МЕЖДУНАРОДНАЯ ЖИЗНЬ

Гармиш-Партенкирхен
2017

ГОСУДАРСТВО • БИЗНЕС • ГРАЖДАНСКОЕ ОБЩЕСТВО • ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Digest 2016

INTERNATIONALES LEBEN

Probleme der Aussenpolitik, der Diplomatie und der nationalen Sicherheit

Н.А.Симония, А.В.Торкунов

Глобализация

структурный кризис и мировое лидерство

мифы и реальность

2013

Библиотека «Международной жизни»

文摘 2016

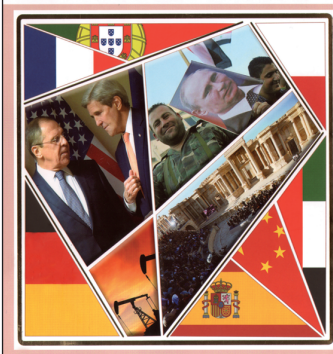
国际生活

俄罗斯对外政策、外交和国家安全

Digest 2016

الاحداث السياسية الدولية

قضايا السياسة الخارجية، والدبلوماسية، والأمن القومي



INTERNATIONAL AFFAIRS

МЕЖДУНАРОДНАЯ ЖИЗНЬ

Special issue

BRICS RUSSIA UFA 2015

BRICS 2014 Fortaleza · Brasil

Digest 2016

LA VIE INTERNATIONALE

Politique étrangère, diplomatie, sécurité nationale

Декабрь 2016

МЕЖДУНАРОДНАЯ ЖИЗНЬ

Проблемы внешней политики, дипломатии, национальной безопасности

С Новым, 2017 годом!

Российское направление: Б.Обама оставляет после себя просто руины

Сергей Рябков

Заместитель министра иностранных дел России

О наследии Пан Ги Муна и глобальных проблемах

Виталий Чуркин

Постоянный представитель России при ООН

25 лет СНГ: мы обречены быть вместе

Сергей Лебедев

Председатель Исполнительного комитета - исполнительный секретарь СНГ

Братислава-2016

«Россия и Европа: актуальные проблемы современной международной журналистики»

Москва. Издается с марта 1922 г.

Special Issue 2010

INTERNATIONAL AFFAIRS

RUSSIA – ASEAN

www.INTERAFFAIRS.ru

VOLUME 59 NUMBER 2, 2013

International Affairs

A Russian Journal of World Politics, Diplomacy and International Relations

In This Issue

Press Conference of Sergey Lavrov

On the New Security Architecture in Asia-Pacific

Russian Muslims and the "Arab Spring"

Eurasian Vector of Development

Citizen Voting Rights in the 2012 U.S. Election

The Little World War in South America

Stalingrad, an Imperative of History

east view

Приложение к журналу «Международная жизнь»

ГОСУДАРСТВО • БИЗНЕС • ГРАЖДАНСКОЕ ОБЩЕСТВО • ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

XI Международный форум

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

Гармиш-Партенкирхен, Германия
24–27 апреля 2017 года

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

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

Научные редакторы:
Редактор журнала «Международная жизнь»
А.Д.Дубина
Обозреватель журнала «Международная жизнь»,
кандидат исторических наук
И.И.Кравченко

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

Выпускающий редактор и дизайн:
И.Н.Знатнова

Верстка:
А.С.Родченкова
М.С.Тюрина

Материалы, публикуемые в приложении к журналу «Международная жизнь» Государство • Бизнес • Гражданское общество • Информационная безопасность, не обязательно отражают точку зрения редакции

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

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

Тираж 4600. Цена свободная.
Дата выхода в свет 08.11.2017. Заказ №.14
Компьютерный набор, верстка и дизайн редакции.
В оформлении дизайна обложки использовалась информация из презентации Kaspersky.

© Редакция журнала «Международная жизнь». 2017.

МЕЖДУНАРОДНАЯ ЖИЗНЬ

СОДЕРЖАНИЕ

XI Международный форум

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

24 апреля 2017 г.

Пленарное заседание

Владислав Шерстюк, *сопредседатель оргкомитета форума, советник секретаря Совета безопасности РФ, директор Института проблем информационной безопасности МГУ им. М.В.Ломоносова*

Актуальные проблемы формирования системы международной информационной безопасности 10

Приветствие **Олега Храмова,** *сопредседателя оргкомитета форума, заместителя секретаря Совета безопасности РФ* 17

Приветствие **Виктора Садовничего,** *академика, ректора МГУ им. М.В.Ломоносова* 18

Андрей Крутских, *специальный представитель Президента РФ по вопросам международного сотрудничества в области информационной безопасности, посол по особым поручениям*
Актуальные проблемы международного сотрудничества в области информационной безопасности 19

Владислав Гасумянов, *вице-президент - руководитель блока корпоративной защиты ПАО «ГМК «Норильский никель»*
Актуальные векторы угроз в киберпространстве: взгляд «Норильского никеля» 25

Вени Марковски, *вице-президент ICANN по взаимодействию с ООН*
Дискуссии в ООН и межправительственных организациях - принцип «мультистейкхолдеризма» и многосторонняя дипломатия 32

Чарльз Барри, *Институт национальной стратегии Университета национальной обороны США*
Перспективы подходов США и ЕС к защите критически важной инфраструктуры 35

Анатолий Смирнов, *президент Национального института исследований глобальной безопасности, Чрезвычайный и Полномочный Посланник РФ*
Киберпроекты НАТО в дискурсе гибридных войн - взгляд из России 38

Армен Оганесян, *главный редактор журнала «Международная жизнь»* 41

XIV Научная конференция Международного исследовательского консорциума информационной безопасности (МИКИБ)

Владислав Шерстюк, *сопредседатель оргкомитета форума, советник секретаря Совета безопасности РФ, директор Института проблем информационной безопасности МГУ им. М.В.Ломоносова* 43

Ноюнг Пак, *Центр киберправа Университета Корё (Республика Корея)*
Как осуществить универсализацию норм, согласованных на уровне ГПЭ ООН 44

Павел Пилюгин, *Институт проблем информационной безопасности МГУ им. М.В.Ломоносова*
Проблемы определения «виртуальных границ» - зоны ответственности государств в ИКТ-среде 46

Хиро Фудзимаки, *Университет Токай (Япония)*
Международное взаимодействие в области кибербезопасности в евразийских государствах - сотрудничество или соперничество? 54

Адам Хэдли, *Фонд «ИКТ ради мира» (Швейцария)*
Противодействие использованию ИКТ в террористических целях 57

Санджай Гоел, *Университет штата Нью-Йорк (США)*
Важность атрибуции в реализации мер укрепления доверия и норм в киберпространстве 63

Ринат Шаряпов, *ответственный секретарь МИКИБ* 68

25 апреля 2017 г.

Семинар - «круглый стол» №1

Механизмы выполнения правил ответственного поведения государств в ИКТ-среде

Андреас Кюн, *Институт Восток-Запад*
Создание негосударственных норм: роль технических сообществ и последствия для государственной политики 71

Энекен Тикк, *Лейденский университет (Нидерланды),*
Мика Кертуннен, *Институт киберполитики (Эстония)*
Принципы международной информационной безопасности . . 75

Михаил Якушев, *ICANN*
Фактор доверия в обеспечении информационной безопасности: опыт корпорации ICANN 83

Татту Мамбеталиева, *Общественный фонд «Гражданская инициатива интернет-политики» (Киргизия)*
Потенциал субрегионального сотрудничества как один из механизмов выполнения правил ответственного поведения государств в ИКТ-среде 88

26 апреля 2017 г.

Семинар - «круглый стол» №2
Сессия 1

Потенциал использования ИКТ в военно-политических целях в контексте стратегической стабильности

Анатолий Стрельцов, *Институт проблем информационной безопасности МГУ им. М.В.Ломоносова* 92

Дженис Хэмби, *Колледж информационного и киберпространства Университета национальной обороны США* . . 93

Вадим Запивахин, *Генеральный штаб Вооруженных сил Российской Федерации* 95

Найджел Инкстер, *Международный институт стратегических исследований (Великобритания)* 100

Джон Мэллори, *Массачусетский технологический институт (США)* 102

Эльза Кания, *Группа выработки долгосрочных стратегий* 104

Томас Уингфилд, *Национальный университет обороны США* 108

Чарльз Барри, *Институт национальной стратегии Университета национальной обороны США* 113

Анатолий Стрельцов, *ИИнститут проблем информационной безопасности МГУ им. М.В.Ломоносова* 114

Владислав Шерстюк, *сопредседатель оргкомитета форума, советник секретаря Совета безопасности РФ, директор ИИнститута проблем информационной безопасности МГУ им. М.В.Ломоносова* 120

Филипп Бомард, *Политехническая школа Парижа (Франция)* 120

Семинар - «круглый стол» №2
Сессия 2
Потенциал использования ИКТ в военно-политических целях в контексте стратегической стабильности

Джон Мэллори, *Массачусетский технологический институт (США)*
Управление конфликтами и деэскалация в условиях многоуровневого киберконфликта 122

Энекен Тикк, *Лейденский университет (Нидерланды),*
Мика Кертуннен, *ИИнститут киберполитики (Эстония)*
Стратегическая стабильность в киберпространстве 127

Павел Карасев, *ИИнститут проблем информационной безопасности МГУ им. М.В.Ломоносова*
Актуализация содержания понятия «стратегическая стабильность» 129

Андрей Масалович, *«ДиалогНаука» (Россия)*
Армии «умных ботов» - инструмент достижения превосходства в информационном пространстве 137

Наталья Ромашкина, *ИИнститут мировой экономики и международных отношений им. Е.М.Примакова РАН*
Обеспечение информационной безопасности - одна из составляющих стратегической стабильности . . . 150

Филипп Бомард, *Политехническая школа Парижа (Франция)*
Деэскалация роботизированной войны 157

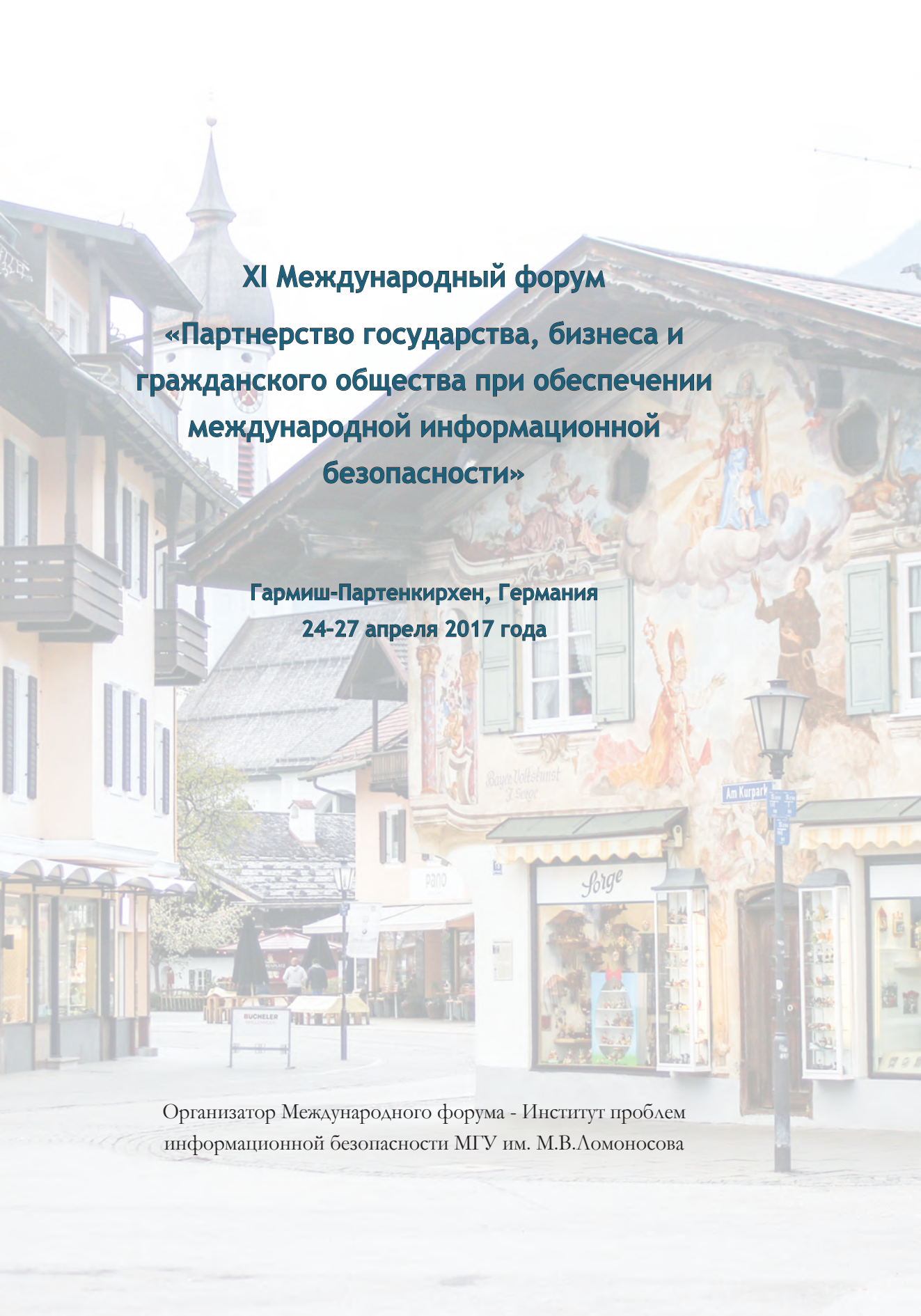
Семинар - «круглый стол» №3
Проблемы обеспечения информационной безопасности критически важных объектов промышленности

Чарльз Барри, *Институт национальной стратегии Университета национальной обороны США* 164

Андрей Ярных, *«Лаборатория Касперского» (Россия)*
Уязвимости и новые угрозы для критически важной инфраструктуры 166

Томас Ламанаускас, *Вымпелком Европа*
Обзор юрисдикций государств в киберпространстве: вызовы для IT-бизнеса 170

Александр Баранов, *Национальный исследовательский университет «Высшая школа экономики» (Россия)*
Обеспечение информационной безопасности объектов промышленности - необходимое условие развития человечества 175



XI Международный форум

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

Гармиш-Партенкирхен, Германия

24-27 апреля 2017 года

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

Гармиш-Партенкирхен, Германия

Пленарное заседание

Актуальные проблемы формирования системы международной информационной безопасности

Владислав Шерстюк, сопредседатель оргкомитета форума, советник секретаря Совета безопасности РФ, директор Института проблем информационной безопасности МГУ им. М.В.Ломоносова: За 11 лет наш форум, проходящий в Гармиш-Партенкирхене, превратился в уникальную внеблоковую площадку для встреч представителей заинтересованных государств, экспертов в различных областях деятельности человечества, связанных с развитием и применением ИКТ. Об этом говорит и количество участников форума - более 100 человек.

Как правило, в работе форума принимают участие представители ведущих государств в области развития ИКТ. Их усилия направлены на исследование проблем обеспечения стабильности и безопасности глобального информационного пространства и его национальных сегментов. На форуме участники могут свободно и открыто обсуждать наиболее острые вопросы, возникающие в результате злонамеренного и враждебного использования ИКТ как государственными, так и преступными, в том числе и террористическими, организациями.

За год после нашей последней встречи мир существенно изменился. Стремительно растет количество интернет-сайтов, а также людей, использующих информационную телекоммуникационную инфраструктуру в повседневной и профессиональной жизни. По некоторым данным, на конец 2016 года число доменных имен, зарегистрированных во всех общих доменах высокого уровня, достигло 329 млн. 900 тысяч. В 2015 году их было 314 миллионов. На конец 2015 года количество пользователей Интернета составило 3,5 миллиарда, а на конец марта 2017 года эта цифра возросла до 3,7 миллиарда. Большинство государств мира ощущают на себе позитивные последствия широкого применения ИКТ, повышения эффективности экономической деятельности и расширения возможностей системы образования, активизации научных исследований в различных сферах человеческой деятельности.

Особым явлением было развитие ИКТ-среды и промышленного Интернета. С этим мы будем жить в ближайшее десятилетие. Такие понятия представляют собой единую сеть, соединяющую окружающие нас предметы с виртуальным миром. В 2008 году компания «Сыск» сообщила о том, что количество устройств, подключенных к Интернету, превысило число людей на Земле. А к 2020 году оно возрастет до 50 миллиардов.

Как вы понимаете, наряду с несомненными неудобствами это приведет к возникновению большого числа новых, еще пока неосознанных угроз для человека и общества. На базе достижений искусственного интеллекта развивается робототехника, появляются роботы различного направления, в том числе автономные боевые роботы, которые, по существу, могут рассматриваться как мобильные устройства ИКТ-среды.

По сообщениям СМИ, около 40 стран - США, Россия, Великобритания, Франция, Китай, Израиль, Южная Корея и другие - ведут разработки роботов, способных воевать без человеческого участия. Считается, что рынок подобных вооружений может достигать 20 млрд. долларов. 30 государств разрабатывают и производят до 150 типов беспилотных летательных аппаратов, из них 80 приняты на вооружение 55 армиями мира. Все эти автономные системы могут быть уязвимы для кибератак.

К сожалению, развитие ИКТ, их использование в различных сферах деятельности не сделали мир безопасным и более комфортным для людей. Продолжает возрастать опасность угрозы враждебного использования ИКТ в целях силового разрешения международных споров по поддержанию деятельности международных террористических организаций, совершению трансграничных нарушений корыстной направленности, нарушению прав и свобод человека. Становится трендом современной международной политики использование фейковых событий в качестве повода для нагнетания международной напряженности. Все более сложными и изощренными становятся компьютерные атаки, количество которых на критически важные объекты и инфраструктуры государственного управления, кредитно-финансовой сферы не уменьшается.

Секретарь Совета безопасности РФ Николай Патрушев сообщил, что в 2016 году количество кибератак на сайты госорганов увеличилось, было зафиксировано около 52,5 млн. случаев, а в 2015 году их было 14,4 миллиона. За один год произошло их трехкратное увеличение. По данным ФСБ России на январь 2017 года, за последние годы ущерб от хакерских атак по всему миру составил, по разным оценкам, от 300 миллиардов до 1 трлн. долларов. Эти потери составляют от 0,4 до 1,5% мирового ВВП и имеют тенденцию к неуклонному росту. В связи с этим повышается риск враждебного использования ИКТ для нарушения работоспособности критически важных объектов и инфраструктур со стороны международных террористических организаций, а также некоторых государств.

Реальные, виртуальные и фейковые события превращают современную информационную сферу в фантасмагорию и создают значительные неопределенности в политической жизни человека. В связи с обвинением России в якобы имеющихся случаях хакерских атак пресс-секретарь главы РФ Дмитрий Песков в интервью американскому каналу NBC рассказал, что интернет-сайт президента подвергается атакам хакеров сотни, а иногда и тысячи раз в день. Атаки идут в том числе и с терри-

тории США. Но, отметил Д.Песков, никто не обвиняет в заказе кибератак лично Президента США или Белый дом.

Доверие между государством, бизнесом и частным сектором в киберпространстве, информационной сфере в целом не может рассматриваться как явление, независимое от политической, экономической и социальной сфер, международной жизни. Доверие никогда не появится, если не поддерживать международное сотрудничество и процессы обсуждения сложных проблем международной безопасности, надо стремиться к предотвращению международных конфликтов, используя как традиционное, так и информационное оружие.

По нашему мнению, одним из факторов повышения безопасности враждебного использования ИКТ в информационном пространстве является то, что такие действия могут негативно повлиять на экономическое развитие отдельных государств, конкурентоспособность крупных компаний, а также на устойчивое развитие международного сообщества в целом.

Враждебное использование ИКТ существенно сужает пространство политического маневра для руководителей государств в критических обстоятельствах и с неизбежностью повышает угрозу использования вооруженных сил в рамках 51-й статьи Устава ООН. Это особенно опасно в современных условиях, когда некоторые государства активно продвигают широкое толкование права использования силы в рамках индивидуальной и коллективной самообороны. В их трактовке факт вооруженного нападения, порождающего такое право, включает в себя почти все, что может показаться опасным для их национальных интересов.

Подобная трактовка данного факта существенно повышает риск вооруженных конфликтов между государствами, рассматривающими друг друга в качестве источника реальной или кажущейся угрозы. За прошедшее время мы еще больше укрепились во мнении, что для предотвращения использования ИКТ в несовместимых с Уставом ООН целях, другими международными договорами необходимы новые соглашения, возможно «мягкого» права, определяющие порядок междуна-

родного сотрудничества в области поддержания стабильности и безопасности в киберпространстве.

Исследованием проблем формирования системы международной безопасности в соответствии с резолюциями Генеральной Ассамблеи и решениями Генерального секретаря ООН уже длительное время занимается Группа правительственных экспертов (ГПЭ) ООН в области информатизации и коммуникации в контексте международной информационной безопасности. В 2015 году усилиями группы, которую возглавлял Андрей Крутских, был подготовлен доклад Генеральному секретарю ООН, содержащий положения о применимости международного права в ИКТ-среде, а также предложения по нормам и правилам ответственного поведения государств в киберпространстве по мерам укрепления доверия между государствами.

На наш взгляд, признание применимости международного права в ИКТ-среде является нормой принципа, который открывает дорогу к прогрессивному развитию существующих источ-

ников международного права. Он не должен рассматриваться в качестве констатации самодостаточности с учетом существующих норм права международной безопасности или норм международного гуманитарного права.

Мы полагаем, что требуется дальнейшее развитие концепции суверенного применения в ИКТ-среде. Это особенно важно в связи с тем, что данная концепция является одним из краеугольных камней современной системы мирового порядка. Необходимо научиться очерчивать пространство и пределы суверенитета и правовой ответственности государств в киберпространстве, научиться закреплять эти границы в международных договорах.

Надо развивать международное процессуальное право, чтобы, во-первых, придать юридически значимый, объективный характер виртуальным событиям, связанным со злонамеренным и враждебным использованием ИКТ, а также осуществлять атрибуцию организаций, государств для сохранения международного права деятельности. Только на этой основе можно укреплять доверие между государствами в киберпространстве и внедрять в практику деятельности государства предложения, выработанные Группой правительственных экспертов ООН в 2015 году, по правилам, принципам и нормам ответственного поведения государств в ИКТ-среде. По нашему мнению, значительный потенциал прогрессивного развития международного права состоит в адаптации к отношениям в ИКТ-среде норм и правил, заключенных в источниках международного права безопасности и международного гуманитарного права.

В настоящее время завершается формирование проекта доклада действующей Группы правительственных экспертов ООН, который должен появиться в этом году. Хочется верить, что этот доклад продолжит именно формирование условий для предотвращения конфликтов в киберпространстве, создание механизмов повышения объективности в оценке опасных событий в киберпространстве, укрепление международного сотрудничества в данной области.

Комитет нашего форума в качестве одного из основных моментов рекомендует нам рассмотреть вопрос о механизмах

выполнения правил ответственного поведения государства в ИКТ-среде. Принятие Группой правительственных экспертов ООН этих правил символизирует осознание всеми заинтересованными государствами важности развития международного сотрудничества в данной области.

На наш взгляд, это обусловлено прежде всего реальностью угрозы дестабилизации ИКТ-среды. Не придает оптимизма и недостаточный уровень международного сотрудничества в области расследований инцидентов в ИКТ-среде, создающий комфортные условия для возникновения фейков как по поводу фактов кибератак, так и по поводу атрибуции якобы произошедших киберинцидентов. Правила, нормы и принципы ответственного поведения государств в киберпространстве, предложенные Группой правительственных экспертов ООН, могут стать политическим императивом современности.

Следующим шагом в этом направлении могли бы стать, во-первых, подготовка универсального международного документа, создающего условия для применения этих правил в практической деятельности государства; во-вторых, подготовка международных нормативных актов, закрепляющих ответственность государств за устойчивое функционирование глобальной системы цифровых идентификаторов и систем информационной инфраструктуры.

Укрепление доверия между странами способствовало бы принятию группой заинтересованных государств на себя ответственности за обеспечение безопасности глобальных цифровых идентификаторов. Обсуждение выделенных вопросов на форуме может помочь выявлению препятствий на пути их решения.

Следующий важный вопрос, который надо затронуть на форуме, - это предотвращение враждебного использования ИКТ для нарушения стратегической стабильности. Стратегическая стабильность, поддерживаемая с конца прошлого века по настоящее время, во многом базируется на военно-политическом балансе вооружений, в том числе и ядерных. На наш взгляд, сейчас факторами нарушения стратегического баланса способны стать враждебные использования ИКТ в качестве

силового средства разрешения противоречий между государствами. С этой точки зрения нельзя рассматривать киберстабильность в отрыве от стратегической стабильности в целом. Тем более что в процессуальных документах ряда государств, в том числе и США, посвященных применению вооруженных сил в информационном противоборстве, изучаются увязки с использованием всех средств вооруженной борьбы.

Еще одной важной темой дискуссии должна стать проблема участия бизнеса в обеспечении информационной безопасности критически важных объектов. Особую привлекательность этой дискуссии придает то, что одним из ее модераторов будет представитель большой российской компании «Норильский никель». Становится понятно, что при всех обстоятельствах обеспечение безопасности и функционирования критически важных объектов в инфраструктуре общества без участия бизнеса и частных структур практически невозможно. Но степень участия негосударственных структур и их роль во многом зависят от особенностей развития национальных обществ, национальной культуры и традиций, взаимодействия бизнеса и государства.

В работе нашей конференции зарегистрированы эксперты из 16 стран, а также представители трех международных организаций. Подготовка такой представительной конференции была бы невозможна, если бы нас не поддерживали наши друзья, партнеры.

Приветствие Олега Храмова, сопредседателя оргкомитета форума, заместителя секретаря Совета безопасности РФ: Приветствую организаторов, участников и гостей XI Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Лавинообразное нарастание новых трансграничных вызовов и угроз в глобальном информационном пространстве диктует потребность в выработке научно обоснованных подходов к обеспечению информационной безопасности. Традиционные встречи на баварской земле представителей государственных структур, научного и бизнес-

сообществ посвящены актуальным проблемам противодействия угрозам в информационной сфере.

В 11-й раз политики, известные ученые и эксперты научных и образовательных центров, коммерческих организаций из 16 государств примут участие в работе форума. За эти годы форум стал авторитетной международной дискуссионной площадкой для предметного, профессионального анализа существующих проблем в области информационной безопасности в поисках взаимоприемлемых путей их преодоления. Комплексный подход к предметному рассмотрению ключевых вопросов формирования системы международной информационной безопасности по праву стал визитной карточкой в Гармиш-Партенкирхене.

По традиции повестка дня форума, тематика его пленарных заседаний и «круглых столов» ориентированы на обсуждение актуальных задач обеспечения безопасности в информационной сфере. Полагаю, что в центре внимания участников встречи будет обсуждение правильного ответственного поведения государств в информационном пространстве, а также механизмов его выполнения. Дискуссионными станут вопросы, связанные с потенциалом использования ИКТ в военно-политических целях в контексте стратегической стабильности. Отдельное внимание будет уделено проблемам обеспечения информационной безопасности критически важных объектов промышленности.

Убежден, что форум выполнит свою главную задачу - сближение позиций сторон, достижение понимания по ключевым проблемам формирования систем международной информационной безопасности. Желаю успешной и плодотворной работы!

Приветствие Виктора Садовничего, академика, ректора МГУ им. М.В.Ломоносова: Позвольте от многотысячного коллектива Московского государственного университета приветствовать вас с началом работы международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». 11-й год подряд Московский университет собирает в Гармиш-Партенкирхене международный междисциплинарный коллектив ученых, спе-

циалистов и политиков для обсуждения сложнейших проблем международной информационной безопасности. На базе ИКТ формируется информационное пространство, или ИКТ-среда, которая пронизывает все сферы деятельности человека - от быта и отдыха до науки и производства.

Из-за резкого ускорения процесса обмена обработки информации существенно преобразились научные исследования, которые зачастую проводятся коллективами ученых, физически находящихся в разных странах. Набирает обороты такое новое явление, как интернет вещей. Но при массовом освоении ИКТ-среды в ней возникают как позитивные, так и негативные явления. За последние годы новости о негативном влиянии в ИКТ-среде перешли на первые полосы СМИ. Ширится многообразие средств вредоносного использования ИКТ в криминальных, террористических и военно-политических целях. Раздается даже вопрос: а не может ли потенциал злонамеренного применения ИКТ нарушить стратегическую стабильность в мире?

В этих условиях и гражданское общество, и бизнес, и политики ждут от экспертного сообщества технических, гуманитарных и юридических рекомендаций, как обуздать ИКТ-джинна. Уверен, что сложившемуся вокруг форума уникальному международному составу экспертов под силу решить эти задачи. Желаю всем участникам форума плодотворной работы и значимых результатов!

Актуальные проблемы международного сотрудничества в области информационной безопасности

Андрей Крутских, специальный представитель Президента РФ по вопросам международного сотрудничества в области информационной безопасности, посол по особым поручениям: Для начала хочу пропеть оду форуму в Гармише, поскольку это уникальное политическое мероприятие. Уникально оно не потому, что здесь собираются представители специальных служб и имеют возможность общаться друг с другом. Значимость этого форума состоит в том, что мы можем объяснить себя. Мы можем реально рассказать, что мы думаем, и, строго говоря, здесь с рос-

сийской стороны присутствует вся та переговорная команда, которую временами я возглавляю. Но главное, это единственный форум, созданный благодаря Владиславу Петровичу Шерстюку, где ведутся переговоры и который позволяет в доверительной обстановке разговаривать друг с другом.

Здесь состоятся встречи, на которых могут быть достигнуты определенные результаты между Россией и США, Россией и европейскими странами, если мы поймем, что никто из нас не хочет умирать. Мы не хотим погибнуть ни в третьей мировой войне, ни в кибервойне. Томагавки не определяют мировую политику. Это неприятный момент, но они ее не определяют.

На встрече С.В.Лаврова и Р.Тиллерсона во время его визита в Москву на повестке было широкое и глубокое обсуждение проблемы безопасности. Как бы американцы ни называли своего президента - системным или несистемным, - это их дело. Американцы умные и серьезные люди, которые несут ответственность за нашу планету. Американцы богатые люди, и они не хотят умирать. И если политика будет на уровне томагавков, то мы все погибнем. Но у них есть свои принципы, у нас тоже есть свои принципы. Россия при В.Путине не уступит своих принципов. В.Путин принял Тиллерсона и очень четко объяснил, что есть красные линии, такие же благородные принципы, как в США. И Тиллерсон это понял.

Мы предложили американцам серьезную и разнообразную повестку переговоров по информационной безопасности. Госсекретарь США не только выслушал С.В.Лаврова, но и был готов обсуждать данные темы, потому они, даже без желания Вашингтона или Москвы, могут привести нас к столкновению. А нам это не надо - ни Америке, ни НАТО, ни Европе, ни России, ни Китаю. Мы не хотим конфронтации. Так было и с ядерным оружием, так будет и с киберпроблемами. Мы их решим. Надеюсь, что тональность и скорость их решения будут предложены в рамках двусторонних переговоров.

