э. Сноудена), а в результате нарушаются не только демократические процедуры, но и разрушается атмосфера доверия, без которой любое сотрудничество невозможно.

Представляется важным, чтобы политические, экономические и технические вопросы, имеющие отношение к управлению Интернетом, решались при участии всех заинтересованных сторон, так как обеспечить информационную безопасность и сохранить связность глобального Интернета без многостороннего сотрудничества ни одно государство не в состоянии.

Именно поэтому Россия, в рамках международных переговоров, настаивает на интернационализации управления Интернетом и передачи управленческих функций Международному союзу электросвязи, где одна страна имеет один голос, и решения принимаются на основании межправительственной модели.

Международный союз электросвязи – одна из старейших ныне существующих международных организаций, деятельность которой не вызывает вопросов в плане объективности принимаемых решений.

Настоящим выражаем надежду, что в обозримом будущем (а именно, в рамках саммита под эгидой ООН по вопросам развития информационного Общества в 2020 г.) произойдет передача функций по контролю над Интернетом «в руки» МСЭ.

Принцип наднационального управления предполагает отсутствие у какого-либо государства монопольных, исключительных прав влиять на общий процесс. Сегодня же США, по сути, являются монополистами в сфере управления Интернетом.

Инициативы России по выводу управления Интернетом на независимый уровень остаются, если не проигнорированными, то, как минимум, в состоянии «паузы». При этом санкционный прессинг со стороны США не снижает обороты.

Актуальная стратегия национальной кибербезопасности США содержит нормы, наделяющие их правом отключения иностранных государств от мировой сети в случае угроз, возникающих в отношении национальной безопасности США. В документе декларируется принцип «сохранения мира силой», а Россия обвиняется в совершении хакерских атак, и не скрывается возможное «наказание».

В связи с этим Россия обязана предпринимать адекватные меры для обеспечения своей национальной безопасности. Такой мерой стало принятие законов об изменении некоторых положений ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ «О связи». В пояснительной записке к данному закону подчеркивается, что главной целью его принятия является обеспечение долгосрочной и устойчивой работы сети Интернет в России, а также повышение надежности работы российских Интернет-ресурсов. Повторюсь, принятие данного закона – исключительно зеркальная мера ответного реагирования, на которую Россия вынуждена пойти ввиду текущего стиля управления Интернетом.

В завершение добавлю, что принятие данного закона не отменяет нацеленности России на продвижение идеи наднационального управления Интернетом в мире.

СЕМИНАР–КРУГЛЫЙ СТОЛ № 4

РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Ведущие:

Григорьев Д.И., Национальная Ассоциация международной информационной безопасности, ГК «Норильский никель», Россия

Джэнис Хэмби, контр-адмирал ВМС США (в отставке), Колледж информационного и киберпространства, Университет национальной обороны США

Д.И. Григорьев,

Национальная Ассоциация
международной информационной
безопасности, ГМК «Норильский никель»,
Россия

ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО И МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПОДХОДЫ КОМПАНИИ «НОРНИКЕЛЬ»

Тема государственно-частного партнерства уже давно присутствует в повестке дня «Норильского никеля», и в плане информационной безопасности мы имеем долгую историю сотрудничества с Министерством внутренних дел Российской Федерации, Министерством иностранных дел Российской Федерации. Мы начинали не с проблем международной информационной безопасности, а с работы с Таможенным комитетом России и с государственными структурами других стран. И основной темой нашего сотрудничества была тема борьбы с контрабандой цветных металлов. Эту тему мы успешно развивали и получили самые лучшие результаты в этом сотрудничестве. И, в частности, на площадках Международной платиновой ассоциации, объединяющей основных производителей металлов платиновой группы.

Ярким примером является наша кооперация с Министерством внутренних дел Южно-Африканской Республики, которая продолжается до сих пор. Посредством этого сотрудничества с госструктурами ЮАР мы вышли на уровень Организации Объединенных Наций по поводу борьбы с финансированием терроризма путем контрабанды цветных металлов. В связи с этим была принята специальная резолюция ООН. Все это показало нам, насколько может быть эффективно, важно и нужно для частного бизнеса развитие линии государственно-частного партнерства. И когда время заставило нас обратить самое серьезное внимание и взоры на тему информационной безопасности наряду со всем, что мы делаем в «Норильском никеле» в плане развития государственно-частного партнерства, на данном направлении это стало для нас приоритетной задачей. Скажем так, что при реализации масштабных проектов, когда мы в принципе не можем обойти эту тему без участия государства, тем более, что результаты работы «Норильского никеля» по линии



цифровизации и ее неотъемлемой части, такой как информационная безопасность (а цифровизация нашей деятельности включена в план пятилетнего развития бизнеса «Норильского никеля»), для нас очень важны.

Например, мы проложили оптоволоконную сеть связи для города Норильска, что позволило не только улучшить работу компании, но и получить нормальный быстрый интернет жителям этого города.

Не могу обойти и тему экологии, потому что развитие цифровизации промышленных циклов «Норильского никеля», а главное, развитие систем информационной безопасности, напрямую влияет на экологическую безопасность в регионах присутствия нашей компании.

Но поскольку мы смотрим не только на какие-то тактические задачи, но и пытаемся развивать эту тему на стратегическом уровне, совершенно неизбежно мы вышли на уровень международной информационной безопасности. И деятельность «Норникеля» как представителя частного бизнеса и тезис, с которым мы пришли в этот переговорный процесс, – это заявление голоса и формирование позиции не только производителей и регулятора, которым является государство, но и потребителей продукции IT и обеспечения информационной безопасности. Это и формирование для нас гармоничной, удобной и правильной среды, благодаря которой мы можем решать

три основные задачи: обеспечивать безопасность, непрерывность и эффективность ведения бизнеса.

В России мы активно развиваем эту линию в области информационной безопасности, в частности, по линии ГосСОПКА сотрудничаем с государственными органами в деле предотвращения и профилактики инцидентов информационной безопасности.

В этом контексте для нас крайне важно сотрудничество и участие в деятельности Национальной Ассоциации международной информационной безопасности (НАМИБ). Бизнес должен быть прагматичным, он не может лишь бороться за идеальный мир, не думая о рисках, о возможных прибылях и о том, зачем мы это делаем.

В силу этого очень важно, что Национальная Ассоциация международной информационной безопасности послужила для нас как бы проводником наших идей, той дискуссионной площадкой, где мы можем продвигать наши позиции.

В настоящее время мы крайне заинтересованы в переговорном процессе по выработке условий для эффективной работы с нашими коллегами в Арктическом регионе. Арктика является для нас важнейшим регионом, имею в виду обеспечение безопасности критической информационной структуры «Норильского никеля» и иных промышленных предприятий в регионе.

Напомню, что на площадке НАМИБ нами была запущена Хартия информационной безопасности критической инфраструктуры промышленности, тезисы которой мы озвучивали в рамках конференции, проводимой под эгидой НАМИБ в ОБСЕ. Этот документ вызывает интерес и обсуждается на различных международных площадках, в частности, на конференции в Киркенесе в Баренцсекретариате весной 2019 года.

Мы надеемся, что наши предложения будут поддержаны НАМИБ, и в ней будет создана соответствующая рабочая группа, в которой мы с огромным удовольствием примем самое активное участие, так как для нас это жизненно важный вопрос. В этих же целях нами был создан неформальный Клуб «Безопасность информации и промышленности», объединяющий руководителей информационной безопасности ведущих российских промышленных компаний. Клуб используется как дискуссионная площадка для обмена между нами лучшими практиками, в том числе по линии организации государственно-частного партнерства. В перспективе мы рассматриваем данный Клуб и как международную площадку при тесном взаимодействии с Национальной Ассоциацией международной информационной безопасности.

Дженис Хэмби,

контр-адмирал ВМС США (в отставке),
Колледж информационного и
киберпространства, Университет
национальной обороны США

ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО ПРИ ЗАЩИТЕ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

Мой доклад сегодня будет кратким. Я очень рада, что мой коллега упомянул важность прагматического подхода к тому, как мы развиваем защиту критически важной инфраструктуры, защиту компаний, способствующих развитию и процветанию наших стран.

На мой взгляд, в этом суть силы государств. Я хочу вернуться к теории вопроса, так как я работала в исследовательских организациях, с точки зрения прагматического подхода.

В 1999–2000 годах я служила в ВМС США и координировала силы по смягчению последствий проблемы «Y2K», так называемой «проблемы 2000». Мне было поручено этим заниматься, так как признавался тот факт, что информационные технологии могли быть источником риска при переходе рубежа нового тысячелетия. Однако эти опасения не оправдались. Но в достижении успеха военные силы США в той ситуации полностью зависели от способностей частных партнеров.

В настоящее время я работаю в Совете одной из оборонных корпораций США и понимаю, что эта проблема существует не только в границах США, а это – проблема, которую мы должны обсуждать вместе с другими странами в силу глобальной взаимозависимости, которая существует между нашими глобаль-



ными корпорациями. Мы должны понимать, какие существуют мировые практики решения подобных вызовов и проблем, чтобы создавать государственно-частные партнерства для работы не только внутри страны, но и для взаимодействия с глобальными партнерами.

Мы живем в то время, когда существует тесная взаимозависимость компаний не только в плане осуществления потоков информации, но и в плане осуществления потоков товаров и услуг. Это система систем. Поэтому очень сложно осуществлять защиту таких систем. Я полагаю, что это вопрос на злобу дня.

Несмотря на то, что тема совершенствования государственно-частного партнерства существует уже давно, в настоящее время она приобретает особую важность по причине того, как мы можем вести свой бизнес, не нарушая кодекса поведения в киберпространстве.

Спасибо за внимание!

Ганс-Вильгельм Дюнна (Hans-Wilhelm Duenn)

Президент Совета по Кибербезопасности
Германии

ТРАНСПАРЕНТНОСТЬ, ДОВЕРИЕ И СОТРУДНИЧЕСТВО: ПРЕДПОСЫЛКИ МЕЖДУНАРОДНОЙ КИБЕРБЕЗОПАСНОСТИ

Друзья! Верно! Мой друг Евгений Касперский сказал, что времени у нас не осталось! Совет по кибербезопасности Германии, который я представляю, – один из лучших примеров государственно-частного партнерства. Если мы имеем проблемы в нашей промышленности, в критически важной инфраструктуре, то нам необходимо все организовывать самим. Германия – одна из ведущих экономик в Европе, где есть Национальное агентство по кибербезопасности со штатом в 700 сотрудников. В Германии 16 федеральных земель, Бавария – лишь одна из них. Так сложилось, что лишь два человека в правоохранительных органах отвечают там за кибербезопасность. Это очень мало.

Национальное агентство по кибербезопасности делает ежегодный доклад. Однако нам необходима информация, поступающая в режиме реального времени. Если обратиться к СIO, например DeutscheBank, или к информации правоохранительных органов о деятельности малого и среднего бизнеса. Мы организуем обмен информацией между частными компаниями. Это очень важный момент нашей деятельности. Для эффективного осуществления этой деятельности мы нуждаемся в технических средствах, кадровом обеспечении, в высококвалифицированных экспертах и специалистах, в знаниях. Это является большой проблемой для Германии. Необходимо создавать новую модель образования, а также оказывать поддержку стартапам.

На встрече в Сколково в прошлом году мы могли наблюдать проблему, когда человек имеет очень хорошие знания в сфере информационной безопасности, а теперь он – бизнесмен и ему необходимо защищать информационные системы своей компании.

В Германии имеется соответствующая нормативная база, в частности, закон о кибербезопасности. При этом организациям необходимо больше инвестировать в кибербезо-



пасность для защиты своих информационных систем, сейчас это очень малая часть от всех расходов организаций, а в некоторых случаях и ее отсутствие.

Каждый месяц в Национальное агентство по кибербезопасности поступают сведения по киберинцидентам от различных компаний Германии, но в 90% случаев на эти обращения не следует никакой реакции. И это не значит, что сотрудники Национального агентства по кибербезопасности плохо работают. Приведу пример. Один сотрудник правоохранительных органов, отвечающий за кибербезопасность земли Берлин, должен реагировать на обращения более 400 средних и малых предприятий. В силу этого мы остро нуждаемся в государственно-частном партнерстве.

Мы имеем собственный хаб атрибуции в Совете по кибербезопасности, мы обеспечиваем обмен информацией между представителями государственной власти и промышленности, а также научными и экспертными кругами. Мы полагаем, что деятельность по обмену подобной информацией является очень важной.

Именно поэтому наша сегодняшняя встреча является в высшей степени актуальной, так как мы имеем возможность общаться и обмениваться опытом представляемых нами стран.

Результатом нашего мероприятия станет подписание Меморандума о взаимопонимании между Советом по кибербезопасности

Германии и Национальной Ассоциацией международной информационной безопасности. Это будет первым шагом. Мы должны продолжать наше общение, обмениваться информа-

цией напрямую. И подписание данного документа положит хорошее начало нашему сотрудничеству!

Большое спасибо!

А.Ю. Ярных,

Лаборатория Касперского, Россия

ОПЫТ ЛАБОРАТОРИИ КАСПЕРСКОГО ПО РАЗВИТИЮ ДОВЕРИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Большое спасибо за предоставленную возможность выступить здесь, в Гармиш-Партенкирхене.

Я хотел бы кратко презентовать центры доверия Лаборатории Касперского, которые мы запустили, развиваем и надеемся, что наша инициатива будет позитивно принята как сообществом, так и государственными структурами. Мы надеемся, что этот опыт, возможно, будет полезен для других компаний с пониманием того, что развитие сетей связи, в том числе 5G, большую часть информации будет переносить в облако и, соответственно, информации будет требоваться больше защиты, и в этой связи используемые программные и аппаратные средства нуждаются в некотором аудите, в некотором центре доверия, в экспертной оценке сообществом.

Лаборатория Касперского пошла по этому пути и, в общем-то, уже достаточно хорошо продвинулась, поэтому я хотел бы показать видео с созданными нашей компанией центрами доверия, в частности, в Цюрихе (Швейцария). Этот город был выбран не случайно. Мы посчитали, что раз Швейцария является центром доверия финансов, эта страна может также стать и центром доверия данных, в том числе персональных. Если схематично объяснять, то у нас, конечно, нет таких вот роботов, которые собирают из отдельных элементов автомобиль, но технологически наш программный продукт не менее сложен, только мы действуем не с помощью роботов. Из исходных кодов собирается готовый программный продукт, подписывается цифровой подписью, которая гарантирует, что данные не изменяются, что они целостны и в них нет никаких дополнительных включений.

Еще одним уникальным свойством нашего центра является то, что верифицируются не только исходные коды, и любой сотрудник и даже конкурент может прийти и посмотреть наши программные коды, конечно, с собой мы вынести ничего не дадим, но поработать там экспертом, посмотреть, в том числе и отдель-



ные элементы возможно, там все это открыто. Центр доверия работает не только с исходным кодом, но и с обновлениями. Самое важное – это то, что программный продукт обновляется много раз за день, и такие обновления тоже могут нести риски, ставить вопросы о доверии к ПО. В наших центрах есть электронный адрес, по которому можно отправить заявку на посещение центра, и все, кто заявился, будут допущены в центр с возможностью изучения исходных кодов и вынесения своих экспертных оценок по поводу открытости и достоверности того, что мы делаем все добросовестно и прозрачно.

По данным на апрель 2019 года, наша инициатива получила определенную поддержку и развитие. Мы получаем запросы на открытие подобных центров в других странах. В частности, в Мадриде (Испания) мы открыли второй центр доверия Лаборатории Касперского. В этом центре точно также предоставляется доступ и возможность аудита данных. В планах нашей компании открытие центров доверия в Америке и в Азии. При этом мы всячески стараемся наш позитивный опыт предложить другим компаниям как некий определенный стандарт повышения доверия к программному обеспечению. В тех случаях, когда встает такой вопрос, обоснованный или необоснованный, относительно того, что программы могут содержать какие-либо недекларируемые возможности, позитивным

ответом на это может быть именно развитие центров доверия. Что касается передачи программного кода на аудит, то в настоящее время наш центр открыт только для Лаборатории Касперского, однако в будущем и другие эксперты смогут проводить аудит, верификацию и подтверждать целостность и отсутствие не-

декларируемых возможностей и других программных средств.

Мы полагаем, что это является позитивным опытом частно-государственного партнерства, который может тиражироваться и другими странами и компаниями.

Спасибо за внимание!

А.С. Марков,

*Группа компаний «НПО «ЭШЕЛОН»,
Россия.*

ВОПРОСЫ ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СРЕДСТВ

Добрый день!

Я хотел бы поблагодарить руководство и программный комитет, организаторов конференции за приглашение выступить здесь.

Я обратил внимание на то, что конференция у нас тринадцатая, а если мы посмотрим на резолюцию, которую мы обсуждали, принятую всем прогрессивным человечеством, за исключением некоторых стран, она тоже насчитывает 13 пунктов. Следует сказать, что мир все время меняется и не исключено, что появятся новые прецеденты об улучшении упомянутых в резолюции норм и правил, и некоторые моменты я хотел бы затронуть в своей презентации.

Я представляю МГТУ им.Баумана и сертификационную лабораторию, имеющую международные проекты и в настоящий момент являющуюся лидирующей лабораторией по рейтингу ФСТЭК в части результативности в выявлении уязвимостей. Сегодня я хотел бы рассказать о таком основном факторе безопасности программного обеспечения в рамках международной информационной безопасности, как наличие уязвимостей. А также о мерах доверия к разработчикам, поставщикам и другим сторонам, которые влияют на повышение уровня безопасности.

В рамках международной безопасности следует отметить, что программная безопасность непосредственно связана с этим вопросом, так как программное обеспечение влияет на техногенные риски. Это – наша объективная реальность. Как отмечают эксперты, инфогенный нарратив привел нас к пятому театру военных действий.

Одновременно отмечу, что термины и факторы в данной области уже сложились. Так, основными факторами любой безопасности являются риски, угрозы, уязвимости и дефекты.

Если мы будем воздействовать на начальные факторы, то мы сможем заблокировать причину возникновения инцидента в области киберпространства. Многие не понимают



сложности программного обеспечения, так как она выходит за рамки когнитивных способностей человечества. Человечество не может проверить даже элементарную функцию достоверными точными методами.

Сегодня уже неоднократно обсуждался рост количества уязвимостей, появление новых вызовов. При этом цена уязвимостей и ошибок очень велика. Например, российская делегация на 2 дня вынуждена была не бриться, потому что был потерян багаж. Аналогичный случай в бльших масштабах произошел в аэропорту Хитроу (Лондон), когда 42000 чемоданов путешествовали без хозяев. Существует много примеров и из других областей, показывающих колоссальный ущерб от киберинцидентов.

При этом амбиции правонарушителей растут, например, в Бангладеш злоумышленники сняли нелегально 1 млрд. долл. В силу отсутствия формальных методов многие компании прибегают к аутсорсингу, и это также является предметом криминального рынка, даркнета и т.д.

Упомянувшийся сегодня уже WannaCry – это тоже результат утечки уязвимостей, что признали сотрудники Microsoft.

Отмечу, что мы живем в сложном мире, и пришло время договариваться в данной области. К сожалению, существующие современные методы – запретительные. В этом плане они, конечно, имеют право на жизнь, но

NPO ECHOLON: INTERNATIONAL PROJECTS



npo-echolon.ru

2

TWO CYBERSECURITY FACTORS IN INTERNATIONAL SECURITY

- Critical modern software complexity causes high level of technogenic risks
- Development of information technology expands remote access threats related to exploitation of software vulnerabilities



npo-echolon.ru

5



GOOGLE SPENT 12 MILLION AS REWARDS FOR BUGS DISCOVERED



HACK PENTAGON

- 5 times was conducted
- 2018 results: Hackers filed over 100 security vulnerability reports for a total payout of \$80,000
- The Hack the Pentagon initiative in totality has disclosed over 3,000 vulnerabilities in government systems.



16

они малоконструктивны, если мы интегрируемся или договариваемся. Это черные списки различного плана, это противоречия между сертификациями и другие проблемы, уже упоминавшиеся сегодня.

Пути решения данной проблемы заключаются в следующем. Необходимо правовое регулирование об извещении, что соответствует п.11 российской революции, а также техническое регулирование, которое непосредственно связано с нормативным регулированием.

В этом плане я хотел бы отметить два аспекта. Первое – это зрелость компании и второе – это действие третьей стороны. При этом зрелость компании непосредственно пропорциональна безопасности программного обеспечения. Разница в компаниях, которые мы проверяли, один к пяти. То есть в компании, в которой отсутствуют процессы, в них уязвимостей в 5–6 раз больше, чем в крупных компаниях, где эти процессы регламентированы, например, в таких как Microsoft или Лаборатория Касперского.

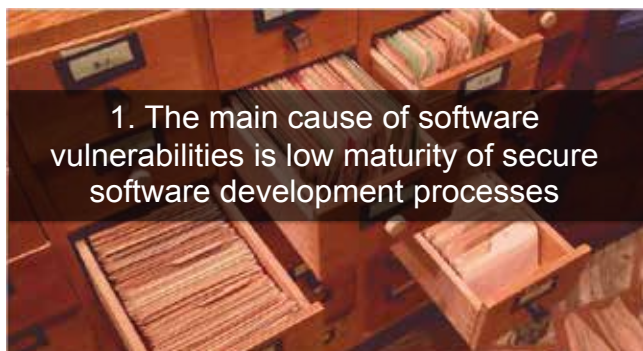
Часто приходится слышать мнение о том, что виноваты не только разработчики, но и вся цепочка поставок. Отмечу, что весь этот процесс можно регламентировать в процессе менеджмента компанией. Имеется много хороших практик, но в настоящее время они все являются частными.