Уверен, что тема киберпереговоров будет включена в число приоритетных во время встречи президентов наших стран. Именно там нас могут сделать гладиаторами, которые в битве друг с дру-

гом сожгут эту планету. Ни Россия, ни Америка - никто не хочет мирового пожара. Безусловно, та ответственность, которая лежит на этих двух державах, приведет к тому, что мы так или иначе договоримся с США, как в 1969 году договорились по стратегическим вооружениям и химическому оружию.

На переговорах именно американская сторона выступила с инициативой о мерах доверия в информационном пространстве, которую Россия поддержала.

Посмотрите, как далеко прошли американские инициативы, мгновенно поддержанные Россией. Когда в Вашингтоне выдвинули идею применительно к ОБСЕ, мы сразу поняли, что предлагается серьезный разговор. И в Вене с тех пор проходит очень сложный, болезненный, тяжелый разговор. Из 56 предложений, которые были сделаны, 16 уже приняты. Процесс, начатый американцами с нашей поддержкой, развивается. Это лучше, чем друг друга электронно уничтожать.

Но у Америки есть свои проблемы, может быть более значимые для нее, чем многие переговорные процессы, которые идут. В стране, обладающей 20% валового продукта мира, имеются большие внутренние проблемы. Страна, где живет больше миллиардеров, чем в остальном мире, имеет право разобраться в своих внутренних делах. Важно, чтобы нас никто не втравил в конфронтацию, а кибероружие, кибертехнологии, кибер-методологии могут нас стравить. Именно поэтому Тиллерсон был принят нашим президентом в Москве.

У американцев есть претензии к России, по крайней мере у их средств массовой информации. Это здорово, конечно, что российские хакеры, если верить американским СМИ, избрали Трампа, именно благодаря российским хакерам во Франции Ле Пен прошла во второй тур, наверное, российские хакеры также повлияют на выборы в Германии. Все это полная ерунда.

В разгар избирательной кампании, в августе, мы провели беседу с коллегами в американской миссии при ООН. В итоге представитель Президента США официально объявил, что у Америки нет претензий ни к нам, ни к хакерам. Аналогичная ситуация была и в Германии. После наших переговоров министр иностранных

дел Германии в Москве на пресс-конференции с С.В.Лавровым четко заявил, что у германской власти нет претензий к России в плане хакерских и прочих атак. Более того, мы ставим вопрос о том, чтобы скопировать опыт российско-американских переговоров при Б.Обаме, которые сумели привести нас к заключению трех соглашений о мерах доверия в сфере использования ИКТ, которые существуют только между Россией и США.

Мы предложили США продолжить переговоры. Это российская инициатива договориться с США, а вслед за этим и с другими странами, кто этого пожелает, о предотвращении инцидентов в сфере использования ИКТ. Чтобы не было больше попыток сорвать нашу Олимпиаду, чтобы мы больше не слышали, как об этом говорил Б.Обама, что будут нанесены удары по кремлевской системе управления или по энергетической системе России.

Я лично имел поручение донести до американской стороны, что мы «до Волги не отступим», мы «щеку не подставим». Можно сказать, что Россия в киберсфере опережает Соединенные Штаты на определенное количество лет. И американские силовики, к их чести, донесли до политического руководства США, что играть словами нельзя.

Мы, россияне, никогда не станем американцами, европейцами. В отличие от наших украинских коллег, мы не рвемся быть европейцами. Мы такие, какие есть. Но мы можем договориться.

В заключение хочу озвучить прогноз. Не будет никаких ударов по Северной Корее - этого не позволит Китай. Но ситуация в Корее должна «лечиться» в киберотношении. Я был в Корее, возглавлял российскую делегацию, которая приехала на первые переговоры в Сеул по информационной безопасности. Американцы выступили против наших переговоров с корейцами и японцами в области информационной безопасности.

Несколько лет назад мне довелось быть в Сеуле свидетелем того, что такое кибератака. А теперь задаю вопрос профессионалам и надеюсь, что они на него ответят: это считается вооруженным нападением на страну? Группа правительственных экспертов из 25 стран сказали «нет», что означает, что в киберотношении можно уничтожить любого. Россия может, США могут. Про другие страны не знаю. Но это не вооруженное нападение. 51-я статья не работает, потому что юридически она формулирует, что право на самооборону возникает только тогда, когда есть вооруженное нападение.

Никто не признал внедрение вируса Stuxnet, который нанес миллиардный ущерб экономике Ирана, вооруженным нападением. В Белом доме в офисе советника по национальной безопасности его заместитель говорил мне о нанесенном в ответ Ираном миллиардном ущербе Америке, когда в августе 2011 года Иран сумел «нагреть» банковскую систему США на миллиарды долларов.

Как быть? Мы должны договориться о правилах игры, должны себя обезопасить, мы не должны играть в безумство. Поэтому никакой войны на Корейском полуострове не будет. Это не нужно нам, потому что мы находимся всего в 700 км от Кореи. Это не нужно ни корейцам на Юге, ни японцам. Но кто гарантирует, что ответный удар, который я наблюдал в Сеуле, не может быть ударом по любой другой столице тех стран, которые я упоминал? И как эти страны отнесутся к этому?

США во многом для нас являются образцом, и я не боюсь об этом говорить. Но что Америка показала миру как пример? Американцы сказали, что если на США будет совершено кибернападение, то они воспримут это, независимо от того, что

записано в Уставе ООН, как нападение на США и в ответ применят все ресурсы, которые у них есть, включая вооруженные силы. Это очень серьезно. Если кто-то нас спровоцирует, если кто-то попытается подставить российско-американские отношения, а кибертехнологии позволяют это сделать, то может случиться ядерная война и мы все погибнем. И мы больше не приедем в Гармиш?!

Для меня было честью сделать доклад в Кремле перед руководством нашей страны. Там я сказал, что ядерное оружие - это оружие сдерживания, его применяют, когда терять уже нечего, а кибероружие применяется каждый день, и оно применяется наступательно.

Один эпизод. В ноябре 2016 года во время второй сессии Группы правительственных экспертов ООН ФСБ России выступила с официальным заявлением о том, что через Нидерланды была совершена массированная кибератака на Россию. Возможно, можно было бы пройти мимо этого эпизода, но наши технологии позволили определить, что эта атака была генерирована на Украине и, наверное, наши украинские товарищи решили наказать сразу две стороны - Голландию и Россию.

Я обратился к послу Нидерландов в Группе правительственных экспертов и сказал ему, что мы знаем, что вы на нас напали, вы натовская держава. Хорошо, что силы ФСБ России позволяют не только вовремя определить атаку, но и предотвратить ее. И ущерба не было, все было остановлено. Потом в Гамбурге на встрече министров иностранных дел ОБСЕ я говорил с замминистра иностранных дел Нидерландов и задал вопрос: «А если бы ущерб состоялся? Что бы осталось от Нидерландов?» Натовская страна ответила, что она даже не заметила, что украинцы взорвали ее информационное пространство и через нее ударили по атомной стране - России. Так в чем же натовская безопасность? Да никто и никогда не выстрелит в сторону России. А электронное поле - это проходной двор. Поэтому Россия заинтересована в безопасности всей Европы, США. Надо договариваться, чтобы никто не погибал.

Актуальные векторы угроз в киберпространстве: взгляд «Норильского никеля»

Владислав Гасумянов, вице-президент - руководитель блока корпоративной защиты ПАО «ГМК «Норильский никель»: Мне предоставлена честь выступить здесь от имени правления компании. «Норильский никель» - лидер металлургической промышленности России, крупнейший в мире производитель никеля, палладия, платины, меди, кобальта и родия. Доля компании в объемах металлургического производства России составляет 12%, а в промышленном производстве - почти 4%, в мировом производстве доля никеля составляет 14%, а палладия - 40%. О значении нашей компании для экономики страны наиболее красноречиво свидетельствует следующая цифра - 0,6% валового продукта России производит группа компаний «Норильский никель».

«Норильский никель» относится к группе предприятий, чья бесперебойная стабильная работа имеет критическое значение как с точки зрения экономики, так и в контексте сохранения социальной стабильности и развития территорий пребывания нашей компании. Мы понимаем и полностью разделяем подходы к процессам глобальной международной безопасности, обозначенные Президентом РФ, Советом безопасности России и зафиксированные в Доктрине информационной безопасности РФ, принятой в конце 2016 года. Как уже отмечалось, «Норильский никель» является глобальной и системообразующей компанией. Достаточно перечислить направления деятельности предприятий компании, чтобы понять ее масштабы. Это и геологоразведка, и обогащение, и металлургия, и бытовая система, и морской и авиационный транспорт, а также энергетика, информационная структура, научные комплексы и т. д.

Стоит отметить, что основные производственные мощности компании находятся за 68-й параллелью, то есть севернее Северного полярного круга, в особых климатических условиях. Основные производственные площадки расположены на Таймырском полуострове (Заполярный филиал) и на Кольском полуострове (Кольская ГМК), кроме этого, есть еще и в Забайкальском крае Бы-

стринский горно-обогатительный комбинат, который мы вместе с нашими китайскими коллегами осенью 2017 года пустим в промышленную эксплуатацию.

По советским меркам, подобные комбинаты строились один в пятилетку. Это крупнейший комбинат, в который мы вложили более 90 млрд. рублей. Поэтому вопросы непрерывности функционирования наших предприятий в сфере производства энерго-теплогенерации, связи, транспорта и социальной сферы могут быть критичными не только с точки зрения экономики, но в первую очередь являются процессами, обеспечивающими полноценную жизнь целых российских регионов.

Немаловажный факт, что большинство предприятий, входящих в «Норильский никель», градообразующие. Глобальная сеть представительств, офисов компании находится в России, Великобритании, Китае, США, Швейцарии. Продажи осуществляются через Лондонскую биржу металлов. Компания участвует в реализации ряда государственных инициатив в сфере высоких технологий, обладающих значительной социальной компонентой.

В частности, «Норильский никель» завершает строительство волоконно-оптической линии связи (ВОЛС) по маршруту Новый Уренгой - Норильск протяженностью более 1 тыс. км, благодаря чему не только предприятиям «Норильского никеля», но и всем жителям норильского промышленного района будет предоставлен доступ к скоростному широкополосному Интернету. Таким образом, компания содействует решению государственной задачи преодоления так называемого цифрового неравенства, обозначенной в Послании Президента РФ и входящей в перечень поручений правительства России.

Оценка рисков информационной безопасности - ключевой этап формирования стратегии и политики «Норильского никеля» в профильной сфере. В компании динамично развивается, модернизируется ее IT-инфраструктура, повышается уровень автоматизации технологических процессов. Дигитализация и усложнение процессов автоматически повышают риск стабильности и безопасности функционирования информационных систем, что может привести к утечке критически важной информации, нару-

шению доступности информационных систем и целостности информационных активов.

По нашим оценкам, уровень автоматизации в «Норникеле» через десять лет может превысить 80%. При этом доля выручки, которая напрямую будет зависеть от безопасного и непрерывного функционирования информационной инфраструктуры, приложения инфосистем в целом, существенно возрастет.

Совместно со службой риск-менеджмента «Норникеля» и с привлечением консультантов из «Большой четверки» нами проведено исследование, по результатам которого корпоративные риски в сфере информационной безопасности оцениваются в сотни миллионов долларов. С учетом обозначенных выше тенденций, по нашему мнению, они будут только расти.

Форум в Гармише стал для нас своего рода годовой отсечкой для подведения итогов и анализа ситуации в сфере информационной безопасности. В связи с этим полагаю полезным поделиться с уважаемыми участниками форума примерами тех вызовов и угроз, с которыми «Норникель» столкнулся за последний месяц.

Примерно с конца 2016 года нашими специалистами при расследовании инцидента информационной безопасности отмечается значительный рост негативного воздействия на инфраструктуру «Норникеля». В текущих реалиях самыми эффективными и опасными атаками являются APT-атаки, которые проводятся в корпоративной сети при помощи фишинговых посланий и специально написанных вредоносных программ. Мы видим большую опасность в том, что возможности, в том числе и крупных компаний, по выявлению и отражению кибератак в среднем остаются на прежнем уровне, даже после внедрения передовых решений в области информационной безопасности, а арсенал хакеров совершенствуется очень быстро.

Многие хакерские группировки научились обходить механизмы выявления активного заражения. Существующие классические средства защиты - антивирусы, системы предотвращения вторжения и ряд других - не позволяют эффективно бороться с этими системами. Зачастую атаку удается выявить по косвенным признакам, например по аномальному трафику из корпоративных сетей на

неизвестные ресурсы. Особое беспокойство вызывает рост атак на промышленные системы.

В «Норникеле» используются современные автоматизированные системы управления технологическими процессами (АСУ ТП), системы диспетчерского управления и сбора данных - SCADA, распределенная система управления - DCS, более мелкие системы программируемых логических контроллеров PLS и т. д., развернутые на различных объектах: рудниках, заводах, объектах топливно-энергетического комплекса, портах и других.

Нарушение работы АСУ ТП в целом или отдельных элементов вследствие нарушения свойств информационной безопасности - доступности, целостности, конфиденциальности - ведет к ощутимым финансовым и репутационным потерям, увеличивает риски техногенного экологического характера, может приводить к самым негативным и непоправимым последствиям. Область негативного влияния инцидента охватывает широкий спектр угроз и методов воздействия с целью получения несанкционированного доступа к инфоструктурам, бизнес-системам и АСУ ТП.

Например, несанкционированное вмешательство в управление технологическими процессами, нарушение функционирования АСУ ТП или отдельных его элементов, несанкционированный доступ к информации, хранимой в базе данных АСУ ТП и передаваемой по информационным каналам. Блок корпоративной защиты «Норникеля» активно участвует в обеспечении функционирования АСУ ТП в штатном режиме в условиях воздействия угроз информационной безопасности. Компания руководствуется международными и российскими требованиями, стандартами и рекомендациями, включая лучшие мировые и российские практики. Мы учитываем опыт Международной организации по стандартизации (ISO), Европейского агентства по вопросам сетевой и информационной безопасности (ENISA), следуем регламентирующим документам ФСБ, ФСТЭК России, а также ГОСТ. Положительно оцениваем наработку ОБСЕ в формате руководства передовой практики защиты важнейших объектов ядерно-энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства.

При обеспечении комплексной информационной безопасности активов группы компаний «Норильский никель» блок придерживается консервативного подхода. Данное видение мы также учитываем при корпоративном выборе решения платформ в IT-сфере.

Поясню на конкретном примере. В последнее время сложился устойчивый тренд перевода данных и их обработки в публичные облака, в первую очередь перевод личных данных. Однако мы также наблюдаем все более активное использование публичных облачных явлений корпоративными клиентами. С ростом использования облаков увеличивается и число утечек.

Все инциденты характеризуются большим объемом скомпрометируемых данных, долгим сроком обнаружения или огласки факта нарушения целостности, конфиденциальности и доступности информации. При этом перевести ответственность облачного оператора за информационную безопасность в юридическую плоскость достаточно затруднительно. Перевод данных критических производств в публичные гибридные облака впоследствии приведет к риску нарушения целостности и доступности, а предлагаемые на рынке страховые покрытия реализации киберугроз далеко не всегда могут компенсировать возможные потери.

Следовательно, преимущества тренда перевода критических данных в публичные облака, по нашему мнению, не очевидны. Тем не менее мы не можем не использовать преимущества, которые предоставляют современные передовые технологии. В этой связи на уровне компании мы приняли решение об использовании корпоративных облачных платформ, которые разворачиваются на собственной IT-инфраструктуре и позволяют применять наши корпоративные стандарты в сфере информационной безопасности.

Программа нашего мероприятия затрагивает фундаментальные международные вопросы: выработку механизмов и правил ответственного поведения государства в информационном пространстве, потенциалы использования ИКТ-технологий в военно-политических целях в контексте стратегической стабильности, а также обеспечение информационной безопасности критически важных промышленных объектов. Все эти вопросы являются для

нас предметом первоочередного внимания. У нас нет разногласий в подходах, есть некоторые различия в расстановке приоритетов.

Например, следует учитывать, что предприятия «Норникеля» являются объектами критической инфраструктуры, с точки зрения национально-экономической безопасности могут стать мишенью кибератак. Для компании вопрос атрибуции определения происхождения источника кибератаки не всегда является первоочередным. Главная задача минимизировать ущерб от злонамеренных действий и потом при наличии соответствующих возможностей, в том числе совместно с государственными правоохранительными органами, провести расследования со сбором доказательной базы и определением законных мер реагирования.

Развитие технологий и инструментов работы с большими базами - один из основных трендов развития ИКТ. По мнению ведущей IT-консалтинговой компании «Gartner», Big Data - в списке основных трендов развития виртуализации. Сам термин «большие данные» введен всего несколько лет назад, но уже сейчас эта тематика входит в вузовские программы. Практически все гиганты информационных технологий развивают свои собственные линейки по обработке больших данных.

Как практически любая новая технология, Big Data открывает новые возможности развития бизнеса. Для «Норникеля» это прежде всего новые технологии в области маркетинга управления производством и логистики. Но в то же время эти же новые технологии порождают новые вызовы и угрозы для безопасности бизнеса. Прежде всего, это новые возможности для недобросовестной конкуренции и ведения бизнес-разведки.

Здесь хочу обратить ваше внимание на отсутствие адекватных юридических норм, защищающих исходные данные для технологий Big Data. Это самые большие данные, включая метаданные, в коммуникационных системах, агрегированные данные из различных источников и прочее. Примеры у нас перед глазами. Мы говорим о том, что в США не прекращаются дискуссии о правомерности сбора спецслужбами метаданных о телефонных звонках.

Месяц назад Конгресс США, несмотря на бурные выступления, разрешил интернет-провайдерам использовать и продавать

данные о посещении сайтов в целях проведения рекламных кампаний. Мы считаем, что в ближайшем будущем отмеченные угрозы войдут в списки топ-угроз информационной безопасности. Бороться с угрозами нам, конечно, помогает наше участие в Международном исследовательском консорциуме информационной безопасности (МИКИБ).

Совсем недавно мы столкнулись с серьезными трансграничными инцидентами информационной безопасности. Детали в силу конфиденциальной информации я привести не могу, и только благодаря членам консорциума нам удалось их локализовать и минимизировать существенные риски для компании. Поэтому наше участие в МИКИБ носит не только общеполитический и научно-исследовательский характер, но имеет абсолютно эмпирическую компоненту, принося практическую пользу нашей компании.

Рассматривая первоочередные задачи консорциума, «Норникель» особое значение придает обеспечению информационной безопасности критических объектов, являющихся ключевой компонентой промышленной мощи компании. Полагаем, что аналогичного подхода придерживаются и остальные участники консорциума - представители стран, чья крупная промышленность сталкивается с такими же вызовами и угрозами. Мы, конечно, предлагали бы включить в решение конференции консорциума нашу инициативу по разработке хартии информационной безопасности важных объектов промышленности.

Что имею в виду? У «Норникеля» есть опыт проведения подобных инициатив. В частности, несколько лет назад мы выходили с инициативой предотвращения незаконного оборота драгметаллов, который мы рассматривали как форму финансирования преступности и терроризма. Вместе с МИД России, южноафриканскими коллегами и ООН мы эту инициативу продвигали и довели ее до Экономического и социального совета ООН, получив резолюцию.

Считаем, что если объекты промышленности являются активными акторами нашей площадки, то мы могли бы выйти с инициативой о том, чтобы подписать данную хартию и понемногу ее продвигать, имея в виду, что она объединена общим единым замыслом того, что у нас делается на площадке.

В хартию мы хотели бы включить следующие принципы: принцип разделения сферы ответственности собственника-промышленника и государства; принцип объективного определения ответственности собственника с учетом специфики и возможностей бизнеса; принцип ответственности государства за недопущение использования технологического лидерства в качестве инструмента негативного воздействия на критические инфраструктуры; принцип использования лучших мировых практик при выборе международных документов по обеспечению информационной безопасности критических инфраструктур.

Мы готовы по вашему поручению подготовить первоначальный проект и в интерактивном режиме совершенствовать его с остальными заинтересованными членами консорциума. Результаты работы могли бы вынести на обсуждение на следующем заседании нашего консорциума. Учитывая важность обсуждаемых здесь проблем, хотел бы выразить уверенность в дальнейшем плодотворном сотрудничестве.

Дискуссии в ООН и межправительственных организациях – принцип «мультистейкхолдеризма» и многосторонняя дипломатия

Вени Марковски, вице-президент ICANN по взаимодействию с ООН: Диалог с российскими коллегами очень важен для обеспечения информационной безопасности и ответственного поведения государств, для того чтобы сохранять устойчивость работы Интернета. Это невозможно сделать без взаимодействия друг с другом. Мы общаемся с дипломатами из различных стран мира, постоянными представителями в ООН, разными специализированными агентствами по линии ООН (международная радиосвязь в Женеве, ВОЗ, ОБСЕ и др.), то есть со всеми организациями, которые связаны с Интернетом, ИКТ-сферой. Работа ведется по нескольким направлениям: образовываем, рассказываем, что такое ICANN, как работает Интернет, что такое ИКТ. Мировое сообщество далеко не всегда понимает ценность и важность ООН и других межправительственных орга-

низаций в сфере ИКТ, а также не знает важности и значения работы Международного союза электросвязи. Пользователи Интернета тоже могут не понимать значение работы ICANN.

После двух лет, в течение которых я курировал взаимодействие ICANN и ООН, мною сделаны некоторые выводы. Многие дипломаты - профессионалы в своей сфере, но они не инженеры и не понимают, как работает Интернет. И наоборот, инженеры не знают, как работают дипломаты. Мы как раз объединяем эти две сферы, поэтому мы должны объяснять, что такое взломы, хакерство и т. п. За эти два года я встретил только двух дипломатов, которые закончили не гуманитарные вузы, а инженерные. У меня с ними диалог был простым. Они хорошо понимали, что такое наша оперативная группа, стандарты, протоколы и прочее. С остальными приходилось проходить ликбез. В частности, в Нью-Йорке мы стали применять модель многостороннего подхода - мультистейкхолдеризм, то есть междисциплинарное взаимодействие. Инженеры объясняют дипломатам, как нужно предотвращать новые киберугрозы. Были встречи также с коллегами из Китая, России, Франции, США, Кореи, Японии, Болгарии, мы объединяем эти страны в рамках междисциплинарного диалога.

После 1 октября прошлого года ICANN стала полностью независимой организацией, без каких бы то ни было договорных обязательств перед американским правительством, но у нас появились новые обязательства в отношении ответственного подхода к использованию Интернета и ИКТ. Мы, собственно говоря, не контролируем Интернет, а координируем усилия участников.

Один из отцов российского Интернета - Алексей Солдатов дал очень интересное интервью одному российскому издательству, где он сравнил роль ICANN с ролью таких организаций в России, которые занимаются названиями улиц, городов. На муниципальном уровне эти организации не контролируют, где улицы будут проходить, они отвечают только за процесс их наименования. Мне понравилось это графическое сравнение.

У нас есть стремление к наращиванию усилий в данном направлении, чтобы ООН и другие межправительственные организации не только понимали бы Интернет, но и активно участвовали в этом процессе. Нужно обязательно заручиться ответственным отношением всех участников процесса - некоммерческих и государственных организаций, физических лиц и предприятий. Более 170 стран входят в нашу организацию, а роль государства, конечно, развивается, эволюционирует. Каждая входящая в ICANN организация тоже обретает новый набор возможностей, кстати, это вызывает озабоченность со стороны некоторых политиков США.

Для меня лично и для ICANN это мероприятие, которое проходит уже в 11-й раз, создает хорошие возможности для обсуждения вопросов информационной и кибербезопасности. Здесь у нас нет споров, как мы называем информационную или кибербезопасность, в отличие от многих международных структур. Известно, что, какие бы слова ни использовали, мы думаем в одном направлении. Хочется, чтобы Интернет был более безопасным, чтобы компании были защищены от угроз и чтобы пользователи Интернета тоже чувствовали себя более комфортно.

Перспективы подходов США и ЕС к защите критически важной инфраструктуры

Чарльз Барри, Институт национальной стратегии Университета национальной обороны США: Для меня большая честь выступать на пленарном заседании. Здесь собралось представительное сообщество.

Хотел бы рассказать о перспективах подходов США и ЕС к защите критически важной инфраструктуры. На пороге появления нового в Интернете мы наблюдаем возросшее количество крупных атак с использованием ИКТ. Нам надо пытаться иначе решать вопросы защиты критически важных объектов.

Что такое критически важный объект? Дело в том, что жизнь меняется, экономика постоянно расширяется, общество все в большей степени зависит от ИКТ, все больше людей выходят в онлайн. Сегодня уже приводили статистику пользователей. Создается иллюзия, что невозможно объять необъятное, а мы как раз должны это делать, потому что все промышленные и бизнес-процессы не могут в настоящее время существовать без ИКТ. Это и производство, и торговля, и сфера услуг, да и все направления экономической деятельности. Мы должны с точки зрения ИКТ понимать, как мы можем обеспечить безопасность, предотвратить попытки взломов.

Дома мы пользуемся электричеством, которое тоже управляется ИКТ. Прогресс отмечается и в отношении обмена информацией. Есть здесь определенное замедление, но банковские системы заинтересованы в том, чтобы не допускать кибератак. Когда была цепочка со стороны кибермошенников и подходили к третьему, четвертому банкам, эти банки уже были готовы к отражению атак именно благодаря обмену информацией.

«Норильский никель» - очень хороший пример сохранения устойчивости и целостности информационной системы не только при организации бизнес-процессов, но также и для обеспечения инфраструктуры, которая имеет трансграничный характер. Самое важное, что кибератаки, которые в будущем будут происходить, скорее всего, будут направлены на критически важные инфраструктуры.

Пока нет единого определения, что такое критически важные инфраструктуры. В каждой стране есть свои традиции и подходы. По данным Международного союза электросвязи, есть порядка 36 определений, более четырех международных, но есть общие слова во всех этих определениях. Допустим, в США недавно убрали исторические памятники из Сети, в частности Всемирный торговый центр, который был уничтожен 11 сентября 2001 года и входил в список критически важной инфраструктуры. Не все согласились с этим. То же самое больницы, ТЭС, ГЭС, строительные объекты, мосты да и памятники культуры. Считаю, что они не могут не включаться в категорию критически важных объектов. Это структуры, которые нуждаются в защите.

Мы говорим о том, как это делается в США, а в ЕС дело обстоит несколько иначе. В ЕС ответственность лежит на государстве, каждое отдельное государство отвечает за свою безопасность. Хотя нельзя не учитывать трансграничный характер информационной безопасности. В США еще в 1996 году приступили к разработке концепции информационной безопасности, а в 2007 году была создана соответствующая комиссия.

На эту тему было выделено 16 категорий, установлено государственное партнерство, подключены Министерство обороны, ключевые профильные министерства, а в частном секторе стали работать банковские сообщества, крупные торговые организации. Была создана специальная сеть групп командного реагирования на инциденты с использованием ИКТ, разработан план защиты структуры в 2015 году, были пересмотрены стандарты защиты ИКТ по линии Министерства торговли. В 2013 году приняли концепцию безопасности и обеспечения устойчивости критически важной инфраструктуры. Сначала акцент делался на транспорт, банковскую систему, потом подключили воздушные пространства.

В Европе тоже созданы группы командного реагирования на инциденты с использованием ИКТ, но они не очень продвинутые. Тем не менее 28 стран ЕС объединяют свои усилия в плане обеспечения информационной безопасности. Это может служить хорошим примером того, как следует объединять усилия на международном уровне для решения общих проблем. Посмотрим, как это проявится.

Европейское агентство по сетевой и информационной безопасности (ENISA) было создано с целью повышения эффективности функционирования внутреннего рынка. Оно проводило учение по реагированию на инциденты информационной безопасности.

Есть чем заняться, в частности воспитанием пользователя. Люди зачастую не знают, как разворачивается атака, какие последствия могут быть. Сейчас растет новое поколение пользователей, которые уже осознают эти угрозы, они проявляют высокую степень сознательности, бдительности, понимают, как работают вредоносные программы. Такой опыт надо распространять на всех пользователей. Нужно выработать подходы к тому, как обеспечить безопасность промышленных систем управления.

Например, крупное предприятие управляется с помощью сетевых решений, которые надо постоянно актуализировать. Это касается круглосуточного обеспечения работы систем общественного транспорта, метро в Москве, Вашингтоне или где-то еще. Все опирается на программные продукты, требующие постоянного обновления, причем в процессе, не останавливая работу этой системы, чтобы все было бесшумно и не сказывалось на функциональности всей системы.

Хочу отметить, что мы унаследовали из прошлого незащищенные операционные технологии, которые по-прежнему существуют и используются объектами инфраструктуры, но они, когда изначально создавались, не были заточены на современные киберугрозы.

Думаю, что большинство угроз, которые нас сейчас интересуют, носит такой характер, например, 90 тыс. человек в финансовом округе Сан-Франциско были отрезаны больше чем на сутки от электричества в результате перебоев в системе электроснабжения. Это, безусловно, волнует всех и означает, что мы конкурируем друг с другом. Мы обеспечиваем безопасность в киберсреде, но наши конкуренты поднимают вопрос об обеспечении устойчивости.

О Stuxnet мы говорили, были взрывы в «Sony», в декабре 2012 года прошла атака на энергосеть на Украине и т. д. Речь идет о том, что к кибератакам прибегают некоторые государства, террористические организации, негосударственные субъекты, это осложняет вопросы.

Есть хорошая новость: те преступники, которые в основном в ИКТ-среде совершают подобные атаки, практически не выбирают в качестве объекта атомную электростанцию. Для этого нет средств. Это наполняет нас уверенностью, что можно обеспечить безопасность критически важных объектов, чтобы лучше понимать, как нужно работать, чтобы не оказаться на той арене, где придется как-то реагировать на атаки.

Надо опираться на партнерство, и здесь есть о чем говорить. Я набросал тезисы. Мы будем обсуждать данные вопросы в ходе конференции.

Киберпроекты НАТО в дискурсе гибридных войн - взгляд из России

Анатолий Смирнов, президент Национального института исследований глобальной безопасности, Чрезвычайный и Полномочный Посланник РФ: Основатель Давосского форума Клаус Шваб сказал, что сегодня различие между военными и невоенными аспектами стирается, становится расплывчатым. Именно он в своей книге «Четвертая промышленная революция» описал угрозы, о которых сегодня уже частично говорили.

В этом контексте хотелось бы сказать, что мы вошли во второе десятилетие XXI века, наверное самое драматичное за всю историю человечества, но стольких нарратив угроз - техногенных, протогенных, социогенных, гибридных, адаптивных смен режимов, «цветных революций», рецессий, санкций и т. д. - мы, пожалуй, не найдем и не увидим, надеюсь, в будущем. В этом плане самое неприятное в том, что сегодня ломка миропорядка, Вестфальской системы в целом ведется с помощью еще и инфогенной составляющей. Инфогенные риски и угрозы зафиксированы во всех международных документах.

Недавно появились публикации WikiLeaks о новых утечках информации из ЦРУ, которые могут использовать «флаг третьей страны» для атаки. Эта технология стала теперь известна всем. К счастью, она недоступна для многих международных преступников. В этом контексте мы должны посмотреть, что мы сказали

своей Стратегией национальной безопасности. В ее 12-м пункте отмечено, что усиление, укрепление России идет на фоне попыток США и их сателлитов оказывать давление на четырех треках, а именно: дипломатическом, экономическом, военном и информационном. Мы видим, что эти четыре составляющие были объявлены Робертом Гейтсом как составляющие гибридной войны. Очень интересно, что эксперты Всемирного экономического форума в Давосе отнесли киберугрозы по уровню их опасности на уровень межгосударственных конфликтов.

В целом история войн - это история технологических прорывов. В этом плане хотел бы привлечь ваше внимание к тому, что в основном человечество идет к поколению новых войн - гибридных. Если в XIX веке было около 10%, во Второй мировой войне - до 30%, то в начале века - до 40%, а в середине будет более 50% невоенной составляющей.

НАТО ведет достаточно агрессивный курс против России. Она уделяет огромное внимание гибридным аспектам воздействия на противников, среди которых на первом месте стоит Россия. Нами было проанализировано комплексное воздействие на Союзное государство во внешнеполитическом, экономическом, оборонном аспектах в использовании иных, в том числе «цвет-

ных», революций и т. д. Вот так устрашающе выглядит этот многофакторный «питон», который обжимает и удушает наши и другие структуры, в частности Союзное государство.

НАТО создала огромное количество центров передового опыта - уже свыше 20. Возьмем, к примеру, Центр киберзащиты НАТО в Таллине, который один из первых разработал руководство по международному праву, применимому к ведению военных действий в киберпространстве, собственно, легализацию кибероружия в условиях действующего международного права. Но такого права нет. Выдумали и написали 95 правил, а в феврале появилось второе издание, показывающее более комплексно всю эту степень милитаризации киберпространства.

Мы, естественно, не можем спокойно смотреть, как наши соседи, находящиеся в 300 км от Санкт-Петербурга, занимаются такими делами. В декабре 2016 года были проведены крупнейшие учения, 700 экспертов из 27 стран. 24 апреля 2017 года начались очередные учения - 800 участников из 25 стран и гигантская программа. Участвуют оборонные силы Эстонии, Финляндии, Швеции, Великобритании, европейское командование США и т. д. Убедительно!

А теперь посмотрим, чем занимается еще один центр НАТО - Стратком, который находится в Риге. Продуктов их работы за 2016-2017 годы - огромное количество, но абсолютно везде Интернет-троллинг - инструмент гибридных войн. Практически антироссийская, русофобская, по сути, направленность этого центра, не вызывающая сомнений.

11 апреля было подписано соглашение об открытии Центра по противодействию гибридным угрозам в Хельсинки. Финляндия имеет границу с Россией в 1300 км. Направленность этих противодействий абсолютно понятна даже непосвященному.

В России не создается подобных центров, а у НАТО их больше 20. Где пропорция? Где логика в утверждениях?

Что же делает Россия? У нас недавно принята Концепция внешней политики России. В ней есть замечательный 28-й пункт, где прописаны все четыре составляющие - военно-политическая, криминальная, террористическая и цифровой суверенитет, плюс

вопросы взаимодействия с ООН в сфере Интернета, о чем сегодня уже сообщил коллега из ICANN.

Глава МИД РФ С.Лавров, выступая на конференции в Мюнхене, говорил о политике постправды - это когда эмоциональное закрывает объективное. Есть и политика постфейков. Огромное количество фейков. Так, например, в «Facebook», на момент выборов американского президента число фейковых новостей превзошло количество реальных. Продолжают утверждать, что в этом замешены русские хакеры.

Киберпроекты в гибридных войнах сверхопасны. Ибо в условиях создания искусственного интеллекта - это отдельная тема, которая сейчас набирает обороты и она засекречена во многих государствах. В России тоже засекречена. Но мы знаем, что идет огромная военная составляющая использования данного потенциала.

Информационное противоборство - уже не война между ботами и людьми, а война между армиями ботов. Здесь в военно-политических целях проигрываются неожиданные варианты. Надо ускорить продвижение российской резолюции о правилах ответственного поведения государства, то есть создание «цифрового Вестфаля». Коль под воздействием технической революции вестфальские принципы пали, то мы должны создавать новые. Альтернатива иррациональна - «Киберармагеддон».

Владислав Шерстюк: *Должен сказать, что сегодняшний форум не состоялся бы на всех этапах его подготовки, если бы нас так активно не поддерживали редколлегия и главный редактор журнала «Международная жизнь».*

Армен Оганесян, главный редактор журнала «Международная жизнь»: Для нас большая честь работать с вашим институтом, который столько лет поддерживал эту актуальную, важнейшую тему.

Хотел бы обратить внимание на некоторые гуманитарные аспекты. В России, по данным Росстата, 84 млн. пользователей Интернета, при этом почти половина граждан России, по данным ВЦИОМ, считают, что без Интернета их жизнь не изменится. Интересно было бы знать, как на эту статистику влияет тот имидж, который Интернет имеет сегодня.

Во время полета сюда я открыл одну российскую газету с многомиллионным тиражом - «Аргументы и факты», в которой дана, я бы сказал, сверхжесткая характеристика Интернета: Интернет - это, по сути дела, слежка, выкачивание данных, вбросы фейков, боевые вирусы, с помощью которых одно государство может воевать с другим.

В марте текущего года Конгресс США принял закон, который позволяет покупать и продавать данные пользователей без их согласия, что, конечно, вызывает огромное беспокойство среди самых рядовых пользователей Интернета. Трудно не согласиться с автором данной статьи, который считает, что приведение Интернета в безопасное состояние является зоной ответственности государства.

При этом речь не идет исключительно о безопасности государств и их ответственном поведении, хотя это очень важно. Поэтому необходимо реально осознавать, что в одиночку ни один из потенциальных объектов нападения, киберугроз не может справиться с таким глобальным вызовом. Здесь необходимо понимать, что информационная безопасность неделима на интересы государства и личности, реального бизнеса и банковского. Необходим комплексный подход, который демонстрирует наша конференция.

Недавно вышла алармистская статья в журнале «The Economist» как раз на злобу дня, на обложке которого написано: «Почему компьютеры никогда не будут безопасны?» Нельзя делить безопасность между разными ее объектами и субъектами. Та же защита, которая охраняет программы типа «WhatsApp», также дает защиту банкам и онлайновой идентификации. Компьютерная безопасность обеспечивается шифрованием, которое сильно для всех. Одна из причин недостатка компьютерной безопасности состоит в том, что вчера очень немногие серьезно относились к данному факту. Когда Интернет был новым, было простительно, а сейчас непростительно повторять такую ошибку.

Хочу пожелать нашей конференции положить камень в строительство системы международной информационной безопасности, которая давно назрела.

XIV Научная конференция Международного исследовательского консорциума информационной безопасности (МИКИБ)

Владислав Шерстюк: *В 2010 году здесь, в Гармише, был образован Международный исследовательский консорциум по разрешению проблем информационной безопасности (МИКИБ). Мы тогда с вами решили, чтобы нам не прерывать исследовательских работ между форумами, необходимо создать МИКИБ, проводить совместные двусторонние и многосторонние мероприятия по различным аспектам международной информационной безопасности. И такая работа уже в течение семи лет ведется. Проведены не самые большие, к сожалению, но определенные исследовательские работы с Международным институтом сотрудничества Восток-Запад и другими организациями, которые на самом деле сыграли важную роль в выработке путей преодоления тех проблем, которые существуют в сфере международной информационной безопасности.*

На сегодняшний день в консорциум входят 24 организации из 16 государств. Мы с вами тогда определились, что в консорциум мы принимаем тех, за кого все проголосовали «за». В консорциуме представлены университеты, научные центры, организации, которые ведут научную работу в сфере международной информационной безопасности. Страны - участницы консорциума: Азербайджан, Белоруссия, Болгария, Германия, Израиль, Индия, Италия, Казахстан, Канада, Киргизия, Китай, Республика Корея, Россия, США, Швейцария и Япония.

На нашей нынешней встрече мы поставим вопрос о приеме еще четырех организаций в МИКИБ. Содержательную часть начнем с того, что дадим слово давнему нашему другу, который в Республике Корея предоставил площадку для проведения осенней сессии. Он расскажет о том, как осуществить универсализацию норм, согласованных на уровне Группы правительственных экспертов (ГПЭ) ООН.

Как осуществить универсализацию норм, согласованных на уровне ГПЭ ООН

Ноюнг Пак, Центр киберправа Университета Корё (Республика Корея): Большое спасибо за теплые рекомендации. Недавно состоялось 13-е заседание Группы правительственных экспертов ООН, которая приняла решение о применимости международного права в киберпространстве в полном объеме. Это соглашение было поддержано крупнейшими организациями, а также группами «Двадцатки» и «Семерки». Страны выразили озабоченность тем, что в условиях киберпространства могут существовать некоторые ограничения при применении международного права. Есть предсказуемость, которая требуется в отношении государств и некоторых субъектов как в киберпространстве, так и за его пределами.

Мы изучили также практику разных стран относительно кибердеятельности в киберпространстве. ГПЭ от имени стран - членов ООН с успехом продолжает работу по обеспечению ответственного поведения стран с учетом норм в киберпространстве. Эти нормы разработаны на уровне ГПЭ, могут быть дифференцированы соответственным образом в обычное право и должны быть взяты на вооружение национальными государствами.

В декабре 2015 года очередной этап был преодолен. До этого Генеральная Ассамблея ООН только принимала к сведению рекомендации, которые были разработаны ГПЭ. Была принята резолюция, которая носит рекомендательный характер, но тем не менее это свидетельствует о том, что страны - участницы ООН должны выполнять требования, содержащиеся в отчете ГПЭ.

Эта группа столкнулась с трудностями достижения консенсуса по ряду норм в силу конфликтов между национальными интересами и разными уровнями развития потенциалов ИКТ. Генеральная Ассамблея ООН уполномочена реализовывать эти нормы. Есть также другие препятствия по разработке и реализации этих норм. Страны - участницы ООН должны выполнять соответствующие рекомендации и при этом изыскивать способы

повышения эффективности защиты безопасности киберпространства.

ГПЭ предложила целый арсенал инструментов, направленных на сохранение безопасности киберпространства. Такая работа была начата еще в 2008 году. Генеральная Ассамблея обратилась к странам-участницам дать свою оценку по опубликованному отчету при выработке своих позиций, поэтому есть общее понимание, что предлагаемые ГПЭ нормы носят руководящий характер.

Например, в соответствии с резолюцией Генеральной Ассамблеи ООН 17/37, страны-участницы должны информировать Генерального секретаря о своих взглядах и оценках по таким пунктам: а) вопросы информационной безопасности; б) усилия, которые предпринимают национальные органы, по укреплению мер безопасности и продвижению международного сотрудничества в этой сфере для обеспечения стабильности; в) содержание этой концепции, направленное на укрепление глобальных ИКТ-систем; г) возможные меры, которые можно предпринять силами международного сообщества, чтобы укрепить информационную безопасность на глобальном уровне.

63 страны-участницы отправили свои оценки Генеральному секретарю за последние 18 лет - с 1999 по 2016 год. Страны-участницы оказались более активными в подаче своих заключений, например, Австралия подавала 4 раза, Боливия - 3, Канада - 5, Китай - 4, Колумбия - 4, Куба - 3, Сальвадор - 4, Грузия - 5, Россия - 4, Германия - 5, Иордания - 4, Мексика - 6, Нидерланды - 3, Панама - 4, Португалия - 4, Канары - 7, Сербия - 4, Испания - 5, Украина - 5, Великобритания - 7, США - 3 раза. ГПЭ включила пять постоянных членов Совета Безопасности в работу заседаний, они выполняли свою функцию.

Конечно, вопросы национальной оценки должны быть усовершенствованы, получить детальные взгляды, отражающие нормы, рекомендуемые ГПЭ для дальнейшей работы над ними. Если посмотреть на пункт 13, подпункт b, четвертого отчета Группы, то увидим, что все государства должны рассмотреть

имеющуюся по делу информацию, включая контекст того или иного события. Этот отчет также предусматривает необходимость сотрудничества государства в области обмена информацией и оказания помощи друг другу, преследования террористов, которые в преступных целях используют ИКТ.

Хочу отметить следующее. Взгляды и оценки, представленные странами - участницами ООН, могут составить государственную практику, связанную с деятельностью в ИКТ-среде. Это поможет членам ООН лучше понимать суть вопросов в сфере международной информационной безопасности.

Если рассмотреть направления совершенствования международного права в киберпространстве, то страны-участницы, видимо, должны обеспечить лучшее оснащение и привлечение дополнительных групп экспертов для работы в сфере международной информационной безопасности.

Соответствующим образом все страны-участницы призываются к тому, чтобы предоставлять на рассмотрение Генеральной Ассамблеи ООН свои оценки, и делать это нужно чаще и быстрее. Как и в ВТО, крупные страны могут встать перед необходимостью хотя бы раз в два года давать такие заключения в сфере международной информационной безопасности, а страны среднего размера - раз в четыре года, малые страны - раз в шесть лет.

Проблемы определения «виртуальных границ» - зоны ответственности государств в ИКТ-среде

Павел Пилюгин, Институт проблем информационной безопасности МГУ им. М.В.Ломоносова: Мы в университете после того, как появился соответствующий доклад Группы правительственных экспертов, задумались над вопросом: а как, собственно, государства будут осуществлять свое ответственное поведение. В частности, с профессором А.Стрельцовым мы написали статью на тему цифрового суверенитета государств и о том, как из этого вытекает необходимость введения цифровых границ в виртуальном пространстве.

Сразу встал вопрос: а что такое граница в цифровом киберпространстве, как она может строиться и если она будет построена, то как государства могут осуществлять контроль за этой зоной ответственности и насколько это будет эффективно? Рассматривая эту проблему, мы выделили три главных подхода: границы реальности, физические границы как они есть и некие виртуальные границы.

Помню, что в конце 1990-х годов возникло такое мнение, что киберпространство - это некое отдельное, другое место, даже не как Антарктида, а как Луна, где вообще правовые нормы никак не рассматриваются и там никакого влияния государства не оказывают. Те, кто туда придут, сами определят, что им надо делать.

Это отчасти имеет отношение к киберпространству, потому что было очень интересно наблюдать, особенно в 1990-х годах, как развивались некоторые сообщества информационного обмена. Проводились конференции, потом появились социальные сети, которые начали сами себя регулировать. Что тогда остается на долю государства? Где проходит граница при такой концепции? В данном случае граница проходит через компьютеры, смартфоны и другие устройства, которыми пользователь с этим пространством взаимодействует. То, что за ними, - это некое виртуальное пространство, которое, по этой концепции, регулировать нельзя.

Что может быть реально осуществлено с позиции государства, которое регулирует действия своих граждан по взаимодействию с этим устройством? Можно, конечно, пытаться что-то блокировать, запрещать, но это не конструктивно. Единственная конструктивная ситуация заключается в том, что можно было бы заняться четкой идентификацией тех, кто входит в это виртуальное пространство.

Мы имеем ряд замечательных примеров. Во-первых, при фиксированной связи по проводам у нас все провайдеры знают, кого и как они в Сеть впускают, они платят деньги, договоры составляют. Значительно сложнее ситуация, когда сейчас крупные города, крупные культурные центры, вокзалы, аэро-

порты накрыты сетью Wi-Fi, там зачастую сделан вход бесплатный, свободный - кто и как входит, неизвестно. Но в последнее время, насколько мне известно, и в России, и в Евросоюзе появилась необходимость регистрации при работе с Wi-Fi.

Хочу обратить ваше внимание, что это, конечно, важный шаг к проблеме атрибуции различных компьютерных инцидентов, но, как всегда, каждый следующий шаг порождает много новых вопросов. Один из них заключается в том, что если мы аутентифицируем пользователя Wi-Fi через сотовую связь, смартфон, GSM, то насколько возможна аутентификация самой GSM-системы. Она ведь использовалась совсем для других целей, исключительно для получения каких-то денег, для выгоды, и незначительные потери, с точки зрения сотового оператора, допустимы. А если мы разбираем вопрос компьютерного инцидента, то, конечно, мы хотели бы иметь более надежную аутентификацию.

Второй подход - это принцип физической границы. Во многих документах, в частности нашего Министерства связи, рассматривался вопрос о контроле за трансграничными переходами, где линии связи переходят с территории одной страны на территорию другой. Во-первых, здесь есть масса технических проблем. Условно говоря, такие скорости, которые возникают на магистральных каналах, контролировать достаточно тяжело, во всяком случае детально. Это все равно что у пассажиров летящего самолета при пересечении некой воздушной границы успеть проверить паспорта.

Во-вторых, проблема заключается в том, что многие утверждают, что такой контроль будет недостаточно эффективен, его можно обойти тем или иным способом. На самом деле этот контроль за трансграничными переходами - это не что иное, как обычный сетевой экран, который является обязательным элементом, атрибутом от внешнего воздействия практически всех сетей. Только подобную практику надо рассматривать уже в государственном масштабе, каждой отдельной страны. Как показывает опыт Китая, это довольно успешно функционирует. Если не для контроля всех потоков, то в социальном плане является достаточно эффективным.

А любая граница никогда не будет абсолютно защищенной. Мы знаем, существуют всякие лазейки, контрабандисты.

Третий подход - виртуальная граница. Очень заманчиво было бы поделить все виртуальное пространство по странам, исходя из их адресов. Мы эту проблему обсуждали, но технически она не реализуется. Во-первых, у четвертой версии Интернета закончились IP-адреса. Во-вторых, кроме IP-адресов, существуют такие IP-адреса, с которыми можно, независимо от провайдера ездить из одной страны в другую. В-третьих, у нас активно для экономики используется так называемая техника замены-подмены адресов - за одним реальным адресом могут находиться более шести десятков различных устройств в Интернете. Адреса, как правило, получаются временными, никто не хочет платить лишние деньги за постоянный адрес. Вместе с тем такой географический подход маршрутизации будет в большей степени реален при переходе на шестую версию - там пространство адресов практически не ограничено.

И самое главное - можно посмотреть на эту проблему совершенно по-другому. Вначале весь Интернет создавался как федерация различных сетей. Эти сети обладают своей политикой, у них есть юридические владельцы - в данном случае

имею в виду автономную систему. Эти системы взаимодействуют между собой уже по специальному протоколу. Они могут говорить, что мы хотим с кем-то связываться, получать информацию только таким способом. Часто их можно сравнить со странами или городами на карте, между которыми есть определенные типы дорог, и сами города или страны выбирают, какой дорогой они хотят пользоваться.

Вот специальный протокол Border Gateway Protocol (BGP). Я ввел некое графическое пояснение, как выглядели бы такие границы. Дело в том, что они перестанут быть линиями, как обычно на карте, это будут точки некоего соприкосновения автономных систем. И пусть они находятся в разных государствах, есть соответствующие граничные переходы, те точки, где граничные BGP-маршрутизаторы осуществляют взаимодействие между разными странами. В принципе, политика, по которой работает эта маршрутизация, может даже стать предметом межгосударственного соглашения.

Естественно, все перечисленные подходы имеют свои плюсы и минусы. Но вместе с тем, если использовать эти механизмы, которые предусмотрены тем или иным подходом, то можем получить некий комплекс мероприятий. В частности, если взять идентификацию границы входа только в виртуальное пространство, как это было на границе реальности, где нужно использовать контроль трафика, как на физической границе, и управлять безопасным роутингом, безопасными маршрутами, как это было сделано для виртуальной границы. Как показывает тот пример с самолетом, с магистральными каналами с большой проходной способностью у нас есть технические и организационные ограничения. Здесь, в принципе, мы рассматривали вопросы, как эти ограничения преодолеть.

Функции, связанные с реализацией цифровой границы, нужно распространить по большинству элементов Сети, которые занимаются передачей трафика. То есть на самом граничном переходе мы смотрим безопасные маршруты, потом эти маршруты, потоки уходят в другие автономные системы, где мы

можем с позиции межсетевых экранов смотреть более детально адресацию, типы потоков. Дальше, когда мы доходим до автономных систем конкретных провайдеров, которые оказывают услугу конечному клиенту, мы там можем посмотреть и содержание, там скорость потоков уже не такая значительная, и технически это вполне осуществимо.

Таким образом, получается интересная ситуация: виртуальная граница как таковая начинается с границы реальности и заканчивается на физической границе, где линии осуществляют трансграничный переход. И на всем этом пространстве - от начального входа в виртуальную реальность до выхода из зоны контроля или ответственности того или иного государства - у нас везде могут находиться различные средства по контролю за проходящим трафиком.

Хочу отметить две интересные концепции, которые сегодня определяют парадигму развития вычислительных сетей, - это программа коммутирования сети (Software Defined Networking) и программа виртуализации сетевых функций (Network Functions Virtualization), которые помогают, в частности, очень гибко управлять прохождением трафика. По адресации вообще непросто контролировать трафик и заниматься тривиальной фильтрацией, но наряду с маршрутизацией можно смотреть и анализировать заголовки пакетов, по-моему, с первого по четвертый уровень. Виртуализация сетевых функций позволяет для каждого пользователя строить его представления Сети, в которой он хочет работать, - с элементами защиты, типами аутентификаций, с тем или иным контролем. Если представить, что такие технологии будут распространены практически по всем средствам маршрутизации, то можно предположить, что единый центр управления станет проводить политику, которая будет управлять движением информационных потоков в такой структуре в зоне ответственности этого единого центра управления.

Хотел бы отметить, что никто из рассматривающих эту проблему специалистов не выразил сомнения в технической возможности ее реализации. Нужно, чтобы у нас было время

на эту реализацию, средства, чтобы это сделать, и, главное, добрая воля.

Джон Мэллори: *Что касается возможности обнаружения сетей. Примитивная защита сетей не сработает, если мы не докажем невозможность прохождения. Это может быть jive driver, какие-то модемы, которые могут решить данную проблему. Поэтому нужны жесткие, укрепленные точки, чтобы работать в такой Сети. Это можно сделать, в таком случае мы сталкиваемся с проблемой аутентификации для тех, кто находится за пределами страны. Это одно ограничение.*

А безопасность платформы - другая проблема, потому что если она недостаточно надежна, то тот, кто работает под чужим именем, может пробить эту оборону. Пакеты передвигаются через аутентификацию, без соответствующей авторизации. Что вы об этом думаете?

Павел Пилюгин: *Есть две позиции. Могу четко доказать совершенно противоположное, что в пакетной сети передачи данных я могу математически организовать любой канал, который никогда и никак не будет обнаружен, а будет работать сквозь маршрутизатор, сквозь шифратор. Это особенности работы системы передачи данных. Поэтому абсолютной защиты никогда не будет Вы правы.*

Мы знаем также, что защита всегда отстает от нападения. Когда появятся более эффективные средства атаки, тогда появятся и соответствующие средства защиты. Такие соревнования будут идти постоянно. Я не готов представить универсальный способ аутентификации на все случаи обеспечения безопасности всей сети. В конкретной зоне ответственности могу допустить только зарегистрированных и определенным образом аутентифицированных пользователей. Это выглядит приблизительно так: с территории каждой страны может быть только гражданин, обладающий ее паспортом, а с другой территории, если вы хотите попасть в эту Сеть, вы должны получить визу и т. д. Вот тут и возникают ограничения. Действительно, лю-

бое мероприятие, связанное с обеспечением безопасности, будет накладывать ограничения, только чтобы они не были обременительными и были удобными для большинства тех, кто работает в Сети.

***Найджел Инкстер**: Как вам представляется, это предложение будет воспринято в США с учетом первой поправки, к которой очень серьезно относятся в Америке? Как легко практически создать стимулы для провайдера работать в рамках такой системы? Или это можно сделать путем принятия государственного решения?*

***Павел Пилюгин:** Не только в США. У нас тоже возникают некоторые противоречия. Хотелось бы, чтобы Сеть развивалась самостоятельно и был свободный обмен информацией. Если интересно, мы сможем рассмотреть варианты, тогда сохраним и безопасность, и полный обмен информацией, и свободу. Если помните, на некую технологическую основу (в данном случае Интернет, Глобальную сеть) можно положить виртуальные глобальные сети - зашифрованные, защищенные. Это для тех случаев, где мы хотим добиться общей безопасности и провести там всю цепочку мероприятий, о которых говорил, все механизмы можно реализовывать.*

С другой стороны, на ту же технологическую Глобальную сеть можно положить TOR, ITUP, где никто не знает, кто с кем общается, нет никакого контроля, и содержимое контролю не поддается. Единственное ограничение, которое при этом возникнет, - думаю, что противоречий там быть не должно, - связано с тем, что вход в эту технологическую сеть все-таки должен быть не анонимным. Тогда в конечном итоге мы сможем проследить, кто совершил противоправное действие.

Теперь о том, что должны и могут делать провайдеры, как их заинтересовать такой деятельностью. Во-первых, это новая услуга. То есть, могу предложить небезопасный Интернет, а могу предложить безопасный, который будет дороже. Если данная услуга будет востребована, то чисто практически провайдер будет этим заниматься. Думаю, ему это будет интересно.

Анатолий Стрельцов: *Хотел бы добавить несколько слов. Мы решаем не столько вопрос развития сферы услуг, сколько вопрос определения ответственности государства за безопасное использование национального сегмента ИКТ-инфраструктуры. За это, по идее, отвечает государство. Как написано в докладе 2015 года, это суверенитет, ответственность государств. В любом случае, государственное регулирование здесь необходимо.*

Международное взаимодействие в области кибербезопасности в евразийских государствах - сотрудничество или соперничество?

Хиро Фудзимаки, Университет Токай (Япония): Я попытался рассмотреть ряд кейсов, конкретных примеров сотрудничества, и, откровенно говоря, к сожалению, не так много примеров нашел у нас в регионе, в Юго-Восточной Азии. Как нетрадиционные вопросы информационной безопасности функционируют в региональном контексте и на международном уровне?

Сегодня мы активно участвуем в динамике отношений Института проблем информационной безопасности МГУ и Университета Токай. В рамках этого сотрудничества нам удается обеспечивать диалог между лидирующими экспертами РФ и Японии. Имеются специальные центры ИКТ при старом Институте информации и коммуникационных технологий. В рабочем порядке мы также общаемся с нашими коллегами во всем мире.

У нас разгорелся спор с профессором Ишикава, который принимал участие в семинаре в Корее. Он указал в своем сообщении, что киберпространство находится за пределами государственного суверенитета, поэтому каждое государство должно пытаться контролировать хотя бы то киберпространство, которое к нему имеет отношение. Во всяком случае, тут же начался разговор о том, кто должен контролировать - каждое национальное государство или США. При любых усло-

виях с этим связаны большие затраты, крупные государства тоже не будут этого делать.

Профессор Ишикава предложил, что киберпространство должно контролироваться каким-то киберрежимом, можно установить международный киберрежим. Он подкрепил данный факт таким наблюдением: киберпространство - это международный рынок. Сами участники вступают в рыночные отношения с учетом определенных правил, но все равно нет некой структуры, которая бы диктовала волю участникам этого рынка с точки зрения заключения между ними транзакции, сделок.

Суверенность государства в духе традиционной Вестфальской системы - как она вписывается в новую киберсреду? Может быть, мы возвращаемся к анархии, может быть, нет возможности поместить концепцию киберпространства в нашу традиционную систему ценностей с точки зрения государственного суверенитета, насколько наша система сдвигается в сторону иерархического порядка или, наоборот, укрепляется анархическая традиция?

Давайте посмотрим на динамику. В условиях холодной войны существовало две системы - США и Советский Союз, тогда Китай не представлял угрозы как экономическая держава. Иерархический или анархический порядок? Суверенное государство, нет центрального правительства - получается анархия. Вот так графически я представляю иерархический порядок. Согласен с такой аналогией, которую привел мой оппонент относительно того, что киберпространство напоминает рыночные отношения между независимыми субъектами. Но все равно есть какие-то порядки, правила.

Региональные и международные организации устанавливают некие торговые правила. То же самое и в Интернете - получается паутина, хаотичная сеть, в которой нет иерархического порядка. В каждом регионе есть свои центры влияния, центры принятия решений - это тоже определенный порядок. ШОС - там Россия и Китай. Говорим НАТО, подразумеваем США. Альянс США и Японии. То есть все проявления регионализма

находят олицетворение в той или иной организации, которые вписываются в их иерархическую систему. Она может быть не обязательно вертикальной, а горизонтальной, но необходима некая иерархия, красота и гармония.

Приведу примеры управления на региональном уровне - ЕС, НАТО, АСЕАН. Построим такую матрицу - А и Б. Вот основные игроки, можно сказать, что обе стороны А и Б отражают некий порядок суверенной иерархии. Требования к членству: обеспечивать прозрачность демократической системы влияния, спонтанность и суверенное равенство. Это, конечно, относится и к киберпространству. Когда я говорю о стороне Б, то имею в виду следующее: например, ШОС, когда страны-участники выполняют особые требования.

Мы вторгаемся в сферу нетрадиционной безопасности, взять хотя бы военный потенциал государств. Если сравнить Россию и Молдову, то военный потенциал России в 200 раз превышает военный потенциал Молдовы. Или, например, население Эстонии, оно в 100 раз меньше, чем в России, или сравнить ВВП Казахстана и России. Это также касается и продолжительности жизни.

По всем параметрам государства отличаются друг от друга. Поэтому государства, которые относятся к стороне Б, склонны к тому, чтобы требовать установления более иерархического порядка. Подобное проявляется в борьбе с террором с использованием ИКТ, чтобы контролировать распространение враждебной информации, а также не допускать вредоносного использования ИКТ, обеспечивать легитимность государства в киберпространстве, бороться с незаконной торговлей наркотиками, обеспечивать безопасность физических границ государств и экономическое сотрудничество. В такой же плоскости лежит проблема признания суверенитета на взаимной основе, потому что твой суверенитет начинается там, где заканчивается мой. Мы должны найти какую-нибудь формулу, которая позволит существовать этим двум суверенитетам, то есть легитимность национального государства - не только в физическом смысле, но и в киберпространстве.

Киберпространство тоже является объектом суверенной защиты и атрибутом государственности. К примеру, кризис в

постсоветском пространстве: страны Центральной Азии сталкиваются с проблемами, в частности конфликт в Таджикистане и т. д. Здесь я смешал обе стороны А и Б.

Мое предложение: региональные функции обеспечения управления должны подчиняться определенной иерархии, поэтому я вступил в спор с профессором Ишикава.

Противодействие использованию ИКТ в террористических целях

Адам Хэдли, Фонд «ИКТ ради мира» (Швейцария): Я являюсь директором проекта, который состоит из четырех компонентов. Во-первых, помочь определить и проанализировать нынешние новые угрозы. Во-вторых, помочь понять существующие и возникающие развивающиеся подходы отрасли к принципам и нормам. В-третьих, разобраться в тенденциях участия частного сектора. В-четвертых, понять существующие механизмы, которые помогают формировать знания и соответствующие обучающие механизмы по этим понятиям.