Россия здесь пошла вперед, она выступила с инициативой, в которой все известные

практики и стандарты объединены в рамках стандарта 56939. Этот стандарт гармонизирован с международными стандартами, не противоречит никакому из направлений, затрагивает все этапы разработки, связан с процессом разработки программного обеспечения в плане безопасности. Например, Лаборатория Касперского одна из первых прошла сертификацию по данному стандарту, что значительно повышает доверие к этой компании.

Следующий этап – это действие третье – независимые страны. Международное сообщество в плане информационной безопасности придерживается международных подходов. Здесь существует два подхода: это тестирование черным и белым ящиками.

Тонкость заключается в том, что существует достаточно много методов, при этом все они не являются универсальными, так как виды уязвимостей различаются: это может быть преднамеренная или непреднамеренная ошибка. Поэтому на сегодняшний момент нет универсального метода, и опыт нашей лаборатории показывает, что большинство уязвимостей были найдены только с доступом к исходному коду. То есть если есть исходный код, то существует вероятность, что все уязвимости будут выявлены. Если доступа к исходному коду нет, то доверие к программному обеспечению абстрактно, так как мы не сможем реконструировать событие, мы не сможем понять, что в нем находится.



CLEAN ROOM — AS A FACTOR OF CONFIDENCE IN THE WORK OF THE TESTING



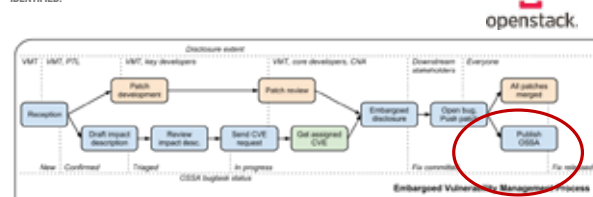
- The source code does not open, it is organized access to the source code in the protected area for the period of inspections
- Access, carry-out of any media and devices, the formation of materials is carried out only when agreed and with full control by the customer's security service
- Certification laboratory cannot provide details on vulnerabilities discovered due to strict NDA with our customers

npo-echelon.ru

42

THE RELATIONSHIP BETWEEN VULNERABILITY DETECTION AND COMPANY MATURITY

IF THE DEVELOPER HAS MATURE DEVELOPMENT PROCESSES, THEN IT ALSO PUBLISHES INFORMATION ON THE VULNERABILITIES IDENTIFIED.



Publishing a Vulnerability Bulletin

source: <https://security.openstack.org/vmt-process.html>

npo-echelon.ru

45

За рубежом существуют различные подходы, такие как коллаборативные профили безопасности, которые применяются США для европейских стран, и новый европейский акт о кибербезопасности, который усиливает эти требования. В силу этого ряд европейских стран, таких как Франция, Германия, Нидерланды, проводят теневую сертификацию, потому что не доверяют коллаборативным профилям защиты.

В прессе идет дискредитация процесса сертификации, часто выступают непрофессионалы, которые обвиняют ее в различных угрозах, хотя это математически невозможно. Существуют подходы, так называемые защищенные комнаты под контролем заказчика, и ни одного инцидента в области сертификации выявлено не было. Ряд компаний эту проблему понимает, например, Microsoft открыла код для 32 стран, а Лаборатория Касперского также заявляла, что готова открыть код.

Отмечу, что все эти направления взаимосвязаны, и те компании, которые имеют у себя сертифицированные проработанные процессы, публикуют эти уязвимости.

Подводя итог, отмечу, что теоретически мы можем усилить п.11 в нашей резолюции в направлении повышения ответственности разработчиков и поставщиков: если мы хотим воспринимать программное обеспечение не как потенциальную угрозу международной безопасности, то мы должны повышать качественный уровень управления международных систем, а также предоставить доступ к исходному коду на этапах испытаний, как это делает, например, Лаборатория Касперского.

Пользуясь случаем, хочу сказать, что я — главный редактор технического журнала «Вопросы кибербезопасности», мы публикуем много аналитических материалов и приглашаем к сотрудничеству авторов.

Спасибо за внимание!

А.И. Тихонов,

Лаборатория Касперского, Россия

ДОВЕРИЕ И БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ

Добрый день!

Я хотел бы затронуть вопросы, связанные с доверием и безопасностью критической информационной инфраструктуры. В рамках этого форума я выступал в Гармиш-Партенкирхене год назад, поэтому позвольте мне довести до вашего сведения, какие изменения произошли за этот год в этой сфере.

Предлагаю сначала определиться с тем, что у нас имеется, далее поговорим о достижениях и взглянем в будущее. Не так давно мы работали на мейнфреймах, потом появились облачные вычисления, а нынешние наши отношения являются более сложными и подвергают нас новым серьезным вызовам, т.к. чем сложнее система, тем больше вызовов и проблем.

Итак. На основе отчета, подготовленного Институтом ИТ, можно выделить десять основных целей относительно безопасности IoT (*Internet of Things, Интернет вещей – ред.*), все они имеют одинаковую природу. Объектом этих рисков является критическая инфраструктура (транспортные, энергетические сети и др.), которая становится все более интеллектуальной, а чем выше интеллектуальность, тем больше подверженность рискам. Что и вызвало появление нового понятия – «эволюция безопасности», т.к. «безопасность» сама по себе становится все более сложным термином и существует не только в сфере ИКТ, а еще и включает такие составляющие, как отказоустойчивость, надежность и др.

Система существует в трех направлениях: физическое пространство, киберпространство и аналоговая среда, которая как бы колеблется между первым и вторым направлениями. При планировании защиты своих объектов критической инфраструктуры необходимо учитывать три вышеупомянутые направления.

Есть исследования, касающиеся того, как злоумышленники используют физические объекты для того, чтобы на них обратить свои действия, и, соответственно, мы должны эти намерения предотвращать.



Второе. Принцип «эволюции доверия», который проявляется сейчас на фоне усложнения систем. Раньше чаще встречались централизованные и иерархичные системы, сейчас мы наблюдаем все больше децентрализованных и горизонтальных систем.

В этой связи стоит отметить блокчейн, являющийся автономной и распределенной системой. Здесь можно выделить такие вызовы, как правовое и технологическое регулирование данной системы.

Многие государства стремятся к защите своих объектов критической информационной инфраструктуры. В частности, Российская Федерация, Китай, Великобритания развиваются в одном и том же направлении в данной сфере, и девизом этого движения является интегрированный комплексный подход к безопасности еще при конструировании таких систем. Имеется в виду, что все законодательства подгоняются под эти требования, и в этой связи законодательства различных стран имеют много общего.

Что касается рекомендаций в сфере международной информационной безопасности, то здесь необходимо отметить, что каналы доверия должны быть встроены в инфраструктуру уже на этапе создания систем, и это может быть применимо, в том числе к таким сценариям, как платежные системы. Должны быть предусмотрены так называемые меры «компьютерной гигиены» не только на уров-

не пользователя, но и масштабируемые на уровень государства, что позволит формировать некие полномочия по управлению сложными системами информации с точки зрения безопасности. Таким образом, в основе всего должно быть доверие к информационной среде.

Для справки. Лаборатория Касперского работает с моделью зрелости информационной безопасности с тем, чтобы адекватно реагировать на основные риски. Мы предполагаем, что в будущем будет происходить формирование передового опыта в авиакосмической отрасли, который в дальнейшем будет расширен и на гражданскую сферу.

Хотелось бы также рассказать о предистории развития этой темы в России. Известная сказка о смерти Кощея, т.е. иголке, находящейся в яйце, яйцо – в утке и т.д. вплоть до сундука, в котором спрятана смерть Кощея, является хорошей иллюстрацией многоуровневой системы безопасности. Это говорит о том, что любая система должна по умолчанию уже иметь защищенность. Здесь также речь идет не только о защите, но и об иммунитете и доверии. И, наконец, о гарантии, т.к. ни доверие, ни безопасность не возможны без гарантий, поэтому чем шире гарантии, тем лучше.

Та же ситуация складывается и в ИКТ-среде, т.е. зона доверия – это защищенная среда, которая предусматривается, например, даже в любом смартфоне, операционной системе, облаке и др. Нам необходимо формировать иерархическую цепочку доверия и сохранять его на каждом уровне.

Было проведено исследование, в ходе которого изучались предпочтения разработчиков приложений по всему миру. В результате было обнаружено, что есть несколько особен-

ностей, которые должны быть присущи безопасности. Однако основная проблема – это разработчики, которые в своей деятельности отдают предпочтения требованиям заказчиков, бюджетам и т.д., при этом безопасность очень часто отходит на задний план.

Учитывая эту проблему, мы имеем более сложное решение, т.к. необходимо при этом защищать инфраструктуру. Это очень сложное явление. И здесь выделяют три уровня: доверие, активная защита от различных угроз, защита от динамических угроз, сгенерированных в том числе искусственным интеллектом. В рамках защиты критической важной инфраструктуры мы учитываем эти три уровня и осуществляем сотрудничество по ним со своими партнерами, в том числе и на международной арене.

Отмечу, что защита и безопасность – это как стены, которые возводятся ради своего собственного комфорта и удобства, а это – нечто иное, это – общий знаменатель. Ведь мы живем в глобальном сообществе, где каждый строит свои собственные технологии, где мы все обмениваемся передовым опытом. И тут встает вопрос доверия: как измерять степень доверия, как управлять доверием и каковы гарантии доверия? Ответ на этот вопрос приведет нас к единому знаменателю.

В мире ведутся дискуссии о будущем инфраструктуры 5G, при этом правильный подход (а, например, Евросоюз движется именно в этом направлении сейчас) представляет собой открытость, применение строгих требований по сертификации, прозрачность, четкое поддержание стандартов. Все эти меры будут являться чрезвычайно важными в деле поддержания стабильности функционирования критически важной инфраструктуры в будущем.

Благодарю за внимание!

А.П. Баранов,

ООО «Сов-технология», Россия

ТЕХНОГЕННАЯ УСТОЙЧИВОСТЬ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПОНЕНТЫ МИРОВОГО ИНТЕРНЕТА

Сегодня я решил сосредоточиться на таком аспекте информационной безопасности, как устойчивость. Конфиденциальность, целостность и доступность – это три аспекта информационной безопасности. Доступность – это как раз устойчивость. Но не в связи с происшествиями или с злонамеренными действиями, а именно в связи с техногенной устойчивостью. Это, на мой взгляд, сейчас самая актуальная проблема. И последний печальный инцидент в этой области с «Боингом» показывает, что те колоссальные, сложные системы, которые мы стали делать, которые стало создавать человечество, они чрезвычайно сложны и не поддаются исследованиям, по крайней мере, одним производителем. С этой целью созданы как бы системы аттестации авиационной техники, но зачастую мы видим, что эти системы пробуксовывают, что вместо участия разных специалистов сертификация производится отдельной фирмой, а зачастую и самой фирмой-производителем, что, конечно, никакой объективности и полноты исследования не обеспечивает.

Проблема заключается в том, что трудоемкость аттестации, трудоемкость получения уверенности зачастую выше, чем трудоемкость самого производства. И, конечно, производители с неохотой выделяют на это средства, т.к. на сертификацию необходимо даже больше средств, чем на разработку продукции.

Я сосредоточусь на Интернете, а именно на его телекоммуникационной платформе. Поскольку наша конференция в большей степени гуманитарная, поэтому я решил, что вначале следует понять, как так произошло, что мы сейчас оказались в такой технико-гуманитарной ситуации: с одной стороны, у нас должны быть юристы, с другой стороны, – техники. Юристы слабо понимают технарей, а технари немного лучше вникают в юридические проблемы, но тоже не до конца. Такая неочевидная связь между технарями и юристами является большой проблемой. Если мы оглянемся на то, как эволюционировал Интернет, то мы



увидим, что сначала он функционировал на имевшихся сетях телефонной связи, а потом, в конце прошлого века, произошла модернизация, и в первое десятилетие 21 века сети фактически использовались для обмена информацией. А что мы имеем сейчас? Сейчас мы имеем телекоммуникационную сеть Интернет, т.н. Интернет-телеком. И здесь сразу появляется множество вопросов, создающих безбрежность возможности исследований. В предыдущем докладе эти различные аспекты были хорошо продемонстрированы.

Я поставил себе цель попытаться вычленив в устойчивости телекома то слабое звено, которое, как мне кажется, является сейчас наиболее актуальным и которое требует объединения усилий и объяснений, в том числе руководителей различных государств, в понимании того, что же является для нас важным и опасным в такой общей среде, как Интернет-телеком.

Возьмем для примера наши сотовые телефоны, с которыми мы здесь все находимся. Ведь если отключится Интернет, то отключатся все сотовые телефоны. А, казалось бы, какая связь между сотовым телефоном и Интернетом. На самом деле, сейчас все провайдеры телефонов сидят на Интернете, и вся передача ведется через цифру. То преобразование, которое раньше осуществлялось, когда цифра преобразовывалась в аналог, аналог передавался по телефонной линии, а потом опять



1. Современные системы крайне сложны, по этому для внедрения важных аспектов используют модели
2. Модели упрощают неактуальные для обсуждаемого аспекта детали, огрубляя их, но выделяя принципиальные для существа проблемы моменты
3. Одну и ту же техническую систему можно описать различными моделями даже в интересах одного и того же обсуждаемого вопроса
4. Разные модели порождают различное понимание принципов заложенных в техническую систему и различную трактовку причин сбоев



1. Представим коммутатор-маршрутизатор в виде двух взаимодействующих блоков: блок управления (БУ) и блок коммутаций (БК)



2. БУ как правило может быть выполнен по технологии ПЭВМ с подключением к ней консоли администратора, т.е. БУ представлена как ПЭВМ с известными и исследуемыми уязвимостями ПО
3. БК состоит из одной или нескольких специализированных микросхем (чипов, ASIC), быстро выполняющих фиксированный набор программ, регламентирующих переключение пакетов с одних входов на другие

преобразовывался в цифру, чтобы по радио пройти, это уже все ушло в прошлый век. Везде идет чистая цифра, т.е. практически везде используется IP-трафик.

Поэтому сбои телекоммуникационной сети будут означать сбои не только сотовой связи, при этом отключение Интернета в разных странах показывало различные убытки. Например, Госдума России недавно озабочилась этой проблемой, и один из депутатов в своем выступлении назвал цифру в 20 млрд. рублей потерь в сутки в случае отключения Интернета в России. Можно себе представить, что может произойти, если большие сегменты начнут отключаться. Обычно, мне на это говорят, что так не бывает, чтобы все отключилось, ну, может быть, какие-то элементы отключатся, но все это не может отключиться.

На самом деле это не совсем так. Проблема заключается в том, что не все понимают или, точнее, все по-разному смотрят на те устройства, которые используются в образовании Интернет-сетей. Кажется, что Интернет состоит из совершенно различных узлов, разных производителей, разных моделей, разных принципов работы, а на самом деле, это совсем не так. На самом деле, можно взглянуть на все устройства, которые образуют Интернет, с единых позиций. Что я и попытался сделать. Очевидно, что здесь можно внедрить единую модель, по крайней мере, для упрощения понимания причин сбоя, для выработки единого подхода, для того, чтобы потом можно было друг с другом нормально разговаривать. Иначе все начинают разговаривать на разных языках, т.к. каждый из нас видит мир в своей модели. И модель российская может отличаться от английской модели, модель английская может отличаться от американской,

модель американская может отличаться от модели итальянской и т.д. И все будут смотреть на вещи по-разному. Я по ходу своей работы в разных учреждениях сталкивался с различными телекоммуникационными устройствами, и каждая фирма-производитель рисовала свое представление устройства, которое является ключевым для Интернета.

На самом деле, модель проста: всего лишь 2 блока, при этом технически это понятно даже любому гуманитарю, т.к. используются лишь блок управления и блок коммутации, и все устройства работают именно по этому принципу. Как бы мы не старались привнести в них дополнительные красоты, всегда устройства можно будет разбить на эти два блока.

Блок управления – это, как правило, блок, выполненный по технологии персонального компьютера: эта операционка и т.д., то есть это обыкновенный компьютер, который задает правила работы системы коммуникации следующего блока. Что очень интересно, что с этим блоком управления за последние 10 лет все научились более-менее работать и его защитили точно так же, как защитили и ПК. Он уже имеет достаточно серьезный уровень надежности. Система связи этого блока шифруется, устойчивость его дублируется, файерволы вставлены, а также внедрены и иные наборы средств, повышающие устойчивость работы системы управления. И на этом очень многие успокаиваются. И зря! А самая неприятная часть лежит как раз в блоке коммутации, потому что блок коммутации состоит из специализированных блоков микросхем. Это чипы, которые специально заточены под выполнение одной и той же команды, одного и того же набора команд, который фиксирован. Именно из таких узлов и состоит весь Интернет!



1. ASIC производится и применяется миллионами экземпляров известных производителей как Marvell, Mellanox, Broadcom и др.
2. Соответственно в миллионах коммутаторов - узлов коммутации используются эти чипы
3. Архитектура программного обеспечения и алгоритмы являются фирменной тайной и не публикуются общедоступно. Это проприетарная информация
4. Тестирование и аттестация ASIC полностью осуществляется самими производителями. Этого недостаточно. Патчи поставить нельзя. Нельзя поменять даже ASIC, как правило он впаян



1. Производители ASIC имеют полное описание алгоритмов и программ, а также инструментов, используемых для разработки и тестирования
2. Для повышения надежности и объективности результатов тестирования предлагается рассмотреть возможность создания международной системы аттестации ASIC, учитывая их межнациональное применение и взаимодействие
3. Международная система аттестации может базироваться на группе признанных, высококвалифицированных экспертов разных стран, изучающих предъявляемые изделия
4. Естественно, упомянутые эксперты должны дать обязательства нераспространения ноу-хау, что повысит заинтересованность производителей в расширении продаж аттестованной техники

Теперь давайте выясним, кто производит эти узлы. Если ПЭВМ могут быть изготовлены разными производителями, то блоки коммутации, которые работают с телекомом, представляют из себя достаточно сложную систему, разработка которой носит ярко выраженный фирменный характер без распространения принципов работы или без исходных программных текстов. Моделирование их, как правило, происходит на кристаллах с программируемой логикой, потом осуществляется отдельное производство, но описание работы этих блоков, как правило, является фирменным секретом. Здесь возникает вопрос, кто сертифицировал этот блок?

Эти блоки стоят во всех узлах телекома, и, к сожалению, допущение ошибки там может привести к тому, что вся система может встать, а эту ошибку могут эксплуатировать в том числе и хакерские организации. Поэтому возникает следующая проблема. Как международным образом сертифицировать эти блоки, которых на самом деле не так много, их производителей всего 4 или 5 в мире? Это примерно как производство крупных гражданских самолетов. Но там есть Международный комитет по сертификации. А блоки коммутации устроены таким образом, что они друг с другом работают по IP-протоколам, а IP-протокол фиксирован вплоть до битов. А стоит нам ошибиться в паре бит в формировании IP-пакета, ваш аппарат будет работать либо очень плохо, либо вообще не будет работать. Поэтому блоки коммутации в этом смысле выверены достаточно неплохо. Но, на самом деле, внутри этих блоков «сидит» довольно большая программа.

Как вы знаете, изготовление безупречно работающего программного обеспечения является абсолютно невыполнимой задачей, всегда основывается на тех или иных допущениях, принципах

и моделях, и каждая фирма использует свои модели, свои принципы. В этом смысле приходится полагаться на ответственность этих фирм. Поэтому возникает вопрос о том, что нужно объединять усилия для осуществления сертификации, для того, чтобы повысить трудоемкость исследования. Специалистов, которые исследуют эти детали во всем мире немного, их нужно объединить, при этом придется пойти на то, что им придется раскрывать ту программу, по которой работает этот блок коммутации, но можно при этом взять с этих людей обязательства о нераспространении этой информации, и таким образом обеспечить устойчивость этой ключевой компоненты, которая бы не была отключаема, и которая бы работала устойчиво в любых условиях.

Самое неприятное в том, что если вы купили устройство, то технологически блок коммутации уже заменить нельзя. Из этого следует, что все блоки коммутации должны быть тестируемы всеми организациями, всеми коллективами, всеми обществами, которые используют Интернет. Так как Интернет стал уже всемирной структурой, все эти блоки стали уже международным достоянием, какими бы производителями они не были изготовлены. И производство этих блоков коммутации рентабельно только тогда, когда оно изготавливает сотни миллионов штук. И поэтому тем более должна быть уверенность в устойчивости, надежности и безопасности этих устройств.

Выработка такого соглашения, организация такой работы в дополнение ко всей очень важной юридической информационной безопасности, как мне кажется, могло бы быть первым и достаточно успешным шагом на пути к международному сотрудничеству в области информационной безопасности.

Спасибо за внимание!

А.Ю. Толстухина,

*Российский совет по международным
делам*

ИНИЦИАТИВЫ БИЗНЕСА ПО ФОРМИРОВАНИЮ ПРАВИЛ И НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Большое спасибо за возможность поучаствовать в этой конференции. Мой доклад не будет носить технического характера, а будет больше гуманитарным, политологическим.

В названии конференции, на которой мы с вами присутствуем, имеются три ключевых элемента, без которых невозможно построить полноценную систему международной информационной безопасности. Это государство, бизнес и гражданское общество. В своем докладе я сосредоточусь на бизнесе, расскажу об инициативах частного сектора в деле создания правил поведения в цифровом пространстве. Эта тема интересна тем, что в то время, когда государства пытаются договориться о создании киберкодекса, бизнес во многом идет на опережение и выдвигает свои инициативы, многие из которых уже сегодня успешно реализуются.