Мы провели консультации в рамках трех семинаров в Цюрихе, Куала-Лумпуре и Кремневой долине, в которых приняли участие более 120 представителей технологической отрасли, гражданского общества, государственных структур и других организаций. Мы доложили о результатах на специальном заседании Комитета ООН по борьбе с терроризмом в декабре 2016 года. Хотел бы поделиться некоторыми из наших результатов и объяснить, как будет развиваться проект в 2017 году. Мы представили краткий отчет, который находится на веб-сайте проекта techagainstterrorism.org, есть перевод на русский язык.

Наша консультативная группа состояла и состоит из лидирующих технологических компаний, представителей научных кругов, гражданского общества и межправительственных организаций. В частности, нам хотелось бы поблагодарить «Microsoft», «Facebook», «Google», а также «Лабораторию Касперского» за оказанную помощь. Кроме того, у нас есть дополнительные участники инициативы.

Нам повезло, что у нас есть представители отрасли со всего мира - компании социальных сетей «Twitter», «Facebook», а также «Dropbox», другие компании. Межправительственные организации включают Всемирный экономический форум, ОБСЕ, Европол и другие. Кроме того, в работе принимали участие организации гражданского общества и по защите прав человека, например, SecDev, ACCESSNET, представители научных кругов, включая Оксфордский университет и Королевский колледж Лондона.

В настоящее время мы наблюдаем возникновение принципа открытости, который сейчас продвигается крупными организациями в условиях технологических угроз со стороны террористов. Например, «Facebook», «Google» и «Twitter» опубликовали статистику того, как они реагируют на такие воздействия. Все выразили обеспокоенность в ходе консультаций. Важным вопросом является легитимность частного сектора в формировании норм поведения. Он добился больших успехов в борьбе с терроризмом. Тем не менее многое делается изолированно от намерений и целей других заинтересованных лиц.

Кроме того, в рамках консультаций обнаружили, что небольшие компании, стартапы, обладают ограниченными потенциалом и знаниями, необходимыми для понимания решения технологических проблем в условиях использования ИКТ террористами. Это очень важный момент, потому что многие применения технологий террористами осуществляются на небольших технологических платформах, например разные криптографические средства. Поэтому необходимо взаимодействовать со стартапами, небольшими компаниями в борьбе с этими явлениями.

Также есть ограниченная доказательная база для разработки особых политических ответов на угрозы, отсутствует связь между онлайновыми и офлайновыми усилиями по борьбе с насильственным экстремизмом в этой сфере. Все это будет успешным при одном условии - увеличении инвестиций в образование, просвещение и критическое осмысление технологических понятий и процессов граждан.

В заключение первой фазы проекта - частный сектор разрабатывает достаточно сложные средства по противодействию использованию технологий террористами. Однако в других регионах существует реальный риск излишнего регулирования государственными органами. Некоторые меры, применяемые госорганами, не всегда являются пропорциональными, соразмерность ответственности тоже очень важный фактор, который необходимо учитывать.

В рамках этой работы мы хотим подчеркнуть тот факт, что частный сектор уже поддерживает противодействия контенту и принимает соответствующие меры в борьбе с использованием ИКТ в злонамеренных целях. Что касается криптографической защиты - рождается определенная система саморегулирования, это успешный проект. Публичная статистика свидетельствует о том, что «Twitter» удалось заблокировать более четверти миллиона аккаунтов, учетных записей за последний период.

Дело в том, что часто не учитываются важные факторы, касающиеся Интернета, в ходе миллионных поисков в «Google» или «Facebook», каждые две недели выкладывается более 200 млн. фотографий. Существует множество веб-сайтов, и в этом отношении нам хотелось бы подчеркнуть тот факт, что масштабы Интернета просто трудно представить, поэтому их нужно учитывать в поисках ответов на существующие террористические угрозы.

Мы пришли к заключению, что, хотя государственное частное партнерство успешно развивается, необходима дополнительная поддержка в целях углубления и расширения этих государственных частных проектов сотрудничества. Так, существует необходимость наращивания усилий по взаимодействию с небольшими технологическими компаниями и некоторыми государствами. В прошлом году мы разработали ряд рекомендаций.

Мы хотим на этом этапе проекта в рамках ООН сосредоточиться только на двух из них. Во-первых, нам хотелось бы укреплять диалог по формированию нормативной базы на основе мультистейкхолдеровского подхода посредством проводимых семинаров в 2017 году. Нам также хотелось бы развивать и

нарабатывать практические конкретные инструменты, документы, которые можно использовать в работе небольших компаний и государств.

Второе направление, четвертый пункт данного документа, а именно - создание некой платформы для обмена знаниями, это веб-сайт, с помощью которого люди могут получать примеры услуг, сервисов и общественные рекомендации, разработанные для более крупных технологических компаний. Прежде всего, мы сотрудничаем с ООН по разработке ряда многосторонних семинаров. Очень важно обеспечить устойчивый диалог, с тем чтобы представители различных стран и компаний могли продолжать обсуждение разработки норм политики, принципов и процедур. Эти семинары также предоставляют возможность обмениваться опытом и практическими уроками и выводами. Платформа по обмену знаниями даст практические инструменты и ресурсы для консолидации закрепления фактов и рекомендаций.

Мы будем тесно взаимодействовать с «Microsoft», «Facebook», «Google», «Twitter» и другими компаниями в целях разработки контента, с тем чтобы стартапы и небольшие государства могли лучше разобраться в тех мерах, которые уже успешно разрабатываются и применяются. Для этой цели мы запустили первую страницу, проект называется «Tech Against Terrorism» - технологии против терроризма. В ближайшие месяцы мы будем выстраивать сайт, который превратится в такую платформу для обмена знаниями.

В 2017 году сосредоточимся на трех направлениях нашей работы, а другие три будут справочной базой. Первое - будем работать со стартапами. Запускаем пилотный проект в Лондоне, работая с венчурными компаниями и фондами прямых инвестиций, а также с ведущими технологическими компаниями, чтобы взаимодействовать со стартапами, стимулировать приобретение ими новых знаний и инструментов, которые позволят стартапам успешно бороться с угрозами терроризма.

Более того, будем стимулировать внедрения добровольных обязательств, с помощью которых стартапы берут обязательства

уделять внимание рискам злоупотребления их технологиями со стороны террористов. В этом отношении продолжим популяризовывать успешные подходы, применяемые уже крупными компаниями. Именно такое направление демонстрирует эффективность вопросов саморегулирования.

Во-вторых, мы будем работать с рядом государств, для того чтобы понять, какие процессы и документы мы могли бы разработать для них с целью улучшения, совершенствования системы телекоммуникаций в этих странах. Мы понимаем, что многие технологические компании сосредоточены на работе на Западе, но не всегда идеально приспособлены для работы незападных государств. В рамках данного направления будем организовывать ряд глобальных семинаров, например, в Таджикистане, Бангладеш, Корее, Тунисе и Москве в начале 2018 года.

В-третьих, мы работаем над условиями обслуживания сервиса. Речь идет о правовых документах, на которые опираются технологические компании, чтобы их технологии использовались в соответствии с корпоративными требованиями и принципами. На самом деле в рамках первой фазы проекта мы обнаружили, что в некоторых компаниях нарушение этих условий используется в качестве запроса для блокирования того или иного контента. Страны принимают условия нарушения предоставления услуг или рекомендаций для блокирования нелегального контента. Это самый любимый способ для большинства государств оказывать влияние на контент на платформах социальных сетей.

Кроме того, мы будем поддерживать другие инициативы. Например, ООН сознает, что финансовые услуги - это одна из областей, которая потенциально может быть использована в этом плане с точки зрения технологий, поэтому мы работаем в тесном контакте со структурами ООН по борьбе с терроризмом, которые будут проводить симпозиум, объединяющий представителей и заинтересованных лиц, включая финансовые компании, инвестиционные и коммерческие банки и другие представительства финансового сектора.

Работа, которую мы проводим во взаимодействии с ООН, связана с противодействием идеологии экстремизма. С этой целью мы провели семинар в Цюрихе и организовываем симпозиум в Нью-Йорке «на полях» заседания Совета Безопасности для продвижения передового опыта при противодействии компаний и программ идеологического характера. Наконец, мы взаимодействуем с учеными, компаниями в области технологий и научных разработок, объясняем, как технологии могут применяться для проведения и предотвращения использования технологий для террористической пропаганды.

На этой ноте хотелось бы закончить свое выступление. Мы надеемся на дальнейшее взаимодействие с заинтересованными лицами всего мира, включая представителей Центральной Азии и РФ. Мы были бы рады возможности продолжать с вами сотрудничество по данной проблематике.

Анатолий Стрельцов: *Прекрасно понимаю, что такое реклама. Когда мне рассказывают про то, что есть успешные проекты по противодействию терроризму, у меня возникает вопрос, по каким показателям эта успешность оценивалась. Судя по тому, что происходит в мире, успешность противодействия терроризму пока оставляет желать лучшего. В связи с этим участие технологических компаний в реализации таких проектов очень уместно. В какой мере вы используете опыт организаций, которые занимаются содержательной стороной данного вопроса - именно противодействием идеологии терроризма?*

Адам Хэдли: *Наш проект направлен на оказание помощи малым компаниям, чтобы они лучше понимали, как крупные технологические компании успешно себя регулируют. Мы предлагаем им большой арсенал средств, чтобы они лучше понимали эти особенности, оформляли свои инструкции и документы с учетом опыта других и обращали внимание на риск, связанный с тем, что террористы могут использовать ИКТ в злонамеренных целях.*

На фоне широкомасштабного распространения современных технологий, конечно, это сложно делать в одиночку. Надо процесс

оптимизировать и находить конструктивные решения, чтобы установить баланс между разными конфликтующими интересами.

По поводу противодействия идеологии терроризма - это не является основным лейтмотивом нашей работы. Мы делаем упор на вызовы, которые стоят перед частным государственным партнерством, что является важным вопросом. Наши коллеги в ООН предпринимают усилия для того, чтобы обобщать и применять опыт, связанный с преодолением таких вызовов. Поэтому наш проект по линии отдельных агентств юридических коммуникаций в плане участия в информационной работе поддерживают в Великобритании, где мы работаем во взаимодействии с министром внутренних дел, а в Европе - с разными государственными структурами, которые обладают экспертными знаниями и знают, как эффективно бороться с идеологией терроризма. Например, в Цюрихе мы планируем организовать однодневную конференцию по изучению международного опыта в этом контексте. Мы также будем работать с аналогичной организацией в Нью-Йорке.

Важность атрибуции в реализации мер укрепления доверия и норм в киберпространстве

Санджай Гоел, Университет штата Нью-Йорк (США): Я также преподаю и возглавляю кафедру в Школе бизнеса при Университете штата Нью-Йорк в Олбани и являюсь исследователем в области международной информационной безопасности, поэтому не мог пропустить ни одной нашей встречи, это большая честь для меня.

Я не дипломат, а инженер. Все говорят о выработке норм кибердипломатии, киберполитики и мерах доверия. Кажется, мы приближаемся к принятию решения, но все-таки оно удаляется от нас, есть такое ощущение, что мы никогда не выйдем на него. Но при всем при этом мы не можем уменьшить усилия. Как только мы хотим ухватиться за решение, то вновь прибавляется множество проблем. Мир очень быстро меняется. Сейчас проблемы, которые стоят перед нами, сильно

отличаются от тех, которые были раньше, поэтому мы отстаем от динамики развития мира.

Предлагаю свой анализ динамики за последние несколько лет - как проблемы информационной безопасности менялись и меняются в контексте атрибуции. Проведем анализ последних инцидентов, связанных с нарушениями киберпространства. Операция «Aurora» была проведена с целью выйти на сеть 30 крупных компаний - от «Google» до «Adobe», что привело к большой потере данных с помощью использования вредоносной программы.

С марта 2014 по апрель 2015 года хакерами была запущена программа, с помощью которой украли около 21,5 млн. документов, - это данные о людях, которые являлись объектами разных оперативных проверок силовых структур. Осенью 2016 года было взломано 60 тыс. электронных писем, которые хранились на сайте центра Демократической партии, что в конечном итоге поставило в неловкое положение выборную кампанию Хиллари Клинтон.

Что мы наблюдаем? Любой может стать объектом взломов - и политические партии, и государственные структуры, и частные крупные компании. Поэтому невозможно определить конкретный субъект или объект нападения. Либо силы защиты оказываются слабыми, либо слишком изощренными и хитрыми становятся хакеры. Давайте с этим разбираться.

Далее. Хакеры хотят «уколоть» и исчезнуть? Нет, они приходят надолго и всерьез и остаются. Раньше они уходили, а теперь они проявляют настойчивость и многие месяцы, годы могут продолжать свою работу.

Можно говорить и о человеческом факторе - отсутствии бдительности, многие становятся объектами фишинговых атак, но это не приводит к повышению эффективности защиты. Люди начинают задумываться - это вопрос не «если», а «когда». Что произойдет, когда нас взломают? А это неизбежно случится. Надо перейти от выявления к прогнозированию и надо должным образом реагировать на случившиеся инциденты и их последствия.

Сейчас многие компании делают серьезные вложения, чтобы разобраться с этим, преодолевать последствия и пытаться их прогнозировать. Что общего между такими атаками? Опять же атрибуция.

Многие обвиняют Китай, Россию, Северную Корею в том, что они являются, по мнению многих наблюдателей, виновниками данных инцидентов. Но все-таки не было представлено ни одного доказательства, только голословные утверждения, которые не выдерживают критики.

Кибердипломатия запущена в разных конференциях, очень много написано о кибернормах в сфере международной информационной безопасности. ГПЭ ООН тоже активно продвигает нормы и меры доверия, но все равно воз и ныне там, перед нами верхушка айсберга. Эти явления оказываются более глубокими.

Без решения вопроса атрибуции, без механизмов верификации очень сложно двигаться вперед и укреплять меры доверия. Как можно установить доверие, если невозможно установить причину и верифицировать источник атак. В рамках атаки данные распределяются на разных серверах, поэтому их нужно оперативно мониторить до того, как они исчезнут. Потом их практически невозможно изыскивать.

Мы должны постоянно мониторить, коррелировать с тем, что имеется, и отслеживать деятельность таких групп, которые занимаются взломом. Как только мы выявляем, кто это - группа или индивидуальные лица, - надо определить их мотивы - они сами по себе работают или они выполняют чей-то заказ. Косвенные доказательства опираются на разведданные, которые у нас имеются. Ни одна страна не будет раскрывать свои источники информации. Это затрудняет работу по взаимодействию между спецслужбами.

Нам нужны не только источники данных, но и разведка непосредственно на местах, чтобы каждый разведывательный орган мог иметь глаза и уши везде, чтобы прогнозировать потенциальные атаки. Тогда мы можем приблизиться к пониманию вопроса атрибуции, и в таком случае, например, Россия, Китай

или любая другая страна смогут защититься и сказать, что это не мы и что на самом деле это сделало третье лицо.

Но мы далеки от этого. По мере того как мы стараемся выработать меры доверия, мы не осознаем, что без решения вопроса атрибуции меры по укреплению доверия обречены на неудачу. Нет верификации, нет возможности проверить атрибуцию, соответственно, нет доверия. Созданы центры групп обмена информацией по ликвидации компьютерных инцидентов. Из разных стран поступает информация, нужно установить программу стандартов, чтобы они были универсальными. Это касается и приватности, неприкосновенности частной жизни, защиты данных и т. д.

Следующий момент - отсутствие доверия. Можно считать, что киберпространство воспринимается в качестве новой плоскости противодействия и конфронтации в дополнение к классическим средам. Через киберпространство можно следить за перемещением войск в физическом пространстве. В условиях отсутствия надежной информации страны наращивают свои киберарсеналы и изыскивают слабые места в системах других стран, которые можно использовать в ходе военных конфликтов. В плане взаимодействия успехов мало. До того, как мы найдем способ установить атрибуцию, будет очень трудно увидеть, как эта гонка вооружений в киберпространстве может быть остановлена и обуздана. Кибергонка вооружений переходит в киберпространство.

Здесь важным моментом является информация или дезинформация, пропаганда, информационно-массовая работа и вмешательство во внутренние дела. Мы это наблюдали во время революций, которые были инспирированы социальными сетями. Нужно четко различать использование ИКТ отдельными лицами или организациями и наконец делать ставку на те организации, которые могут выполнять задачу третьих лиц. Ни одно государство реально этим не занимается и поддерживает эти организации опосредованно, чтобы скрыть свои следы, поэтому трудно определить источник тех или иных атак.

Что нас ждет в будущем? Будут наблюдаться три инновации. Все они связаны с коммуникациями. Во-первых, это Smart Grid - сеть, которая приведет к революционным изменениям в плане генерирования распределения электроэнергии. Во-вторых, автономные машины, без водителя. В-третьих, мобильные устройства, которые управляются на расстоянии и могут имплантироваться в человека. Все это может активно использоваться для нанесения серьезного ущерба государственным и критически важным инфраструктурам. Сетевая интегрированность машин будет связана с другими автомобилями, производителями, со станциями техобслуживания. То же самое наблюдается и в других отраслях. Если вывести из строя систему управления автономными транспортными средствами, то будет хаос на дорогах и массовые ДТП через отключение светофора.

По мере движения вперед нам надо двигаться параллельно, для того чтобы создать эти правила. В конце концов, нам надо решить вопрос атрибуции, без чего мы не можем продвигать меры доверия.

Павел Пилюгин: *Понимаю, что к решению любого вопроса надо идти шаг за шагом. Начинать нужно, наверное, со списка атрибутов, а потом смотреть, какие механизмы внедрять, чтобы можно было их получать при расследовании инцидентов. Вы можете предложить хотя бы такой список?*

Санджай Гоел: *Во-первых, вопросы технической атрибуции. Это, пожалуй, самый легкий аспект. Компании, спецслужбы собирают данные и объединяют эти пунктирные линии. Во-вторых, стандартные шаблоны сбора данных, с тем чтобы все понимали, что означают эти данные. В-третьих, в этом велика роль спецслужб, нужно понять, какие регионы наиболее важны, с тем чтобы сосредоточить анализ именно на этих регионах, откуда поступают атаки. Наконец, понять, есть ли связь с государственными органами. Мы считаем правильным пошаговый подход. Проблема сложная, но мы достаточно далеко продвинулись в этом направлении, и пора конкретно решать эти вопросы.*

Владислав Шерстюк: *Полностью согласен с Санджаем, готов подписаться под каждым его словом. На наших форумах в 2004 и 2005 годах мы говорили, что нужно вводить правила, сравнивая их с дорожным движением - без правил не может быть дорожного движения. Десять лет - срок приличный, особенно на фоне того, с какой скоростью развивается Интернет. Можно сказать, что мы все вместе эти десять лет потеряли. Но вместе с тем за эти годы ШОС направил документ в ООН, появились его сторонники, начала работать Группа правительственных экспертов.*

Сегодня все наши усилия должны быть направлены на то, чтобы эти правила были приняты как можно раньше. Установим правила, потом мы должны научиться им следовать, затем должна появиться атрибуция, а дальше не спеша появится доверие, потому что на ровном месте доверие не построишь.

Я наблюдаю, как форум модернизируется, мы меняемся в последние годы. У нас действительно нет принципиальных разногласий. Есть задача в донесении до научной общественности, политиков, руководителей нашего экспертного мнения. Еще раз хочу сказать, что по принципиальным позициям мы имеем одинаковые точки зрения.

Нам надо решить организационные вопросы. Я уже говорил о том, что в наш консорциум входят 24 организации из 16 стран. Сегодня мы будем принимать в МИКИБ четыре организации. Но прежде чем мы это сделаем, давайте заслушаем информацию о выполнении решений 13-й научной конференции МИКИБ.

Ринат Шаряпов, ответственный секретарь МИКИБ: *У вас, уважаемые коллеги, на руках текст прошлогоднего решения, с тем чтобы вы могли вспомнить, что мы запланировали на этот год. По нашему мнению, все решения, которые были зафиксированы в том документе, в той или иной мере выполнены.*

По пункту 1 было предложено включить в перечень научных направлений восемь тем. Практически все доклады - как участников консорциума, так и других выступающих этого форума - пересекаются или полностью дополняют тематику, отраженную в этом пункте. Обратите внимание, что три «круглых стола»

нынешнего форума полностью соответствуют трем из восьми направлений. В рабочем порядке постоянно происходит обсуждение с участниками консорциума, как и в каком виде продолжать работу по тому или иному направлению.

Пункт 2 - по поводу работы интернет-ресурса нашего консорциума. Напомню, что организационно-техническое сопровождение консорциума осуществляет Научно-исследовательский институт информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева из Республики Казахстан, организацией - членом МИКИБ. Наибольшую активность проявляет информационный портал Digital.Report - организация, которая работает с членом консорциума The SkDev.FOUNDATION из Канады. За последние полгода на сайте консорциума нами было размещено не менее 20 материалов, в том числе 15-16 ссылок на аналитические материалы, обзоры публикаций, которые были подготовлены как нашим институтом, так и коллегами информационного портала Digital.Report.

Мы продолжаем сотрудничать в этом направлении, собираемся отбирать наиболее актуальные материалы и оперативно размещать на сайте консорциума. Еще раз призываем всех наших коллег активнее использовать возможности нашей интернет-площадки по ее информационному наполнению.

Пункт 3 - участники МИКИБ согласились оказывать методическую и информационно-аналитическую поддержку Аналитическому и учебно-методическому центру, созданному при Институте электроники и телекоммуникаций Кыргызского государственного технического университета им. И.Раззакова. По нашей последней информации, этот центр проходит процедуру юридического, финансового, организационного оформления в Республике Киргизия. Просим вас не забывать о том, что мы взяли на себя обязательства помогать этому центру и, когда он начнет работать, будем все вместе его поддерживать.

Пункт 4 - все участники МИКИБ были проинформированы о мероприятиях, запланированных еще в прошлом году, как в Киргизии, так и США. Члены консорциума знают, что на ноябрь прош-

лого года намечалось проведение 14-й научной конференции консорциума. Была предложена программа, приглашены спикеры, большое количество участников консорциума собирались прибыть в Бишкек, принять участие в этой конференции, но по серьезным и объективным причинам данное мероприятие в Бишкеке не состоялось. Поэтому 14-я научная конференция консорциума была перенесена на апрель сего года.

Пункт 5 - о вступлении в консорциум новых членов. Предполагалось вступление в МПКПБ двух институтов на несостоявшейся конференции в Бишкеке, которые постоянно участвуют в наших мероприятиях, - это Международный институт стратегических исследований из Великобритании и Институт киберполитики из Эстонии. Процедуру принятия новых членов не удалось провести, поэтому мы перенесли данное мероприятие на сегодня.

За текущий год к нам обратились еще две очень серьезные и авторитетные в России организации: «Лаборатория Касперского» и редакция журнала «Международная жизнь», представители которых уже не в первый раз принимают участие в нашем форуме. Год назад при поддержке журнала «Международная жизнь» мы провели прекрасный «круглый стол» в рамках нашего форума, а зимой этого года журнал организовал очень авторитетную конференцию на площадке МИД России, посвященную тематике международной информационной безопасности. Мы разослали всем участникам консорциума обращения этих двух организаций с просьбой о приеме. Мы не получили ни одного отрицательного отзыва, поэтому считаем, что имеем сегодня право принять и два института, и две организации в члены нашего консорциума.

Владислав Шерстюк: *Мы приступаем к торжественной части подписания документов. Спасибо большое за участие и в пленарном заседании, и заседании консорциума. Считаю, что мы очень достойно поработали сегодня. То, что нам удалось сделать, конечно, будет учтено в дальнейшей работе, и в практическом, и научно-исследовательском смыслах.*

Семинар - «круглый стол» №1

Механизмы выполнения правил ответственного поведения государств в ИКТ-среде

Валерий Ященко, Институт проблем информационной безопасности МГУ им. М.В.Ломоносова: *Продолжим обсуждать вопрос: как можно выполнить правила поведения в информационной сфере, которые, надеюсь, будут приняты? Было обозначено порядка 19 правил, они замечательные, но не раскрывают характера декларации. Остается масса вопросов о том, как понимать то или иное слово, каков механизм реализации и какой способ контроля. Это мы и продолжим сегодня обсуждать.*

Создание негосударственных норм: роль технических сообществ и последствия для государственной политики

Андреас Кюн, Институт Восток-Запад: Наш институт всегда с большим удовольствием принимает участие в гармишевском форуме. У нас подписано много соглашений, мы проявляем свою приверженность необходимости укрепления диалога для обеспечения ответственного поведения в киберпространстве. И гармишевский форум как раз и представляет замечательную платформу, которая позволяет нам наращивать данный процесс.

В марте этого года у нас в Калифорнии проводился семинар на аналогичную тему, был подготовлен список норм универсального назначения для обеспечения ответственного поведения в киберпространстве. Поделюсь своим личным мнением, как сделать технические сообщества драйверами применения норм ответственного поведения. Позвольте сразу акцентировать основной вывод: есть действительно нормы,

которые определяются государствами, и они должны обеспечивать безопасное использование киберпространства.

Давайте разделим это на три части. Первое - нет негосударственных норм, которые отличны от норм, устанавливаемых государством. Второе - есть технические сообщества, которые также выполняют важную функцию в киберпространстве и надо к ним тоже прислушиваться при разработке таких правил и норм, чтобы сделать киберпространство более безопасным. И третье - нужно найти равновесие между нормами поведения, которые устанавливаются государством, и теми, которые устанавливаются сообществом. Государственные нормы фиксируются межгосударственными соглашениями, уже имеется порядка сотни двусторонних соглашений в области информационной безопасности, информационной политики и сферы ИКТ. Однако мы упускаем из виду важную часть реальности - серьезное техническое развитие, которое провоцирует инциденты, часто остающиеся за пределами нашего внимания, вне действия этих правил. Мы отстаем от реального технического развития.

Чем занимаются государство и технические сообщества и как между собой они могут договориться относительно определения норм? Есть очень важные институты, о которых мы часто забываем, но они также имеют отношение к управлению Интернетом и утверждают, что эти технические нормы, которые продвигаются техническими сообществами, вызывают серьезные последствия для реальности киберпространства. Можно также попытаться установить некий этический кодекс поведения. Хочу обратить внимание только на ряд примеров для того, чтобы обсудить такие технические нормы и их последствия для государственных норм. Но сначала нужно договориться об определениях, что́ такое нормы и что́ такое методы управления. Говорят о сдерживании и стимулировании, о моделировании, о рамочных отношениях и установлении обычных правил, направленных на восстановление тех процедур, которые должны учитываться всеми акторами при реализации их поведения в киберпространстве. Акцентируется необходимость согласования усилий между государственными и негосударственными инсти-

тутами для выработки согласования таких норм. Итак, стимулирование или ограничение, моделирование, и рутинное взаимодействие, и согласование усилий. Вот, по этим разным моделям можно строить отношения между государствами и техническим сообществом.

Поговорим о негосударственных институтах, которые вырабатывают технические нормы, но и они имеют непосредственное отношение к выработке государственных норм, регулирующих безопасность в информационной среде. «Майкрософт» отработал в 2014 году свои подходы, предложил нормы для государственного поведения и в 2016 году внес уточнения с учетом мнений глобальных компаний ИКТ. Это - первая универсальная попытка разработки технических норм техническим сообществом, которые могли бы быть взяты на вооружение государствами. Это стало важной вехой на пути разработки норм ответственного поведения государств в киберпространстве, причем по инициативе технического сообщества.

Вчера мы выслушали доклад представителя «Норильского никеля», который впечатлил мерами, направленными на критические объекты инфраструктуры, для обеспечения устойчивости, и преемственности, и целостности бизнеса на уровне

крупного предприятия. Что касается Internet Engineering Task Force - создана оперативная группа для описания стандартов, необходимых при учете и составлении таких норм. Это техническое сообщество, которое объединяет инженеров, ответственных за стандарты, через разные публикации развивает тему общих стандартов информационной безопасности. Технические стандарты согласовываются с указанной группой на основе принципа «грубого» консенсуса, и именно такой подход - вертикальный, снизу вверх, который продвигается указанной группой, - признает важность этого мероприятия по двум причинам.

Первое - памятуя о важности такого вертикального процесса, создаются и реализуются стандарты и технические нормы по всему техническому сообществу Интернета; второе - признается необходимость того, чтобы эти процессы учитывались государствами также при разработке государственных норм, направленных на обеспечение ответственного поведения. И еще момент - раскрытие информации об уязвимости. Это связано с процессами выявления разных уязвимостей. Техническое сообщество уже 30 лет ведет дебаты на эту тему: что должно быть сделано, когда мы выявляем уязвимость в программном обеспечении, - раскрывать информацию или сохранять в секрете? Нужно выработать стандарт - как будет выглядеть ответственное поведение, ответственная реакция таких разработчиков программного обеспечения, которые обнаруживают уязвимость? Нужно, несомненно, предусматривать механизмы, стимулирующие таких разработчиков принимать оперативные меры по ликвидации, устранению выявленных недостатков. И это тоже должно учитываться государствами при выработке норм относительно установления порядка в раскрытии информации о вскрываемых уязвимостях.

Думаю, что лучше иметь правила, чем их не иметь, и в 2013 году как раз было разработано понятие «Intrusion Software», то есть вредоносное программное обеспечение, которое внедряется в систему для враждебного использования. Если такие меры не принять, то будет в значительной степени ослаблена информационная безопасность, это должно учитываться в государствен-

ных нормах, которые устанавливаются на десятилетия. Приведу пример, связанный с работой нашего Института Восток-Запад. Мы продвигаем нормы безопасности в киберпространстве вместе с нашими партнерами, такими как «Майкрософт» и др. Разработали наставление для сферы ИКТ, где установили ряд требований относительно преодоления рисков для разработчиков и компаний, которые оказывают услуги в области ИКТ.

Государства должны учитывать предложения, выдвигаемые техническим сообществом при разработке норм, все стороны заинтересованы в установлении этих норм и их жестком соблюдении. Чтобы этого добиться, необходимо устанавливать когерентные нормы по всем режимам, о которых мы говорили, не важно, технические они или государственного происхождения, нужно работать для обеспечения координации всех мер и обмениваться подходами с техническим сообществом. Нужно быть в постоянном контакте, государство не может не извлекать выгоду из активного взаимодействия с представителями научных кругов, технического сообщества, ведь частный сектор в значительной степени управляет и владеет технологией ИКТ и инфраструктурой, которая, собственно говоря, и обеспечивает функционирование Интернета.

Принципы международной информационной безопасности

Энекен Тикк, Лейденский университет (Нидерланды), Мика Кертуннен, Институт киберполитики (Эстония): Мы посвятим свое сообщение государственным нормам и процессам. Международные нормы кибербезопасности находятся в некоем тупике, вернее, диалог относительно разработки норм поведения в киберпространстве переживает тупиковое состояние. Несмотря на уже 20-летний период переговоров по линии ООН, в частности, не удалось выработать эффективный режим международной информационной или кибербезопасности. Более того, к сожалению, нужно отметить, что мы наблюдаем эрозию, размывание существующих международных норм. Речь

идет о различиях в толковании международного права. Не выработана общая политика относительно того, как действующие международные нормы могут или не могут применяться к киберпространству. Наоборот, зачастую используется правовая казуистика, придирки к каким-то формальным признакам для непризнания применимости существующих международных норм к киберпространству. Правильно говорил вчера посол Крутских, что крупные страны, которые обладают серьезным потенциалом в плане ИКТ, заинтересованы в обеспечении стратегической стабильности и безопасности.

Но что же такого произошло с процедурами, почему мы оказались в тупике? 111 стран присоединились к резолюции и поддерживают ее. Казалось бы, есть определенный прогресс, есть рост. Но, несмотря на этот успех, изначальная идея недопущения использования ИКТ в качестве оружия трансформировалась в разговор о выработке добровольных принципов и норм ответственного поведения. Принципы, нормы и правила - это все-таки разные вещи. Ведь в данной аудитории находятся носители разных взглядов, и как мы можем определиться с тем, что такое справедливо, что правильно, что неправильно, что хорошо, что плохо и где причина, где следствие, где яйцо, где курица?

Мы предлагаем новые нормы. Нормы - это ожидание поведения, определяемого в условиях прав и обязательств, то есть это та совесть, на которую мы рассчитываем у соседа, да? Правила же - это конкретные предписания относительно действий, например, на национальном уровне, в отрасли, где отсутствие принципов или каких-то ценностных убеждений является менее проблематичным. Часто приводят пример с правилами дорожного движения. Ограничение скорости - какое правильное? У нас 70-90, в Финляндии - 80-100. Это правила. Каковы принципы? Мы разделяем одни и те же принципы даже с американцами, которые исчисляют это в милях. Скорость в определенных местах, на определенных типах дорог может повышать или понижать количество ДТП, и это влияет на понимание того, что правильно и что неправильно. И правильно то, что, ска-

жем, перед школами или детскими садами мы едем медленнее. Это принципы. Они едины, но правила разные. Есть правостороннее, есть левостороннее движение в мире. Опять же, принцип состоит в том, чтобы движение было бесперебойным и безопасным. Некоторые страны делают это так, другие - иначе, но принцип единый.

Пока мы не договоримся об этих принципах, абстрактных, но достаточно четких и распространенных взглядах на проблему, на факты, на решения проблем, мы не сможем добиться реального консенсуса по нормам. Пока мы не договоримся о принципах, нормы и правила не дадут определенности или ясности понимания вещей. Мы понимаем, что то, что имеется в плане норм, недостаточно, поэтому мы предлагаем новые нормы, но мы не можем решить, пока не договоримся о том, что является тем или иным понятием.

На сегодняшний день существуют 58 регуляторных документов, имеющих отношение к преступности, 20 - касается телекоммуникаций, 25 - по защите личных данных и прав человека, 16 - по защите сетей, 24 - по международному предотвращению конфликтов и т. д. Они раздроблены, разные режимы в рамках различных организаций, но это не принижает их роль как существующих норм, на основе которых мы должны формировать, выстраивать новые предложения и вопросы практической реализации.

А чего нет у нас? В качестве ответа или размышления предлагаю следующее: когда я задаю себе вопрос: «Нужны ли нам новые нормы?», то задаю еще много вопросов, а именно: первый - какую проблему нужно решать? Следующий вопрос - есть ли существующие принципы и нормы, охватывающие эту проблему? Они могут быть разбросаны по разным режимам. В некоторых случаях мы должны также спросить: а могут ли эти существующие нормы применяться к решению данной проблемы? Могут быть политические вопросы или политические препятствия на пути решения этой проблемы. Например, принцип неагрессии, регулирование Международного союза электросвязи и т. д.

Если мы оказались в ситуации, к которой не можем эффективно применять существующие нормы и правила, вопрос следующий: этот пробел, эта лакуна качественная или количественная? Если это количественная лакуна, это означает, что норма есть, но недостаточно стран к ней присоединились. Классический пример - конвенция о киберпреступлениях. Должны спросить, насколько реалистично надеяться на то, что все страны подпишутся. Качественная лакуна состоит в том, что норма есть, или, может быть, есть, но необходимо преодолеть различные проблемы, связанные с разной интерпретацией и толкованием. Есть меньшинство, которое считает, что шпионаж запрещен по международному праву, я не хочу выступать за эту точку зрения, но она - одна из возможных.

Мир не может договориться по многим вопросам. Если мир раскололся, то тогда необязательно нужна новая норма. Может быть, необходимо просто убедить друг друга в справедливости той или иной нормы? Если это так, надо задаться вопросом: есть ли уже существующее предложение о введении такой нормы? Мы знаем, что́ предлагает отрасль, мы знаем, что отдельные страны представили предложение в рамках ГП по каким-то нормам. Можно ли воспользоваться этими предложениями, потому что это означает экономию усилий в рамках нормативного процесса? Затем, может быть, существуют какие-то практики, имеющиеся или рождающиеся, которые надо поддержать для достижения наших целей, потому что очень часто труднее добиться практической реализации? Надо учитывать опыт организации профессионалов в этой сфере.

И следующий вопрос, который здесь не обозначен, нужна ли нам совершенно новая норма? Если нам нужна новая норма, мы все равно должны задать еще ряд дополнительных вопросов. Должна ли эта норма быть международной? Должна ли она носить обязывающий или необязывающий характер? Может быть, вводя такую норму, мы разрушим баланс или создадим новое равновесие сил. Другое возможное последствие состоит в том, что результаты введения такой нормы могут быть контрпродуктивными, отрицательными. Следующий во-

прос - как я буду поддерживать, продвигать введение, внедрение этой нормы, какие процессы-акторы нужны для имплементации той или иной нормы?

Южная Корея, Финляндия, Эстония, Нидерланды больше внимания уделяют данным принципам и нормам, чем другие страны. На этом основании некоторые обвиняют нас в казуистике, в том, что мы тормозим процесс этими мелочами. Да, но, говоря о правилах, о международном праве, нам действительно нужно заниматься казуистикой и мелочами. Надо говорить о принципах прежде всего. Когда мы договоримся о принципах, тогда сможем дальше договориться о конкретных нормах. Что касается основного вопроса - как нам реализовывать уже предложенные нормы? - консенсуса пока прочного нет. Профессор Стрельцов предлагает хороший путь - широкое обсуждение норм, которое объединяет различных специалистов, владеющих передовой практикой международного права, знающих о том, как объединить эти нормы. Думаю, это наиболее оптимальный способ использования с учетом рекомендаций Генерального секретаря. И надо учитывать, что эти нормы могут применяться к реальным проблемам.

Вопрос: *Классификация - принципы, нормы, правила - представляется очень точной и корректной, и мне особенно понравился вывод, который я тоже хотел бы проговорить в своем выступлении, о том, что коалиции по поводу принципов могут отличаться от коалиций политических. Считаете ли вы, исходя из той классификации, которую предложили, что правила поведения государств - это удачная формулировка того, что имеется в виду, или бы вы все-таки считали, что это лучше сделать более точно в соответствии с тем, как вы излагали в презентации? То есть насколько удачна та форма, в которую предлагается облечь нормы, касающиеся регулирования деятельности государств в киберпространстве?*

Ответ: *Ответ может быть таким: неважно, какого цвета кошка, главное, чтобы мышей ловила. В этом контексте более важно то, как хорошо управляется эта процедура и как она оформляется. В контекс-*

те ГП мы увидели, что это формула норм, правил и принципов привела к единому толкованию, без разграничения этих понятий в ходе процесса. Можем ли мы решить эту проблему? Да, конечно, это вносит определенную путаницу, и, наверное, нам надо уточнить терминологию. Я не юрист и поэтому использую слова так, как хочу, свободно, и у меня есть определенные возражения к термину «правила поведения государств», потому что в моем понимании это касается того, что, так сказать, подписано, утверждено. Здесь ведь нет ссылок на какие-то договоры. Мы просто должны договориться о том, что представляет собой ответственное поведение государств. И в рамках этой договоренности мы будем обсуждать содержание, принципы. Нам необходимы принципы здесь. На этом можно было бы остановиться. И что касается государственной практики, обычной практики, возможно, постепенно надо более четко выражать эти принципы и двигаться по направлению к правилам, но начинать с правил - это все равно что на дерево взбираться с верхушки, а не снизу.

Анатолий Стрельцов: *Я, конечно, во многом согласен с тем, что говорили Энекен и Мика. Но хотел бы дать небольшой комментарий к тому, что было изложено в докладе. Прежде всего, основное, с чем согласились все группы правительственных экспертов, - принципы международного права применимы к киберпространству. И дальше мы от этих принципов пытаемся двигаться вперед. Второе - совершенно понятно, что не все принципы и не все нормы международного права связаны с ИКТ-средой. Поэтому можно было бы выделить те нормы, которые связаны с использованием ИКТ-среды. Например, 51-я статья Устава ООН. Понятно, что если мы не договоримся о том, как трактовать вооруженное нападение применительно к враждебному использованию ИКТ, то трудно говорить о применимости данной нормы. А если взять весь Устав ООН, а там больше 100 норм, то основная часть этих норм вообще не связана с ИКТ. Они применимы ко всему, и к ИКТ в том числе.*

Ведь что сделала Группа правительственных экспертов ООН? Она сказала - да, все принципы применимы, но мы сейчас не в состоянии обсуждать все принципы сразу. Давайте выберем какое-то маленькое направление, с точки зрения экспертов, принципиальное, и по-

пытаемся по нему продвинуться. Вот 25 стран выбрали маленькое направление, мне даже само название не важно - нормы, принципы, правила. Основное - они попытались предложить и договорились между собой о том, что эти формулировки могут привести нас в сторону поддержания мира. Если мы научимся подобные формулировки наполнять конкретным юридическим содержанием, научимся их применять, то дальше можно будет продвигаться к следующим принципам и нормам.

Таким образом, когда мы говорим о том, что нам нужно продвигаться вперед, мы совершенно четко понимаем, что нужна команда, в которую входили бы юристы, военные, инженеры, возможно, спецслужбы, если это не военные. Эти люди должны были бы подумать над тем, что мешает нам сейчас применять эти принципы, правила и нормы ответственного поведения в киберпространстве.

Ведь что такое правила ответственного поведения? Есть проект конвенции о международно-правовой ответственности государств за нарушение международного права. Он не двигается вперед. Каждые три года его вносят на рассмотрение Генассамблеи и каждые три года возвращают обратно на доработку. Боюсь, что и в нашей сфере дела так и будут двигаться туда-сюда. Самое плохое в этих предложениях, что они предоставляют каждому государству возможность самостоятельно определять, есть ли нарушение международного права или нет нарушения международного права со стороны других государств, и самим применять санкцию по поводу данного нарушения, никого особенно не спрашивая. Хотелось бы, чтобы классификация тех или иных деяний или действий в ИКТ-среде была более-менее объективной.

Есть два рода презумпции: презумпция доверия к национальным органам обеспечения правопорядка и безопасности, это так, как мы сейчас работаем. Когда каждый глава государства или аппарат опирается на ту информацию, которую ему предоставляют снизу соответствующие органы, и исходя из этих заключений принимаются какие-то решения. Последние пять лет, а два года особенно, показали, что работа на презумпции доверия к своим правоохранительным органам имеет определенные недостатки. Впервые в Соединенных Штатах меня атаковали так агрессивно по поводу того, что

мы якобы помешали проведению выборов в Соединенных Штатах. И это на основе презумпции доверия к работе своих правоохранительных органов.

Давайте перейдем на презумпцию доверия к третьей стороне. Это придумано человечеством не сегодня, это было всегда. Когда есть два спорящих, всегда появляется некто третий, это может быть император, суд, не важно кто, но это тот, кто независим, кто находится вне дела, кому доверяют и кто обладает объективной информацией по поводу того, что́ надо делать.

У нас практически во всех странах есть национальные CERTы. Я далек от мысли, что мы сейчас будем разрабатывать какие-то технические стандарты, заниматься техническим регулированием, но CERTы на уровне каких-то политических договоренностей могли бы заняться разработкой технических правил, объективизацией событий, происходящих в ИКТ-среде, в процессуальных действиях, которые необходимо применять для того, чтобы зафиксировать эти события в форме, в которой это можно было бы представить суду или для двусторонней консультации и т. д. Так вот, если бы мы смогли создать под эгидой ООН, Красного Креста и Красного Полумесяца и других, но не технических организаций типа Международного союза электросвязи, а организаций, отвечающих за безопасность, мне кажется, вполне можно было бы решить эту проблему.

Комментарий из зала: *У меня более пессимистичный взгляд на ГП, он определяется следующим: это мета-соглашение, применимость неприменимости международного права, - это лучшее, что нам удалось добиться? Некоторые страны отказываются от большего в силу трех соображений. Это якобы не мандат ГП, ГП не имеет таких полномочий, второе - мы не должны создавать нормы международного права и третье - у нас нет потенциала, физического, кадрового и т. д. Вот этим объясняется мое пессимистическое настроение относительно ГП.*

Что касается применимости 51-й статьи Устава ООН. Приравнивается ли кибератака к вооруженному нападению? Это понимание воспринимается одними как слишком позволительное, разрешительное, другими - слишком ограничивающее. Проблема в том,

что нет общего понимания и нужно найти какое-то компромиссное решение между двумя крайностями. В противном случае мы сталкиваемся с проблемой, что, допустим, будет два набора правил, по одному - применять силу, по другому - не применять силу.

Следующий момент - добросовестность. Есть отчеты минимальные, по минимально согласованным вопросам, тогда можно добиваться консенсуса. Но все равно мы упираемся в одну и ту же проблему. Один и тот же отчет может по-разному толковаться в разных странах. Если страны не готовы отдавать полномочия кому-то еще, то этого не произойдет. Не хотят, так сказать, третьим лицам доверять, чтобы они выполняли их задачи и заказы. Ну это вопрос больше философский. Под эгидой какой организации восстанавливать такую структуру? Это не самый сложный вопрос, и если мы не сможем решить проблему на принципиальном уровне, то как мы дальше сможем двигаться и создавать вот такую структуру, о которой вы говорите, не на техническом, а на политическом уровне.

Фактор доверия в обеспечении информационной безопасности: опыт корпорации ICANN

Михаил Якушев, ICANN: Хотелось бы убедить коллег в двух основных моментах. Во-первых, почему наша организация, глобальные интернет-сообщества так активно выступают за соблюдение принципа учета интересов всех связанных с этим вопросом сторон. И во-вторых, насколько важен в выработке норм, касающихся кибербезопасности, управления Интернетом, фактор доверия. Мы называемся «корпорация по присвоению имен и номеров», основываемся на принципе «участия всех заинтересованных сторон». Наша миссия - координация системы глобальных идентификаторов, не более того. И к этим идентификаторам относятся как всем известные доменные имена, IP-адреса, так и менее понятные номера автономных систем, протоколы и порты, и, соответственно, мы отвечаем за реализацию результатов координации этих глобальных процессов. Сейчас эти процессы выделились в организацию, не связан-

ную уже никак с американским правительством, под названием «Public Technical Identifiers» (PTI).

Мы не являемся единственной организацией, которая этими вопросами занимается, мы обеспечиваем работу Интернета вместе с другими организациями глобального сообщества, причем не только технического плана, но и таких организаций, как межправительственные, межгосударственные, например Международная организация по стандартизации. Мы предоставляем и регулируем домены верхнего уровня и в этой связи, скажем, домены Западной Сахары или Тайваня, которые не признаются независимыми государствами, так было решено межправительственной организацией, а доменов, связанных, например, с Косово или Абхазией, - нет, пока соответствующие решения не будут приняты межправительственной организацией ISO.

Но есть и еще более широкое сообщество, в рамках которого мы работаем, это организация, которая предоставляет интернет-технологии, связанные и с культурой, и с безопасностью, и с образованием, и с множеством других аспектов. В выработке решений участвуют многие тысячи если не десятки тысяч людей, экспертов, политиков на добровольной основе,

на взаимном доверии к друг другу, поскольку сам Интернет в значительной степени развивался именно как техническая система, основанная на доверии тех людей, которые ею управляли первоначально.

Важно подчеркнуть, что те нормы, которые разрабатываются в рамках сообщества ICANN, - стандарты, политики, процедуры - относятся не столько к нормативно-правовому регулированию, сколько к нормативно-техническому, технологическому регулированию. Именно поэтому все работает достаточно успешно, и именно поэтому такое важное значение имеет профессионализм, компетентность людей, которые вовлечены в процесс принятия решений. Правление ICANN - это 21 человек, оно формируется по достаточно сложной демократической процедуре и утверждает решения, которые принимает сообщество. Каждый имеет шанс стать членом правления, быть избранным в его состав и участвовать непосредственно в утверждении соответствующих решений, но и без того, чтобы быть причастным к Правлению ICANN, можно участвовать в процессе разработки таких решений.

Наша организация сравнительно небольшая, нас всего лишь 370 человек, представляющих 50 стран мира, мы базируемся примерно в 30 странах мира. Наш офис, отвечающий за регион Восточной Европы и Центральной Азии, находится в Москве. У нас три глобальных штаб-квартиры - в Лос-Анджелесе, Стамбуле и Сингапуре. Среди вопросов, которые мы решаем, и корневые серверы, и новые домены, как национальные страновые, так и домены общего пользования, это распределение IP-адресов, номера протоколов, то есть это все те технические параметры, благодаря которым Интернет работает как Интернет. Но я еще раз хочу подчеркнуть, что мы не единственные в этом процессе, и, скажем, принципы распределения сетевых адресов, то есть тех технических цифровых символов, которые объединяют компьютеры в единую сеть, мы формулируем на глобальном уровне, но непосредственно операторам связи эти сетевые адреса предоставляются уже другими организациями. Таких организаций по всему миру пять.

Что же можно взять из опыта работы ICANN для того, чтобы мы могли говорить о разработке уже не технологических, а правовых нормативных правил. Во-первых, собственно постановка проблемы - возможно ли международно-правовое регулирование использования технологий на государственном, межгосударственном уровнях и т. д. Если да, то что и какими методами регулировать, если нет, то почему и каковы альтернативы. Споры эти не закончены, и до сих пор международно-правового глобального механизма нет. Хотя имеется позитивный опыт в смежных сферах. Можно найти аналогии в теории международных пространств, будь то морское или космическое право или регулирование радиочастотного спектра, который также имеет транснациональный характер.

Этот опыт нужно учитывать при разработке международно-правового регулирования ИКТ, поскольку участников того, что мы называем Интернетом, кибербезопасностью, информационной безопасностью, уже даже не десятки и не сотни миллионов, а миллиарды. Это касается каждого из нас, что резко выделяет сложность проблемы по сравнению с морским правом. Но нужно определиться, что именно можно регулировать методами международного права, какие конкретные здесь могут быть предметы, принципы или конкретные проблемы.

В этой работе возможны различные подходы. Применительно к Интернету мы видим, что используются все возможные способы, начиная с исторически первого многостороннего, коллективного управления, учета всех заинтересованных сторон, где есть роль и правительств, и частного бизнеса, и гражданского общества, и других заинтересованных сторон. В последние годы мы видим более активное использование многостороннего межгосударственного взаимодействия, но, безусловно, продолжаются регулирование, попытки воздействия на соответствующие правовые отношения, и односторонними действиями принимаются национальные законы.

Что же может являться потенциальной сферой регулирования? Разумеется, очень важным вопросом является недопущение милитаризации киберпространства. Следующее - это во-

просы безопасности критической инфраструктуры глобального Интернета, борьба с использованием интернет-технологий в противоправных целях, недопустимость причинения трансграничного ущерба односторонними действиями каких-либо государств, применимость так называемых трансграничных законодательных актов и практический вопрос, скажем, создания общепризнанной системы идентификации пользователей Интернета, владельцев сетевых ресурсов.

Безусловным принципом, который требует согласования имплементации на международно-правовом уровне, является обеспечение свободы информации. Мы помним, что еще на первой сессии Генеральной Ассамблеи ООН в 1946 году было отмечено, что главная свобода, главное право человека, по отношению к которому регламентируются и определяются все остальные права человека, это свобода доступа к информации, свобода слова, свобода того, что собственно Интернет и предоставляет. Существует целый ряд проблем, связанных с защитой права на анонимность и защитой персональных данных, атрибуцией лиц, использующих информационные технологии в противоправных целях, создание определенных критериев этой противоправности, чтобы они были единообразно применяемые во всех странах мира.

Частные проблемы, но очень важные для того, чтобы эффективно бороться, скажем, с киберпреступностью, - это создание единой общепризнанной системы идентификаторов. Например, Эстония - страна с очень продвинутым электронным правительством, но признается ли электронный паспорт и электронные документы, выдаваемые в Эстонии, в соседней Латвии? Если да, то прекрасно, и почему этот опыт нельзя применить повсеместно как в масштабах Евросоюза, так и всего мира, если нет, то что этому препятствует? Если бы мы решили данную задачу хотя бы на региональном, еще лучше на глобальном уровнях, то огромное количество проблем, связанных с атрибуцией деятельности в Интернете, было бы решено. Ну и, конечно, международной правовой проблемой является проблема разрешения правовых коллизий. Интернет един, Интернет трансграничен, соответственно,

соотношение договоров, конвенций универсального характера и национального законодательства очень значимо.

Важно деполитизировать процесс международно-правового регулирования ИКТ. Ведь за вычетом вопросов милитаризации все вопросы здесь исключительно неполитические. Вопросы безопасности, борьбы с преступностью никоим образом не должны быть политизированы. Важно обеспечить открытость процесса выработки решений. Если мы деполитизируем тему, о которой говорим, то, безусловно, обсуждения должны быть открытыми, чтобы каждый понимал, о чем мы говорим, чтобы материалы были доступны, чтобы все участники предварительно были уведомлены о каждом этапе разработки того или иного документа, и, наконец, безусловно важной является регулярная отчетность.

Далее, компетентность участников процесса выработки решений. Компетентность участников выявляется, вырабатывается именно в процессе открытого обсуждения данного вопроса. Все мнения должны быть выслушаны, но все мнения должны быть аргументированы. Следующий принцип - это непрерывность процесса выработки имплементации и контроля за соблюдением процедур. Иначе говоря, одновременно с разрабатываемыми процедурами необходимо предусматривать обязательность постоянной, регулярной проверки их исполнений всеми участниками. И, наконец, последнее, это институционализация процесса выработки решения, особенно когда мы говорим о международном уровне, то есть любые дискуссии, любые процессы должны завершаться тем документом, которым достигнутые договоренности фиксируются и тем самым распространяются на всех, кто принимал участие в разработке данного решения.

Потенциал субрегионального сотрудничества как один из механизмов выполнения правил ответственного поведения государств в ИКТ-среде

Татту Мамбеталиева, Общественный фонд «Гражданская инициатива интернет-политики» (Киргизия): Я являюсь директором общественного фонда в Киргизстане, мы занимаемся

вопросами развития Интернета уже 17 лет. Хотелось бы показать практический пример межгосударственного взаимодействия по поиску общих правил поведения и выработке норм, в соответствии с которыми мы можем двигаться вперед. Мы выбрали узкую тему киберэкстремизма и кибертерроризма, потому что последние события заставляют наше государство принимать меры против них, и наше государство четко понимает, что в этом вопросе нужно договариваться и взаимодействовать друг с другом.

В связи с этим мы организовали проведение Центральноазиатского форума по безопасности» в феврале этого года. Мы поняли, что если мы объединимся, то наш голос, голос нескольких стран, возможно, будет услышан в этом глобальном процессе. Наши страны являются участниками ОДКБ и ШОС, мы являемся наблюдателями глобальных дебатов. Четыре страны - Казахстан, Киргизстан, Таджикистан и Узбекистан - решили выразить свою позицию. Для нас тема экстремизма, терроризма исключительно важна, мы являемся странами, в которых нет стратегии кибербезопасности на национальном уровне и нет программ по борьбе с экстремизмом и терроризмом, но мы начинаем об этом задумываться.

Мы решили для начала собрать неправительственный сектор, то есть исследователей, теологов, социологов, специалистов, которые занимаются кибербезопасностью, пригласили национальные институты стратегических исследований, частный сектор, это были CERTы, которые работают в наших странах, и такие представители крупных поставщиков программных продуктов, которые серьезно занимаются реализаций своих программ в Центральной Азии. В форуме захотели участвовать представители спецслужб, но в качестве наблюдателей, а не в качестве участников этих дискуссий. Таким образом, форум собрал 60 участников из 12 стран, но основное количество представляли четыре страны.

Понятно, что Интернет является одним из главных инструментов онлайн-вербовок. В каждой стране было огромное количество заблокированных веб-сайтов, но оказалось что все,

заблокированное в Казахстане, доступно в Киргизстане, Таджикистане, Узбекистане. Все, что заблокировано в Узбекистане, доступно в других наших странах. Выяснилось, что законодательство и местная практика больше подчинены политическому регулированию политического экстремизма или больше связаны с этническими проблемами. Практически мы не нашли сайтов, которые заблокированы всеми четырьмя странами в рамках борьбы с радикальным экстремизмом.

Еще проблема. Россия настаивает на исключении из всех нормативных актов слова «насильственный», то есть чтобы в законодательных актах остался только термин «экстремизм», а слово «насильственный» не использовалось. Однако наши теологи говорят, что в среднеазиатских странах нужно говорить о насильственном экстремизме, потому что практическая борьба просто с экстремизмом в том смысле, в котором используется в наших странах, вела бы к ограничению прав человека.

На этом форуме мы рассматривали положительный опыт борьбы с терроризмом и экстремизмом в онлайн-режиме, говорили о «Фейсбуке», «Твиттере», «Одноклассниках», российском опыте, Северной Америке, европейских странах. Поднимался вопрос о стратегическом планировании и установлении правил и т. д., и в результате мы поняли, что необходимо согласовывать свои действия, причем наибольшую готовность к этому проявил частный сектор. Он быстрее начал взаимодействовать, и на симпозиуме был подписан меморандум между CERTами, которые договорились о следующих встречах по согласованию технических регламентов по обмену информацией.

Мы пришли к выводам, что меры и мероприятия, которые проводятся в офлайн, должны быть синхронизированы с онлайн, они должны быть тщательно обдуманы, целенаправлены и т. д. В Казахстане, Киргизстане уже были проведены онлайн-компании, информационные компании, чтобы заставить население отказаться от экстремистских идей, но получили обратный отрицательный эффект. Фактически эти контраргументы сыграли в пользу радикализации. Наши ученые,

эксперты говорят, что надо больше проводить дискуссий, исследований, что может лучше воздействовать на интернет-пользователя.

Дальше мы говорили о социальных медиа, оказалось, что все меры и механизмы, которые предусмотрены законодательством, практически не учитывают специфику социальных медиа, социальных сетей, а больше направлены на конкретный тип информации. Мы пришли к выводу, что у нас эффективные онлайн-компании по дерадикализации сообществ должны привлечь людей, представляющих такие сообщества, особенно тех, которые вышли, вернулись домой и признались в том, что они были в экстремистских организациях, потому что они больше могут делиться своим опытом. Оказалось, что около 3 тыс. активных игиловцев, которые сейчас сконцентрировались в Афганистане, - выходцы из Средней Азии.

Мы также говорили о превентивных мерах. Выяснилось, что мы не готовы к ним и не знаем, какие превентивные меры в Интернете наиболее эффективны. Мы пришли к тому, что негосударственные игроки, негосударственный сектор неправительственный сектор, эксперты, частный сектор имеют больше потенциала мотивировать государственные и правительственные органы к сотрудничеству и взаимодействию друг с другом. Мы не должны ждать, пока правительства между собой придут к согласию, именно воздействие снизу быстрее сподвигнет их к тому, чтобы договориться о правилах игры. И, естественно, практически все признали приоритет прав человека в этих будущих правилах.

Вопрос: *Как вы оцениваете потенциал государственных органов в Центрально-Азиатском регионе в определении и регистрации деструктивного контента, экстремистского контента в социальных сетях?*

Татту Мамбеталиева: *Мы создали постоянно действующий Аналитический центр по информационной безопасности для Центральной Азии. Практически все участники конференции захотели стать членами этого центра, и мы приступили к обсуждению про-*

блем. Начали с терминологии. Выяснили, что основное различие по вопросу толкования терминов «экстремизм» и «терроризм» связано с определением политического экстремизма. Поэтому мы решили этот вопрос выделить отдельно. Когда же заговорили о настоящем экстремизме, оказалось, что понимание не отличается. Мы четко понимаем, что является экстремизмом, в том числе и религиозным экстремизмом, в котором мы видим главную угрозу. Второе важное событие за прошедшие четыре месяца это то, что CERT Казахстана и CERT Киргизстана уже начали обмениваться данными. Мы продолжаем исследования. На сегодняшний день закончили исследования судебной практики по экстремистским материалам и поняли, что у нас не хватает теологической экспертизы контента. Думаю, что мы пошли правильным путем и уже есть успешные результаты.

Семинар - «круглый стол» №2

Сессия 1
Потенциал использования ИКТ в военно-политических целях в контексте стратегической стабильности

Анатолий Стрельцов: Хотел бы сразу обозначить особенность нашего разговора. Мы прекрасно понимаем, что эта тема достаточно чувствительная и, прежде чем мы могли бы что-то говорить на эту тему, по-хорошему, мы должны были получить ценные указания от нашего политического руководства. Насколько мы знаем, определенные международные соглашения между Китайской Народной Республикой и США в области военного сотрудничества существуют. Между РФ и США пока никаких военных соглашений или соглашений о сотрудничестве в военной сфере нет. Есть вроде бы три соглашения между президентами РФ и США о предотвращении опасных инцидентов в киберпространстве, и мы исходим из того, что это та база, которая позволяет нам начать диалог. С российской стороны у нас есть добрая воля руководства РФ, которое направило сюда представителя Генерального штаба Вооруженных сил РФ, и мы видим достаточно боль-

шую делегацию со стороны и США, и некоторых других заинтересованных государств, которые хотели бы поучаствовать в этом разговоре. К сожалению, посольство или Министерство иностранных дел Германии не смогли обеспечить визами представителя Вооруженных сил Китая. В связи с этим вам раздали доклад, который нам передали наши китайские коллеги.

Дженис Хэмби, Колледж информационного и киберпространства Университета национальной обороны США: Хотелось бы представиться, я вице-адмирал в отставке, в настоящее время занимаю должность канцлера Колледжа информационного и киберпространства в Университете национальной обороны США. Этот университет входит в систему Министерства обороны США, но в то же время является академическим, научно-исследовательским, мы не подчиняемся, скажем так, в научном отношении Министерству обороны. Нам предоставляется полная свобода научных исследований. Благодаря этому мы имеем возможность принимать участие в таких конференциях, как гармишевская, не спрашивая разрешения политического руководства, потому что наша компетенция включает необходимость выработки идей, направленных на решение тех актуальных вопросов, которые мы включили в повестку дня, и потом выдвижение этих идей на рассмотрение Министерства обороны. Коллеги, относитесь к нам не как к военной структуре, а как к структуре научно-исследовательской.