Почему же бизнес заинтересован в становлении правил в киберпространстве? Приведу некоторые причины. Во-первых, частный сектор больше всех страдает от хакерских атак, это факт. Их количество и качество с каждым годом лишь возрастает. Всего, по оценкам Сбербанка России, ущерб для мировой экономики от хакерских атак составляет около 1 трлн долл. в год. А к 2022 году потери могут уже составить 8–10 трлн долл. Вторая причина, почему бизнес заинтересован в правилах, заключается в том, что многие технологические компании по причине недоверия со стороны правительств сталкиваются с серьезными трудностями при продвижении своих бизнес-проектов, своих бизнес-продуктов за рубежом. Так, например, продукты Касперский Лаб запрещены в госструктурах США. Еще один пример. Сегодня в Великобритании, Норвегии, Польше и других странах развернулись дебаты, следует ли допускать компания Huawei к строительству сетей пятого поколения мобильной связи 5G, т.к. эту компанию подозревают в шпионаже в частном и государственном секторах.



В США, Австралии, Новой Зеландии уже введен запрет на использование 5G-оборудования от компании Huawei. С проблемой недоверия сталкиваются и такие компании, как Google, Apple, Microsoft, которые также зачастую обвиняются в незаконной слежке за людьми.

В-третьих, IT-компании вынуждены тратить внушительные суммы на защиту своих клиентов от кибератак. Например, компания Microsoft в этих целях тратит свыше 1 млрд долл. в год.

В условиях отсутствия политического решения, касающегося обеспечения международной информационной безопасности, частные компании, стремясь обезопасить себя и своих клиентов, начали договариваться друг с другом о сотрудничестве и выдвигать свои инициативы. Таким образом, создается параллельный с правительством бизнес-трек по информационной безопасности.

Перечислю наиболее интересные инициативы.

В феврале 2017 г. президент компании Microsoft Б. Смит выступил с инициативой цифровой Женевской конвенции. Конвенция, по задумке Microsoft, должна обязать правительства не предпринимать кибератак на компании частного сектора или критически важную инфраструктуру других государств, а также не использовать хакерских атак для хищения интеллектуальной собственности.

Однако в то время, как цифровая Женевская конвенция пока остается лишь идеей, 34 технологические компании, не дожидаясь решений на правительственном уровне, подписали в апреле 2018 г. технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord). Это важный договор между крупнейшими корпорациями в истории группы компаний, обязующихся защищать клиентов по всему миру от действий киберпреступников. Сегодня участники TechAccord также выступили с инициативой запретить любые соглашения о неразглашении уязвимостей между правительствами и подрядчиками, посредниками и специалистами в области кибербезопасности. Они призывают расширить финансирование для обнаружения уязвимостей и их исследований. В настоящее время к соглашению подключилось около 90 компаний, среди которых Microsoft, Facebook, Cisco, Panasonic, Dell, Hitachi и др.

Еще одна инициатива была представлена компанией Siemens. В 2018 году она выступила с инициативой Хартии доверия (Charter of Trust). Хартию подписали 16 компаний, включая IBM, Airbus, Total и др. Документ призывает компании создать строгие правила и стандарты, чтобы укрепить доверие к ИКТ и способствовать дальнейшему развитию цифровизации.

Не остался в стороне и Facebook. В конце марта 2019 г. Марк Цукерберг предложил правительствам активнее участвовать в регулировании Интернета. В частности, М. Цукерберг выступил за разработку новых норм в ряде областей, касающихся Интернета и социальных сетей, в числе которых защита личных данных пользователей, пресечение попыток влияния на выборы и распространение нежелательной информации, а также решение проблемы переносимости данных.

Есть инициативы, которые исходят от российского частного сектора. На конференции о них уже говорили. Это одна из инициатив от компании «Норникель», которая с 2017 года продвигает на международной арене Хартию информационной безопасности критических объектов промышленности. Сбербанк выступил с инициативой проведения крупнейшего в мире международного конгресса по кибербезопасности.

Резюмируя, хочу отметить, что, на мой взгляд, сегодня инициативы частного сектора прекрасно могут быть синхронизированы с теми инициативами, которые продвигают государства на площадке ООН. Ведь правительства в этой сфере по большому счету преследуют те же цели, что и бизнес. Использование ИКТ в мирных целях, укрепление мер доверия, предоставление информации об уязвимостях и др. – все это важно, как для бизнеса, так и для большинства правительств. К счастью, глобальная дискуссия в рамках ООН по международной информационной безопасности после продолжительной паузы почти в один год вновь возобновлена. Теперь в ней будут принимать участие представители частного сектора. В российской резолюции отмечено, что будущая Рабочая группа открытого состава предусматривает возможность проведения межсессионных консультационных встреч с бизнесом, неправительственными организациями и научным сообществом для обмена взглядами по вопросам, входящим в мандат группы. Кстати, уже на ноябрь 2019 г. запланирована первая межсессионная встреча с представителями глобального бизнеса.

В заключении, хотелось бы отметить несколько рекомендаций.

1. Проблема информационной безопасности имеет динамичный характер, поэтому решать ее нужно только при тесном взаимодействии правительств и технологических компаний, т.к. именно последние идут в ногу с развитием технологий и являются главными драйверами цифровой экономики.
2. Правительства должны внимательно следить за инициативами негосударственных акторов, крупных корпораций и небольших предприятий и включать наиболее удачные нормы в повестку дискуссий на международном уровне.
3. Принятые и утвержденные нормы должны иметь юридическую силу, а не иметь рекомендательный характер, т.к. только так можно обеспечить порядок в киберсреде.

Спасибо за внимание!

Чарльз Барри (Charles Barry),

независимый эксперт, США

МЕЖДУНАРОДНЫЕ ГОСУДАРСТВЕННО- ЧАСТНЫЕ ПАРТНЕРСТВА: ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ

Благодарю организаторов конференции за то, что в такую замечательную погоду мы работаем здесь и пытаемся находить решения серьезнейших проблем современности.

Я думаю, что это не случайно и на это есть причины.

Я хотел бы продолжить мысль, которая прозвучала из уст одного из докладчиков, относительно доверия и важности телекоммуникаций ИКТ-сферы в целом.

И еще необходимо обратить пристальное внимание на расширение сотрудничества между частными компаниями, крупными игроками в сфере ИКТ для продвижения их общих целей на государственном уровне.

Итак. В настоящее время государственно-частное партнерство – очень актуальная тема. Здесь речь идет о сотрудничестве между государственными структурами и частными организациями, так как во многих странах именно провайдеры являются частными структурами. Госдепартамент США и Министерство финансов США сотрудничают с частными структурами, которые обеспечивают функционирование критической инфраструктуры, например в финансовой сфере.

Я также хотел бы обратить внимание на различные отрасли с точки зрения опыта США. Я с удовольствием выслушаю также мнения коллег относительно того, что они считают наиболее важным в данной проблематике, так как в каждой стране есть свои подходы к обеспечению безопасности критически важной инфраструктуры. Но, в любом случае, обеспечение защищенности критически важной инфраструктуры требует партнерства между государством и частными компаниями. Частные организации, как правило, владеют, управляют и используют основную критическую инфраструктуру. И именно они будут в большей степени подпадать под угрозы, и именно они будут страдать не только от сбоев в сфере ИКТ, но и от различных чрезвычайных ситуаций, таких как природогенные и техногенные



катастрофы. На наш взгляд, именно частный сектор является объектом всех этих рисков, но при этом он ориентирован на рынок, нацелен на получение прибыли, конкурирует друг с другом. При этом существует такое понятие, как «собственная информация», которая тоже не должна стать объектом кражи.

Организации, которые отвечают за безопасность на государственном уровне, также заинтересованы в создании благоприятных условий для экономического развития. Государство оказывает услуги населению, в том числе в цифровой среде, и поэтому государство тоже может оказаться под угрозой в связи с различными рисками, и поэтому само государство также заинтересовано, чтобы эта инфраструктура, которая создается в том числе и частными организациями и которая используется государством для оказания своих услуг, включая сферу безопасности, была защищена.

Говоря об обмене информацией, государства и частные организации объединяют усилия и выполняют требования, предъявляемые со стороны государства относительно недопущения срывов или катастроф. Два года назад у нас были перебои с электричеством, и это сразу вызвало падение доверия к поставщикам этих услуг. Следовательно, необходимо разрабатывать методы отказоустойчивости.

Именно поэтому, деятельность государственно-частных партнерств должна строить-

Public Private Partnerships (PPPs)

PPPs are organized steady collaborations between a public sector agency and many private sector service providers.

One area where PPPs have been deemed essential: Critical Information Infrastructure Protection



2

Essential Elements for PPP Success

- Robust, broad-based, two-way information sharing among participants
- Trust – built-up, protected and sustained over time through value-added experience



5

ся на потоке информации, носящем двусторонний характер, имеется в виду доверительный характер обмена информацией.

Второй вопрос: как делиться информацией компаниям, которые конкурируют между собой? В данном случае, естественно, компании не заинтересованы делиться информацией о том, что у них возникали какие-либо проблемы, либо был какой-то сбой, или, наоборот, не спешат предупреждать, что кому-либо грозит какой-то сбой и т.д. Поэтому, как можно обеспечивать устойчивость при наличии подобного конфликта интересов?

В этой связи я хотел бы упомянуть об организации, созданной в США, которая называется Национальный комплексный центр кибербезопасности и связи и подчиняется Министерству внутренней безопасности США.

Напомню, что среди критической инфраструктуры мы выделяем 16 отраслей, том числе как наиболее критичные – энергетическую отрасль, телекоммуникации, реагирование на чрезвычайные ситуации. За функционирование каждой отрасли отвечает то или иное министерство или ведомство на государственном уровне.

Я полагаю, что телекоммуникации находятся в центре данной проблемы. Но еще один важный момент – это трансграничность всех этих отраслей.

По всем 16 отраслям в США созданы аналитические центры по обмену информацией, работающие круглосуточно и связанные с Национальным центром кибербезопасности США. Деятельность данных центров включает в себя отслеживание угроз, выработку методик ликвидации последствий чрезвычайных ситуаций и др. Эта конструкция обеспечивает взаимодействие между частными оператора-

ми, являющимися владельцами элементов инфраструктуры, и государственными органами, которые их курируют. Эти центры обеспечивают поддержку собственникам и операторам критической инфраструктуры в части обеспечения защиты объектов, персонала и клиентов от кибер- и иных угроз.

Информация, подпадающая под критерии распространения и обязательного взаимного обмена, включает в себя информацию об инцидентах, уязвимостях, последствиях, взаимозависимости по межотраслевым секторам, подготовке кадров в сфере кибербезопасности.

Приведу пример. В 2012–2013 годах была атака на финансовый сектор США, информация поступила в соответствующий аналитический центр, где к тому времени уже была разработана схема действий в случае возникновения угрозы. Там были представители 37 банков, которые стали жертвами этой атаки. Скоординированные действия аналитического центра позволили объединить усилия в плане выработки мер ликвидации последствий данной атаки. Эти меры были также тиражированы и другим членам банковского сектора США. Это конкретный пример, когда пострадало несколько банков, а рекомендации по безопасности были направлены всем организациям банковского сектора США. Для этого надо было изучить опыт ликвидации последствий, снижения и смягчения рисков, и какие могут быть предприняты меры по ликвидации последствий киберинцидентов. Это яркий пример государственно-частного партнерства.

В настоящее время Европейский Союз выработал свои меры защиты помимо общей директивы, определяющей меры по защите

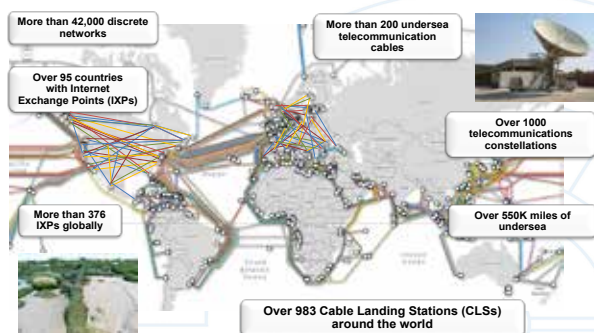
INFORMATION SHARING AND ANALYSIS CENTER'S (ISACS)

- ISACs help owners and operators of Critical Infrastructure protect facilities, personnel and customers against cyber, physical security threats and other hazards
- ISACs collect, analyze and disseminate actionable threat information to members, and provide members with tools to mitigate risks and enhance resiliency.



9

Commercial Telecommunications Dependencies



15

2016 Network & Information Security (NIS) Directive Highlights

- Define minimum harmonization across EU for Critical Infrastructure Protection
- Establish requirement to identify, report and keep current lists of contacts across states for all critical service providers
- Establish criteria for "significant incident" reporting
 - number of users affected; geographic spread of affect
 - cross-sector interdependency impacts
 - duration of affect; market share of entity
 - Alternative means of service provision

13

Telecommunications Interdependencies
Critical Information Infrastructure Protection (CIIP)

20

данных. И признание того, что большая часть критической инфраструктуры носит трансграничный характер и охватывает территории нескольких государств, позволила ЕС сформировать специальные директивы, принятые в 2016 году по обеспечению защиты информационных сетей. Наблюдается общая гармонизация во всех странах ЕС в отношении мер защиты критической инфраструктуры. При наличии трансграничной услуги в сфере ИКТ, которая используется критическими инфраструктурами, в плане безопасности необходимо соблюдать вышеупомянутые директивы. В каждой стране назначен координатор, который курирует данный вопрос. Примечательно, что в настоящее время все страны ЕС подключились к этому проекту. В Европейском Союзе также разработана система оповещения государств о киберинцидентах.

Несколько слов хотелось бы сказать о деятельности, носящей международный характер. Это взаимозависимость компаний, предоставляющих услуги телекоммуникаций и связи, это очень динамичный процесс. Мы видим, что по всему миру проложено более

200 коммуникационных кабелей. Места стыков подводных и наземных кабелей являются местами уязвимостей. И эта система телекоммуникаций сама становится очень уязвимой, учитывая ее размах.

Какие же препятствия необходимо преодолеть в этой связи? Очень трудно осуществлять и налаживать взаимодействие, когда частные компании и государственный сектор неохотно идут на обмен информацией. В частности, коммерческие компании боятся утечки их запатентованной чувствительной информации.

В заключении хотелось бы отметить, что эффективная защита всех участников процесса требует диалога между частными компаниями и государственным сектором. В то же время необходимо создать платформу для обмена информацией, что гораздо более эффективно, чем пытаться в одиночку решать данные проблемы. И в этой связи государственно-частное партнерство означает конструктивный диалог между частным и государственным секторами.

Большое спасибо!

**МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО
В ОБЛАСТИ ИНФОРМАТИЗАЦИИ
В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ
НА ПРИМЕРЕ СОТРУДНИЧЕСТВА
ЦЕНТРАЛЬНЫХ БАНКОВ ЕАЭС**

Добрый день, уважаемые коллеги!

Спасибо большое организаторам за возможность принять участие в интересной и содержательной дискуссии. Отмечу, что обсуждаемые здесь вопросы точно также беспокоят и Центральный банк как регулятора финансового рынка Российской Федерации. Центральный банк очень активно включен в международные процессы и международное сотрудничество, в том числе на площадках Совета финансовой стабильности (Financial stability board) и Базельского комитета по платежам и расчетам, а также в рамках G20 на треке, связанном с финансовыми технологиями.

Все вопросы, которые здесь обсуждались: и атрибутирование, и атаки, и международное право, – все они актуальны и для финансовой сферы.

Однако я хотел бы остановиться на взгляде Центрального банка России и попытаться ответить на вопрос: где место регулятора, где место финансовых организаций и как выстраивать процесс, связанный с информационной безопасностью финансовых организаций. Прежде всего, отмечу, что, безусловно, обеспечение информационной безопасности перестало быть частной задачей конкретных финансовых организаций. Это серьезный вызов для финансовой стабильности не только конкретной организации, но и всего финансового сообщества. Кстати, это также касается и мирового финансового сообщества. Неработоспособность конкретной организации может негативно отразиться на ее контрагентах, а этот контрагент совершенно необязательно находится в той же самой юрисдикции, что и он. Поэтому мы все-таки считаем, что риски, связанные с киберустойчивостью, риски, связанные с кибератаками, – это одни из основных глобальных рисков, которые могут повлиять на финансовую систему.

С другой стороны, мы прекрасно понимаем, что заниматься просто информационной



безопасностью ради информационной безопасности бесполезно. Любая деятельность должна быть измерена, должно быть понятно, где точки эффективности, и чего мы хотим достичь. В Российской Федерации такое измерение есть, мы для себя определяем два показателя, которые во многом характеризует ситуацию на финансовом рынке с точки зрения информационной безопасности. Первый показатель – это доверие населения к финансовым услугам с точки зрения информационной безопасности, и второй показатель – это уровень несанкционированных операций по отношению к общему уровню транзакций на территории Российской Федерации.

Если говорить об этих показателях, то за последнее время мы достигли определенных результатов. Это – не заслуга Центрального банка, это – заслуга финансовой системы в целом, вместе с Центральным банком и вместе с правоохранительными органами, но, тем не менее, такой результат есть.

Если говорить об измерении, которое мы проводили в 2017 и 2018 годах, то уровень доверия у нас существенно поднялся. Если мы начинали с 40% населения, сейчас 70%, и население в принципе понимает, что оно может ожидать с точки зрения информационной безопасности от кредитных и финансовых организаций. С точки зрения второго показателя, здесь мы немного находимся в этом состоянии ухудшения, но это тоже понятно, поскольку

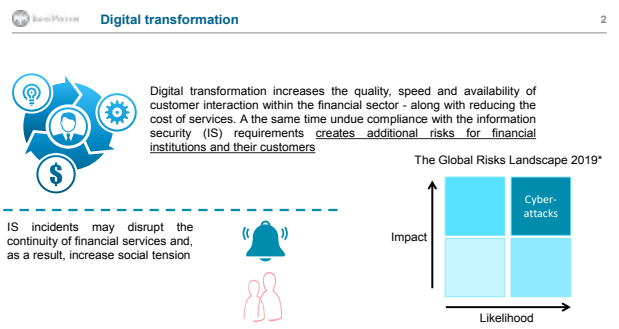


выявляемостей атак, выявляемостей хищений с точки зрения информационной безопасности стало гораздо больше.

Это как раз один из вариантов того самого государственно-частного партнерства, о котором здесь только что говорили.

Что мы видим для себя? Какие направления и взаимодействие? Безусловно, драйвером этой работы является идентификация направлений диджитализации, то есть цифровизация финансовой сферы и появление новых финансовых технологий. Эта деятельность приносит новые риски и ставит перед нами совершенно другие задачи с точки зрения управления, методологии обеспечения информационной безопасности, контроля ее реализации. Каким образом это может быть достигнуто? Существует несколько параметров: выпуск нормативных документов Банка России, определяющих требования к финансовой инфраструктуре с точки зрения информационной безопасности; разработка определенных стандартов, выпускаемых Банком России совместно с кредитными организациями; деятельность Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ). Структура ФинЦЕРТа – это как раз один из ярчайших примеров работы государственно-частного партнерства. На текущий момент к нему подключены все кредитные организации, все организации страхового рынка, продолжается подключение других участников рынка, а также участвуют и государственные органы. Таким образом, общее количество участников информационного обмена в настоящее время составляет порядка 800 организаций.

Каждый день мы получаем информацию об инцидентах, связанных с информационной безопасностью, и таких инцидентов достаточно много. Основная форма работы обратной связи для ФинЦЕРТа – это рассылка информационных бюллетеней, за последнее время



направлено более 500 таких бюллетеней. Существует 3 вида рассылок: рассылка, связанная с общей ситуацией, касающейся информационной безопасности, второе – рассылки с конкретными метриками компрометации и с рекомендациями относительно выявления таких атак и реагирования на них, третье – информация для конкретных участников по конкретным проблемам, выявленным на его информационных ресурсах.

Самый яркий результат такой деятельности – это отсутствие любого влияния вирусов-шифровальщиков, которые так «гремели» недавно – WannaCry и Petya, результаты воздействия которых никак не отразились на финансовой деятельности Российской Федерации.

Причина этого проста: имея информацию от ФинЦЕРТа, банки смогли вовремя подготовиться к такой атаке, и в результате она прошла незамеченной.

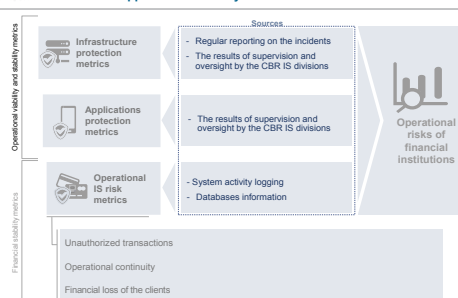
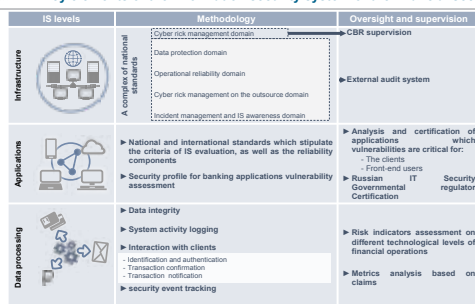
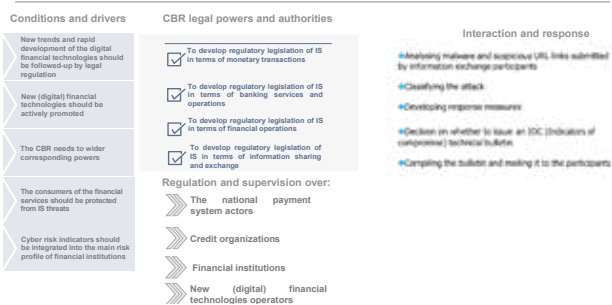
Тем не менее, мы говорим о регулировании, которое распределяется по трем основным направлениям: инфраструктура, уровень приложений и анализ тех данных, которые формируются и в банках, и в Центральном банке.