Теперь позвольте поделиться мыслями, как обеспечить стратегическую стабильность в условиях нестабильности, в условиях киберпространства, в условиях сферы применения ИКТ, где, к сожалению, наблюдается потенциал для проблем и конфликтов. Начиная дискуссию на данную тему, понимаю, что она всегда было областью конфронтации, еще с того времени, когда мы только стали зависеть от электронных средств связи, поэтому ничего нового нет. Мы сталкивались с наведением препятствий, электронной борьбой и т. д., все это было достаточно давно, и электронная сфера в любом виде и сфера

применения ИКТ в особенности является полем конфликтов. Наша с вами задача найти точки соприкосновения для того, чтобы обеспечить стабильность информации с учетом оперативности, чтобы люди, которые опираются на эти сети, могли нормально заниматься своим бизнесом или государственными делами, соответственно, с опорой на те продукты, которые предлагает ИКТ-среда.

К сожалению, далеко не все разделяют понимание и знание того, как работает эта среда. Вот, наши государственные чиновники, которые активно используют разные продукты, могут не знать о том, как работает эта система и предприятия. А бизнес, который разрабатывает эти продукты и владеет инфраструктурой, использует ее, может не знать о том, какие правила нужно соблюдать. Поэтому нам и нужно объединить усилия всех сторон; перед тем, как принимать решения, нужно заблаговременно предусматривать возможный потенциал для конфликтов.

Давайте посмотрим, что можем сделать для того, чтобы внести свою лепту в подготовку нового поколения руководителей, которое очень скоро придет на смену нынешнему руководству, вооруженного ИКТ-продуктами. И, наконец, мы должны также подумать, что в этой сфере взаимодействуют много игро-

ков, не только государства, не только частные компании, которые разрабатывают продукты, но и огромная популяция самых разных субъектов, которые могут составлять то, что мы называем «туман войны», используя терминологию Клаузевица.

Сначала давайте отработаем те концепции, которые позволят нам обеспечить стабильность и устойчивость без того, чтобы суетиться, без того, чтобы принимать необоснованные решения, не подкрепленные реальным пониманием, что такое ИКТ, что такое сфера ИКТ и какие побочные эффекты могут наблюдаться с осознанием необходимости обеспечения стратегической стабильности, чтобы разнести во времени и пространстве разные сферы применения, чтобы не было конфликта. Усилия должны подкрепляться необходимостью расширения кадровой базы, подготовки нашего руководства. Это не мы от них должны получать указания, как было сказано, а, наоборот, мы их должны воспитывать, наших руководителей, новое поколение, которое будет жить в условиях ИКТ.

Вадим Запивахин, Генеральный штаб Вооруженных сил Российской Федерации: Представлюсь, я являюсь экспертом от Минобороны России. Хочу остановиться на проблеме обеспечения стратегической стабильности в условиях использования современных информационных технологий. Одной из основных характеристик стратегической стабильности, как известно, является ее устойчивость к воздействию различных дестабилизирующих факторов, однако появление, развитие и возможность использования информационных технологий в качестве информационного оружия стали оказывать серьезное дестабилизирующее влияние на военно-стратегическое равновесие.

Отмечу, что под информационным оружием мы понимаем такие информационные технологии и средства, применение которых может привести к разрушительному ущербу, сопоставимому с последствиями применения обычного оружия. Если деструктивное использование таких технологий нарушит функционирование критически важной инфраструктуры

или систем управления стратегическими силами, то, безусловно, военно-стратегическое равновесие может быть нарушено. Нетрудно представить, какие последствия могут быть, если вирус, подобный Stuxnet, будет внедрен в систему управления технологическими процессами атомных электростанций, гидроэлектростанций или других промышленных опасных производств и использован для нарушения их работы или внедрен в систему управления стратегическими силами и использован для дезорганизации управления ядерным или иным стратегическим оружием. Безусловно, последствия могут быть колоссальные.

Кроме того, для дестабилизации военно-стратегического равновесия могут использоваться и другие виды информационных технологий и средств. Министерство обороны РФ не рассматривает кибербезопасность как самостоятельную, отдельную от информационной безопасности. Мы это рассматриваем в комплексе, поэтому по ходу своего выступления постараюсь охватить все аспекты информационной безопасности. Например, точные, дезориентирующие виды психологических воздействий, осуществляемые с использованием современных СМИ, Интернета и иных каналов передачи информации, могут значительно повлиять на эффективность реализации существующих алгоритмов, задействование сил стратегического назначения в кризисных ситуациях.

Практика проведения массивного информационно-психологического воздействия, реализуемого через СМИ, электронные СМИ, социальные сети для эскалации внутриполитических конфликтов, инициирование так называемых «цветных революций» последние два десятилетия показали свою высокую эффективность. В результате такого воздействия, гипотетически возможна неконституционная смена руководства в государствах «ядерного клуба», что определяющим образом повлияет на стратегическую стабильность. Если бы Ливия или Украина обладали ядерным оружием, где бы сейчас оно было? В стране, где управляют не совсем адекватные люди, это оружие может оказаться где угодно - и у террористов, и продано третьим

странам и т. д. То есть контроль над ядерным оружием был бы потерян полностью.

На стратегическую стабильность оказывают влияние и другие сопутствующие факторы, например избранные внешнеполитические стратегии государств, содержание и направленность положений военных доктрин государств, связанных с использованием информационного оружия. Ярким примером является принятое на Уэльском саммите в 2014 году решение о том, что военные силы, в соответствии со статьей 5 Вашингтонского договора, будут применяться в ответ на кибернападение. Или признание на прошлогоднем саммите НАТО в Варшаве информационного пространства такой же сферой борьбы, как и наземная, воздушная, сухопутная и морская. Приравнивая информационную сферу к выше названым, мы говорим, что будем воевать там. Но как? А кто определил, кто сказал, что такое агрессия в информационном пространстве? Кто определит эти критерии? То есть нормативно-правовых норм у этого нет, но мы уже говорим, что будем воевать там. На наш взгляд, это вызывает очень большую озабоченность.

Безусловно, такие решения не способствуют укреплению стратегической стабильности. Кроме того, наши западные партнеры избрали путь гонки информационных вооружений. Твердо двигаясь по нему, США в информационной сфере сделали ставку на так называемое киберсдерживание противника, причем основными противниками названы Россия, Китай, Северная Корея, Иран. Это записано в действующей киберстратегии Министерства обороны США от 2015 года. Мы рассчитываем, что подобные подходы не войдут во внешнеполитическую доктрину новой администрации США.

Безусловно, это требует от нас принятия соответствующих защитных мер. Если одна сторона активизирует работу, мы понимаем, что это угрожает нам, и должны принимать защитные меры. Главная проблема обеспечения стратегической стабильности это создание военно-политической обстановки, которая нивелирует дестабилизирующие факторы, связанные с информационными технологиями. Она не приведет к переходу международных отношений от мирного существования государств

к войне. Формирование таких условий применительно к информационной сфере предполагает решение следующих задач.

Это обеспечение технической устойчивости и потенциала стратегического сдерживания к информационным воздействиям. Здесь все страны принимают определенные меры для того, чтобы обеспечить устойчивость своих систем ядерного сдерживания от информационного воздействия.

Снижение риска провоцирования ошибочных управленческих решений, которые могут привести к развязыванию военной конфронтации вследствие непреднамеренных информационных воздействий на систему боевого управления стратегическими силами и средствами. Стратегическая стабильность должна обеспечиваться запасом устойчивости, позволяющим компенсировать влияние дестабилизирующих информационных факторов.

Создание таких военно-политических условий, когда у сторон будут отсутствовать стимулы для совершения актов агрессии с использованием информационных технологий. Здесь может быть применен целый арсенал средств, как международно-правовых, политико-дипломатических, так и информационно-психологических, обеспечивающих убежденность противоборствующей стороны в неизбежности нанесения неприемлемого ущерба в случае совершения подобных актов.

Недопущение использования средств массового информирования, в том числе Интернета, для дезорганизации внутриполитической обстановки в государствах мирового сообщества, которое может привести к неконституционной смене руководства этих стран.

Оперативное разоблачение и нейтрализация дезориентирующих и иных негативных воздействий, оказывающих влияние на выработку и принятие решений на применение стратегических сил, особенно в кризисных ситуациях.

Решение задач, связанных с повышением уровня доверия между государствами мирового сообщества. На этом пути серьезную проблему представляет отсутствие гарантий в том, что

стороны не будут использовать достигнутый уровень доверия для извлечения собственной односторонней выгоды.

Выявление механизмов влияния на обеспечение стабильности двух сторон информационных потенциалов третьих сторон, в том числе и негосударственных. Неконтролируемое распространение информационных технологий, которые могут использоваться негосударственными структурами, в том числе террористическими, экстремистскими организациями, может привести к появлению дополнительного дестабилизирующего фактора, который также будет оказывать влияние на стратегическую стабильность. Для этого решения нет иного пути, кроме как налаживание международного сотрудничества в противодействии такому противоправному явлению. В условиях наращивания информационных потенциалов государств требует решения проблема поиска баланса взаимного стратегического предотвращения и сдерживания возникновения вооруженных конфликтов. В частности, меры предотвращения должны базироваться на адаптации существующих общепризнанных норм и принципов и выработке новых норм международного права. В свою очередь, меры сдерживания не должны приводить к возникновению гонки информационных вооружений.

Справедливости ради, следует отметить, что пока наши озабоченности носят гипотетический характер, потому что ядерным оружием и другими стратегическими силами обладают государства, которые ведут себя вполне адекватно в информационной сфере. Однако совершенно очевидно, что гонка информационных вооружений, а также межгосударственные конфликты и споры, вызванные применением информационных технологий в разведывательных и подрывных целях, уже расшатывают устои стратегической стабильности в мире. Особенно этому способствует настойчивое стремление военно-политических кругов ряда западных стран, а также руководства придать практическую направленность обсуждению возможности военного реагирования на факты совершения компьютерных атак и связанных с этим проблем.

Мы убеждены, что основным направлением сохранения стратегической стабильности в современных условиях является осуществление комплексных мер, нацеленных на то, чтобы возможность дестабилизирующего использования информационных технологий и средств была бы минимизирована в силу приверженности политическим и правовым способам разрешения возникающих противоречий путем развития международно-правового и военно-политического сотрудничества. В рамках этого большого направления предлагаем продолжить поиск совместных решений проблем политико-дипломатического, правового предотвращения военных конфликтов, которые могут возникнуть вследствие враждебного или иного неправомерного использования информационных технологий. Представляется, что именно на этом пути могут быть найдены наиболее приемлемые и практически значимые результаты.

В рамках ООН, ШОС, ОБСЕ и других международных организаций уже создан определенный задел, включающий адаптивные нормы существующего международного права, меры укрепления доверия, а также правила поведения государств в информационной сфере. При этом не по всем вопросам удалось, безусловно, добиться необходимого консенсуса. Нужно продолжить работу до тех пор, пока не будет создан универсальный режим обеспечения международной информационной безопасности, позволяющей надежно обеспечить гарантированный уровень стратегической стабильности в мире. Хочу еще раз со своей стороны сказать, что Министерство обороны РФ постоянно выступает с позиции не урегулирования возникающих проблем, а их предотвращения.

Найджел Инкстер, Международный институт стратегических исследований (Великобритания): Международный институт стратегических исследований занимается конфликтологией, причинами и путями разрешения разных конфликтов, которые имеют и военное измерение. Генерал Шерстюк упомянул ряд источников озабоченности в сфере безопасности. Господин Смирнов в том же духе высказался относительно деятельности НАТО. Он выде-

лил классические дилеммы безопасности, которые стоят перед нами, и мы по-прежнему продолжаем с ними сталкиваться. Если сконцентрироваться на стабильности в сфере ИКТ, то в ней также есть серьезное военное измерение. Поэтому участие военных в обсуждении этой проблемы необходимо.

Очевидно, что есть три основных игрока, чье участие имеет ключевой характер для достижения некоего глобального нормативного оформления всех этих принципов, - США с союзниками, РФ и КНР. Все остальные тоже могут вносить важный вклад, например Индия, Пакистан. Хотелось бы особенно выделить Саудовскую Аравию и Иран.

Деятельность в сфере ИКТ имеет большой потенциал стать катализатором дестабилизации. Да, можно опираться на договоренности, которых удалось добиться в сфере ядерных наступательных вооружений, но, к сожалению, надо отметить, что и эти договоренности потихонечку начинаются размываться. Уже есть элементы нестабильности, новые технологии, лазерное и обычное вооружение, ракеты уже попадают не в те руки, в которые хотелось бы, а также ИКТ могут активно использоваться не в дружественных целях.

Нужно стимулировать дискуссию, продолжать диалог, наращивать взаимодействие между профессионалами, военными в любой форме. Мы выполняем свою домашнюю работу, продолжаем анализировать много проблем и, может быть, уже даже добились в определенной степени консенсуса по ряду хотя бы наиболее важных тем и вызовов, которые мы хотели бы избежать, чтобы все оставалось действительно в гипотетической плоскости. Полезность этой работы высока, позволяет нам обмениваться информацией, мнениями, взглядами, задавать вопросы, получать ответы друг от друга.

В 1975 году в Хельсинки был подписан исторический Заключительный акт, устанавливающий ответственное поведение сторон, но все равно понадобилось несколько лет, чтобы потом эти договоренности оформить другими документами. Это не полностью решило вопрос стабилизации ситуации в Европе, на это понадобится еще не одно десятилетие, но, в конце кон-

цов, надо сказать, что это хороший пример для подражания и может наполнить надеждой на будущее.

Джон Мэллори, Массачусетский технологический институт, (США): Итак, три темы: кризисное урегулирование, деэскалация, урегулирование конфликта и обучение высшего руководства. Еще в 2011 году на встрече в Китае был разработан механизм определения проблем, норм, мер укрепления доверия и других стратегий сотрудничества, которые можно применять для снижения остроты проблемы. Это хороший подход, потому что он не абстрактный, а обоснованный, есть проблема, и мы рассматриваем решение.

Мы применили подход «круглого стола», людям понравилось, мы заслушали точки зрения России, Китая, было заседание по международному праву, и на Бишкекской конференции обсуждалась концепция в преддверии этой встречи. В 2012 году цель состояла в том, чтобы рассмотреть, какова киберсоставляющая военной стабильности и безопасности. Впоследствии обсуждалось создание новых уязвимостей.

В случае ядерного оружия потребовалось 40 лет для понимания доктрины управления этими системами, но эта проблема гораздо проще, чем проблема кибероружия, поэтому надо начать с того, как управлять этой ситуацией. Нам нужно исходить из негативных последствий. Противная сторона должна иметь большую степень уверенности в надежности систем, для этого вы должны быть готовы обменяться информацией и технологиями компьютерной безопасности.

Если взять ядерное оружие, эти вооружения обеспечены криптографическим контролем по решению руководства. В случае если ваша система командования и управления зависит от телекоммуникационной инфраструктуры и возникает кризис в отношениях с другой крупной державой, а третья сторона совершает нападение на инфраструктуру, это имеет негативные последствия. Возьмем Карибский ракетный кризис. Очень острый кризис, он очень внимательно изучался, мы стояли на краю пропасти. Сейчас же, в условиях ИКТ, кризисная стабиль-

ность будет не такой высокой, как тогда. Это очень опасно, поэтому нужен больший запас прочности и стабильности.

Я беседовал с американскими политиками, знакомился с исследованиями и сталкивался с тем, что у них односторонняя точка зрения, они не думают о том, какова точка зрения другой стороны. Разговаривал с руководителями разведки, они отвечают, что только собирают информацию и передают руководству. На уровне высшего военного руководства я услышал: «А у меня только наступательные вопросы разрабатываются», - то есть у них нет представления об интерактивной стабильности.

Обращаясь к россиянам, хочу сказать: «Спросите у ваших политиков, как они ответят на эти вопросы, думают ли они об этих вопросах, если нет, надо уже сейчас начинать об этом размышлять». Что касается китайских коллег, то ситуация немного отличается, там работают талантливые «суперзвезды», с хорошими связями в верхушке Коммунистической партии и в руководстве по кибервопросам, в национальном оборонном университете, доктора наук, которые изучали вопросы кризисной стабильности, это наши партнеры. Американские официальные лица пока не готовы напрямую взаимодействовать и участвовать в таких военных дискуссиях, может быть, они не продумали эти вопросы, может быть, есть политические препятствия.

Общая идея состоит в том, чтобы фактически встречаться дважды в год, собираться вместе, проводить заседания, говорить за закрытыми дверями, в рамках экспертного сообщества, затем излагать результаты на бумаге, то, что мы готовы публиковать, затем консультироваться со своей стороной, обсуждать извлеченные уроки и опять возвращаться к новым встречам. У нас работает очень хороший коллектив не только специалистов в области кибервопросов, это функциональные эксперты, специалисты по конкретной проблематике, они знают, как добиваться решений таких проблем. То есть мы пытаемся создать уровень осведомленности, наращивать знания и опыт в трех странах, развивать динамичное взаимодействие по вопросам архитектур безопасности, с тем чтобы все об этом думали, размышляли и старались избегать ошибок.

Что касается конкретных результатов, то позиции Америки и Китая достаточно близки. Российские эксперты больше зависят от процесса принятия решений и стремятся к достижению конкретных результатов. У нас ушло два года, прежде чем мы начали обсуждение на уровне военных специалистов с Китаем. Не знаю, насколько это возможно с Россией.

Эльза Кания, Группа выработки долгосрочных стратегий: Расскажу о некоторых рекомендациях и вопросах, возникших на встрече в декабре. Итак, пять основных проблем. Первая - улучшение кризисного урегулирования, снижение риска военной кибернестабильности на основе более эффективного кризисного урегулирования. Возникновение киберпространства как военной среды повышает риски кибернестабильности. Мы видим, что доминирование в киберпространстве часто усиливает наступательные доктрины, и, хотя точные разведданные были вначале стабилизирующим фактором, сейчас они больше связаны с кибероперациями и могут стать фактором, который на самом деле увеличивает риск неправильного восприятия.

Рекомендации и заключения: коллективные международные действия по укреплению стабильности, в частности оценка возможностей повышения доверия среди крупнейших кибердержав, включая меры повышения стабильности, оперативные меры и меры повышения транспарентности.

Несколько исследовательских вопросов: риск опасного взаимодействия наступательных доктрин, как снизить риск возникновения новых технологий, искусственный интеллект, квантовые коммуникации, в будущем вызовы красной линии, вопросы атрибуции и т. д.

Вторая проблема - как повысить предсказуемость киберинтеракции, кибервзаимодействия. Результаты: двусмысленность этой среды и отсутствие транспарентности относительно национальных потенциалов повышает общий уровень неопределенности, риск неправильного расчета и неправильных решений. В этом случае необходимо обсудить терминологию и, таким

образом, повысить уровень понимания и коммуникации. Кроме того, нет четких способов оценки киберпотенциалов, транспарентность очень ограничена.

Мы обсудили эти неправильные представления. Была отмечена необходимость создания словаря, терминологического справочника, сравнения китайских, американских и российских концепций. Мы также обсудили критический характер рассмотрения различных вариантов, по крайней мере, в определенной ограниченной степени развития вопросов транспарентности при рассмотрении доктрины и организации, это позволит более эффективные обмены мнениями и информацией. Кроме того, мы обсудили, как в будущем можно повышать взаимопонимание за счет трехсторонних штабных учений и имитации тренировок. Каким образом снизить риск провоцирования конфликта из-за неправильного расчета на основе неверной информации.

Третья проблема - улучшение вопросов принятия решений в условиях кризиса, что будет иметь значение для руководства в кризисных условиях. В настоящий момент лица,

формирующие решения, недостаточно информированы о последствиях военной кибернестабильности, включая так называемое групповое мышление или информационные перегрузки. Есть определенные психологические факторы, которые могут повлиять на толкование киберсигналов, в частности из-за отсутствия традиционных контекстуальных подсказок, характеризующихся обычными политическими и военными системами сигнализации.

Рекомендации: формулировка детальных рамочных основ для политиков, возможно в форме справочников, в которых будут обозначены критические моменты и вопросы для лиц, принимающих решения, которые необходимо учитывать при разработке этих вопросов с тем, чтобы обратить внимание аудитории, участников на эти важные вопросы, заниматься просвещением соответствующих лиц, распространением информации о возможных серьезных последствиях.

Вопрос с точки зрения научных исследований: эффективные способы донесения этой информации до принимающих решения политиков - как мы можем повысить уровень осведомленности о стратегической стабильности среди лиц, формирующих решения, каковы требования с точки зрения обучения и образования и, наконец, каковы важнейшие психологические факторы, влияющие на принятие решения.

Четвертая проблема - моделирование нынешней динамики военного соревнования в киберпространстве. Сейчас существует негативная тенденция к военному соревнованию в этой среде, что может оказать дестабилизирующее воздействие. Участники согласились с тем, что крупные державы несут главную ответственность за снижение этой динамики и выход из порочного круга гонки вооружений. Если малые державы будут чувствовать себя в опасности, они тоже будут стремиться к разработке наступательных сил и средств, что приведет лишь к обострению такой гонки вооружений.

Рекомендации: крупные кибердержавы должны стремиться к кооперативному подходу на основе деэскалации, урегулированию нынешних дилемм в области кибербезопасности, требует-

ся переоценка со стороны крупных держав последствий подходов, основанных на наступательных кибервооружениях. Больше внимания необходимо уделять устойчивости и другим оборонительным подходам для защиты от киберугроз, например использовать сотрудничество между CERTами, обмен данными, это может быть важнейшим шагом в направлении дальнейшего движения вперед.

В этом случае вопросы с точки зрения научных исследований: каковы целесообразные показатели оценки киберустойчивости? насколько реально создать международный режим регулирования в этой области? Также был затронут вопрос о том, надо ли обмениваться информацией об атаках на критическую инфраструктуру.

И пятое, наконец, обсуждалась проблема долгосрочного характера - создание архитектур для военной киберстабильности в будущем для укрепления международной кибербезопасности. Мы пришли к выводу, что создание такой архитектуры будет иметь критическое значение. Для этого необходима соответствующая новая база с использованием существующих систем и применением новых. Те модели, которые у нас имеются, например ГП, могут быть реализованы в существующих условиях.

Рекомендуется рассмотреть варианты технологического сотрудничества по укреплению совместной устойчивости на системном уровне. Крупные державы также должны оценить варианты создания архитектуры с точки зрения укрепления потенциалов и уточнения цели, в том что касается направления сигнала.

Вопросы относительно научных исследований: каким образом уязвимость влияет на киберстабильность? является ли такая устойчивость стабилизирующим или дестабилизирующим фактором, в том что касается влияния на риск и принятие решений руководством? как мы можем определить действия, способствующие большей предсказуемости и стабильности. Обсуждались различные подходы к таким моделям. И, наконец, мы обсудили, что рекомендовать в качестве идеальной модели международной киберархитектуры безопасности, какие аспекты

этой модели могли бы быть реализуемы в рамках сегодняшней международной системы. Это краткая попытка подытожить результаты нашего обсуждения.

Томас Уингфилд, Национальный университет обороны США: Есть телесериал «Дедвуд», в нем речь идет о вымышленной стране, которая существовала на территории нынешней Америки, там не было закона, не было суверенитета, а были сильные личности, борьба без закона и правопорядка. Там были и норвежцы, и канадцы, представители Австрии, Великобритании, России и т. д. Все пытались захватить власть, потому что не было закона, но были прекрасные возможности. Это неплохая аналогия для объяснения или описания киберпространства до недавнего времени. С помощью группы государственных экспертов мы начинаем исправлять ситуацию, и сейчас существует консенсус о том, что международное право действительно применимо и в киберпространстве.

Действительно, государства формируют международное право и обеспечивают его исполнение. Отсутствует какой-то мировой законодательный орган, который мог бы принимать международные законы вопреки мнению государств. Нет единого исполнительного органа, который обеспечивал бы исполнение этих законов без учета мнений государств, нет даже международных судов, обладающих обязательной юрисдикцией или подсудностью, которые могли бы навязывать государствам такие решения. То международное право, которое у нас имеется, - результат консенсуса и договоренностей государств, часто государств с совершенно разными интересами.

Так в чем же состоит это право, на основании которого мы можем дальше выстраивать нашу работу в киберпространстве, что подлежит общему согласию? Это так называемые императивные нормы - jus cogens (неоспоримое право). Эти абсолютные нормы - jus cogens являются обязательными для государств, даже для тех государств, которые постоянно против них возражают. Это небольшая категория международных норм, это созданное международное право. Обычно государства могут вы-

бирать нормы, которые они соблюдают и не соблюдают. Что касается jus cogens, то они, по согласию государств, должны соблюдаться всеми.

Что это такое? Это, например, запрет на рабство, геноцид, пиратство, использование химического или биологического оружия, намеренное нападение на гражданских лиц в военное время. Нет ни одного государства, которое возражало бы против применения данных норм. Даже если иногда государства их нарушают, они делают это не потому что считают, что эти нормы не соблюдаются, они просто отрицают наличие тех или иных действий.

Рассмотрим пример суверенитета. Некоторые рассматривают суверенитет как концепцию, как понятие, откуда вытекают другие нормы. Другие считают, что суверенитет - это правило, которое может нарушаться. По принципу международного права «все, что не запрещено, разрешено». Исходя из этого принципа идея суверенитета как общее правовое понятие дает основу для конкретных правил, которые существуют в силу договорных обязательств или обычного международного права.

Есть широкий международный консенсус, в соответствии с которым нарушение суверенитета происходит в результате запрещенного или незаконного вмешательства. Это тоже широкое понятие. Здесь присутствуют две составляющие - в киберпространстве и реальном физическом мире. Например, одна составляющая предусматривает вмешательство в то, что по-французски называется «domaine reserve» (сфера исключительной компетенции), то есть это функции или институты, над которыми государство обладает юрисдикцией, контролем. Наши разногласия касаются второй составляющей. Незаконное вмешательство предусматривает также не только вмешательство, не только вовлеченность, а фактическое принуждение, элемент принуждения, это предотвращение каких-то действий государства или силовая попытка заставить государство предпринять определенные действия.

Думаю, что здесь есть возможность для согласия по этим двум составляющим и тому, как они применимы к киберпро-

странству. Приведу пример: проведение какого-то политического выступления в ходе предвыборной кампании. Это может означать многое, но не означает принуждения, не правда ли?

Гипотетический пример. Вижу ряд коллег из Канады, поэтому сегодня для примера выберу Канаду. Представьте себе, правительство Канады наконец решило: все, хватит, надоели американцы, надо с ними разбираться, и они выпускают информацию, часть - правда, часть - неправда, неважно, они дают утечку информации во время американской предвыборной кампании. Мы не знаем, какие будут последствия этой утечки. Даже если мы согласны, что выборы - это пример «domaine reserve», трудно спорить с тем, что такие действия Канады соответствуют критерию принуждения. Это не подпадает под данную категорию, несмотря на то что информация может быть неверной. То есть это не является нарушением суверенитета с точки зрения незаконного вмешательства. Но если канадская спецслужба будет собирать компромат против ведущего кандидата и готова использовать этот компромат против кандидата в качестве средства шантажа, то тогда мы действительно достигаем уровня принуждения и здесь мы вынуждаем государство что-то делать или, наоборот, предотвращаем его действия. Это уже четкий пример нарушения суверенитета за счет использования принуждения.

Данные примеры в качестве аналогии могут также направлять наши действия и в киберпространстве. Почему это важно? Это важно потому, что, если есть незаконное вмешательство в киберпространстве или физическом пространстве, тогда возникает право, вводится действие права на контрмеры. Что такое контрмеры? Обычно это меры, которые одно государство применяет против другого в случае незаконного вмешательства, например американцы могли бы применить контрмеры против северного соседа в случае использования такого компромата. Данные меры должны быть соразмерными. Не бомбить, а применить соразмерные меры. И при условии, что они направлены на восстановление ситуации законного поведения со стороны канадцев. Если эти меры со-

ответствуют двум критериям соразмерности и целесообразности, тогда это незаконное поведение становится законным с учетом данных условий и целей.

Насколько контрмеры работают в киберпространстве? Как нас учат на первом курсе юридического факультета, ответ на любой вопрос начинается со слов «все зависит». Так и здесь, «все зависит…», и главное различие состоит в том, является ли уровень стратегическим или тактическим. На стратегическом уровне есть время для формулировки позиций, есть время для предупреждения, выдвижения требований, ознакомления общественности, выработки тех или иных мер. На тактическом уровне контрмеры, как правило, носят другой характер. Говоря с американскими коллегами, которые работают в этой сфере, я узнал их мысли о том, почему контрмеры не всегда срабатывают на тактическом уровне в киберпространстве. Они выдвинули три очень хороших аргумента и один плохой.

Первое - контрмеры требуют предупреждения. Я должен сказать канадцам: «Прекратите, господин премьер-министр, это неприемлемо. У вас есть 30 дней, если не прекратите, тогда мы опять пожалуемся». В киберпространстве у вас нет такого времени, такой возможности. Пока вы ждете, ущерб продолжается.

Второе - контрмеры не предусматривают коллективного ответа. Это проблема, потому что это стимулирует агрессивное поведение, потому что жертва может только реагировать индивидуально, а не коллективно, в отличие от других случаев.

Третье - контрмеры не позволяют так называемый упреждающий, предусматривающий ответ, то есть ущерб продолжается в течение определенного времени, прежде чем страна может ответить. Даже при наличии хорошей разведки, хороших данных вы узнаете об атаке уже после того, как она началась. Все юридические специалисты скажут вам, что право самообороны предусматривает определенные упреждающие действия до совершения нападения, но не контрмеры.

И четвертый, слабый аргумент. Контрмеры по закону могут быть применены только против государств. Если вы участвуете

в военной операции в борьбе за жизнь или смерть с негосударственным субъектом, как это сейчас происходит в отношениях между моей страной и ИГИЛ, то контрмеры по праву не могут применяться против такого противника. Это большая лакуна в международном праве. Считаю, что это слабый аргумент, потому что есть параллельная доктрина необходимости, так называемая доктрина необходимости. Фактически она состоит в том, что предусматриваются контрмеры против негосударственных субъектов. Это сфера права, которая формируется на основе практики государств и практики юридического сообщества. Она еще полностью не сформирована, тем не менее это еще одно новое правовое средство для борьбы со злоумышленниками в киберпространстве.

В заключение позвольте сказать следующее: очевидно, что существуют широкие сферы, в которых у кибердержав есть противоречащие интересы, это никого не удивляет, но в стратегических условиях сотрудничество может возникать даже среди самых ярых противников. Мы видели такие примеры на стратегическом уровне много раз в течение XX века, были свидетелями такого сотрудничества в определенных областях, где есть общие интересы. Если это так, то мы должны искать точки соприкосновения и способы взаимодействия. Суверенитет, особенно идея незаконного вмешательства и роль контрмер тактического или стратегического характера, является такой сферой потенциального взаимодействия.