На уровне приложений мы исходим из того, что должна проводиться всесторонняя оценка их защищенности, в первую очередь, это касается приложений, которые находятся на границе между финансовой организацией и клиентом. Почему мы считаем это крайне важной задачей? Потому что самое уязвимое звено во всей финансовой цепочке – это клиент, и как бы мы ни говорили о его защищенности с точки зрения банков, он в любом случае, к сожалению, будет пренебрегать элементарными мерами безопасности. Поэтому мы считаем, что максимально усложнить задачу злоумышленника и не оставлять ему дырок для «захвата» пользовательского устройства и «перехвата» управления финансовыми сче-

The target title	Target rate 2017	Actual rate 2017	Target rate 2018	Actual rate 2018	Target rate 2020
Level of trust	30%	40%	60%	70%	80%
The rate of unauthorised fund transfers via payment cards*	0.005%	0.0016%	0.005%	0.0018%	0.005%



*Our objective is to keep this rate for the whole banking system under 0.005%.



тами, было бы одной из важных мер обеспечения безопасности.

Кроме задач, связанных с ФинЦЕРТом и анализом законодательства о новых требованиях информационной безопасности, особо актуальным представляется также переход к рискориентированному подходу, к формированию рискпрофиля кредитной организации. Это дает возможность понять, насколько руководство той или иной финансовой организации озабочено вопросами информационной безопасности.

Не секрет, что при наличии существенных рисков финансирование задач по информационной безопасности практически не осуществляется. Здесь ситуация заключается в том, насколько внимание менеджмента к вопросам киберрисков есть, и если есть, то

на что оно, действительно, направлено. Это одна из задач, которую Центральный банк будет решать.

В заключении хотел бы обратить внимание на то, что мы в рамках международной деятельности стараемся продвигать данный подход с точки зрения регулирования киберриска и отношения к киберриску как к серьезному вопросу с точки зрения финансовой стабильности.

Надеемся, что опыт, наработанный сегодня в Банке России, будет интересен, в том числе и на площадке группы международных экспертов в рамках ООН, поскольку нам есть чем поделиться, есть что обсудить, и мы готовы идти на контакты с нашими коллегами из зарубежных стран.

Спасибо за внимание!

Шень И (Shen Yi),

Директор центра БРИКС, Фуданьский университет, Китай

ПОЗИЦИЯ БРИКС В УПРАВЛЕНИИ КИБЕРПРОСТРАНСТВОМ

Спасибо, господин председатель!

Уважаемые коллеги! Для меня огромное удовольствие выступать здесь перед вами! Я представляю два центра Фуданьского университета.

Цель моего выступления – осветить сотрудничество в рамках БРИКС и представить позицию БРИКС в управлении киберпространством.

Я хотел бы затронуть два вопроса. Первый – каково общее понимание киберпространства и управление им в настоящее время, и как использовать новый режим в управлении киберпространством? Второй вопрос – каковы позиции стран БРИКС в данной сфере?

В первую очередь, хотел бы привести несколько примеров того, как разные акторы и субъекты понимают проблему управления глобальным киберпространством. Несколько дней назад в Китае прозвучала новость о том, что компания Huawei в Германии рассматривает вопрос о заключении соглашения с немецким правительством о неосуществлении шпионажа. Целью этого соглашения является обеспечение доверия к китайской продукции, улучшение бизнес-климата после того, как США подняли этот вопрос. В то же время правительство Германии планирует подписание подобного соглашения и с США. Это очень важный шаг, особенно после того, как Э. Сноуден сообщил об осуществлении шпионажа со стороны США по отношению к Германии.

Подписание таких соглашений позволит правительствам задавать так называемые правила игры в киберпространстве. С другой стороны, возникает вопрос, насколько компании стремятся влиять на глобальную среду, и это касается не только Huawei. Например, компания Microsoft занимается тем же самым, они также задаются вопросом, возможно ли иметь цифровую Женевскую конвенцию в киберпространстве, чтобы акторы могли вести себя соответствующим образом в киберпространстве, в том числе и при возникновении конфликтов между компаниями.



Для осуществления нового режима управления в киберпространстве необходима разработка методологии, и Россия уже запустила такой проект. При составлении подобных методологий очень важно учитывать исторический аспект. Хочу отметить, что говоря об управлении киберпространством, учитывая все имеющиеся уже документы на сей счет, мы видим, что историческая перспектива всегда забывается. Я имею в виду, что в некоторых случаях, к сожалению, отсутствует историческая память для лучшего понимания проблемы. Еще в 2016 году много говорилось о попытках контроля за большим количеством фейковых новостей, однако все забыли о том, что этот вопрос уже поднимался несколькими годами ранее, в том числе и в США.

Это говорит о том, что подобное невзвешенное поведение некоторых акторов может выставить, например, Китай, не в лучшем свете, говоря об ответственном поведении государств в киберпространстве, независимо от того, необходим ли какой-то новый мировой режим или ведется поиск каких-либо ассиметричных преимуществ, которые могли бы быть у США или других акторов в киберпространстве.

Поэтому необходимо разработать новую, единую для всех концепцию, ведь даже на платформе ГПЭ (*Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности – ред.*)

не было выработано общего определения «управления глобальным киберпространством». Нам нужно выработать общее понимание таких дефиниций, как «киберпространство» и «управление киберпространством». В настоящее время, когда мы говорим о киберпространстве, необходимо учитывать уровни функционирования киберпространства и взаимодействия в нем. Первый уровень – это инфраструктура, программное обеспечение и все то, что поддерживает наше поведение в киберпространстве; второй уровень – это стратегические ресурсы, третий уровень – уровень поведения акторов в киберпространстве, четвертый уровень – уровень регулирования, касающийся всех кодексов поведения, норм и законов, служащих для управления поведением в киберпространстве. Разработав все эти дефиниции, мы сможем двигаться дальше в нашей дискуссии управления киберпространством.

Что касается трех основных вызовов, то первый из них – это скорость разработки ИКТ для управления Интернетом вещей, второй вызов – это ассиметричное распределение возможностей и потенциалов различных акторов, третий вызов – необходимость сбалансированного распределения ресурсов среди различных категорий акторов, в том числе государственных и негосударственных субъектов.

В настоящее время мы сталкиваемся с вызовом распространения потенциалов. Если вернуться в 90-е годы, когда США разработали стратегическую оценку сети Интернет и существовали предположения, что Интернет используется как средство западных демократий, то сейчас вызовы, связанные с проблемами в киберпространстве, стоят перед всеми странами, независимо от их внутреннего режима.

Но при этом ряд стран считает, что они могут осуществлять режим одностороннего управления киберпространством, который дает им особые преимущества в глобальном киберпространстве по сравнению с их стратегическими конкурентами. Я полагаю, что данное ошибочное представление необходимо исправлять. И это становится важным предварительным условием для значимого прогресса в обсуждении данного вопроса.

БРИКС имеет особую позицию по управлению киберпространством. В настоящее время

мы разрабатываем 2–3 различных сценария возможного будущего управления киберпространством. Первый сценарий заключается в том, что США имеют явное преимущество, являются гегемоном, и это единственный актор, который может обеспечить суверенитет и безопасность в глобальном киберпространстве, при этом остальные страны подобного суверенитета иметь не будут. По нашему мнению, подобный односторонний порядок может привести к сильной реакции со стороны других акторов. Второй сценарий – это сценарий, основанный на принципах закона Европейского Союза о защите персональных данных, касается управления киберпространством на основе личных ценностей. Однако это повышает во многом требования к управлению киберпространством. Необходимо искать баланс между личными персональными ценностями и предпочтениями компаний по прибыльности, а также требованиями государств по вопросам национальной безопасности. Любые резолюции, которые могут быть применимы, должны содержать в себе именно этот баланс.

В настоящее время уже создано несколько институтов в рамках БРИКС. Однако еще многое предстоит сделать. Во-первых, нам необходимо разработать механизмы исследований, чтобы координаторы кибербезопасности от БРИКС при проведении конференций могли вносить также свой вклад. Мы должны также создать рабочие группы в рамках БРИКС для разработки общего понимания глобального киберпространства, чтобы в будущем в рамках G20 и на других площадках БРИКС имел свой скоординированный подход. Наша задача также – создать единый подход в рамках ГПЭ ООН со стороны БРИКС для создания альтернативных подходов в рамках ООН, среди которых можно было бы выбирать, как в будущем будет выглядеть управление глобальным киберпространством.

И, наконец, нам необходимо вкладывать больше ресурсов в общие проекты по киберпространству не только в рамках БРИКС, но и привлекать для этого большее количество стран, чтобы в будущем иметь лучшее понимание вопросов управления глобальным киберпространством, в том числе и с точки зрения социальных аспектов.

Г.Д. Толорая,

*Национальный комитет по исследованию
БРИКС, Россия*

БРИКС И ВОПРОСЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Спасибо большое!

Я хотел бы больше сосредоточиться не на технических вопросах.

Итак. Тема БРИКС и вопросы международной информационной безопасности. Каким образом БРИКС может поспособствовать их решению и какие направления взаимодействия можно здесь выделить?

Почему вообще речь зашла о БРИКС? Дело в том, что БРИКС был создан 10 лет назад как инструмент повышения роли незападных государств в глобальном управлении. В первую очередь, в управлении экономикой и финансами, а также и в дальнейшем управлении безопасностью и во всех других сферах, которые сейчас несколько пробуксовывают в связи с изменением мирового порядка. Образуются новые центры силы, и односторонние решения США не всегда могут быть реализованы.

За прошедшие годы был создан серьезный механизм взаимодействия внутри БРИКС. В настоящее время действует более 70 различных дорожек и консультационных механизмов между странами. Существуют и совместные проекты. Естественно, что не все области сотрудничества в равной степени выгодны.

БРИКС начинался с чисто финансово-экономических вопросов, и сейчас произошло постепенное расширение тематики. Сегодня с учетом некоторых политических противоречий внутри самого БРИКС, например, между Китаем и Индией, мы стараемся выбрать те области, где мы имеем единую точку зрения и где наша деятельность была бы наиболее эффективной.

Политики и эксперты пришли к выводу, что наиболее результативным взаимодействием БРИКС может быть в области общих пространств. Именно здесь БРИКС может заполнить те ниши, которые образовались в глобальном регулировании новых процессов, и именно здесь БРИКС может не создавать какие-то параллельные структуры управления, как это произошло в финансах, когда стал



действовать Банк развития и другие механизмы, а создавать новые системы и структуры глобального управления, которые были бы полезны или даже обязательны для всего мира. И как раз вопросы информационной безопасности, вообще управления Интернетом здесь занимают особую роль. Многие их считают даже тем полем, на котором БРИКС может выступать с наиболее сильных позиций, как в силу быстрого технологического развития в сфере ИКТ, так и исходя из того простого факта, что страны БРИКС – это больше половины пользователей Интернет, и те решения, которые они будут принимать, так или иначе будут если не обязательны, то учитываться другими странами и структурами.

Если говорить о том, каковы задачи сотрудничества БРИКС в области международной информационной безопасности, это, в первую очередь, совместная разработка правил, норм и принципов ответственного поведения государств в сфере использования ИКТ, и мы настаиваем на том, что это должно происходить под эгидой ООН.

Вторая задача – это создание неких юридически обязывающих механизмов сотрудничества против угроз транснациональной преступности. Страны БРИКС заинтересованы во взаимном трансграничном сотрудничестве для того, чтобы бороться с международным терроризмом. Это задача сейчас в рамках БРИКС является одной из основных



в сфере сотрудничества в области ИКТ. Еще одним фактором является продвижение к изменению структуры глобального управления Интернетом, хотя надо отметить, что в своих официальных документах страны БРИКС довольно сдержанно высказываются по этому поводу, чтобы не быть обвиненными в том, что они, как говорится, «тянут одеяло на себя».

Если взглянуть на историю, то еще в Декларации БРИКС на саммите в г.Санья (Китай) в 2011 году была указана необходимость борьбы с международным терроризмом, в частности, укрепление международной безопасности и борьба с киберпреступностью. В 2013 году в Дурбане (ЮАР) было упомянуто о важности мирного, безопасного, открытого киберпространства, и то, что ИКТ должны использоваться с учетом применения универсальных стандартов и практик.

Гораздо больше внимания стало уделяться ИКТ, начиная с 2014 года. На саммите в Форталезе (Бразилия) была поставлена задача приверженности выработке универсального, имеющего обязательную юридическую силу международно-правового документа в данной области под эгидой ООН. В частности, отмечено, что Интернет должен использоваться как инструмент развития и не допускать его использования в качестве оружия. Также была поставлена задача совместных действий в области безопасности ИКТ, и в соответствии с решением высоких представителей по вопросам национальной безопасности была создана группа экспертов, которые будут заниматься решением соответствующих задач.

Несколько пунктов, 4 или 5, было посвящено информационной безопасности в Уфимской декларации саммита БРИКС, прошедшего в России. Было упомянуто о важности

ИКТ в целом и включении проблематики ИКТ в повестку дня в области развития на период после 2015 года, а также подчеркнута недопустимость использования ИКТ и Интернета в целях нарушения прав и свобод человека, в том числе неприкосновенности частной жизни, поставлена задача по формированию системы, позволяющей обеспечить конфиденциальность и защиту персональной информации пользователя. Подчеркнуто, что Интернет является международным ресурсом и что государства должны в равной степени участвовать в его развитии, он должен быть открытым, единым и безопасным. Вся эта деятельность должна осуществляться под эгидой ООН. Выражена озабоченность в связи с использованием ИКТ для целей транснациональной организованной преступности, разработки оружия и осуществления террористических актов. Подчеркнуто, что необходимо развивать ИКТ на основе норм и принципов международного права. В тот момент также были актуальными проблемы осуждения актов массовой электронной слежки и сбора данных частных лиц, нарушения суверенитета государств и прав человека. Пожалуй, впервые на таком уровне было об этом сказано.

Одновременно подчеркнута приверженность к всеобщему доступу к средствам цифровой связи и повышению информированности, а также приверженность к созданию под эгидой ООН юридически обязывающего инструмента по борьбе с использованием ИКТ в преступных целях.

Созданы рабочие группы экспертов государств БРИКС по вопросам безопасности в сфере использования ИКТ, инициированы сотрудничество по обмену информацией о передовых практиках по вопросам безопас-

Working Group of Experts of the BRICS States on Security in the use of ICTs

- **BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICT**
- **Digital BRICS Task Force (DBTF)** to further commit to the full participation in the work of Partnership on New Industrial Revolution
- **BRICS ICT Regulators Forum** to share and exchange ideas, best practices and capacity building related to the ICT sector

Options

3. Establishment of a common **BRICS-wide repository of technical data** related to ICT security threats
4. Engage in a format of *trust and confidence building measures* (TCBMs) probably focused on ensuring security and protection of *critical information infrastructure* (CII) objects
5. Deployment of *quantum communication channels* between BRICS countries
6. Double and network degree *educational programs* in the area of cyber, digital development, AI and Big Data

ности во всех сферах использования ИКТ, эффективной координации мер противодействия киберпреступности, выделение уполномоченных по связям государств-участников по сотрудничеству между членами БРИКС с использованием групп реагирования на компьютерные инциденты в области компьютерной безопасности, совместные проекты в области НИОКР и разработка международных норм, принципов и стандартов.

Также во время прошлого председательства России в БРИКС в октябре 2015 года прошло совещание министров связи стран-участниц, посвященное данной проблематике. Была подчеркнута важность обеспечения широкополосным доступом к сети Интернет, были приняты решения о содействии развитию внедрения широкополосного доступа в рамках БРИКС, отмечен дисбаланс в развитии программного обеспечения и оборудования, признана необходимость принимать совместные усилия для верификации глобального рынка программного обеспечения информационно-технического оборудования, признана необходимость усилить международное сотрудничество с акцентом на развивающиеся страны, с тем чтобы преодолеть цифровой разрыв. При этом стороны признали право каждого из государств разрабатывать и реализовывать политику в сфере информационных и коммуникационных сетей на своих территориях. Подчеркнуто, что принципы управления Интернетом должны основываться на принципах многосторонности, демократии, прозрачности и взаимного доверия.

В декабре 2016 г. на саммите БРИКС на Гоа (Индия) подчеркнута озабоченность ростом злоупотреблений ИКТ, а также вновь

была подчеркнута ключевая роль ООН на реагирование на вызовы в сфере ИКТ. Продолжена работа по принятию совместных правил, норм и принципов ответственного поведения государств, в том числе в рамках ГПЭ ООН.

В декларации БРИКС 2017 года в Сямэне (Китай) была выдвинута идея создания Института БРИКС по изучению сетей будущего, особое внимание уделено разработкам и инновациям в области Интернета вещей, облачных вычислений, больших объемов данных, нанотехнологий, искусственного интеллекта, сетей 5G, а также их инновационному внедрению в сферу совершенствования инфраструктуры ИКТ. Еще раз подчеркнута важность выработки совместных правил безопасности в области ИКТ, увеличения инвестиций в сферу ИКТ, поощрения партнерских отношений между институтами и организациями стран-членов БРИКС. Отдельный пункт посвящен центральной роли ООН в разработке общепринятых норм ответственного поведения государств в сфере использования ИКТ в целях обеспечения мирной, безопасной, открытой и равноправной среды ИКТ. Особо подчеркнуты принципы соблюдения государственного суверенитета и территориальной целостности, а также невмешательства во внутренние дела других государств и соблюдения прав человека. В Декларации подчеркнута необходимость выработки под эгидой ООН обязательного для всех нормативно-правового документа по противодействию использованию ИКТ в преступных целях, а также отмечено, что сотрудничество будет развиваться на основе разработанной группой экспертов дорожной карты практического сотрудничества БРИКС в области обеспечения безопасности в сфере ИКТ. Отмечена инициатива России о межправи-

тельствующем соглашении БРИКС по сотрудничеству в вопросах безопасности в сфере использования ИКТ.

Аналогичная позиция была повторена и в Декларации саммита БРИКС в 2018 году в Йоханнесбурге (ЮАР).

Какие могут быть дальнейшие направления работы БРИКС?

Представляю выводы рабочей группы экспертов БРИКС, которая предложила дорожную карту практического взаимодействия:

- создание группы по развитию цифровых технологий для взаимодействия в сфере четвертой промышленной революции;
- создание форума регуляторов ИКТ стран-членов БРИКС для обмена идеями, практиками и технологиями.
- К задачам БРИКС в области цифровых технологий в настоящее время можно отнести следующие:
- необходимость создания правовой базы для ответственного поведения государств в сфере ИКТ. В рамках БРИКС по инициативе России большее значение придается деятельности Рабочей группы открытого состава, так как там представлено большое количество стран;
- необходимость создания многостороннего механизма сотрудничества в борьбе с трансграничными угрозами в области ИКТ, а также подписания меморандума о взаимодействии между регуляторами ИКТ в странах БРИКС;
- создание технических баз данных в рамках БРИКС, касающихся угроз в сфере ИКТ;

- что касается взаимоотношений внутри БРИКС, необходимо принятие мер по повышению доверия самими странами-участницами для того, чтобы обмениваться опытом и осуществлять совместные действия в защите критической инфраструктуры;
- создание новых квантовых каналов между странами БРИКС;
- взаимодействие в области обучения, образования и научных исследований.

Очевидно, что в рамках председательства России по подготовке саммита, который состоится в Челябинске в 2020 году, вопросы ИКТ будут занимать важное место. В настоящее время ведется выработка повестки дня, тех тем, которые станут лозунгами российского председательства в 2020 году. Я полагаю, что данная тематика должна быть вынесена в число приоритетных.

Позвольте проинформировать вас, что в соответствии с Указом Президента России создается экспертный совет председательства в БРИКС, где значительное место будет уделено тематике ИКТ. В рамках совета будет несколько рабочих групп. Координирует эту работу Национальный комитет по исследованию БРИКС. Как представляется, должна быть также создана специальная рабочая группа по ИКТ. В этом контексте я хотел бы попросить уважаемых экспертов, находящихся здесь, в случае заинтересованности в сотрудничестве по этой проблематике обменяться со мной координатами.

Спасибо за внимание!

С.В. Лебедь,

Руководитель службы информационной безопасности Сбербанка России

Добрый день, уважаемые коллеги!

Я постараюсь коротко, мой доклад постановочный, возможно, он не требует обсуждения, но я буду готов ответить на вопросы. В рамках данной конференции неоднократно звучала фраза, что нам необходимо больше смотреть на технологии, без технологий невозможно решить сложные вопросы взаимодействия и безопасности. Мой доклад посвящен элементарным техническим проблемам, но которые, на наш взгляд, глобальны. Вместе с тем на экспертном техническом уровне мы не понимаем, почему эти вопросы не могут быть решены, так как мы считаем, что они могут быть решены и ими надо заниматься.

Мое предложение заключается в том, чтобы обсуждать на всех площадках вопросы технологических стандартов, равенств, кибергигиены, культуры, так как обсуждение взаимоотношений без понимания сущности этих проблем становится размытым и непонятным.

Неоднократно звучали тезисы о том, что количество проблем нарастает, мир лучше не становится, новые технологии порождают новые проблемы безопасности и хорошо подтверждают все те проблемы, которые существуют в мире в этой области – это потери мировой экономики. Звучат разные цифры и очевидно, что экспертам в этой области работы хватит надолго. Конечно, нам хотелось бы заниматься немного другими мерами.

Традиционные направления принимаемых мер правильны и понятны. Необходимо работать на уровне коллабораций, взаимодействия, регулирования, инвестиций в технологии, разработки различных правил взаимоотношений. Однако вопрос развития технологий, на мой взгляд, находится немного в стороне.

На сегодняшний день нет площадок, где этим вопросам в глобальном масштабе было бы уделено должное внимание. В подтверждение этого тезиса можно привести тот факт, что, начиная с 1999 года, количество стандартов Интернета составляет около 10000. Практически каждый стандарт учитывает требования безопасности. Есть отдельные технические и организационные стандарты, посвященные вопросам безопасности.



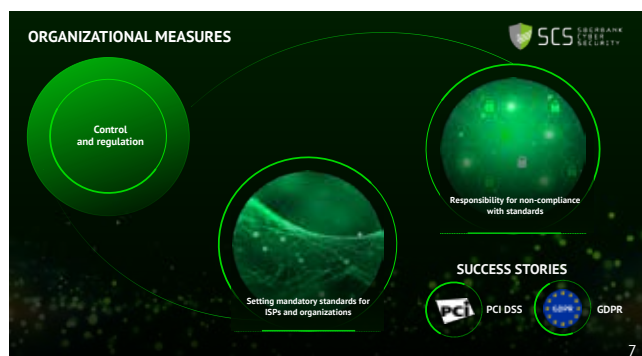
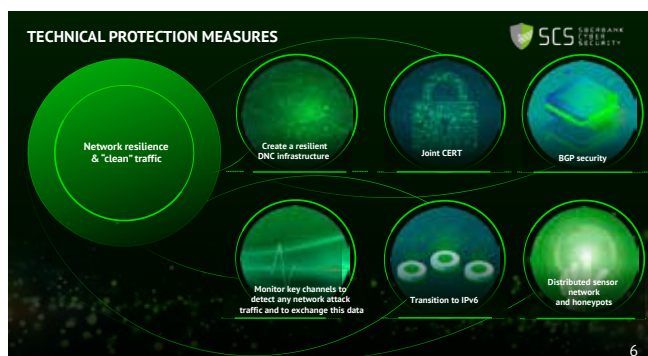
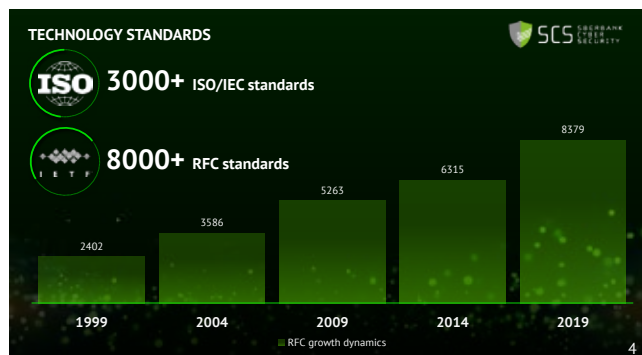
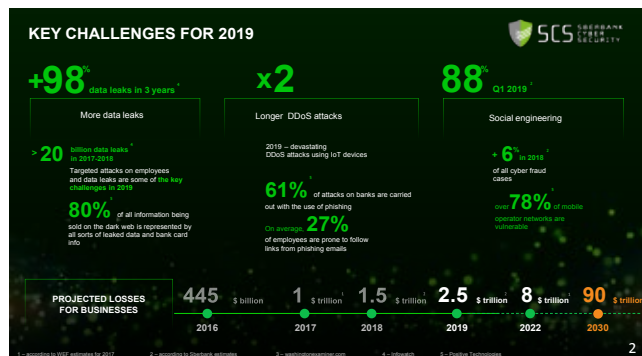
Такое большое количество стандартов возникло вследствие лавинообразного развития технологий, при этом некоторые базовые технологические проблемы сети Интернет до сих пор не решены. Также появляются технологии мошенничества, теневые сегменты сети Интернет, IoT-устройства. Возникает вопрос: что делать?

Хотел бы обратить внимание на некоторые технологические вопросы, ответы на которые человечеством уже давно должны были быть найдены.

Например, мир трясет от DDoS-атак, большинство из которых используют так называемые фейковые IP-адреса, при этом по всем стандартам и правилам оператор связи не должен из своей сети выпускать IP-пакеты, не принадлежащие его адресному пространству. Многие операторы, безусловно, такие требования соблюдают. Вместе с тем существует огромная масса мощных корневых национальных и глобальных операторов, которые почему-то эти правила не соблюдают.

Существует много подходов к обмену трафиком, направленным на сигнализацию о том, что идет распределенная DDoS-атака. Почему операторы связи эти механизмы не включают на своих пограничных маршрутизаторах, хотя для этого даже имеются встроенные возможности оборудования?

Следующий вопрос – IPv6. Напомню, в настоящее время мы работаем на протоколе



версии IPv4, и уже много лет разрабатывается и отлаживается работа протокола IPv6, однако почему-то он до сих пор не находит своего применения в мире, хотя все имеющееся оборудование этот протокол поддерживает.

Не стану уходить в детали, но IPv6 способен спасти нас от многих проблем, но при этом, возможно, он создал бы и другую проблему. Поскольку IPv6 предполагает шифрование трафика на базовом уровне своих возможностей, это может ограничить силовые структуры в контроле трафика.

Организационные меры, конечно, никто не отменял, так как организационная мера – одна из первых мер, которую нужно определять в построении системы безопасности. Вместе с тем мы имеем и истории успеха.

Есть ряд компаний, которые смогли решить проблему в рамках своего сообщества, в частности, противодействовать DDoS-атакам.

Резюмируя, хотелось бы отметить, что необходимо обсуждать технологические проблемы, так как они являются основой всех остальных проблем. В настоящее время существует большое количество технических подходов, которые позволяют решать проблемы на уровне взаимодействия операторов, внутри сообществ и др.

Например, ЕС, как наиболее организованный в плане принятия коллективных решений, мог бы обязать своих операторов связи запретить выход фейковых IP-адресов из их сетей.

Большое спасибо!

СЕМИНАР–КРУГЛЫЙ СТОЛ № 5
ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИКТ
ДЛЯ ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ
ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ, ВКЛЮЧАЯ
ГУМАНИТАРНОЕ ИЗМЕРЕНИЕ

Ведущие:

Куракин М.Б., журнал «Международная жизнь», Россия

Хиро Фудзимаки (Hiro Fujitaki), Университет Токай

М.Б. Куракин,

журнал «Международная жизнь»
(ведущий)

Добрый вечер, уважаемые коллеги!

Мы очень рады, что Вы здесь собрались, поскольку наш круглый стол завершающий, но тем не менее, тема важная, интересующая всех, называется «Противодействие использованию ИКТ для вмешательства во внутренние дела суверенных государств, включая гуманитарное измерение».

Преувеличить или преуменьшить значение этой проблемы сложно, так как мы все понимаем, о чем идет речь. Это могут быть или реальные, или фейковые новости, это могут быть самые различные манипуляции общественным сознанием и фальсификация истории, это могут быть прямые или косвенные вмешательства в деятельность суверенных государств, их органов и т.д.

Напомню, что несколько лет назад хакеры взломали сайт Белого дома, на котором появилось сообщение о том, что якобы Белый дом взорван, а президент Б.Обама ранен. Это привело к замешательству на бирже и многомиллиардным убыткам многим компаниям. Слава Богу, что во время спохватились и это не привело к крупномасштабной панике.

Тем не менее, такие факты существуют. Я предлагаю начать наш круглый стол и с большим удовольствием передаю слово своему коллеге, представителю университета Токая Хиро Фудзимаки.



**Хиро Фудзимаки
(Hiro Fujimaki),**

Университет Токай, Япония

ВОПРОСЫ БЕЗОПАСНОСТИ ЧЕЛОВЕКА В КИБЕРПРОСТРАНСТВЕ

Университет, который я представляю, называется «Дух», включает в себя Институт по исследованию вопросов международных отношений Университета Токая.

Мой доклад будет состоять из трех частей. В первой части мне хотелось бы сказать несколько слов о конференции, которую провел наш Университет в 2017 году, вторая тема – это регионализм, третья – вопросы безопасности человека в киберпространстве.

Начну с того, что представлю свой институт, который был создан для того, чтобы обеспечить связь между научными кругами, политиками и журналистами. Наша миссия – способствовать делу мира благодаря изучению вопросов безопасности человека. И третье – распространять информацию о результатах наших исследований в обществе.

В декабре 2017 г. мы провели международный симпозиум «Диалог в сфере кибербезопасности: смена глобальной парадигмы». На этом симпозиуме задавался вопрос, как информационные технологии могут способствовать социально-экономическому развитию и качеству жизни?

С приветственным словом выступал Председатель кабинета Министров Японии, Посол России в Японии Е. Афанасьев, Президент НАМИБ В. Шерстюк и другие официальные лица. Среди выступавших хотелось бы отметить также А. Стрельцова, В. Соколова, Р. Шаряпова, П. Карасева.

Симпозиум широко освещался в прессе. По итогам симпозиума в марте 2019 г. был опубликован сборник докладов.

Перейдем к безопасности человека в киберпространстве.

Вопрос, который хотелось бы задать в этой связи, кто является жертвой инцидентов кибератак или ИКТ в целом: государство, компании или человек? Возникнет ли кризис безопасности человека в киберпространстве, если мы создадим новые нормы после окончания холодной войны? Сегодня уже воз-



никло такие понятия, как «кибербеженец», «кибербедность» или «политические гонения в киберпространстве».

Среди условий, сложившихся сейчас на международной арене, можно выделить сокращение влияния Японии в Азиатско-Тихоокеанском регионе и рост влияния Китая. Растет азиатский рынок, количество пользователей Интернета, а также влияние негосударственных субъектов, и в этой связи возникают нетрадиционные угрозы. То есть все большее влияние оказывают региональные державы, происходит процесс регионализации, снижается влияние государства в обществе. Таким образом, люди становятся жертвами в битвах, которые происходят в киберпространстве. Таковы предпосылки для моих аргументов.

Далее я хотел бы поделиться некоторыми тезисами Концепции безопасности человека. В ООН в 1994 году был опубликован доклад «Развитие, сфокусированное на человеке». Основные положения доклада заключались в том, что необходимо перестраивать политику в сфере безопасности, т.е. переходить от безопасности государства к безопасности, ориентированной на человека. В ходе холодной войны особое внимание уделялось безопасности на уровне государства, так как мир стоял перед угрозой третьей мировой войны, а сейчас мы сталкиваемся с совершенно иным измерением: это новые вызовы, связанные с ИКТ, в силу этого происходит перераспре-

деление военных бюджетов. Была оставлена без внимания безопасность человеческого развития, поэтому этот вопрос должен ставиться сейчас не только на национальном, но и на международном уровне.

Существует ряд угроз человеческой безопасности: гражданская война, нищета, авторитарный режим, пандемия, информационная безопасность и др. Государства должны предпринимать меры для решения этих беспрецедентных проблем, так как вопросы обеспечения безопасности в настоящее время эволюционировали и вышли за рамки традиционных исследований. Они должны включать в себя такие аспекты, как экономическая, продовольственная, кибербезопасность и др.

Исследования в области безопасности также должны расширять количество субъектов и их роли, например, неправительственных организаций, транснациональных компаний, научных кругов.

Среди новых тенденций в изучении вопроса безопасности человека в киберпространстве можно выделить участие международных организаций, таких как БРИКС, ШОС, АТЭС, в битве за киберпространство. Таким образом, возникает вопрос, нужно ли нам новое управление в киберпространстве или же к нему применимо существующее международное право?

«На полях» кибервойн в баталиях участвуют также и люди. Например, в Юго-Восточной Азии за последние два десятилетия к сети Интернет присоединилась многомиллионная аудитория, которая теперь тоже принимает участие в театре военных действий, совершенно не зная, какие баталии тут происходят и что можно стать жертвами кибератак. При этом если на полях сражений государство забывает об этих пользователях, то 7000000000 людей останутся в стороне, хотя сейчас во многом их жизнь зависит от киберпространства.

Следующий вопрос. Кто может нарушить безопасность человека в киберпространстве? Здесь государство может выступать как жертвой, так и с субъектом кибератак, но самыми главными жертвами являются люди, поэтому исследования вопросов безопасности стали более многоаспектными.

Во-вторых, некоторые государства ограничивают или подвергают цензуре киберпро-

странство, т.е. нарушают свободу слова в киберпространстве.

Для того, чтобы обеспечивать национальную безопасность, государство пытается контролировать общественное мнение. Однако, по данным исследований Freedom House «Свобода в сети», многие государства подвергают цензуре СМИ, пытаются оказать влияние на общественное мнение, это делается и в Японии.

Таким образом, необходимо региональное управление в сфере безопасности, так как безопасность человека не может осуществляться лишь одним государством, необходимо учитывать вопросы кибербезопасности, терроризма, пиратства, нелегальной торговли людьми, контрабанды оружия и т.д. Также на экономическое благосостояние в регионе влияет и развитие инновационных технологий, таких как искусственный интеллект, Интернет вещей, создание новых энергоносителей и др.

В середине XIX века ВВП Индии и Китая составляли четверть мирового ВВП, равно как и сейчас. Это говорит о том, что мы возвращаемся к старым временам, к экономической ситуации середины XIX века.

Как уже говорилось, после Второй мировой войны установился новый миропорядок, однако после окончания холодной войны ничего нового в системе международных отношений создано не было, она лишь превратилась сейчас в многополярную систему.

Очевидно, что система международных отношений после окончания холодной войны слишком опасна, чтобы на нее полагаться, т.е. мы имеем старые правила игры при новой расстановке сил, когда на арену выходят региональные державы, и эти реалии необходимо учитывать в новых нормах, учитывающих также и аспекты человеческой безопасности.

Если мы оставим людей «на полях» битвы в киберпространстве, возникнут большие проблемы. Это то, с чем сталкивается общество сейчас. Сюда же добавляются проблемы в здравоохранении, образовании, солидарности, ведь в обмене информацией люди полагаются на Интернет.

В силу этого нам необходимо учитывать вопросы человеческой безопасности в новой парадигме в области кибербезопасности.

Большое спасибо!

Я.Л. Скворцов,

*Факультет международной журналистики
МГИМО МИД России*

ТРАДИЦИОННЫЕ ЦЕННОСТИ В УСЛОВИЯХ НОВЫХ МЕДИА

Уважаемые коллеги!

Прежде всего позвольте поблагодарить вас за приглашение на форум. Я первый раз принимаю участие в Международном форуме «Партнерство, государство, бизнес и гражданское общество для обеспечения международной информационной безопасности».

Хочу начать с того, как в первый день форума Б.Н. Мирошников спросил, нет ли в зале журналистов. Я сначала хотел поднять руку, так как я декан факультета международной журналистики МГИМО, но почему-то этого не сделал. При этом подумал, как интересно, что мы говорим об обеспечении международной информационной безопасности без средств массовой информации.

Второе наблюдение заключается в том, что мой приятель, журналист со стажем, живущий в Баварии, спросил: «А при чем здесь журналистика? Это же информационная безопасность». Сегодня мы с ним на эту тему поговорили и пришли к пониманию того, что средства массовой информации к миру информации, к вопросам информационной безопасности имеют самое непосредственное отношение. Попробую сейчас это вам доказать.

Будучи на данном форуме в первый раз, я, как мне показалось, уловил некоторые традиции данного мероприятия и постараюсь им следовать. Начну с цитаты Министра иностранных дел С.В.Лаврова, которая уже приводилась, о том, что «войны начинаются в головах людей, там же они должны и заканчиваться». Глубоко убежден в том, что по сей день на то, что происходит в головах людей, средства массовой информации влияют самым непосредственным образом. Мы можем приводить статистику падения тиражей, падения интереса к традиционным печатным медиа, но, тем не менее, мне представляется, что если мы говорим не об узком экспертном сообществе, а именно о людях, о читателях, о пользователях информационных ресурсов, то нужно понимать, что это куда более «разно-



шерстная» аудитория, и, наверное, средства массовой информации играют в решении данного вопроса одну из самых важных ролей.

Ну и еще одна традиция, существующая на форуме, – это цитировать посла А. Крутских. Позвольте, я не буду отступать от этой традиции и приведу цитату, которая, наверное, многим из вас хорошо известна: «Альтернативы гонке кибервооружений могут стать договоренности между странами-лидерами в Интернет-технологиях, которые определяют правила и кодексы поведения в информационном пространстве».

Тут я хочу позволить себе озвучить пять тезисов, которые за два с небольшим дня участия в конференции у меня сложились.

1. В последние дни мы за этим круглым столом много говорили о праве, правилах игры, правилах поведения, о нормах и о рамках. Я по своему образованию гуманитарий и хочу поделиться своим наблюдением. В современной лингвистике есть понятие «динамическая норма». Наличие «динамической нормы» или динамика изменения нормы вовсе не означает, что нормы нет, но норма существует. Но норма по природе своей динамична, поэтому мне кажется, что говоря о том, что является нормой и как ее использовать в международном праве, мне кажется, что этот опыт современных лингвистов может



Практика использования ИКТ в сфере mass media

быть полезен. Повторюсь, норма может быть динамичной, по сути она таковой и является.

2. У обсуждаемых нами проблем, как мне видится, есть юридические аспекты, технические, технологические, а также ментальные аспекты – то, как воспринимается новая информационная реальность аудиторией: людьми, связанными профессионально с миром информации или не связанными, просто потребителями. О ментальных аспектах я как раз и хотел поговорить в основной части своего доклада, так как для журналистов – это является одним из самых важных вопросов, потому что нужно, чтобы было понимание аудитории.
3. Все новое – это хорошо забытое старое. Вчера мы обсуждали гибридные войны и прозвучал тезис, что войны, которые были в истории человечества, все они по сути своей являются гибридными, то есть такие войны всегда имеют составные части. В докладе прозвучало, что выделяют экономическое воздействие, военное, информационное и т.д. Я об этом упомянул сейчас, так как мне кажется, что новые технологические вызовы, о которых мы говорим, они возникали на протяжении целых десятилетий, а может быть, даже и столетий. Новые технологические возможности – новые технологические вызовы. Мы с вами встречаемся на немецкой земле, а самой немецкой газетой является немецкий «Bild», который появился в середине 20 века. Я думаю, что даже люди, не владеющие немецким языком, знают, что «bild» – это «кар-



Джулиан Ассанж Человек, который изменил мир

тинка». Мне однажды посчастливилось в Берлине поддержать в руках первый номер «Bild», и я понял, почему он так называется. Дело в том, что в середине 20 века в Европе появилось массовое телевидение, и на тот момент журналистам – представителям традиционных медиа – казалось, что телевидение, если не сегодня, то завтра убьет печатную журналистику. И если вы возьмете в руки «Bild», то первая и последняя полосы – это только картинки. Прошло уже 70 лет, телевидение не убило печатную журналистику, но новые вызовы, новые задачи перед средствами массовой информации по-прежнему возникают.

4. В последние дни мы много говорили об ИКТ-среде и о том, как она должна отражаться на массмедиа. Мы вскользь упомянули о Джулиане Ассанже и проекте Wikileaks (об этом подробнее будет сказано чуть позже). Приведу некоторую информацию. Несколько лет назад мне попалась очень интересная книга о Джулиане Ассанже, которая называется «Человек, который изменил мир». Я часто своим студентам задаю вопрос: «Насколько справедливо называть Джулиана Ассанжа человеком, который изменил мир? Если да, то в чем он его изменил? Если нет, то откуда возникло такое ощущение его роли?» Об этом тоже будет сказано чуть позже.
- ИКТ и новые медиа. В некоторых презентациях появлялись социальные сети, мы вскользь эту тему затронули, и пока информация к размышлению: «А сколько мы еще будем «новые ме-



«Когда умрут газеты?»

диа» называть «новыми»? А, может, они уже и не новые, может, они стали частью нашей повседневности?» И тут я хочу предложить свое определение. Я полагаю, что «новые медиа» – это та информационно-коммуникационная среда, в которой существуют и старые медийные институты, и новые, появившиеся уже в электронную эпоху. И каждый из них привнес что-то свое: новые медиа нуждаются в старых, а старые – в новых. Повторюсь, «новые медиа» – это новая медийная среда.

5. В качестве прелюдии к моему выступлению, я полагаю, что новую ИКТ-среду мы должны изучать, постигать и искать пути мирного и эффективного комфортного существования в этой ИКТ-среде. И еще одна функция, которая тоже ложится на экспертов, – образовывать аудиторию. То, чем должна заниматься академическая среда не только внутри академического сообщества, но и в более широком аспекте.

Итак, практика использования ИКТ в сфере массмедиа. В самом начале доклада моего выступления я обещал остановиться на ментальной стороне этого вопроса. Но так как мне приходится общаться со студентами, поделюсь одним наблюдением. На одном семинаре месяца 2–3 назад один коллега привел очень забавный пример нового ИКТ-мышления. Будучи в командировке, он вышел из отеля и увидел полицейского, который ехал на сигвее. Ему показалось это забавным и он сделал фотографию на мобильный телефон. Спустя 2 дня он дома, завтракая с женой и дочкой, вспомнил про этот снимок и задал им вопрос: «Девочки мои, а вы знаете, на чем

Журналисты оказались перед угрозой исчезновения профессии не в меньшей степени, чем работники типографий или шахтеры — бывшие герои индустриального общества.

«Вымирание» журналистики

в Стокгольме ездят полицейские?» Жена сказала, что полицейские там ездят на лошади, а дочь сказала, что на велосипеде. После непродолжительной дискуссии мой коллега достал телефон и сказал: «Смотрите, девочки, полицейский ездит на сигвее!» В эту секунду 14-летняя дочь попросила скинуть ей эту фотографию, чтобы она могла разместить ее у себя на странице в социальной сети. Мне кажется, что это хороший пример мышления молодого человека, выросшего, сформировавшегося и живущего в сети. Ту новость, которую я сообщаю, может быть, 100% моя аудитория знает.

Мне кажется, похожий пример есть в фильме «The social network». В самом начале фильма есть диалог героев, когда кажется, что человек одновременно находится в нескольких чатах и отвечает на вопрос с некоторым опозданием.

Я привел эти примеры, чтобы проиллюстрировать так называемую «Проблему 2025» (я прочитал о ней в одном социологическом журнале). Считается, что к 2025 году активная треть населения, а именно те, кто уже не учится, но на пенсию еще не вышел, это будет то самое поколение, которое сформировалось в эпоху социальных сетей, выросшее в ИКТ-среде, о которой мы так много сейчас говорим. Сами люди этого не понимают, так как они в другой среде, в другой информационной реальности не жили. И для них это совершенно нормально.