И последнее. Один из моих любимых писателей-фантастов Артур Кларк сказал, что любая новая идея в науке, технологии, политике, не важно, где, любая новая идея проходит три фазы, три этапа. Первый этап - все говорят: «невозможно, не тратьте время», вторая фаза: «возможно, но не стоит того», и третья фаза: «о, я всегда знал, что это отличная идея». Вот такое сотрудничество по этим доктринам, где мы не всегда не согласны, находится на втором этапе восприятия, и, думаю, при определенной поддержке мы можем выйти на третий этап, когда все эксперты скажут: «да мы всегда считали, что это отличная идея».

Чарльз Барри, Институт национальной стратегии Университета национальной обороны США: Сосредоточусь на прагматических и практических аспектах. Большая часть моего опыта связана с рассмотрением взаимодействия между военными в киберпространстве. Военные ограничены в своих возможностях прямых контактов. В настоящий момент нам нужна, видимо, какая-то суррогатная группа, которая могла бы обсуждать вопросы, пока мы не выйдем на реальный уровень военных контактов, она послужит определенным мостиком, мы будем использовать наш опыт военной и гражданской службы. Конечно, речь идет прежде всего о союзниках, но система должна работать и между потенциальными соперниками, это более важная составляющая и на ней надо сосредоточить наше внимание в первую очередь.

Говорили о последнем саммите НАТО, где киберпространство было включено в сферу военных действий. Недавно также началась работа над этим, есть Совет Россия - НАТО, он трижды заседал в 2016 году, и было заседание в марте текущего года. В идеале мы, военные и гражданские специалисты, могли бы взаимодействовать по данной проблематике и в рамках этого органа, с тем чтобы создавать определенный уровень транспарентности, обсуждать вопросы, как мы это делали с китайскими коллегами. Мы могли бы рассмотреть уже имеющиеся рекомендации и сосредоточиться на конкретной проблематике. Контакты между военными надо распространить и на киберпространство. Стабильность, не только военная, но и на высшем уровне руководства, - это тоже стратегическая стабильность, она может работать особенно эффективно в кризисных условиях для выстраивания отношений, для развития мер укрепления доверия в отношениях между вооруженными силами. Это сложный процесс, очень важно уделять и этим аспектам внимание, так как на этой основе выстраиваются отношения между людьми. Очень важно обеспечивать транспарентность, прозрачность таких контактов.

Более того, страны могут сами выбирать, какие темы приемлемы для обсуждения, какие нет, особенно когда прово-

дятся так называемые штабные дискуссии, эти вопросы носят регулярный, рутинный характер. Это фактически постоянный процесс регулярного взаимодействия. Наверное, можно начать с этой платформы, создать некую постоянную группу, постоянную площадку. Может быть, чаще встречаться, чем раз в год, или в рамках различных групп по тем или иным аспектам киберпространства.

Нам надо обеспечить поддержку данной инициативы на высшем уровне руководства, чтобы была не только поддержка, но и соответствующие инвестиции на регулярной основе, с тем чтобы люди понимали, что процесс военных контактов в киберпространстве необходим. Можно распространить этот процесс вплоть до тактического уровня. Однако оперативно-стратегический уровень, видимо, то звено, с которого надо начинать. Значение таких обменов может показаться ограниченным, но определенные результаты достигаются. Пока не будут налажены зрелые, так сказать, процессы контактов между военными, обмен курсантами, учения - это уже зрелый уровень взаимодействия и сотрудничества. У нас такой опыт есть, в основном среди союзников.

Вопрос в том, как начать такое взаимодействие в киберпространстве. Может быть, стоит начать с двусторонних штабных переговоров с ограниченным количеством тем, чтобы объяснить организацию киберпространства, кто наши лидеры, каковы базовые процессы, обсудить доктрины, организовать совместные публикации, почитать документы друг друга и вводить данную тематику в учебную программу в наших учебных заведениях.

Анатолий Стрельцов, Институт проблем информационной безопасности МГУ им. М.В.Ломоносова: Уважаемые коллеги, хотел бы обратить ваше внимание на некоторые моменты. Я в армии с1957 года, то есть достаточно давно, и эти представления о том, как в РФ организована военная служба, меня несколько забавляют, скажем так. Понимаю наших американских коллег, когда они взаимодействуют в основном с партнерами, союзниками, странами, которые находятся на несравнимо более низком уровне развития в области информационных тех-

нологий и их применения и прочего. Но здесь у нас несколько другой случай. Я прекрасно знаю, что в нашей Военной академии Генерального штаба изучают и военные противоборства, и способы использования различных информационных технологий, и методы определения и отличия ошибочных данных от неошибочных в области киберпространства и т. д., и это не единственное учебное заведение, где всем этим занимаются.

Согласен, что надо общаться, но не могу понять, зачем. То есть мне нравится общаться, особенно когда деньги есть, почему бы не пообщаться, это вообще хорошо. Но хотелось бы понять предмет общения, потому что все-таки общаться для того, чтобы рассказывать друг другу, как мы выглядим со стороны, - это интересно, но не очень содержательно. Может быть, Джон сможет предложить какие-то вопросы, которые представляют интерес для более конкретного обсуждения? Ну какой результат мы хотели бы получить в результате нашего общения? Давайте договоримся на берегу, до начала всех разговоров, какой результат мы ищем.

При этом мы совершенно четко понимаем, что никакого руководящего указания со стороны политических лидеров на достижение того результата, о котором мы будем говорить, пока нет. Поэтому мы пока думаем о том, что можно было бы предложить нашим политическим лидерам, чтобы им было интересно и соответствовало их опасениям. Совершенно уверен, что обсуждать лучше, чем не обсуждать, но обсуждать мы привыкли конкретно. Если куда-то едешь, то вот повестка дня, вот предмет, вот ваше мнение, вот это мнение, давайте обсуждать, в чем мы не сходимся, или давайте обсуждать, в чем мы сходимся и как двигаться дальше. Точно так же мы работаем и с нашими китайскими коллегами. Мы тоже им что-то предлагаем или они нам что-то предлагают, мы обсуждаем, мы выходим на какие-то позитивные решения и потихонечку продвигаемся вперед. Это первая часть.

Вторая часть, относительно суверенитета, вмешательства. Да, я почти согласен, только не очень понимаю, что является источником права в области контрмер на данный момент, кроме практики, которую осуществляют некоторые государства.

Могу сказать, что, наверное, с точки зрения общей справедливости это возможно, но такого источника права я не знаю, и что меня в этом плане пугает, это особенно когда речь идет о киберпространстве.

Во-первых, у нас нет механизма, который позволял бы нам контролировать ход реализации подобных контрмер, у нас нет международного контроля, нет у нас таких механизмов. В киберпространстве и границ-то нет, и непонятно, где заканчивается территория одного государства и начинается территория другого, я не понимаю, что такое вооруженный конфликт в киберпространстве. Не понимаю, потому что не вижу границ, и кто от нейтральных государств войдет в группы высоких представителей и т. д. и т. п. То есть обычное право - оно очень хорошо, в принципе, сделано, но, как представляется, его и нужно адаптировать к нашим условиям.

Если мы ставим задачу, например, подготовить какие-то предложения по уточнению или дополнению к Уставу ООН или Женевским конвенциям, то есть протокол №1, а мы сделаем протокол №2, например по киберпространству, где будем уточнять, как отделить военные объекты киберпространства от гражданских объектов киберпространства. Тогда военные будут понимать, о чем идет речь, и это не будет напоминать общие разговоры относительно того, как хорошо иметь компьютер по сравнению с тем, когда компьютера не имеешь. Мы же, в конце концов, все более-менее одинаково понимаем ситуацию, одинаково пользуемся компьютерами.

Думаю, и у вас, и у нас 100% вооружения и военной техники компьютеризировано в той или иной степени, ну, может, кроме автомата Калашникова, который еще остался. Поэтому давайте как-то выходить на те действительно важные и понятные и нашим политическим руководителям, и нашим коллегам, реально работающим в этой области, темы.

Вот, вопрос, например, о тех же границах киберпространства как пространства в пределе суверенитета в ИКТ. Не вижу необходимости выстраивать какую-то границу наподобие той, какая существует в реальном мире, но прекрасно могу понять

наших коллег, которые работают в ICANN, я отношусь к ним с уважением, они делают свой бизнес. Но у нас возникла ситуация с Крымом, и операторы связи, которые находятся на Украине, перестали обслуживать абонентов в Крыму, обосновав это тем, что им из США сказали, что этого делать не надо. Нас интересует стабильность киберпространства. И, естественно, мы хотели бы иметь некоторые гарантии того, что это пространство будет стабильным. Скажите мне, какое государство отвечает за стабильность работы данного пространства? А в какой суд я пойду, если это, так сказать, мое право на стабильное функционирование данной инфраструктуры будет нарушено? В суд Калифорнии? Кому я должен предъявлять претензии? Ведь никаких отношений на самом деле между ICANN и Россией не существует. Есть отношения между отдельными частными лицами, которые имеют разную юрисдикцию и разное представление о том, что им государство разрешило, что не разрешило и как это все использовать.

Вот одна из проблем, в частности, связана с обеспечением устойчивого функционирования и безопасного использования ИКТ. Проблему надо решать? «Майкрософт» говорил о принципах. Но все шесть принципов можно свести к одному - запретить использовать ИКТ в военных целях. Мы понимаем, что этого никогда не будет, понимаем, что есть государственные, национальные интересы, есть ответственность за национальные интересы у спецслужб, Министерства обороны. Давайте реальные проблемы решать, одну-две проблемы выберем и попытаемся их решить. Хорошо, у нас есть договоренность по группе правительственных экспертов 2015 года. Посол Крутских сказал, что, возможно, не будет итогового документа в 2017 году, но есть документ 2015 года «Принципы, правила и нормы ответственного поведения государств в киберпространстве». Предлагаю взять этот документ и попытаться довести его до логического конца, как применять эти правила. Давайте решим вопрос о том, что такое инцидент в ИКТ-среде, чем он характеризуется, какими показателями, кто его будет фиксировать, как мы будем информацией обмениваться.

В Уставе ООН записано, что мирными средствами надо разрешать все конфликты, которые существуют между государствами. Что мы можем положить на стол при мирных переговорах по поводу инцидента в сфере ИКТ? Какую информацию? Кем собранную, кем закрепленную?

Вы знаете решение Международного суда ООН по делу Никарагуа против США 1984 года. Международный суд сформулировал принципы, на основе которых документы принимаются от государства в качестве доказательств. Они принимаются только в том случае, если ухудшают положение государства по сравнению с тем, что было до принятия этих документов. Кто занимается расследованием инцидентов в ИКТ-среде? Только правоохранительные органы и спецслужбы, больше реально никто. Вот, что надо решать, что действительно составляет проблему. Представитель МИД РФ заявила, что за последний месяц было совершено большое количество атак на сайт МИД с территории США. Ну что мы должны принести в США из МИД? И что США скажут на это? На это АНБ принесет свои бумаги и скажет: «Да мы в это время вообще спали, у нас был обеденный перерыв, и мы не могли работать в это время». Давайте этим займемся.

Итак, было предложено положить в основу существующие наработки. Институт проблем информационной безопасности МГУ им. М.В.Ломоносова совместно с Институтом Восток-Запад в течение двух лет разрабатывал глоссарий терминов применительно к проблематике информационной безопасности, кибербезопасности и т. д. Этот глоссарий переведен уже на пять языков, включая корейский, то есть какая-то основа уже есть. Давайте его возьмем за основу. Коллеги посмотрят, насколько он подходит для использования при ведении военных переговоров. Таким образом, набирается какой-то клубок идей, который можно было бы вынести на следующее обсуждение. Несколько моментов, связанных с отработкой терминологии. Может быть, сократить список тем для работы, я набросал узкий перечень тем.

В каждой стране своя политическая система, государственный строй, в России одна система, в Америке другая, в Китае - своя. В МТ нет никакой вертикали власти, я сам делаю то, что

считаю нужным. Если у меня возникла идея, и если я смогу убедить всех в ее привлекательности и перспективности, то ко мне присоединятся коллеги. В нашей группе участвуют россияне, американцы, специалисты из Китая, Кореи, у нас есть выход на Агентство национальной безопасности, на киберкомандование и т. д. Если мы не сможем отработать данную проблему, то никто этим заниматься не будет.

140 стран сейчас так или иначе имеют определенный потенциал ИКТ и могут его также использовать в военных целях, поэтому ни в коей мере нельзя упускать момент, нужно наращивать доверие. Работать на основе универсального подхода, на основе смешения наших традиций, национальных и психологических особенностей, исторических традиций - в этом уникальность нашего проекта. Мы не должны зацикливаться на различиях, это верно и в отношении нашего проекта. Нужно определить, какие мы ставим перед собой цели, к чему стремимся, и это определит выбор тем, на которых мы должны сосредоточиться. Нужно выявлять самые простые темы, которые не будут вызывать особых разногласий, но будут иметь серьезное влияние и продемонстрируют геометрический прогресс.

Что, если нам составить проект повестки дня следующей, декабрьской встречи так: стабильность, например, в условиях кризиса, как обеспечить эффективные коммуникации, информационно-массовую работу в условиях кризиса, как можно управлять использованием технологий нападения на объекты инфраструктуры. Защита критической инфраструктуры, проблема распространения, контроля над экспортом, технологические вопросы, снабженческая цепочка, меры снижения рисков в результате кибернестабильности, лучшая международная практика - оценка соразмерности, каковы критерии стабильности, правовые вопросы, обеспечение стратегической стабильности на уровне технологической эволюции.

Следующий вопрос: стабильность в военное время, эскалация, как деэскалировать конфликты, каковы правовые аспекты и соображения. Стабильность в условиях многостороннего киберконфликта, когда проводятся информационно-психологические раз-

ведоперации, то есть целый список, перечень вопросов, трудных вопросов, причем он не окончательный, это лишь начало. У вас есть собственные идеи, соображения, вы должны их высказывать. Китайцы высказали свои идеи, а вы - другие. Мы можем посмотреть, что более приоритетно. А непосредственная задача - помочь китайцам спланировать конференцию, обеспечить хорошие результаты в краткосрочной перспективе.

Чем отличается этот форум от других? Национальные университеты обороны Китая и США участвуют в этих форумах, и это дает реальную связь с военными, возможность делиться информацией с ними, стимулировать их участие и взаимодействие в этом процессе.

Владислав Шерстюк: Я не очень понял выступающего, который сказал, что они встречаются на уровне оборонных университетов, общаются и каким-то образом это потом становится известно их военным, и они это как-то используют. А вот представитель нашего Генерального штаба Вадим Запивахин сказал, что мы сегодня лишены диалога. Когда готовился этот форум, мы с вашей подачи включили в него вопросы стратегической стабильности, со своей стороны подготовили большую группу военных, чтобы сюда приехать, а потом узнали, что вы не везете никого из «живых» военных. У нас же участвует представитель Генерального штаба. Где ваши представители генеральных штабов? Нам есть о чем поговорить, и площадка Гармиша располагает к этому. У нас - научный форум, мы сюда приглашаем людей, которые занимаются наукой в этой сфере и вместе с тем приглашаем экспертов, действующих военных, которые владеют темой, им есть о чем поговорить. Наш форум был бы более эффективным, если бы кроме гражданских, ученых, экспертов, здесь бы собирались и «круглые столы» военных.

Филипп Бомард, Политехническая школа Парижа (Франция): Я представляю военное училище, мы подчиняемся министру обороны и премьер-министру. Возвратимся к разго-

вору о нормализации, классификации, терминологии. Мне кажется, что нам надо лучше справляться с этими проблемами, потому что киберконфликт - это новый вид противодействия и каждый раз при возникновении таких новых вопросов появляются новые практические проблемы, мы пытаемся регулировать конфронтацию, которой раньше никогда не было. Сейчас это явление возникло, и мы не знаем, как с ним быть.

Вопреки другим векторам вооруженной борьбы в прошлом, мы теперь действуем не в одиночку. Могут возникать другие субъекты, оказывающие дестабилизирующее воздействие в США, России, Франции, не говоря уже о вопросе атрибуции. Это большая проблема атрибуции этих актов, враждебных действий, то есть возникает новая среда, новая модель противоборства, которая не подлежит интерпретации с помощью традиционных средств. Эти новые средства, новые средства ведения войны, противодействия, имеют непредвиденные, непредсказуемые последствия, выходящие за рамки военной сферы. Некоторые из них могут привести к автоматической эскалации, которая быстро выходит из-под контроля военного и гражданского руководства.

Согласен с тем, что нам необходимо наладить диалог между военными, потому что МИТ или политехнический институт, или университет - это те площадки, где могут вестись такие разговоры, но не только. Я мог бы пригласить несколько генералов из Генерального штаба, но нам необходима определенная степень гибкости такого диалога. Диалог необходим.

Джон Мэллори: Такой диалог можно проводить в рамках программы Гармиша, но он должен проводиться и в других странах, например в Китае, потому что иногда невозможно пообщаться с этими людьми за пределами Китая, в США тоже есть люди, которые не будут выезжать за пределы страны. Наверное, и в Москве тоже стоит, потому что, уверен, есть представители России, которые не будут выезжать для такого разговора. Мы приветствуем участие России в этом диалоге и будем продолжать его и с Китаем.

Гармиш-Партенкирхен, Германия

Семинар - «круглый стол» №2

Сессия 2
Потенциал использования ИКТ в военно-политических целях в контексте стратегической стабильности

Управление конфликтами и деэскалация в условиях многоуровневого киберконфликта

Джон Мэллори, Массачусетский технологический институт (США): Давайте сопоставим информационную среду и кибер-среду. Киберпространство отличается от информационной сферы большей скрытностью и засекреченностью. Здесь трудно понять, что происходит. Нужен более эффективный мониторинг. Для предметной работы требуется фактологическая, доказательная база. Особенно важен криптографический потенциал, чтобы предоставить контрагенту доказательства, не раскрывая ваших данных.

Мы рассмотрим некоторые вызовы и проблемы, о которых я уже говорил две недели назад, выступая в Сингапуре. Мы обсуждали тему кибербезопасности в Азии в контексте нестабильности и многостороннего киберконфликта, распространения киберпотенциала. Рассмотрим, каковы сферы конфликта и потенциального сотрудничества.

Рассмотрим конфликтное регулирование, различные измерения многостороннего конфликта и факторы. У нас несколько таких параметров - каналы, опасности, природа нападения и сдерживания, механизмы деэскалации, ответные меры, затем выводы и заключения. Итак, традиционные фазы конфликта - спор, кризис, военные действия, различные уровни военных действий, высокая, например, степень - это более 100 тыс. жертв, затем спор после боевых действий, еще один кризис и урегулирование.

В многоуровневом киберконфликте у нас присутствуют другие компоненты. Спор - это комплексное понятие, многокомпонентное. На низком уровне интенсивности конкретные претензии вызывают агрессивные действия. Возникает первая фаза приобретения потенциалов. Происходит кража IP-адресов, проводятся операции по оказанию влияния. Затем начинается «серая зона» - это подготовка к боевым действиям, агрессивная разведка, проникновение в промышленные оборонные сферы. Следующим этапом становится кризис. Затем начинаются кибероперации, предшествующие военным действиям, то есть это, так сказать, подготовка поля боя.

Традиционные подходы не освещают эти дополнительные фазы развития конфликта. Итак, каковы наши цели? Мы стараемся обеспечить урегулирование спора путем посреднических действий.

Если не удается урегулировать на этом уровне путем стабилизации и модерирования, возникает предкризисный этап. Этап кризиса - в данном случае необходимо регулировать и проводить деэскалацию. По крайней мере, обеспечивать стабильность, с тем чтобы кризис не выходил из-под контроля на политическом уровне. В киберсфере есть различия, потому что, все действия осуществляются с высокой скоростью. Задействование автоматиче-

ских систем сжимает временной диапазон для принятия решений. Как только начинаются военные действия, нам необходимо снижать интенсивность боевых действий и заканчивать конфликт.

На данном слайде вы видите немножко другую картину, внизу экономические параметры кризиса. Ниже уровня вооруженного конфликта - инфраструктура, экономические действия, технологии, НИОКР, ИКТ, электронно-техническая разведка. Преимущества в этой сфере получают крупные игроки. Поднимаемся выше - традиционные военные уровни, операции разведывательного характера, затем полицейские, правоохранительные вопросы, терроризм, может быть, тоже попадает сюда, помимо преступности. Самый высший уровень - объединение информационных ресурсов, потенциалов кибербезопасности крупных игроков, государств.

Кто является субъектом угрозы, источником угрозы? В основном это государства. Они обладают крупнейшими потенциалами. Есть преступные группы, которые тоже способны наращивать значительные силы и средства. Соответственно, возникает вопрос распространения и возможного попадания этих средств в руки террористов - достаточно опасная ситуация.

Следующий слайд. Киберконфликт - это не просто взлом каких-то систем, хакерство. Серьезные субъекты используют хакерство, взлом для крупных инсайдерских операций, операций по снабженческой цепочке, по оказанию долгосрочного влияния. Акторы высокого уровня тратят миллиарды долларов на создание таких сил и средств.

Если посмотреть на операции оказания влияния - то это стратегические кампании идеологического воздействия, с применением соответствующей инфраструктуры. Цифровые СМИ меняют общую картину, как произошло с возникновением радиосвязи во время Второй мировой войны. Речь идет не только о распространении идеологических сообщений в государственных СМИ. Сюда относится скрытое информвоздействие, работа агентов влияния, кража документов, утечки, компромат, влияние на редактора с целью достижения каких-то определенных задач, проведение кампаний в социальных сетях, применение ботов.

Можно составить некую иерархию таких операций с точки зрения обороны и нападения, потом уже будем говорить о деэскалации таких операций.

Следующий слайд - попытка характеристики такого рода операций. Сама инфраструктура кибероперации не такая уж дорогая. Можно также задействовать рекламные фирмы, пиарфирмы для разработки тех или иных сообщений-месседжей и использовать новые технологии распределения, создавать синергетические эффекты, используя полные спектры технологических средств.

Следующий слайд. Есть три режима конфликта - приобретение конкурентных сил и средств, гонка вооружений; соперническое операции ниже уровня вооруженного конфликта, агрессивная разведоперация, подготовка поля боя; операции по влиянию и экономические и хищнические операции.

Еще слайд. Рассмотрим, как в глобальном масштабе формируются векторы конфликта применительно к киберсреде. В основе лежат взаимоотношения крупных держав между собой и связанная с их деятельностью озабоченность странсоседей.

Так, китайцы обычно оглядываются на США, а соседи смотрят на Китай. В Центральной Азии ведется геополитическая борьба, соперничество за влияние, то же связано с Россией. Южная Корея подвергается хакерским атакам со стороны Северной Кореи на протяжении 20 лет. В Южной Азии Индия, недовольная кибероперациями Китая, быстро наращивает свои возможности. На Ближнем Востоке Иран, недавняя жертва Stuxnet, активно занимается взломом суннитских систем. В Тихоокеанском регионе ситуация обостряется из-за конфликтов в Южно-Китайском море. В Восточной Европе Россия полагает, что деятельность НАТО представляет угрозу. Катализатором служит украинский кризис.

Взаимодействие игроков, конкуренция в области развития сил и средств потенциалов приводят к формированию системы договоров в области кибербезопасности, а также неофициальных схем киберподдержки и обеспечения. Это не официальные

договоры, а некие неформальные отношения к киберподдержке. Страны, находящиеся на периферии договорного процесса, начинают нервничать и искать гарантии безопасности.

Подвожу итоги. У государств в рамках двусторонних отношений возникает ряд взаимозависимых дилемм безопасности, выходящих далеко за пределы этих двусторонних схем и влияющих на все окружение в целом. Здесь очень сложно предложить оптимальное решение. Проблемы крупных держав и обеспокоенность малых государств усложняют ситуацию.

Рассмотрим это в рамках дилеммы, заключенной в теории игр. Если мы стараемся повысить уровень нашей безопасности, используя недостатки другой страны и сотрудничая с ней, а та, другая страна не участвует, - это худший сценарий. Если обе страны отказываются сотрудничать, то положительные результаты тоже исключены. Р.Аксельрод изучил эту теорию и предложил теорию социального порядка. Есть некое понимание о возможности договориться на асимметричной основе, когда обе стороны проявляют определенный уровень терпимости.

Прежде всего, сдержанность должны проявлять крупные страны, потому что от них зависит эта система. Все государства должны подчеркивать важность пассивного сдерживания - оно не приводит к усугублению дилемм безопасности.

С точки зрения технологического и экономического аспектов кибернормы и нормы повышения доверия - как компоненты высокого уровня - должны быть специально приспособлены с учетом регионального контекста и специальных требований.

Итак, новые киберканалы конфликта нуждаются в изучении. Как работает система эскалации, каковы основные понятия конфликтного урегулирования? У нас нет пока таких средств для данной среды. Если возникают проблемы снабженческой цепочки, кто может выступить посредником при урегулировании проблемы? Мы должны определить, кто может выступать конфликт-менеджером, выработать требования к его знаниям и умениям. Необходимо подумать о том, как найти какие-то алгоритмы, позволяющие решать эти проблемы.

Стратегическая стабильность в киберпространстве

Энекен Тикк, Лейденский университет (Нидерланды), Мика Кертуннен, Институт киберполитики (Эстония): Мы говорим о стратегической стабильности в киберпространстве. Ключевое понятие здесь - способность к адаптации. Если вы не адаптируетесь - погибнете. Как произошло с динозаврами, которых можно увидеть в палеонтологическом музее.

Стабильность - это не только противодействие угрозам и изменениям, но и способность приспосабливаться к изменениям, таким как удар метеорита, или другим каким-то непредвиденным обстоятельствам. Эта идея возникла в литературе по стратегической стабильности, есть много исследований на эту тему. Например, Джон Бойд и другие авторы.

Стабильность - это процесс, а не конечное состояние. Предполагалось, что Хельсинкский акт 1975 года должен закрепить состояние послевоенной Европы. Не получилось, Советский Союз распался, Германия объединилась, и даже Эстония стала независимым государством. То есть такое закрепление, цементирование - это не самый лучший способ обеспечения стабильности.

Наш подход состоит в следующем: размышляя о стабильности на основе литературы, мы выделяем предотвращение конфликта, функциональность глобальных технико-стратегических систем и преемственность политических отношений в условиях такого конфликта.

По функциональности: возьмем Тринидад и Тобаго - туризм является критической инфраструктурой для этой страны. Основные финансовые поступления - от туризма. Если критическая инфраструктура нарушена - это для данной страны нарушает стратегическую стабильность. Критическая инфраструктура должна быть безопасной в условиях ИКТ-среды. Прежде всего это относится к ядерным системам сверхдержав, необходимым для стратегического сдерживания.

Но проблемы стабильности не ограничиваются лишь тремя сверхдержавами. И когда речь заходит об ИКТ-потенциалах,

то, в отличие от ядерного оружия, мы не знаем, кто их создает, как они используются, где находятся.

Путем образования более предсказуемой среды, на основе международного права, путем переговоров, определения границ приемлемого и неприемлемого мы приближаемся к стабильности. В этом контексте делаем упор на отношениях США с Россией и Китаем. Но поскольку упоминали также роль П5, П5+1, то можно говорить о повестке, которая тоже должна вносить лепту в обеспечение глобальной стабильности и ответственности стран за глобальную стабильность.

Стабильность достигается через действие. Если не можем договориться, выработать единые нормы в ИКТ-сфере, то нужно принимать меры относительно тех стран, субъектов, сторон, юрисдикций, которые мутят воду и причиняют нам неудобства.

Перейдем к мерам защиты в рамках международного права. Какие механизмы для этого есть? Давайте зададимся вопросом, право у страны пользоваться интернетом - это право или это привилегия, которая может быть как предоставлена, так и, наоборот, изъята, отобрана.

Далее, исполнение функций жандарма. Нужно ли создавать некую полицейскую силу, которая господствовала бы на этом поле, восстанавливала бы правила поведения и следила бы за их соблюдением?

В свете нестабильности нужно говорить о том, что можно условно назвать доверием к своему собственному потенциалу. Ведь технологии распространяются по всему миру, и поэтому снижается степень уверенности страны в способностях охранять свой информационный суверенитет.

Как мы видели в рамках процесса ГПЭ ООН, наблюдается серьезный интерес на международных встречах к выработке некой формулы кибербезопасности. И вот в этой связи предлагаю думать о стабильности, которая может быть достигнута через общие интересы. Речь идет о возложении задач по поддержанию этой стабильности всеми участниками в равных долях.

И наконец, государства не являются единственными или последними гарантами стабильности. На этой сцене имеется очень много других сторон и субъектов.

В заключение надо задаться вопросом, а готовы ли мы? Например, как и на каких условиях мы будем сохранять нашу специфику, наши идентифицирующие характеристики?

Мика Кертуннен: *С оптимизмом отмечаю, что все мы неоднократно упоминали слово «доверие» как основу для достижения стабильности. Однако должны существовать заинтересованность каждого субъекта в стабильности и основывающееся на этом ответственное поведение. При этом стабильность - понятие динамическое, развивающееся.*

Актуализация содержания понятия «стратегическая стабильность»

Павел Карасев, Институт проблем информационной безопасности МГУ им. М.В.Ломоносова: Коллеги, буду говорить с вами об актуализации содержания понятия «стратегическая стабильность».

Начать следует с рассмотрения самого этого понятия. Оно прочно вошло в обиход международных отношений и, как нам всем известно, возникло в результате противостояния двух сверхдержав биполярного мира. Основные положения стратегической стабильности закреплены в ряде документов, которые созданы этими двумя странами. И несмотря на это, сегодня стратегическая стабильность существует без четко выверенного и общепринятого определения.

Попытавшись проанализировать прагматику международных отношений, договоров, заявлений, документов стратегического планирования, в результате пришел к выводу, что за последние 25 лет произошли некоторые изменения.

Во-первых, геополитические перестановки. Биполярная система перестала существовать. Если раньше в систему стратегической стабильности входили только две сверхдержавы, то сегодня мы можем быть очевидцами становления многополяр-

ного мира. И в этом мире надо ответить на вопрос: как формула стратегической стабильности должна быть адаптирована, как применима, например, для выстраивания стратегической стабильности между Китаем и США? Как на систему стратегической стабильности влияют различные несистемные акторы, например те страны, которые не участвуют в договорах об ограничениях оружия массового уничтожения, или, например, такой актор, как международный терроризм?

Во-вторых, если раньше в формуле стратегической стабильности рассматривались стратегические средства обороны и нападения, то есть, соответственно, стратегические ядерные силы и стратегическая противоракетная оборона, то сегодня появляются новые способы стратегического воздействия. Обратимся к документам. В совместном заявлении СССР и США о дальнейших переговорах по сокращению наступательных вооружений 1990 года дана такая формула: «Стратегическая стабильность - это состояние стратегических отношений двух держав, при котором отсутствуют стимулы для нанесения первого удара» - и выделены определенные принципы, которые должны поддерживать стратегическую стабильность. Это уменьшение концентрации боезарядов на стратегических носителях и оказание предпочтений системам вооружения, обладающим повышенной выживаемостью.