В прошлом году журнал «Журналист» обозначил проблему: «Новые медиа стали повседневностью: уже не новые новые медиа». Мне показалась очень интересной такая постановка вопроса. Старые медиа нуждаются в новых, а новые нуждаются в старых.



Фёдор Лукьянов «О мудрёной цифири»

Интересно то, что грань между новыми и новыми медиа стерлась, новые медиа стали текущими. Этот факт должен отрезвлять. Пока новые медиа были новыми, журналисты, редакторы, медиаменеджеры и многие из тех, кто причастен к ИКТ-среде, говорили о них с придыханием, подобно поклонникам какой-нибудь секты.

Книга, которую я купил в Вене несколько лет назад и часто использую ее в своих выступлениях, – «Человек, который изменил мир» – о Джулиане Ассанже. Я до сих пор считаю, что Ассанж дает нам больше вопросов, чем ответов, но очень интересных и актуальных, думать о которых, безусловно, нужно. И опять же сделаю отсыл к одному очень интересному фильму, который называется «Пятая власть». Мне очень нравится этот фильм, и я всегда обращаю внимание своих студентов на самое начало фильма: тяжелый выбор для The Guardian, The New York Times и Der Spiegel. Если вы смотрели фильм, то, наверняка, помните, что главные редакторы этих трех очень авторитетных журналов, которые знают традиции медиа, которые знают, что информацию надо обязательно проверять, никак не могут решиться на ту схему работы с Wikileaks, о которой они вроде бы договорились, то, что называется, по comment. Речь идет о размещении материалов без комментариев, потому что нас учили, что журналист должен проверять любую поступающую к нему информацию. Может журналист проверить информацию Wikileaks? Ответ очевиден – не может. Может ли журналист такую информацию игнорировать? Ответ тоже очевиден – нет, не может. Это те самые новые медиа, которые мне, выросшему по правилам традиционных медиа, не дают спать спокойно: я должен найти какой-то ответ на



Медиа следует активной вовлекать в проблематику ИКТ

этот новый вызов, или, иными словами, на этот новый нюанс ИКТ-среды. Потом происходит фальстарт, кто-то первым размещает эти материалы. Ну а следом и The Guardian, и Der Spiegel тоже могут это сделать.

Новые технологии как новые возможности. Я думаю, это не будет революционным утверждением, что ИКТ-технологии меняют нашу жизнь. Мы начали наш Форум с замечательной истории, жертвой которой я сам стал, я имею в виду глобальный коллапс в Шереметьево, и выяснилось, что поломка компьютера лишила авиаперевозчика возможности доставить вовремя багаж. И мы еще при этом говорили о том, что могли везти что-то более серьезное, нежели чемоданы с вещами пассажиров. На самом деле, что касается информации, казалось бы, второстепенного продукта, мы вообще живем в эпоху иллюзий о доступности информации, иллюзии по поводу того, что информация в избытке, на самом деле, мы прекрасно понимаем, что это иллюзия.

Я позволю себе еще очень короткую цитату из книги Б.Н. Мирошникова, из главы, которая называется «Достоверность. Достоверность ли». Когда-то на одном из серьезных совещаний оратор на трибуне произнес символическую фразу: «Это таблица наша точная, не из Интернета». Фраза была не из доклада, она вырвалась у него в пылу дискуссии. Вот так относятся специалисты к этому источнику знаний.

Для нормального рабочего разговора о будущем и настоящем профессии медийщика, то есть человека, который профессионально работает с информацией, с медиа. Так вот. Для разговора о будущем этой профессии нужно понять, что новые медиа лишь инструменты, которые помогают журналистам



Формирование мер доверия невозможно без «включения» СМИ

делать работу лучше, а не волшебные палочки, которые могут суть этой работы заменить.

На нашем Форуме уже несколько раз затрагивалась тема искусственного интеллекта. В свое время журнал Forbes – издание, которое выходит в Австрии, – посвятило «робосапиенс». Это как бы одновременно и вопрос технологических достижений о том, могут ли, например, машины писать информационные заметки, а могут ли работать пресс-секретарями. Я люблю обсуждать этот вопрос со своими студентами, и их позиция такова: это зависит от того, с кем пресс-секретарем работать. При этом они называют некоторых известных российских политиков, с функциями пресс-секретаря которых вполне бы справился робот.

Новая реальность, новый вызов – безусловно, да. Пока он еще не стал повседневностью, но это должно случиться уже завтра. Не буду останавливаться подробно на этой теме, но эта тема безумно интересная, и с моей точки зрения, это тоже вызов, который новая ИКТ-среда бросает журналистам.

Позволю себе поделиться следующим наблюдением. В медиасреде давно идет дискуссия о том, когда умрут газеты. На эту тему есть очень интересное исследование, потому что это не просто вопрос того, когда мы перестанем покупать газеты по утрам, когда мы перестанем их читать, это вопрос того, как, в каком формате и в какой форме мы воспринимаем медиа, и в каких временных рамках традиция этого мероприятия может существенно измениться.

Хотелось бы сказать еще несколько слов о журналистике в ИКТ-среде. Журналистика – это улитка в поисках нового домика. То, что существует сейчас, – это одновременно про-



Права человека, права граждан- «обитателей» ИКТ-среды...

цесс и формат, но еще и социальная группа с привычным укладом. Журналисты оказались перед угрозой исчезновения профессии не в меньшей степени, чем работники типографий или шахтеры – бывшие герои индустриального общества.

В декабре 2018 г. я читал лекции в Рурском университете и как раз в это время стало известно, что там закрывается последняя шахта. Можем ли мы говорить о вымирании журналистики? Я полагаю, что сегодня термин «журналист» нуждается в пояснении: «журналист» – это профессиональный коммуникатор, человек, профессионально работающий с информацией и поэтому имеющий самое непосредственное отношение к вопросам обеспечения международной информационной безопасности.

Думаю, многим из вас известен Федор Лукьянов – главный редактор журнала «Россия в глобальной политике». Он полагает, что человек вступает в другой мир, а, вероятнее всего, уже и живет в нем, в том, где все не так, как раньше. Прежде, в начале было слово, буква, а теперь – в основании всего число, то есть цифра. Цифра меняет форму, в том числе и работы с информацией. Но меняет ли она содержание?

В завершение приведу несколько легких соображений, просто возникших в блокноте в процессе участия в нашем Форуме.

Медиа следует активнее вовлекать в проблематику ИКТ. Вернемся к тому, с чего я начал. В нашем Форуме не участвуют журналисты. В начале 90-х годов, когда в России только возникал рынок финансовых услуг, я работал в «Коммерсанте». Фактически принимал участие в процессе формирования этого рынка. Я очень хорошо помню отноше-

ние аудитории к теме финансового оборота, как к чему-то очень сложному и непонятному. У людей существовал ряд стереотипов о том, что все банки – это жулики. Кто-то считает, что этот тезис подтвердился, кто-то считает, что нет. Мне кажется, все, что касается ИКТ-среды, сейчас находится в очень похожей ситуации: про кибератаки в России, да и не только в России слышал любой. А что это такое, и какие могут быть этому противодействия – вот это уже вопрос сложный, ответ на который человек не готов получить. Поэтому мне кажется, что если поднимать значимость этой проблематики и выходить за рамки узкого клуба экспертов, то, конечно, для этого нужны медиа.

Формирование мер доверия невозможно без включения СМИ. Мы много здесь в последнее время говорили о доверии. Однако пока сохраняется клубность и закрытость в обсуждении этой тематики, пока СМИ в требуемом формате не привлечены, я полагаю, что здесь скорее нужно будет не доверять друг другу, а как-то договариваться.

Права человека, права граждан – обитателей ИКТ-среды. Приведу следующий тезис. Когда уже почти 30 лет назад объединялась Германия и все еще существовал Советский Союз, в международной журналистике, в том числе в немецких СМИ, говорили так: журналисты выполняют одну из двух задач – они либо строят стены (имелась ввиду Берлинская стена), либо строят мосты. Одно из двух, третьего не дано! Поэтому мне кажется, что если нас волнует будущее обитателей ИКТ-среды, а это не только экспертное сообщество, то надо научиться строить мосты. Но это тоже нужно делать с участием медиа.

И последнее! Хочу вернуться к тезису Б.Н. Мирошникова о доверии. По-моему, это был 98–99 год, в Лондоне на одном семинаре нам сказали: «Если ваша мама сообщила вам через Интернет, что она вас любит, лучше маме перезвоните и перепроверьте эту информацию». С тех пор прошло 20 лет, но тема до сих пор актуальна: лучше перезвонить и перепроверить.

Спасибо за внимание!

А.В. Бирюков,

Центр международной информационной безопасности и научно-технологической политики (ЦМИБ) МГИМО МИД России

К ВОПРОСУ О ТЕХНО-ГУМАНИТАРНОМ ДИСБАЛАНСЕ ЦИФРОВОЙ ЭПОХИ¹

На Тринадцатом международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» представляется целесообразным обратить внимание на вызовы и угрозы цифровых технологий в контексте научно-технического прогресса. В связи с этим остановимся на следующем.

С точки зрения научно-технического прогресса всегда следует помнить о его темных сторонах, включая непредвиденные последствия, издержки, вторичные воздействия и осознанные злоупотребления новыми возможностями. Российские ученые пришли к выводу, что даже самые прогрессивные и социально ориентированные технологии со временем могут нанести ущерб, сопоставимый с позитивным эффектом, который они принесли. Требуется понимание и осторожность еще и в силу субъективного фактора. Вопрос, следовательно, заключается в исключении из рядов человечества субъектов, находящихся во власти и принимающих ответственные решения, которые интеллектуально ущербны и морально готовы на неадекватные движения и шаги. Здесь должны быть поставлены непреодолимые барьеры. Все это означает, что люди, управляющие научно-техническим прогрессом и обеспечивающие инновационный прорыв, должны быть не только знающими, понимающими и умеющими, но и высококультурными и высокоморальными, поскольку НТП поверхностного отношения к себе не прощает.

Думается, уместно привести мысль, зафиксированную в Стратегии национальной безопасности США 2010 года, озвученную Бараком Обамой, о том, что каждая новая технология не только укрепляет государство, но и тех, кто стремится его разрушить. И в этой связи целесообразно обратиться к «цифро-



вому парадоксу мощи», образу, предложенному А.В. Федоровым и Е.С. Зиновьевой. Чем в большей степени ты развиваешь собственный информационный потенциал, тем в большей степени ты становишься уязвим для кибернетических атак. США делали ставку на «всеобщую осведомленность» в международных делах и информационное превосходство, демонстрируя эти качества в отношениях со своими противниками и друзьями. Поэтому растущее понимание собственной цифровой уязвимости вызывает настоящий шок в США. Разворачивающийся скандал вокруг мифа о вмешательстве русских хакеров в избирательный процесс Президента США со всей очевидностью указывает на растущий страх перед собственной кибернетической уязвимостью, несмотря на колоссальный информационный потенциал.

Вчера перечислялись цифровые технологии, которые имеют мощный цифровой компонент в условиях глобальной информационной революции. Важно понимать, что эти технологии особенно эффективны, когда действуют в виде симбиоза. Именно цифровой компонент обуславливает уязвимость современных технологий, каждая из которых сама по себе также имеет двойное назначение. Но здесь хотелось бы особо подчеркнуть, что цифровой фактор предстает фун-

¹ Выступление опубликовано в специальном выпуске журнала «Международная жизнь» «Россия и глобальные вызовы в области информационной безопасности», 2019 г.

даментальным. Именно с ним, как думается, связана интенсивность противоборства на информационно-кибернетическом поле. Компьютерные атаки, как никогда, используются в качестве инструмента политической борьбы, добычи компромата, межгосударственного противостояния. Спецслужбы разных стран применяют его для разведывательной и контрразведывательной деятельности. Вчера было достаточно сказано о лавинообразном росте транснациональной преступности с привлечением корыстных хакеров, а также ее сращивании с цифровым терроризмом.

И, следовательно, необходимы серьезные барьеры перед преступностью и терроризмом, которые рвутся проникнуть в очень многие технологии цифровой эпохи, в опоре на которые можно вызвать колоссальные финансовые потери и нанести мощный политический ущерб. Специальный представитель Президента России А.В.Крутских озвучил на конференции финансовый ущерб от противоправных действий в информационно-кибернетической сфере. Выступая в мае этого года на заседании Комиссии Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, Генеральный секретарь ООН Антониу Гутерриш оценил потери мировой экономики от кибернетических атак в 1,5 триллиона долл. в год. Реальный ущерб значительно больше. Многие государства и корпорации скрывают информацию о своем финансовом ущербе, опасаясь навредить собственной репутации. Соответственно, значительно выросли затраты государственных органов и бизнеса на борьбу с кибернетической угрозой. Прогнозы потерь и вовсе неутешительны, если международное сообщество в ближайшие три года не предпримет срочных и решительных мер противодействия преступной деятельности данного типа.

В связи с этим возрастает значимость международной информационной безопасности, которая становится жизненной необходимостью цифровой эпохи, а не просто передовым рубежом международной безопасности. А если использовать метафору буддизма, то информационная безопасность представляет собой еще одну руку наряду с цифровыми технологиями, которая позволяет хлопнуть в ладоши. Одной рукой это

сделать, как известно, невозможно. В цифровую эпоху, когда интеллект становится драйвером развития, парадоксальными представляются вызовы в области культуры, науки и образования. По мере приближения технологической сингулярности, когда люди без опоры на искусственный интеллект будут не в состоянии адекватно воспринимать социально-экономический и научно-технический прогресс, все большее внимание уделяется человеку, его личности и деятельности. Вовсе не случайно в шестом постиндустриальном технологическом укладе центральное место уделяется высоким гуманитарным технологиям, а автор книг о четвертой промышленной революции и почетный президент Всемирного экономического форума Клаус Шваб особое внимание придает проблематике человеческих ценностей.

В условиях техно-гуманитарного дисбаланса предпринимаются попытки выровнять ситуацию, преодолеть «цифровой эгоизм», концентрацию исключительно на собственных интересах, убогость внимания, обусловленную избытком информации, деградацию милосердия и способности сосредоточиться на эмоциональном состоянии другого человека. Современные люди во все большей степени готовы обменивать конфиденциальность на удобства, предпочитают иметь, а не быть. Поэтому приоритет неприкосновенности частной собственности и личной жизни доминирует.

Один из способов возрождения ценностей связан с культивированием ценностно-ориентированного подхода к научно-техническому прогрессу, который признает политическую природу технологий и делает общественные интересы основой ответственного и эффективного управления. Всемирный экономический форум разработал «Новое социальное соглашение» (a New Social Covenant), которое является еще одной попыткой нахождения общих основ между культурами, религиями и философиями, которые воспринимаются всеми. К таким основам/ценностям относятся: достоинство человека независимо от расы, пола, происхождения и убеждений; важность общего блага, превосходящего индивидуальные интересы; необходимость разумного управления и заботы не только о нас самих, но и наших потомках.

Проблема в области науки связана с последствиями технологии Больших данных, которые позволяют проводить различные и сколь угодно подробные классификации, обеспечивающие точное понимание объекта наблюдения, осуществлять многомерный математический анализ, который содействует нахождению корреляции между самыми различными параметрами, а также прогнозировать оптимальный способ влияния на общественный процесс. В каком-то смысле Большие данные представляют собой альтернативный традиционной науке метод и придали импульс развитию поведенческих и когнитивных наук, которые привели к созданию эффективных технологий воздействия на человека и социальные группы, независимо от размерности. Но ведь кое-кто делает и другой вывод: Большие данные вытесняют науку и познавательную функцию человечества.

К этому же может иметь отношение и искусственный интеллект. Технология искусственного интеллекта является своеобразной интегрирующей технологией и самой стратегически важной и, возможно, самой опасной с точки зрения воздействия на общественную жизнь, поскольку объединяет все возможные угрозы, исходящие от современных технологий. При этом она является самой быстро развивающейся и наиболее перспективной. По мере развития подобной интегрирующей технологии все реальнее опасность новой гонки вооружения в сфере искусственного интеллекта, который может повлиять на глобальное разделение труда и архитектуру международной безопасности. Хотелось бы обратить внимание на то, что в данной области, как и в других сферах, в которых особенно значимо влияние современного НТП на международные отношения, формирующаяся реальность пребывает в международно-правовом вакууме, элегантно именуемой «серой зоной» международного права.

В связи с развитием искусственного интеллекта обсуждается проблема контроля этой технологии. Пока превалирует мнение, что технологию искусственного интеллекта можно использовать дозированно в качестве инструмента влияния или смертоносного оружия. Проблема заключается в том, что 100% контроль этой технологии вряд ли возможен в будущем. На рубеже тысяче-

тия данный сюжет был любим фантастами. Сейчас многие эксперты приходят к выводу о том, что искусственный интеллект в течение текущего века будет занимать все более важное место в управлении общественными процессами, а с наступлением технологической сингулярности начнется движение к феномену Singleton искусственного интеллекта. Это означает, что судьба мира, общества, человека может зависеть от «воли» искусственного интеллекта.

Что касается образования, то его проблемы обусловлены растущей асимметрией интеллектуального потенциала разных групп населения. Отличное образование предоставляется в первую очередь талантам и состоятельным лицам, которые активно ищут новые знания и в опоре на дистанционные образовательные технологии получают возможность учиться у лучших преподавателей по всему миру. Однако в подавляющем большинстве случаев молодые люди получают образование с целью ускоренной адаптации среднего потребителя к жизни и деятельности в условиях информационного потребительского общества. Это ведет к интеллектуальной поляризации населения, формированию устойчивых социальных групп, типичных траекторий индивидуальной судьбы и даже определенной деградации образования. «Цифровой разрыв» и образовательная асимметрия стимулируют материальное неравенство. В 2018 году 1% населения владел 82% богатства, что представляет собой новый рекорд социального расслоения, которое неуклонно растет в цифровую эпоху.

Еще одна опасность современности обусловлена когнитивным и психологическим противоборством, которое, в свою очередь, связано с информационными и кибернетическими технологиями. Использование этих технологий имеет целью агрессивное трансграничное влияние на массы людей, разрушение активных групповых субъектов, противодействующих инициатору воздействия, конструирование проводников собственных интересов в рамках социума, навязывание своей воли людям из элиты, вооруженных сил, специальных служб.

Вывод можно сформулировать следующим образом: вызовы и угрозы связаны не столько с цифровыми технологиями, которые,

как правило, являются двойными. И в этом смысле они могут представлять опасность. Однако нельзя забывать о политической природе технологий и о том, что опасность, от них исходящая, связана с ценностями людей, которые могут использовать технологии во благо или во зло. Отсюда актуализируются требования формировать целостную, обязывающую систему международного права, адаптированную к реальностям цифровой эпохи, а также культивирования этической среды, востребованной социально активным и гармонично развитым человеком, который несет ответственность перед обществом и самим собой.

Вопросы оптимизации участия России в научно-техническом прогрессе становят-

ся как никогда актуальными, поскольку охватывают тематику инклюзивного развития страны в условиях инновационного прорыва. Именно тема становления страны на рельсы шестого технологического уклада наряду с социальной гармонией и развитием реальной экономики может занять достойное место в общественно-политическом дискурсе.

В заключение отметим, что проблематика международных научно-технологических отношений и международной информационной безопасности входит в число приоритетов исследовательской и образовательной деятельности недавно созданного в МГИМО Центра международной информационной безопасности и научно-технологической политики.

А.А. Воробьев,

Координационный центр национального домена сети Интернет, Россия.

ОТВЕТСТВЕННЫЙ ПОДХОД К РАЗВИТИЮ СИСТЕМЫ DNS КАК ВАЖНОГО ЭЛЕМЕНТА ПУБЛИЧНОГО ЯДРА ИНТЕРНЕТА

Координационный центр национального домена сети Интернет – это регистратура национальных доменов, мы разрабатываем политики, правила, а вообще у нас строится управление всеми нашими национальными доменами. Нашу деятельность можно разделить на 3 составляющих: Центр аккредитовывает регистраторов, определяет правила, согласовывает их с государством.

С 2015 года помимо традиционных общественных интернет-организаций, которые были с самого начала, Минкомсвязь России – представитель государства – тоже вошло в состав учредителей. По новому закону вместо Минкомсвязи России должен появиться Роскомнадзор, который будет определять политику доменных имен. Насколько удачным оказался закон, утвержденный Советом Федерации России, покажут подзаконные акты, которые еще предстоит утвердить. Формулировки, имеющиеся в законе, на наш взгляд, достаточно общие, и в них идет отсыл на будущие подзаконные акты. Мы надеемся, что модель саморегулирования, которая была всегда присуща доменной индустрии, начиная от ICANN, реализована в Координационном центре, а до этого в российском НИИ развития общественных сетей, когда мы говорили о национальных доменных именах.

Очень важно упомянуть о российской регистратуре в деятельности международных и региональных отраслевых интернет-организациях. Координационный центр в силу особенности географического расположения России входит и в Совет европейских регистратур национальных доменов, и в Азиатско-Тихоокеанскую ассоциацию регистратур национальных доменов. И в этом вопросе мы можем сравнить европейские и азиатские подходы в этом вопросе, которые, конечно, существенно различаются. При этом мы работаем в составе Комитета национальных буквенных доменов ICANN.

Помимо этого исторически получилось, что за национальными регистратурами закреп-



пилась роль хостов в проведении национальных форумов по управлению Интернетом. Различают 3 уровня подобных форумов: глобальный форум по управлению Интернетом (последний из них проводился не так давно в Париже, Россия была широко представлена на нем, были озвучены тезисы о необходимости создания киберООН, об этом также говорилось уже и на нашем Форуме). Имеется в виду, что без международного регулирования бороться с противоправным контентом, с противоправным использованием доменов уже не получается. Более того, происходит и пересмотр роли участников рынка регистрации доменов в борьбе с противоправным контентом. Если раньше всегда говорили, что мы лишь присваиваем адреса сайтам, то сегодня меняется подход и вместе с государством осуществляются блокировки в досудебном порядке самых разных видов противоправного контента. Европейские коллеги ушли дальше и блокируют контент контрафактной продукции и многого другого, чего у нас пока не происходит, поскольку не определены критерии отнесения, например, недобросовестных интернет-магазинов, контента к разряду противоправного.

Начиная от глобального сотрудничества, мы приходим к пониманию, что нам тоже необходимо предпринимать некоторые шаги в этом направлении, и здесь нам помогают региональные организации. Об-


Координационный центр доменов




- Определяет политику регистрации в доменах RU/РФ
- Разрабатывает регламентирующие документы в доменах .RU/.РФ
- Аккредитует регистраторов в доменах .RU/.РФ
- Поддерживает проекты, направленные на популяризацию и развитие сети Интернет
- Представляет российскую регистратуру в деятельности международных и региональных отраслевых интернет-организаций

 : самый популярный в России

~ 5 015 000

- Делегирован 7 апреля 1994 года
- ТОП-10 TLD, ТОП-5 ccTLD
- ~ 85% доменов .RU зарегистрировано россиянами

 : национальный кириллический
 

~ 800 000

- Делегирован 12 мая 2010 года
- Первый кириллический TLD в мире, самый популярный среди IDN-доменов

ратная история произошла в Японии. В ходе церемонии открытия конференции ICANN в марте 2019 г. президент ICANN заявил, что ICANN видит, какие законодательные инициативы на национальном уровне появляются, и это вызывает обеспокоенность у корпорации, так как возникает опасность нарушения работы ядра Интернета, той технологической платформы, поставив границы которой, мы лишимся того Интернета, который уже привыкли использовать. Это уже будет не Интернет, а могут появиться национальные сегменты. И задача ICANN сегодня – это проведение учебных мероприятий с законодателями разных стран, чтобы показать, как важно сохранить публичное ядро Интернета, не разбивая его национальными законами.

В России мы имеем 3 уровня управления: регулятор – государство; технический центр Интернет, который вышел из недр Курчатовского института и поддерживается в настоящее время Ростелекомом; 47 аккредитованных регистраторов, которые тоже принимают очень активное участие, с одной стороны, в деятельности по развитию национальных доменов, а с другой, по очищению этих национальных доменов от зловредов.

Более 5 млн. доменов в зоне .RU, и мы входим в Топ-10 всех крупнейших доменных зон мира и в Топ-5 двухбуквенных доменов, но тут, конечно, на первом месте Германия, где почти в 4 раза больше доменов в зоне .DE, с чем можем их поздравить. Такой рост в Германии случился за счет активного вовлечения малого и среднего бизнеса, когда при регистрации компании вместе с названием регистрируется и доменное имя этой компании.

Мы имеем также кириллический домен .РФ, который на сегодняшний день один из самых популярных в мире среди доменов, записанных символами национальных алфавитов. Многие удивляются, что лидер здесь не Индия и не Китай. Это связано с количеством официальных языков в стране.

Ранее в России существовала большая проблема, заключающаяся в том, что споры относительно доменов и товарных знаков трудно было урегулировать в российской национальной зоне. На сегодняшний день создан онлайн-сервис, позволяющий сразу на этапе регистрации проверить, не нарушает ли чьих-то прав заявитель, и, соответственно, суды в большинстве своем встают на сторону правообладателя товарного знака, и поэтому сегодня этот конфликт уже не актуален. Это является хорошим примером, когда сообщество само смогло придумать понятные сервисы и снять остроту проблемы «владелец домена – владелец товарного знака».

Одним из главных моментов, касающихся информационной безопасности, является тот факт, что в российском законодательстве до сих пор нет четких норм, которые позволяли бы блокировать в судебном порядке фишинговые ресурсы, ресурсы с вредоносной активностью, управляющие бот-сетями и т.д. Поэтому был разработан механизм института компетентных организаций, когда те компании, которые имеют определенные компетенции, вправе сообщать нашим регистраторам о том, что те или иные домены заподозрены в зловредной активности.

Очевидно, что самой крупной подобной организацией является ФинЦЕРТ Центрального банка Российской Федерации. На сегод-



В наш день все фишинговые атаки проходят через ФинЦЕРТ, он все это мониторит и своевременно уведомляет регистраторов об этих инцидентах. Все это является механизмом саморегулирования. В наших правилах сказано, что регистратор вправе при получении заявки от компетентной организации блокировать домен. Конечно, все регистраторы понимают важность этой миссии и практически всегда блокируют, при этом проверяя дополнительно, происходит ли на самом деле атака или нет.

Данный механизм доказал свою эффективность и востребованность, и сегодня в Госдуме России рассматривается законопроект, подготовленный Центробанком России и Минкомсвязью России, о том, чтобы наделить Банк России полномочиями по включению фишинговых ресурсов в черный список сайтов, реестр которых ведет Роскомнадзор. Это уже будет не механизм саморегулирования, а такая работа будет уже вестись на законодательном уровне.

Отмечу, что система доменных имен достаточно уязвима. Данная система была создана для целей адресации в очень «интеллектуальной» среде, а сегодня приходится ставить дополнительные «заплатки», как, например, протокол DNSsec, все это делается, чтобы сохранить систему Интернет-адресации в должном виде, а также стоит задача помимо использования технических средств еще и повысить достоверность сведений об администраторах доменных имен. Проблема общая. ICANN проводила исследование, при этом оказалось, что в базах данных доменных имен далеко не всегда указаны настоящие контактные данные, и, соответственно, очень

часто злоумышленники, пользуясь достаточно либеральными правилами регистрации доменов, вводят недостоверные сведения, и такие домены используются в противоправных целях.

Для предотвращения этого разрабатываются разные проекты на международном уровне, например, на уровне ICANN, который позволяет при уличении каких-либо доменов в зловредной активности проверять все домены, принадлежащие этому администратору. Соответственно, в российской зоне создан подобный проект, называемый Нетоскоп, и к нему подключены не только регистраторы, но и иные крупнейшие интернет-компании, такие как Яндекс, Mail.ru и другие, работающие с контентом пользователей. Все они, обнаружив какую-то подозрительную активность, моментально сообщают, и затем начинается проверка всех доменов данного администратора. Эта деятельность позволила ускорить реакцию на обнаружение зловредной активности и таким образом делать наши доменные зоны чище, а передавая информацию в аналогичные зарубежные организации, борющиеся с противоправным использованием доменных имен в зловредных целях, нам удастся блокировать подобные ресурсы гораздо быстрее.

Помимо всех технических и аналитических средств, одной из самых важных составляющих является также работа по обучению самых разных слоев пользователей, начиная от судейского и депутатского корпусов и заканчивая студентами и школьниками. Подробнее об этом расскажет Новикова Татьяна Ивановна, руководитель наших социально-просветительских проектов.

Т.И. Новикова,

Координационный центр национального домена сети Интернет, Россия

ПРОБЛЕМЫ ЦИФРОВОЙ ГИГИЕНЫ ДЕТЕЙ

Большое спасибо, коллеги!

Все, о чем я хотела сказать в глобальном смысле, уже сегодня прозвучало: и про безопасность человека, и как не стать жертвой социальной инженерии, и аспекты цифровой гигиены и цифровой грамотности, то есть обо всем этом уже сказали.

Я хотела бы остановиться на образовании детей в плане воспитания пользователей, и почему мы обращаем внимание именно на детей. Почему так важно обучать с молодых ногтей пользователей Интернета, потому что все, что мы делаем, все о чем мы говорили в эти 2 дня, в итоге все это адресовано людям, «живущим» в сети, не знающим порой, как это работает, не думающим, как они это используют, не думают о своей безопасности в сети. В связи с этим проблема персональных данных, которая постоянно усугубляется, она заключается в том, что данные оставляют сами пользователи, и они не думают о том, что они делают.

Что касается детей, то никому не придет в голову выпустить одного маленького ребенка в город и на неделю его там забыть, а в Интернет мы почему-то детей отпускаем. И совершенно не думаем, умеет ли он этим пользоваться, и какие риски и угрозы его там подстерегают, какая информация его там встретит, чему он там научится.

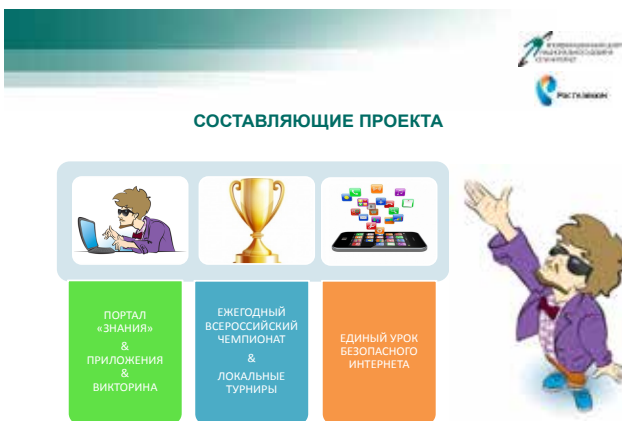
В сентябре-декабре 2018 г. Фондом общественного мнения, компанией «Медиаскоп» и сервисом по анализу информационного поля «Бренданалитикс» (аналитика социальных медиа) было проведено исследование детского сегмента российского Интернета. Результаты исследования показали, что часть Рунета, объединяющая детский контент и его потребителей, – это порядка 24,5 млн. пользователей, включая детей и родителей. А на платформах социальных сетей и видеохостингов – 41 млн. человек. Средний возраст начала пользования Интернетом у детей сегодня – 4 – 5 лет. Более одной трети делают это самостоятельно. И у 44% этих детей 5–7 лет уже есть собственные смартфоны, с которыми они са-



мостоятельно постигают азы Интернета. При этом только 23% родителей используют средства обеспечения безопасности доступа к Интернету, кроме антивирусов.

Отмечу, что с учетом того, что мы уже давно говорим о популяризации безопасности в Интернете, повышении цифровой грамотности, обучении детей пользования Интернетом, их родителей, педагогов, за 3 года доля семей, использующих настройки безопасного детского поиска, выросла с 5% до 23%. По моему мнению, это значительная цифра. При этом в 3 раза выросла доля услуг провайдеров детского Интернета с 4% до 12%. Очевидно, что популяризация проблемы этих вопросов дала свои плоды, и подобных инструментов появляется все больше. Например, недавно социальная сеть «Одноклассники» совместно с компанией Google запустили игровой проект, помогающий пользователям узнать, как работает Интернет, о его угрозах, повысить свою цифровую грамотность и др.

Многие крупные интернет-компании занимаются этим много лет. Приведу некоторые из проектов. Наиболее крупным является проект, охватывающий большую часть детей, – «Ученики до 18 лет». Реализуется этот проект с 2012 года совместно с компанией «Ростелеком», являющейся генеральным партнером этого проекта, в партнерах еще много больших компаний, например, Лаборатория Касперского, Ассоциация Интернет-вещей,



Роскомнадзор. Данный проект в игровой форме дает возможность получить базовые знания об устройстве сети Интернет. В 2017 году данный проект стал финалистом конкурса Ассоциации европейских регистратур. Составляющие проекта: портал «Знание», мобильное приложение, викторина для локальных турниров, работающая также и в офф-лайне. Это ежегодный всероссийский чемпионат, где дети имеют возможность соревноваться как в индивидуальном зачете, так и объединяясь в школьные команды. Этот чемпионат стал довольно популярен, например, в 2018 году было более 11 тысяч участников, и каждый год десятки тысяч школьников принимают участие в проекте.

Единый урок безопасного Интернета, о котором уже было сказано. Приведу немного цифр. Образовательный портал «Знание» насчитывает 141 тысячу пользователей и охватывает все 85 регионов Российской Федерации. Этот инструмент постоянно совершенствуется, и аудитория проекта постоянно растет.

Викторина для локальных турниров построена по формату передачи «Своя игра».

ДОПОЛНИТЕЛЬНЫЕ НАПРАВЛЕНИЯ

- ✓ **Семинары** для сотрудников государственных органов (суды, налоговые инспекции, правоохранительные органы и органы безопасности), представителей бизнеса
- ✓ **Лекции** в вузах и школах для преподавателей и учащихся
- ✓ **Методические пособия и просветительские материалы** (печатные и онлайн версии)

ИТ-МАРАФОН

Одна из дисциплин - локальный турнир по игре «Изучи интернет - управляй им»

Мы объехали с ней очень много городов России, и везде, где проходили мероприятия, ребята с удовольствием принимали в них участие. Более того, этот инструмент переведен и на английский язык, поэтому ее можно адаптировать и под зарубежную аудиторию. Например, на Всемирном фестивале молодежи и студентов в Сочи мы использовали англоязычный контент.

Локальные турниры и IT-марафоны, которые мы проводим совместно со Школой новых технологий «Московская электронная школа», где этот блок проекта включен в одну из дисциплин.

Что касается правовых аспектов, то мы совместно с IP-Club и Московским государственным юридическим университетом им. О.Е. Кутафина проводим конкурс «IP and IT Law», то есть это конкурс юридических работ студентов, которые специализируются на вопросах цифрового права.

В 2019 году на награждении победителей этого конкурса первое место заняла работа «Большие данные: вопрос правомерного использования». Эту работу написала студентка первого курса магистратуры Высшей школы



«ПОЗИТИВНЫЙ КОНТЕНТ»

Конкурс лучших интернет-проектов для детей и молодежи
Проводится совместно с РОЦИТ.

Цели конкурса:

- способствовать созданию и развитию качественных образовательных и развлекательных digital-продуктов, отвечающих современным требованиям информационной безопасности
- содействовать повышению уровня цифровой грамотности пользователей через популяризацию качественных интернет-проектов с позитивным контентом



КОНКУРС САЙТОВ
«ПОЗИТИВНЫЙ
КОНТЕНТ»

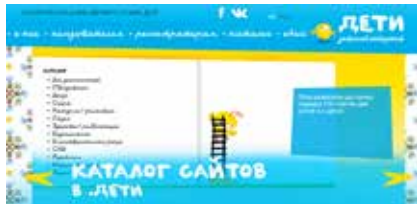


ПОЗИТИВНЫЙ-КОНТЕНТ.ДЕТИ



ДОМЕН .ДЕТИ

- Кириллический домен для размещения сайтов детской тематики
- Круглосуточная система мониторинга вредоносной активности
- Каталог лучших ресурсов в .ДЕТИ
- Интернет-издание «Разумный журнал» о детском интернете



КАТАЛОГ САЙТОВ
в .ДЕТИ



ИНТЕРНЕТ.ДЕТИ

экономики. Второе место с работой «Вопросы правового регулирования E-commerce» занял выпускник Высшей школы экономики 2018 года, а третье место с работой «Правовой режим результатов творческой деятельности искусственного интеллекта» занял студент первого курса магистратуры МГУ.

Все эти молодые люди придут на смену сегодняшним экспертам, занимающимся проблематикой цифрового права. Иными словами, у нас растет хорошая смена.

Также у нас есть конкурс для юных журналистов до 18 лет «Позитивный контент».

«Домен .ДЕТИ» – проект Координационного центра и Фонда «Разумный Интернет». Это кириллический домен, отдельная доменная зона для детских сайтов, где находится

только детский контент. Главное отличие – круглосуточная система мониторинга вредоносной активности. Все сайты, которые включены в этот каталог и находятся в доменной зоне «.ДЕТИ», априори безопасны для детей. Помимо того, что в этом каталоге есть портал наших партнеров «Касперский.ДЕТИ», там имеется и их собственный портал, направленный на образование детей безопасному поведению в сети: как не стать жертвой мошенников, как обращаться с персональными данными, платежными данными, что такое фишинг и др. Все эти знания дети могут получить на этом портале. В этой же доменной зоне Роскомнадзор имеет проект «Персональные данные.ДЕТИ».

Спасибо за внимание!

Г.Р. Солдатова,

Фонд «Развитие Интернет», Россия.

КИБЕРБЕЗОПАСНОСТЬ И ЦИФРОВАЯ ГРАМОТНОСТЬ ПОДРОСТКОВ

Добрый день, уважаемые коллеги!

Я долго думала, какую тему здесь представить, и остановилась на теме, которой лично я, Фонд «Развитие Интернет», Факультет психологии МГУ занимаемся уже более 9 лет. Эта тема связана с исследованием влияния ИКТ на развитие детей и подростков. Поэтому мое выступление будет посвящено детской кибербезопасности и цифровой грамотности.

Причина не только в том, что эти темы мне близки и мы имеем большое количество исследований по этим вопросам, но также и в том, что детская кибербезопасность и цифровая грамотность – важные гуманитарные защиты прав человека, в том числе ребенка в глобальной ИКТ-среде, то есть право ребенка на безопасность и на цифровую грамотность.

Когда в начале этого века ООН ввела категорию цифрового равенства, то среди трех основных аспектов этого понятия, помимо цифровых возможностей и цифровой инклюзии, оказалась еще именно цифровая грамотность.

Во-вторых, казалось бы, вопросы цифровой безопасности далеки от всех тех важных вопросов, которые здесь на очень высоком профессиональном уровне обсуждаются уже третий день. Но это только на первый взгляд.

Международная информационная безопасность – это вид информационной безопасности, и прямо или косвенно она представлена и установками о кибербезопасности, а также уровнями и возможностями грамотного, ответственного и безопасного использования ИКТ разными группами населения внутри стран, которые в свою очередь выступают субъектами информационной безопасности на международном уровне. Среди этих групп населения в число наиболее активно осваивающих цифровое пространство попадают как раз дети и подростки. И именно вопросы детской кибербезопасности и вопросы цифровой грамотности могут стать в недалеком будущем действенной основой формирования норм, правил и принципов ответственного и безопасного поведения в глобальной ИКТ-среде.



Итак. Что мы сегодня можем сказать о вопросах цифровой безопасности и цифровой грамотности подрастающего поколения именно в России. Я хочу коротко представить наше исследование «Цифровая социализация в культурно-исторической перспективе. Внутрипоколенческий, межпоколенческий анализ», финансируемое Российским научным фондом. Мы опросили около 3000 человек в разных федеральных округах России. Это популяционное исследование, сделанное по всем правилам: младшие и старшие подростки, а также родители, свыше 1200 человек, которые имеют детей-подростков такого возраста.

Основные направления исследования включали в себя широкий диапазон, начиная с пользовательской активности и заканчивая взаимодействием с неживыми системами. По данным нашего исследования, 70% детей постоянно общаются с такими чат-ботами, как голосовые помощники, которых сегодня можно отнести к прообразу искусственного интеллекта.

Хотела бы представить портрет цифрового поколения с точки зрения использования ими Интернета. Так как это уже пятое популяционное исследование, мы имеем возможность сравнить данные. Группа с высокой степенью использования Интернета – в среднем 6 часов в сутки, группа с очень высокой степенью использования Интернета – это то, что мы сейчас



«There is no forever childish, but there is a **historically childish**»
L.S. Vygotsky



«The development of **childhood** as a sociocultural phenomenon is not just its lengthening, but a **qualitative change in structure and content**»
D.B. Elkonin

The cognitive and personal development of the digital generation takes place in some other form, subject to a different logic. The complex interaction of traditional activities with online activities leads to a qualitatively different result:
NEW LIFE STYLE OF A MODERN CHILD



Project: "DIGITAL SOCIALIZATION IN A CULTURAL-HISTORICAL PERSPECTIVE: INTERGENERATIONAL AND INTERGENERATIONAL ANALYSIS"

with the support of the Russian Science Foundation

Purpose: to study the features of digital socialization among representatives of different generations

Geography of research: 8 federal districts of the Russian Federation, 15 cities

Data collection: 2018-2019

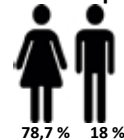


Sample study: 2 generations, 2778 people

Adolescents – 1553 people
12-13 years old (471) 14-17 years old (1082)



Parents - 1219 people



называем гиперподключенностью, – 9 часов в сутки. Обратите внимание, что 29% подростков 12–13 лет используют Интернет в среднем 6 часов и более. Подростки 14–17 лет – 51%. Это количество детей очень резко увеличилось по сравнению с 2013 годом. В 2019 году мы должны уже понимать, что для этой категории использование Интернета в таком временном объеме стало нормой. Интенсивность использования Интернета увеличивается у подростков от будней к выходным, а у родителей – обратная тенденция. Мы видим, что по времени дети и родители очень расходятся, и по выходным они отдыхают в разных мирах.

Сегодня мы четко не различаем онлайн и офлайн-реальность, мы сегодня говорим о том, что дети живут в смешанной реальности. При этом каждый второй ребенок отвечает, что живет в обоих мирах и не видит разницы между реальным и виртуальным или переключается между этими мирами в зависимости от времени и задачи. По самым разным данным, мы постоянно получаем подтверждение этой информации, когда практически каждый второй ребенок сегодня живет в смешанной онлайн-реальности.

Хотелось бы поговорить о пространствах, в которых живут дети и подростки. Обращаю внимание на то, что пространственная конфигурация у них тоже различается: дети живут в основном в социальной сети «ВКонтакте», родители живут в основном в социальной сети «Одноклассники». С 20% до 72% возросло количество детей-пользователей YouTube, а также дети мгновенно осваивают новое пространство.

Таким образом, пространственная конфигурация детей и взрослых очень сильно расходится, и она не совпадает.

Другие наши исследования в рамках данного проекта говорят о том, что исследование когнитивных функций, личностных особенностей, социальных контактов и социального капитала, новых социокультурных практик, – все это нам четко показывает, что дети и родители здесь существенно отличаются друг от друга, и эти показатели и представления родителей о том, что дети делают в Интернете, очень сильно расходятся с самооценками детей.

Сегодня мы можем сказать, что достаточно четко снизилась универсальность фигуры родителя и взрослого вообще, в детско-родительских отношениях снизилась роль взрослого, и у взрослых сейчас гораздо меньше возможностей конструировать детство, чем это было раньше. И все нормы, которые были разработаны и приняты в традиционной педагогике и психологии, сегодня трещат по швам.

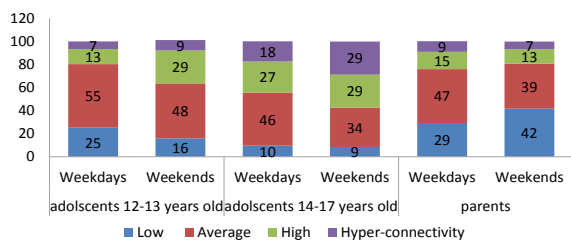
С другой стороны, возможности безопасности. Сегодня мы наблюдаем за тем, что дети сталкиваются с огромным количеством рисков. Мы следим за этим уже очень много лет, разработали классификацию и можем сказать, что каждый второй ребенок признается, что сталкивался с такими ситуациями за последний год, а каждый третий родитель считает, что ребенок его сталкивается с такими ситуациями за последний год намного реже.

Среди всех рисков лидируют коммуникационные, далее – контентные и технические. Риски в настоящее время миксируют, и в соответствии с миксованными рисками возникают новые онлайн-риски, где имеется огромное количество опасностей.

Когда дети живут в ситуации очень высоких рисков онлайн-среды, то здесь очень важно и необходимо иметь определенный уровень грамотности и компетентности. Дан-



Internet use intensity: weekdays VS weekends



Internet use intensity in adolescents increases from weekdays to weekends. Parents have the opposite tendency to decrease activity on the Internet at the weekend. So children and parents often "rest" in different worlds..



How to unify digital worlds of children and adults and to increase the Internet safety level?



ные показатели мы рассматриваем как критическое, безопасное, грамотное поведение в онлайн-среде. Среди критериев можно выделить ответственность и безопасность, которые рассматриваются в разных сферах. В 2013 году мы получили очень низкий уровень цифровой грамотности в своих исследованиях. В 2019 году уровень компетентности родителей и подростков увеличился, причем у подростков с большим отрывом.

В заключение отмечу, что при изменившемся в лучшую сторону отношении государственных органов и различных организаций к проблематике цифровой грамотности у подростков, тем не менее, делается настолько мало всего, что мы должны к этому вопросу отнестись очень серьезно.

Интересен тот факт, что представленные данные с небольшим различием существуют в странах Европы и США. В рамках наших совместных проектов мы имеем возможность эти данные сравнивать. Везде присутствует широкий круг киберугроз, изменившийся уровень цифровой грамотности, а также серьезным образом изменившийся характер межпоколенческих отношений. Этот комплекс проблем требует еще большего внимания к ним государства, бизнеса и гражданского общества, что является сферой частно-государственного партнерства. Необходима широкая информа-

ционно-просветительская деятельность не только среди подростков, но и среди взрослых по проблемам, возникающим в связи с существующими онлайн-рисками и постоянно появляющимися новыми, в том числе и рисками международной информационной безопасности.

Цифровая грамотность – важнейший навык 21-го века и гарант безопасности и успешности как на личном уровне, так и в групповом и международном контексте. В то же время около 80% детей до сих пор, а взрослых тем более, изучают премудрости цифровой грамотности либо самостоятельно, либо с помощью друзей и знакомых.

Значимость этого вопроса и вопроса необходимости профессионального обучения цифровой грамотности ставит его в приоритетный фокус внимания тех, кто определяет сегодня не только политику в IT-сфере, но и образовательную политику.

Таким образом, ответственное, безопасное и грамотное поведение в цифровом пространстве и соответствующее отношение к кибербезопасности должно закладываться в детстве наравне с другими правилами безопасной жизнедеятельности. Каким вырастет это поколение с этой точки зрения, такими и будут наши гарантии в недалеком будущем, в том числе и на стратегическую стабильность.

Спасибо за внимание!

Е.А. Михайлова,

*Факультет государственного управления
МГУ имени М.В. Ломоносова*

НОВЫЕ МЕДИА В ИНФОРМАЦИОННОМ СОПРОВОЖДЕНИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ: СЛАКТИВИЗМ¹

Взаимодействие человека с политической сферой жизни общества происходит посредством информационно-коммуникационных каналов. Политическая повестка дня, баланс сил на государственной и международной арене – «сверка часов» по этим и другим вопросам происходит именно в публичном коммуникационном пространстве.

Данное пространство постоянно трансформируется, развивающиеся ИКТ открывают все новые способы коммуникации политических акторов с обществом, артикуляции позиций лидеров мнений и групп давления, а также налаживания эффективной обратной связи.

По данным Левада-центра по состоянию на декабрь 2019 года 81% россиян являются интернет-пользователями, 2/3 взрослого населения страны – это ежедневные пользователи, в возрасте от 18 до 24 лет данный показатель – 94%. В этой связи вопрос актуальности использования возможностей интернет-коммуникации для установления связи политических акторов с электоратом находится сейчас в фокусе внимания как профессиональных политтехнологов, так и общественных активистов.

Несмотря на то, что существующий общемировой тренд «социальной дипломатии» (публичная коммуникация посредством социальных сетей) только прогрессирует, в российском политическом дискурсе активность политиков в новых медиа пока не становится нормой.

В недавнем большом интервью АиФ, данном пресс-секретарем Президента Дмитрием Песковым, последний так высказывается о своем присутствии в социальных сетях: «Я ни разу в жизни не заходил в Facebook, никогда не был в «Одноклассниках», я не знаю, как выглядит «ВКонтакте» изнутри. У меня нет такой потребности, и я не хочу себя заставлять.» В том



же интервью он предложил политическим деятелям удалить мессенджер Telegram со своих устройств и «жить спокойно».

Важным фактором осторожного отношения политических деятелей нашей страны к онлайн-активности представляются принятые в середине 2016 года поправки в Федеральный закон «О государственной и гражданской службе», предусматривающие необходимость чиновникам отчитываться об имеющихся аккаунтах в социальных сетях в целях контроля соблюдения государственными служащими принципов профессиональной этики. В качестве реакции на нововведение стал массовый уход госслужащих из всех социальных сетей «от греха подальше».

По словам заместителя министра цифрового развития, связи и массовых коммуникаций РФ Алексея Волина: «...есть два больших заблуждения, которые часто приходится слышать: первое – телевизор никто не смотрит, все смотрят интернет, второе – все не читают СМИ, все пользуются социальными сетями». Действительно, на сегодняшний день телевидение остается лидирующим каналом политической коммуникации с целевой аудиторией. Тем не менее, в отчете, подготовленном Левада-центром, отмечается, что в молодежной среде существенно снизилось (и продолжает снижаться) число тех, кто использует телеви-

¹ Выступление опубликовано в 3 номере журнала «Международная жизнь» за 2020 год.

Слактивизм. Современные ИКТ как инструмент формирования и артикуляции общественного мнения

Екатерина Михайлова
Факультет государственного управления
МГУ им. М.В. Ломоносова

Апрель, 2019

дение как главный источник новостей, а число тех, кто ежедневно читает газеты, за последние 25 лет снизилось в 13 раз и сейчас составляет только 5%.

По данным фонда «Общественное мнение» 46% юношей и девушек в возрасте от 14 лет до 21 года не смотрят телевизор. Еще 38% постепенно отказываются от телевидения в пользу других источников информации. Из этого следует, что в России, как и в других развитых странах, в «молодежном сегменте» целевой аудитории есть постоянно расширяющаяся группа, не использующая традиционные СМИ для получения политических новостей и формирования своей политической повестки дня, а текущие тенденции дают основания полагать, что в дальнейшем этот процент будет только увеличиваться за счет естественного выбытия аудитории традиционных СМИ и того факта, что повзрослевший «молодежный сегмент» не начнет внезапно читать газеты, слушать радио и смотреть телевизор. В этой связи перед политическими акторами встает вопрос о способе донесения своей повестки дня до данного сегмента.

Политическая полемика на просторах социальных сетей, инициация разнообразных онлайн-акций получили сводное наименование «слактивизм». Несмотря на то, что изначально термин образовался как производное от английских слов «халтурщик» и «активизм» и имел в этой связи исключительно негативную коннотацию, в настоящее время все чаще можно встретить нейтральные и, на наш взгляд, более точные дефиниции.

Так, Кембриджский словарь дает следующее определение слактивизма: «...деятельность, использующая интернет для поддержки политических или социальных инициатив, не



Популярность интернет-коммуникации в России

- ✓ 76% россиян старше 18 лет являются интернет-пользователями
- ✓ из них 57% опрошенных – это ежедневные пользователи
- ✓ в возрасте от 18 до 24 лет данный показатель – 90%.
- ✓ за последние 25 лет число тех, кто ежедневно читает газеты, снизилось в 13 раз и сейчас составляет только 5%
- ✓ новости из сети получает каждый второй респондент с высшим образованием и каждый второй житель Москвы

требующая больших усилий (например, создание или подписание онлайн петиций)». Далее мы рассмотрим спектр возможностей по эффективному применению социальных сетей в рамках кампаний по информационному сопровождению государственной политики, тем самым обосновав необходимость употребления именно коннотативно нейтрального определения данного феномена.

На наш взгляд, негативная оценка использования слактивистского инструментария в политических коммуникациях связана в первую очередь с отсутствием научного консенсуса по вопросу трактовки понятия слактивизм.

Некоторые американские авторы считают, что двумя признаками, определяющими слактивизм, являются личностное удовлетворение и политическая неэффективность. Следствием данной трактовки является разделение агитационной интернет-деятельности на успешную (т.е. интернет-активизм) и неэффективную (т.е. слактивизм). Несмотря на то, что в рамках данного определения негативная характеристика слактивизма оправдана, в современном научном дискурсе часто встречаются публикации, в которых любая политическая деятельность в социальных сетях априори относится к категории слактивизма, что вызывает предубеждение против применения его «арсенала».

В то же время, не вызывает сомнений тот факт, что социальные сети являются одним из ключевых элементов социализации молодых людей. В этом качестве они имеют большой потенциал влияния на политические воззрения молодежи, и если в борьбу за умы не включаются представители официальной власти, их место занимают оппозиционные лидеры, чьи критические лозунги и призывы

Slacktivism

Slacker + Activism
(Халтурщик + Активист)



Эксперимент Андреаса Колдинг-Йоргенсона (2009 г., Дания)

Было создано Facebook-сообщество, посвященное (якобы) протесту против готовящегося сноса памятника. За две недели число участников группы с 125 человек выросло до 27,5 тыс.чел.

Фонтан Сторка



к радикальным действиям могут встретить активную поддержку в связи с использованием эмоционально «заряженных» элементов.

Оценка эффективности слактивизма зависит от «угла обзора», подтверждением чему является эксперимент, проведенный А. Колдинг-Йоргенсоном. Задачей его исследования стало определение эффективности горизонтальных коммуникаций в Facebook-сообществе при обсуждении общественно значимых проблем.

Он создал в Facebook группу, призывающую бороться с выдуманной проблемой: якобы власти Копенгагена планируют снести одну из известных достопримечательностей города – фонтан Сторка. Изначальную аудиторию группы составляли всего 125 человек, которые согласились вступить в нее для создания стартового импульса. За две недели численность группы возросла до 27,5 тысяч человек. При этом абсолютное большинство участников отказывались верить в то, что снос фонтана – лишь плод воображения автора. Также последующий анализ деятельности группы показал, что лишь небольшой процент членов группы внимательно прочитал контент и перешел по ссылкам, показывающим, что новость является фейком. Примечательным является тот факт, что не все, кто получил доказательства выдуманности данного инфоповода, до конца поверили, что фонтану не грозит демонтаж.

Колдинг-Йоргенсон пришел к выводу о том, что абсолютное большинство пользователей вступают в такие группы исключительно для того, чтобы «отметиться» там и тем самым поддержать общественно-значимый проект, не стремясь к дальнейшим действиям по защите памятника архитектуры.

Несмотря на то, что опыт Колдинг-Йоргенсона был призван доказать неэффективность слактивистского инструментария для политической коммуникации, приведенные им данные о разрастании группы «онлайн протестующих», напротив, являются прямым доказательством эффективности слактивистской деятельности в области распространения информации.

Специалист по вопросам стратегии в области социальных медиа Джай Смит замечает, что, действительно, лишь немногие из поддержавших онлайн протест готовы отстаивать свою позицию более деятельно, тем не менее, «...в основе изменений лежит осведомленность... и люди никогда не начнут волноваться о чем-то, пока не узнают об этом».

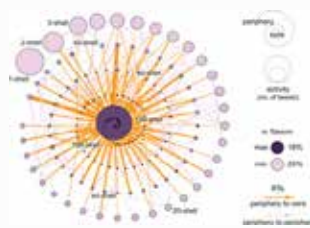
По данным исследований только 3,5% инфоповодов «начинаются» в социальных сетях. Это можно расценивать как дополнительное доказательство того, что слактивистская деятельность не является настолько важной, чтобы государство учитывало ее при создании архитектуры политической коммуникации. Данное утверждение, на наш взгляд, свидетельствует о достаточно узком понимании спектра задач, которые могут быть решены посредством этого канала массовой коммуникации.

Интерес представляет тот факт, что модель распространения политической протестной информации (дерево репостов и его последствия) имеет свои особенности, отличающие ее от модели распространения развлекательных материалов. Группа исследователей во главе с профессором Лондонской школы экономики Пабло Барбера, изучив процесс распространения информации на примере трех различных политических протестных



Эксперимент группы П.Барбера «Влияние критической периферии на рост социальных протестов»

Периферические участники критически необходимы для распространения информации протестного характера, они так же способствуют созданию онлайн-контента, как и ключевые участники



Возможности slacktivismа

- Распространение информации на широчайший круг реципиентов
- Возможность пройти за «стену белого шума» к молодой аудитории
- Универсальный, трансграничный и бюджетный способ объединения людей
- Предлагает пользователю быстро занять позицию по политическому вопросу
- Канал получения обратной связи

инициатив в Твиттере, выявили общую для них закономерность.

Они установили, что информацию о протестных политических акциях люди с большой готовностью репостят, добавляя свои комментарии, ссылки и обогащая дискуссию, даже если не имеют прямой связи с «центром» протеста. При этом отмечается, что вклад каждого отдельного периферийного актора невелик, но их сила – в количестве. Результатом исследования стал вывод о том, что «...периферические участники критически необходимы для распространения информации протестного характера, они так же способствуют созданию онлайн-контента, как и ключевые участники».

Основной функцией slacktivismа в политических коммуникациях является распространение информации на широчайший круг реципиентов. Дженнифер Эрл и Катрина Кимпорт в книге «Социальные трансформации, обеспеченные высокими технологиями» отмечают, что благодаря развитию технологий 2.0, людям «...стало не обязательно быть вместе, чтобы действовать вместе», и данные условия определенно закладывают основу для серьезных изменений в социальной и политической повестке дня, игнорировать которые (полностью или частично) просто недопустимо для политических акторов.

Также важным положительным аспектом slacktivistской деятельности является способность построить эффективную коммуникацию с той группой целевой аудитории, которая по разным причинам не пропускает политическую повестку дня за свою стену информационного белого шума.

Одной из причин критики slacktivismа, наряду с узостью трактовки данного понятия,

является расхождение авторов в понимании успешности той или иной политической акции. Многие исследователи утверждают, что slacktivism без оффлайн акций не в состоянии спровоцировать политические или социальные изменения.

Действительно, slacktivism – это универсальный, трансграничный и бюджетный способ объединения людей, не согласных с тем или иным аспектом социально-политической жизни общества. Но то, что он требует меньше усилий, совершенно не обязательно означает, что он менее полезен. Следуя такой логике, можно прийти к выводу, что чем больше ресурсов – человеческих и финансовых – будет вложено в акцию, тем более она успешна, что, конечно, срабатывает не всегда.

Профессор университета Аризоны отмечает, что даже в 60-х годах прошлого века политические демонстрации, будучи эффективными для привлечения внимания к остросоциальным проблемам, приносили мало результата, когда касались глубоко укоренившихся мировоззренческих норм, таких, как аборты, легализация однополых браков и т.п.

Действительно, далеко не каждая революция и не каждый протест современности происходит благодаря социальным сетям. Так, существует мнение о том, что особая популярность социальных сетей в странах Арабской весны была обусловлена тем, что в отличие от развитых стран там нет укрепившейся традиции нормативных институтов артикуляции мнений: манифестаций, профсоюзов, праймериз, петиций и прочих начинаний «снизу» (grassroots initiatives). Таким образом, slacktivistские акции являются своего рода «виртуальными костылями», помогающими строить гражданское общество, которое формирова-



Обязательно ли переводить онлайн-активизм в оффлайн-акции?

- «Выход на улицы» не всегда приводит к успешному результату
- Не все сторонники оффлайн акции имеют возможность присоединиться к ней, а солидарность с акцией остается
- Оффлайн акции без «штурма баррикад» менее эмоционально заряжены, а значит следует ждать провокаций
- Риск эскалации



- Слактивистом может быть любой человек
- Если в соцсети не идет официальная власть, туда идут радикалисты и оппозиционеры, не встречая конкуренции
- Данные о слактивистских акциях доступны заграничным политтехнологам и могут использоваться для «расшатывания лодки»
- Лайк имеет значение



лась в западных странах путем многовековой эволюции. Это является ярким аргументом в пользу того, что к цели можно прийти многими путями, и совершенно не обязательно повторять длинный, извилистый путь, пройденный пионерами в том или ином направлении, если со временем построена «скоростная магистраль».

Многие скептики отмечают, что произошедшие революции 2.0 далеко не всегда проходили быстро и бесповоротно (что, по их мнению, доказывает неэффективность слактивизма как инструмента координации групп и артикуляции позиций), но то же самое можно сказать о революциях прошлых веков. Революционные движения сформированы не по принципу единого ядра и периферии: революционеры – это совокупность групп, каждая из которых имеет свой взгляд на будущее страны, но все они объединены неприятием существующего строя. После его свержения в «верхах» победителей начинаются противоборства, и их итог может быть крайне печальным для всех.

Слактивистские протесты, благодаря своей трансграничности, могут привести под одни знамена те группы, которые и не узнали бы друг о друге в оффлайне, поскольку находились на абсолютно не пересекающихся линиях жизни социума. Тем не менее, эффективная работа с слактивистскими протестами открывает возможности для государства по сохранению конфликта в законных рамках, снижению напряженности и исключению его эскалации.

Часто слактивистов обвиняют в том, что они боятся отстаивать свои интересы в формате оффлайн сопротивления, без которого невозможно добиться желаемого результата: марши протеста, митинги и т.п. Но не следует

забывать, что такие открытые акции представляют колоссальный риск и для представителей государственной власти. Когда человек стоит в толпе своих мнимых соратников, он перестает мыслить и действовать как отдельный индивид, он становится частью группы, и в ход идет уже психология масс. Если правильно ею воспользоваться, можно добиться от людей действий, которые они никогда бы не совершили, будучи вне влияния толпы, и данная атмосфера имеет мало общего со свободой осознанного волеизъявления.

Подобной эскалации государство может избежать, если будет активнее работать с слактивистскими протестами: отвечать на запросы, участвовать в онлайн-обсуждениях, переносить их в русло традиционного политического процесса работы с обращениями граждан, назначения встреч и общественных слушаний и так далее.

Наконец, стоит сказать еще об одной важной для государства функции слактивистских акций, которая заключается в получении актуальной обратной связи от аудитории. Слактивизм является отличным маркером направленности и динамики социально-политических настроений большой группы людей.

- слактивистом может быть любой человек, безотносительно своих полоролевых, физиологических, географических и социальных детерминант;
- существует доказанная эффективность слактивистских акций при формировании и артикуляции мнений больших групп населения, их информирования и мобилизации. Также исследования показывают существенное отличие принципов формирования и распространения политического контента от



«... Не твиты свергают правительства, а люди»

- Во главе угла стоят люди, их потребности и возможности, ожидания и реакции, и нет «хороших» и «плохих» способов взаимодействия с ними, есть технологии, подходящие к конкретной ситуации и не подходящие

Thank you for your attention!



развлекательного в социальных сетях, что дает право говорить о самостоятельности феномена slacktivism;

- пользователями социальных сетей в большинстве своем являются молодые люди – социальная группа, более восприимчивая к радикальной агитации с одной стороны и менее вовлеченная в информационное взаимодействие с действующей властью посредством традиционных СМИ – с другой;
- пока государственные политические акторы признают нецелесообразным активное участие в slacktivistских акциях, их инициируют оппозиционеры, которым сложно прорваться на центральные каналы и в газеты, но легко – в социальные сети и блоги;
- зарубежные аналитики получают такой же доступ к данным о slacktivistских протестах и настроениях, какой есть у отечественных специалистов, а, следовательно, эти данные активно используются для «расшатывания лодки» извне;

Эффективность той или иной политической акции определяется результатом, к ко-

торому она привела: поставив перед собой желаемую цель, актору необходимо проанализировать весь спектр методов ее достижения и выбрать ту конфигурацию каналов информационного сопровождения, которая наиболее эффективно сработает в каждой конкретной ситуации. Конфигурация может включать в различных пропорциях оффлайн- и онлайн-активизм, вклад каждого из них будет обусловлен рядом факторов, поскольку у каждого из них есть свои сильные и слабые стороны. И если акторы, соглашаясь со скептиками slacktivism, любые акции в социальных сетях априори рассматривают как неэффективные, невоплощенные в реальные изменения и т.п., это приводит к тому, что они сами ставят искусственные ограничения на пути к желаемому результату.

Один из исследователей slacktivism отметил, что «... не твиты свергают правительства, а люди». Именно об этом стоит помнить: во главе угла стоят люди, их потребности и возможности, ожидания и реакции, и нет «хороших» и «плохих» способов взаимодействия с ними, есть способы, подходящие к конкретной ситуации и не подходящие.

Для заметок