Сегодня военно-стратегическая стабильность может пониматься как устойчивое состояние международных отношений, при котором государство или коалиция государств воздерживаются от решения спорных вопросов военными средствами.

Обращусь к расширению понятия стратегической стабильности. Это особенно характерно для Соединенных Штатов. Происходит включение в военное планирование новых сил и средств стратегического воздействия при сохранении существующей роли ядерного оружия. Например, существует Обзор ядерной политики 2010 года. В нем при общем сокращении тех задач, которые выполняет ядерное оружие, возрастает значение систем стратегической противоракетной обороны и конвенционального высокоточного оружия для

обеспечения национальной безопасности и стратегической стабильности.

В Америке также существует так называемая концепция молниеносного глобального удара, которая призвана решить многие из тех задач, которые возложены на ядерные силы. Суть ее в том, что межконтинентальные баллистические ракеты используются в неядерном оснащении и способны очень быстро и точно нанести удар по заданной цели.

И если посмотреть на подходы Соединенных Штатов, важно отметить два момента. Во-первых, что это высокоточное оружие и системы стратегической ПРО рассматриваются именно в общем контексте стратегической стабильности. Во-вторых, что высокоточное оружие должно противостоять новым вызовам и угрозам. А это означает, что его использование жизненно важно для реализации национальных интересов и, таким образом, пока принципиально не ставится вопрос о его возможном ограничении и сокращении.

С другой стороны, существует позиция таких государств, как Россия и Китай. В 2016 году было сделано совместное Заявление руководителей двух государств об укреплении глобальной стратегической стабильности. В нем говорится, что надо перестать трактовать понятие стратегической стабильности как сугубо военную категорию из области ядерных вооружений, потому что это уже не отражает существующих реалий. Дана новая формула стратегической стабильности - это состояние международных отношений, которые характеризуются такими факторами в политической сфере, как строгое соблюдение всеми государствами и объединениями государств принципов и норм международного права и положений Устава ООН, регулирующего вопрос применения силы, соблюдая уважение законных интересов всех государств и народов при решении актуальных и международных региональных проблем, а также не допуская вмешательства в политическую жизнь других государств.

В военной сфере данный фактор - это сохранение всеми государствами своих военных потенциалов на минимальном уровне, необходимом для обеспечения национальной безопас-

ности и направленном на воздержание от шагов в области военного строительства, которые могут быть негативно восприняты другими членами международного сообщества и, естественно, вызовут ответную реакцию. Фактически мы говорим о гонке вооружений. Необходимо смягчение разногласий путем позитивного и конструктивного диалога, укрепление взаимного доверия и сотрудничества.

Формула стратегической стабильности в России уточняется в ряде документов стратегического планирования. В частности, в Военной доктрине 2014 года упоминается угроза, исходящая от системы высокоточного оружия в рамках концепции глобального удара. В основе государственной политики в области международно-информационной безопасности 2020 года говорится об угрозе использования информационного оружия как фактора, способного оказать негативное воздействие на систему стратегической стабильности.

Рассмотрев эти два подхода, мы оказываемся перед другим вопросом. Как можно смотреть на средства стратегического воздействия в XXI веке? Сейчас рассматриваются не только стратегические ядерные силы и системы стратегической ПРО. За последние 20 лет мы увидели расширенное применение высокоточного оружия, крылатых ракет, за последние десять лет - что появляется так называемое кибероружие. И даже поверхностный анализ показывает, что эти новые средства стратегического воздействия - в плане проецирования мощи государства и реализации национальных интересов - обладают значительными преимуществами в сравнении с классическим ядерным оружием.

Если будем думать, как включить эти факторы, новые средства стратегического воздействия в старую формулу, то тут есть два подхода.

С одной стороны, эти факторы могут рассматриваться как потенциально дестабилизирующие для существующей формулы, то есть в которую входят стратегические ядерные силы и системы стратегической ПРО. Они могут, например, путем использования каких-то новых видов кибероружия оказать непосредственное воздействие на системы боевого управления и

контроля или на систему предупреждения ракетного нападения. И по мнению некоторых ученых, именно повышение уязвимости таких систем - систем управления - является прямой угрозой стратегической стабильности.

С другой стороны, можно подойти к этому вопросу иначе и рассматривать новые факторы стратегического воздействия как самостоятельные элементы, способные не только оказать воздействие на существующую систему стратегической стабильности, но и быть стратегическим оружием самим по себе.

Почему это важно? Потому что в современных условиях применение ядерного оружия ограничено рядом критериев и возможно только при определенных условиях. Как показывает анализ стратегических документов, большинство стран, которые обладают ядерным оружием, рассматривают его применение только в контексте каких-то жизненно важных угроз, которые нацелены непосредственно на их территории. Кроме того, использование ядерного оружия сопряжено с морально-этическими и даже экологическими ограничениями. То есть в современных условиях ядерное оружие хорошо выполняет задачи сдерживания, которые традиционно на него возлагаются, но оно практически бесполезно для проецирования реальной силы.

В современном мире сохраняется потребность в таком силовом или ином воздействии, которое, обращаясь к классикам - К.Клаузевицу, - имеет целью заставить противника выполнить нашу волю. Эта потребность никуда не исчезла, наоборот, после распада биполярной системы и появления новых точек напряженности на глобальной карте возросла. И сверхдержавы нашли новые силы и средства для реализации своих национальных интересов, проецирования своей мощи в стратегических масштабах.

Возьмем Афганистан, Ирак, Сирию - везде можно найти пример использования высокоточного оружия. При этом, если мы используем кибероружие, то ему можно отдать предпочтение, так как у него есть ряд преимуществ.

Во-первых, невозможно зафиксировать и оценить его характер средствами объективного контроля и наблюдения. Не-

возможно провести точную и быструю атрибуцию атаки. Таким образом, низкие политические риски его применения и высокая потенциальная эффективность могут в перспективе даже привести к тому, что оно будет использоваться гораздо охотнее, чем высокоточное оружие. Кибероружие станет основным инструментом реализации военно-политических интересов. Представляется, что при актуализации понятия стратегической стабильности надо все эти факторы, о которых я сейчас говорил, учитывать.

Мне кажется, что сохранение стратегической стабильности в формулировке, которая в какой-то мере сохраняется сейчас, может быть выгодно той стороне, которая будет рисковать. У нее будет риск потерять преимущества, которые она имеет при обладании высокоточным и кибероружием. В Концепции внешней политики Российской Федерации говорится о том, что как раз при заключении новых договоров в области контроля над вооружениями и укрепления доверия в военной сфере должны учитываться все без исключения факторы, оказывающие влияние на стратегическую стабиль-

ность. Соответственно, это - развертывание противоракетной обороны, размещение оружия в космосе, использование ИКТ в военно-политических целях, противоречащих международному праву.

Представляется, что должен быть либо единый документ с учетом новых факторов или должен быть принят ряд взаимосвязанных документов по всем отраслям стратегических вооружений. При этом стремление расщепить стратегическую стабильность на ряд маленьких «стабильностей», таких как, например, стратегическая киберстабильность или стратегическая стабильность в космосе, является очень опасным и может привести в конечном счете к дестабилизации.

Потому что, во-первых, все эти факторы являются взаимосвязанными, и нельзя допускать того, чтобы мы договорились по кибероружию и забыли то, что оно может влиять на ядерное оружие или как-то в совокупности задействовать его. А во-вторых, если будут договариваться какие-то группы стран, то это может привести к игнорированию интересов третьих государств, что также приведет к дестабилизации.

Подводя итог, надо сказать, что за последние 15-20 лет понятие стратегической стабильности вышло далеко за пределы баланса и равновесия стратегических наступательных и оборонительных вооружений. Представляется, что в формулу стратегической стабильности на данном этапе должны быть на равных правах включены новые средства стратегического противоборства. В принципе кибероружие является одним из таких компонентов. Многие эксперты и официальные лица не раз говорили о том, что по своему воздействию оно способно сравниться с ядерным. И полем боя с применением кибероружия является весь мир, когда по нажатию кнопки можно произвести атаку в любой точке Земли.

Классическая формула самоподдерживающейся стратегической стабильности предполагает установление определенного паритета, когда наращивание потенциала одной из сторон не ведет к усилению стабильности, а, наоборот, приводит к ее снижению.

Принимая во внимание нереалистичность сценариев классического ядерного противостояния в современном мире, ценность ядерного оружия в поддержании стратегической стабильности, на мой взгляд, снижается. Ядерное оружие не помогает противостоять угрозе терроризма, не способно предотвратить агрессию против третьих стран. Оно никак не способно повлиять на ситуацию и избежать экономических санкций. Оно является последним доводом, фактором абсолютного уничтожения. Сегодня действительно большее значение имеют крылатые ракеты и компьютерные вирусы, которые не столько подрывают потенциал классического ядерного оружия, сколько обладают собственным потенциалом. И в этих условиях представляется необходимым переосмыслить стратегическую стабильность.

Однако, может быть, нам стоит сделать шаг вперед и посмотреть на проблему по расширению содержания стратегической стабильности. До сих пор стратегическая стабильность рассматривала военно-политические факторы. Но сегодня на практике применяется не «жесткая» сила, а так называемая «умная» сила. И совокупный потенциал, таким образом, включает в себя не только военно-политические, но и экономические, и социокультурные факторы. Информационное оружие, о котором мы тоже здесь говорили, имеет сходную природу с кибероружием. И также позволяет решать задачи стратегического характера и реализовывать какие-то свои национальные интересы. Но только в этом случае целью, естественно, являются не критически-важные объекты, а массовое сознание.

Итак, вопрос актуализации понятия стратегической стабильности в условиях глобальной стратегической многополярности должен лежать в плоскости от уточнения и дополнения до полного переосмысления. Когда у множества полюсов влияния существуют различные средства стратегического воздействия, они могут эти средства проецировать на своих потенциальных противников. Новая формула стратегической стабильности должна, во-первых, отражать эту многополярность и, соответственно, в нее должны быть включены все заинтере-

сованные стороны, а также учет их национальных интересов. А во-вторых, в этой формуле должна быть обязательно учтена разнородность факторов стратегического воздействия и появление новых средств.

Армии «умных ботов» - инструмент достижения превосходства в информационном пространстве

Андрей Масалович, «ДиалогНаука» (Россия): Прошу извинить за некоторый непривычный стиль изложения, так как я больше привык к «хакерским» конференциям, чем к серьезным научным обществам, тем более что моя работа лучше всего определяется словосочетанием «менеджер по связям с реальностью».

Тема, которую хотелось бы осветить, надеюсь, будет интересна и здесь, поскольку она касается инструментария, который сейчас используется как на стороне светлых сил, так и во вред. Инструментария для манипулирования массовым сознанием, для воздействия на массовую аудиторию в социальных сетях и даже для задач, которые заставляют эту массовую аудиторию принимать те или иные решения вплоть до победы на выборах.

В ноябре 2016 года в Москве проходила конференция по кибербезопасности. Примерно в 11 часов 10 минут утра у меня пискнул телефон, и наша система экстренного оповещения «Аваланч» прислала мне сообщение, что через пять минут мировые СМИ объявят о том, что победил Трамп. Это уже серьезный повод, чтобы мировое сообщество проявило интерес к тому, что в России есть технологии, позволяющие анализировать ситуацию, и не просто анализировать, но и прогнозировать ее в глобальных сетях. После этого телефон у меня «взорвался», и вот уже который месяц мне задают два вопроса: первое - ответственны ли русские хакеры за победу Трампа, а второе - что я там такое рассказывал про российские методы и технологии для анализа массовой аудитории и для воздействия на эту аудиторию?

Что касается первого вопроса, то ответ простой - единственная в мире доказанная атака российских хакеров произошла в 1242 году, когда русские хакеры взломали лед Чудского озера. Все остальные атаки надо еще доказать.

Второе - что касается технологий, которые использовались для победы Трампа, то я не буду рассказывать о всех перипетиях борьбы и работы его избирательного штаба, но остановлюсь на одном аспекте, который, во-первых, касается работы с Интернетом, во-вторых, волею судеб очень сильно перекликается с тем, о чем мы говорили в этих стенах год назад.

Итак, победа Трампа в соцсетях была обусловлена последовательным выполнением трех шагов. Шаг первый - это использование так называемой психометрики. Это наука, разновидность прикладной психологии, о построении психологического портрета человека по поведению в соцсетях. Традиционно принято связывать данную технологию с Михаилом Казинским как одним из самых активных популяризаторов этой науки.

Самый известный его эксперимент - из доклада трехлетней давности, где он показывал, как по 68 лайкам в «Фейсбуке» удается определить цвет кожи испытуемого, то есть какой расы человек ставил лайки, только лайки, без репостов, без комментов, без фотографий. Далее - гомо- или гетеросексуальной ориентации, поддерживает Демократическую или Республиканскую партию. То есть по некоторому набору действий, которые мы выполняем в социальных сетях, даже самых простых действий, удается демаскировать те признаки, те маркеры, которые мы стараемся спрятать: пол, возраст, принадлежность, отношение к экстремистам, террористам, суицидникам или другим отклонениям. Эти технологии используются, в частности, для анализа психологических портретов подростков, а также для анализа окружения групп вокруг экстремистских сообществ и сообществ националистической направленности в соцсетях.

Вторая часть успеха Трампа базировалась на технологиях так называемого точного таргетирования, или точного выбора целевой аудитории. Лидером в данной области принято счи-

тать компанию «Кембридж Аналитикс», которая просто дальше других продвинулась и более старательно рассказывает и показывает, как эти технологии работают.

Третья часть успеха Трампа базировалась на конкретной группе внутри его избирательного штаба, даже сейчас часто показывают трейлеры, в которых она перемещалась по стране. Эта группа выявляла точки наиболее эффективного воздействия, то есть точки вокруг лидеров мнений, где собирается целевая аудитория, тот контент, который она готова воспринимать, и целевым образом направляла его в эти точки. Это был так называемый ударный контент. То есть та информация, которую хотели впрыснуть в мозги аудитории.

Не знаю, кто взломал мозг 40 млн. американцев, которые в итоге определили победу Трампа, но подозреваю, что вот эта технология очень-очень сильно в этом помогла. Чуть позже расскажу, почему она настолько эффективна. Дело в том, что при таком подходе - очень глубокий точечный анализ, а потом точечное воздействие - резко уменьшаются бюджеты, бюджеты продвижения. Нам не надо облучать большие аудитории, мы можем впрыскивать информацию именно в те мозги, которые готовы ее воспринимать, именно в тех местах, где они находятся.

Итак, после того, как ученые-аналитики подтвердили, что в феномене Трампа достаточно большую если не ключевую роль сыграли новые технологии массового воздействия в соцсетях, тема стала топовой.

Хотелось бы рассказать о некоем базовом механизме, то есть «заглянуть» под капот этой технологии, посмотреть, как она работает внутри.

Возможно, вы спросите: «Если вы такие умные, это все уже знаете и используете пять лет, то почему не пишете научных статей?» Нам не надо писать научных статей, о наших результатах пишет «Форбс», уже дважды российские результаты попадали в «Форбс», например в №2 за 2015 год, статья называлась «Разведка сетью…», а в мартовском номере прошлого года статья называлась «Виртуальный халифат. Как Россия воюет с ИГ в интернете».

Каждый из нас искренне верит, что он видит Интернет, я тоже в это верил и много лет в нем работал, считая, что та среда, в которой я работаю, и есть Интернет. Пока один раз мы к своей программе не приделали трехмерный визуализатор, который стал показывать, как выглядит активность в Интернете прямо сейчас, то есть генерировать картинку в реальном времени.

Каждый из нас видел много-много разных графиков, но эти графики просчитаны, то есть сначала что-то происходит, потом данные собираются, обрабатываются и вам показывают через какое-то время. Оказалось, что когда смотришь на активность в Интернете в реальном времени, то появляется картина, которую раньше не видел и не предполагал даже, как она выглядит.

Итак, давайте наденем очки 3D визуализации и посмотрим, как выглядит одна минута в «Твиттере». Его аудитория представляет собой некую ночную планету, в которой четко выделяются люди, у которых сравнительно мало друзей, плотный, так называемый органический, круг общения. Иногда они группируются обсудить какую-то новость.

Над ними политики, популярные артисты, всевозможные медийные персоны. У них совершенно необычная, раздутая популярность, и их практически не видно. Близко к реальному миру живут так называемые лидеры общественного мнения, или по-русски это называется сокращением «ЛОМ», которые что-то говорят, и их слушает их целевая аудитория, например секта «Свидетели Навального». В этой картине мира есть какие-то странные кластеры, которые живут совершенно по своим законам и их действия не похожи на действия обычных людей, реакция на новости не похожа на реакцию обычных людей.

Это ботнеты. Для того чтобы они стали эффективными, для того чтобы они нормально работали, таких ботов должно быть сотни, тысячи если не миллионы, иначе их действия не будут видны, их результаты, их активность не будет иметь результата.

Если мы возьмем классическое определение бота, так, как оно дано в «Википедии», то бот - это программа, которая ха-

рактеризуется простым, повторяемым поведением. Больше половины мирового интернет-трафика сейчас порождается ботами, а не людьми, то есть, это программы, которые выполняют какие-то свои программные действия, это не органический, не живой трафик.

Боты известны более 20 лет. Когда Интернет начинался, у меня, например, номер пользователя Интернета в России, так называемый «Рунет-АйДи» 2200, то есть, представьте, на всю Россию тогда было всего две с небольшим тысячи человек, которые вообще в Интернет заходили. Но даже из этих 2200 700 номеров было ассигновано под так называемые технические аккаунты, то есть фактически под ботов. Таким образом, боты были уже 25 и 30 лет назад. Но действия бота легко распознаются. Он простой, понятный, он ходит с одного IP. Он не может делать ничего сложного, его очень легко проверить, задав ему какой-нибудь вопрос. Он не понимает, как обойти так называемую «капчу», и долгое время считалось, что любая система может таких ботов фильтровать, тем более система типа социальных сетей или массовых ресурсов. Это одна из самых важных задач - пропускать трафик живых людей и не пропускать всяких рекламных спам-ботов.

Попробуем включить мозг хакера. Хакер знает не больше, у него просто более гибкий мозг. Давайте попробуем обойти капчу. Если перед нами один бот, он хочет попасть в социальную сеть и поговорить с участниками, то у социальной сети возникают сомнения, а живой ли это человек. Она ставит ему капчу.

Технически до сих пор нельзя с высоким качеством распознать капчу, особенно если у нее есть языковые особенности или если у нее есть какое-нибудь визуальное обобщение, например показать на картинке все бензоколонки. Вот, вроде бы бот это пройти не может, если он один. А теперь представьте себе, что у нас есть два бота и один хакер. Один бот должен пройти в соцсеть, но его не пускает капча, тогда хакер берет другого бота, взламывает какой-нибудь форум, где защита послабее, чаще всего, кстати, хакеры любят форумы, где занима-

ются всякой такой тематикой, как «веселые картинки, не вполне традиционное порно». Вот, хакер взламывает этот форум, и тогда один бот, получая капчу, отдает ее другому, другой находит живого участника, который прямо сейчас сидит, разглядывает «веселые картинки», подставляет ему капчу и говорит: «Твои действия оказались подозрительными, пожалуйста, подтверди, что ты человек, а не робот, ответь на эту капчу». Человек в полной уверенности, что он полез туда, куда не надо, что это он, его действия вызывают подозрения, заполняет капчу, которую получает бот, отдает другому, и тот проходит дальше.

Таким образом, два бота смогли совершенно спокойно обмануть, обойти механизм защиты соцсети. А поскольку в таких порночатах всегда есть аудитория, у нас получается бесплатная дежурная смена, которая будет эти задачи решать круглосуточно, причем на том языке, на котором должна быть отработана капча. Не спасет, даже если капча будет китайской или какой-то еще.

Появляются боты со сложным поведением, которые могут копировать или изображать действия человека, что привело к нескольким видам атак. Расскажу о трех простых видах новых атак, о которых еще не знают журналисты.

Первый вид атаки, назовем его «горизонтальный брутфорс», или «брутфорс по мультилогинам». Представим себе, что нам надо сломать почтовый сервер и получить логины и пароли миллионов пользователей. Ну, например, какой-нибудь хорошо защищенной почты, «мэйл.ру» или «gmail». Технически это сделать кажется невозможно. Почему? Базовый вид атаки, так называемый «брутфорс», грубой силой, или атака подбором, будет сразу заблокирована. То есть если я возьму один логин и начну подбирать пароли, то сервер увидит, что идет подбор паролей к одному логину и на третьей попытке заблокирует.

Представьте себе, что у меня уже в руках не один бот, не два, а миллион, и у меня в руках есть список из миллиона логинов, взятый из какой-то спам-рассылки. Тогда миллион ботов одновременно могут обратиться к серверу, задать разные логины и один и тот же пароль, например «123456», и серверу по-

кажется, что к нему одновременно обратился 1 млн. человек, каждый из которых сделал одну ошибку, что вполне допустимо. И он каждому ответит, что ошибся. Но из этого миллиона найдется, по моей практике, примерно 300-350 аккаунтов, у которых действительно будет пароль «123456».

В следующую минуту ботам ничего не стоит организовать атаку, проверить пароль «qwerty», или проверить пароль «ohmygod», или проверить какой-нибудь пароль со словом «Obama». И таким образом, через десять или через тридцать минут в руках у хакера будут тысячи если не миллионы взломанных аккаунтов, при этом сервер ничего не увидит. Просто к такому типу атаки, когда атакуют тысячи, миллионы ботов, серверы не готовы.

Второй вид атаки - атака на «Фейсбук». Один молодой исследователь пару месяцев назад заметил такую штуку. Если нажать кнопочку «напомнить пароль» на «Фейсбуке», то прилетит некоторый код. На почту придет письмо, в этом письме будет код и приписка «нажмите вот этот код подтверждения».

Дважды повторив эту операцию, он в этом адресе, который прилетает, нашел токен, собственно, то место, которое образует уникальный код для операции. Увидел, что оно очень сильно привязано ко времени, то есть его невозможно подделать, его невозможно расшифровать, его невозможно потом повторить, но оно привязано к текущей секунде, это первое. И второе - он обнаружил, что в силу длины таких кодов можно сгенерировать не более миллиона одновременно.

Соответственно, он взял 2 млн. ботов, в одну и ту же секунду отправил их в Интернет, нажав кнопку «напомнить пароль», один аккаунт у него был настоящий, он получил один настоящий токен, соответствующий текущей секунде, и раздал его 2 миллионам. Заставил 2 млн. ботов откликнуться, что «я забыл пароль, вот мой код, вы мне прислали код подтверждения, вот он».

И поскольку кодов было всего миллион, а пользователей было два, для нескольких аккаунтов код совпал. Их было, кста-

ти, не два, их было около 20. То есть за одну секунду он получил доступ к 20 аккаунтам в «Фэйсбуке». Это тоже возможный вид атаки, он тоже сейчас никак не бьется, не покрывается.

Третий вид атаки, который, может быть, будет вам интересен. У вас в руках или в кошельке есть кредитная карточка. Почти все ее данные очень легко восстановить, почти всеми вы делитесь, то есть легко найти номер вашей кредитки, легко понять «экспирейшн дэйт». Естественно, элементарно узнать вашу фамилию и имя, секретным остается единственные три цифры CVV, так называемый код идентификации с обратной стороны карточки. Он не передается, он не открывается, он не фигурирует в открытых базах, но там всего три цифры, то есть таких кодов всего 1 тысяча.

Если я попытаюсь подобрать CVV, работая с каким-нибудь интернет-магазином, банк «Эсквайр» меня заблокирует на третьей попытке. Он зафиксирует попытку подбора кода, но в мире есть 400 интернет-магазинов, из них у 360 нет даже элементарных средств защиты от такого вида атаки. То есть достаточно мне три раза обратиться в каждый интернет-магазин, у меня получится более 1 тыс. обращений на то, чтобы сделать какую-нибудь минимальную покупку на один доллар. То есть трех обращений в один магазин мне достаточно, чтобы перебрать всю тысячу, и через несколько секунд у меня в руках будет ваш код CVV.

Это тоже реальная атака, которая появилась за последний месяц, и связана она как раз с использованием таких вот армий «умных» ботов, когда много ботов с нескольких аккаунтов, с нескольких IP-адресов стартуют одновременно и при этом имитируют активность живых людей.

Такого рода активность используется не только молодыми нарушителями, которые пытаются взломать e-mail или получить доступ к вашей кредитке. Такие технологии используются и при массированных атаках. Например, атака на серверы «Клинтон фаундейшн» и серверы Демократической партии, которые приписывают российским хакерам, на самом деле исходно была инициирована румынским хакером под псевдонимом «Гуччифер 2.0».

Открою секрет. Лингвистический анализ показывает, что по происхождению он молдаванин, так что его можно с натяжкой назвать русским хакером. Скорее всего, его родители жили на территории бывшего Союза. Почему появились основания называть его русским хакером? Он использовал так называемое «дистортинг прокси».

Обычное назначение прокси-серверов - это скрывать, анонимизировать IP-адрес. Но при этом через прокси проходит так называемое ваше переменное окружение, то есть виден ваш язык раскладки клавиатуры, видны ваши дата, время и версия установки браузера, видна ваша версия «Майкрософт Офиса» и самого «Майкрософта», то есть вектор параметров, по которым вас потом криминалисты легко определят.

Поэтому после появления анонимизирующих прокси появились прокси, которые скрывают переменные окружения, но это тоже подозрительно. Сейчас появилось поколение так называемых элитных прокси - «элайт прокси», или их еще называют «дистортинг прокси», то есть искажающие прокси, которые не прячут переменное окружение, а подменяют их, воруя аккаунты, воруя личности у других пользователей. Соответственно, Гуччифер, выполняя атаки, выступал то как китаец, то как русский, то как испанец, то как англичанин. Это те четыре вида, которые я знаю. Поэтому, исследователи схватились, что среди его «скинов», или «масок», была русская и объявили его русским хакером.

Таким образом, подобного рода массированное применение «умных» ботов может быть использовано и теми, кто занимается более серьезными политическими атаками, а не только мелкими правонарушениями.

Мощь этих инструментов можно использовать и на светлой стороне. Можно на их основе делать средства для массированного анализа социальных сетей и решения всяких полезных задач. Например, 18 декабря 2014 года, когда Россию взорвали СМСки о том, что дела у Сбербанка идут плохо, вот-вот прекратятся платежи по кредитным картам, и эти СМСки шли волнами, началось волнение по всей России. Почему? На самом деле средний размер вклада тогда составлял не более 30 тыс. рублей на одно частное лицо. Вроде бы для крупного банка это немного, но у Сбербанка, как оказалось, не было экшн-плана, то есть не было системы отработки, моделирования такого вида атак. И, в частности, они не проверили, как работает колл-центр под нагрузкой.

Что происходило? Люди у нас серьезные, люди у нас спокойные, никто не бежал снимать деньги, все звонили в Сбербанк спросить, что там реально с карточками, и ласковый женский голос отвечал: «Ваш звонок очень важен для нас, к сожалению, все операторы сейчас заняты, ориентировочное время ожидания в очереди две недели». Вот после чего человек понимал, что мир рушится, и уже бежал снимать свои 30 тыс. рублей. И когда таких набралось 10 миллионов и со счетов слетели первые 300 миллиардов, Сбербанк понял, что не такой уж он и крупный.

Мне позвонили 18 декабря в полдень, это была суббота, и к вечеру у нас уже были готовы «тепловые карты»: оказалось, что атака была не равно размазанной, а были такие кластеры по России. И насколько я могу представить, на следующий день по этим адресам уже летели транспортные самолеты с наличными деньгами, загружались банкоматы, с тем чтобы погасить первую волну паники. Такого рода массированный анализ можно использовать и для решения массовых проблем.

Если выбрать некоторый уровень между человеком и соцсетью, а именно выбрать два круга вокруг человека - друзья и

друзья друзей, это примерно 50 тыс. аккаунтов вокруг нас, то они позволяют полностью создавать картинку, чем человек дышит, чем он увлекается, с кем дружит, кто еще вокруг него увлекается тем же.

Очень легко, таким образом, во-первых, ставить первичный диагноз и какой-нибудь школе, и какому-нибудь региону, и даже ребенку, и классу, можно следить за текущем состоянием и нарастанием всевозможных настроений. Буду использовать русские термины из практики нашего МВД: это «суицидники», «зацеперы», «живодерки», «синий кит».

Видно, что одна за другой идут какие-то проблемные виды групп детей, которых на самом деле можно легко контролировать, если эту технологию действительно использовать на благо правоохранителей. Делать это можно, кстати, не только в России.

Весной прошлого года в Казахстане прокатились массовые волнения после объявления о том, что будут, возможно, приватизировать землю и что всю землю скупят китайцы. В Интернете мы эти волнения увидели за два дня до того, как они выплеснулись на улицы. Но, судя по реакции казахских правоохранителей, они это видели только на улицах. Предварительного анализа обстановки в Интернете, как выяснилось, у них не было.

Почему это использовалось в кампании Трампа, почему это важно, в чем здесь экономия бюджета? Дело в том, что такого рода анализ поведения массовой аудитории связан с одной любопытной особенностью Интернета, которой раньше не было, это кнопка «репост».

Если у меня в руках нет кнопки «репост», я могу просто послушать новость и обсудить ее с соседями. Картина распространения новости точно расписывается формулами трехмерной ударной волны. То есть первый всплеск, потом затишье, потом вторая волна, обсуждение уже маленькое, и волна уходит в фон. Вот, смотрите, например новость - день рождения Путина. Поговорили про день рождения Путина, потом еще поговорили, тема ушла в фон. Вот в этот же день полетели калибры, о них говорили меньше. Произошло событие, о нем поговорили, оно ушло в фон. Что это дает?

Это приводит к двум следствиям, которые знает каждый специалист по пиару. Первое - если я трехмерной «бомбой» пытаюсь поразить аудиторию, двухмерное покрытие людей, большая часть осколков, большая часть энергии улетит в никуда и пользы не принесет. Точно так же пиарщик знает, что большая часть бюджета любого события улетает в никуда, но ему придется ее потратить, чтобы нужное количество осколков этой информации поразило его целевую аудиторию. То есть в традиционном пиаре все готовы к тому, что деньги выжигаются, деньги тратятся неэффективно. Второе - если у меня аудитория линейно увеличится, например, в два раза, то размер заряда, размер «бомбы», мне надо увеличить в квадрате или даже в кубе. Точно так же бюджет пиар-мероприятия. Одно дело - мне нужно собрать 30 тыс. человек, другое дело - 60 тыс. человек. Для 60 тысяч бюджет будет не в два раза больше, а в четыре, а то и, может быть, в восемь. И все были к этому готовы.

В реальном мире других путей нет, но в Интернете, где есть кнопка «репост», поведение аудитории лучше всего описывается формулами двухмерного взрыва. Каждый из нас видел, как падает капля дождя на воду. Кажется, что каждая капля становится центром волны. Некоторым каплям не повезло и их энергия будет погашена. Но некоторые капли попадут в резонанс, от них действительно пойдет волна, и эта волна уже не тратит нашей энергии, нашего бюджета, мы просто капнули каплю, а дальше она сама начала распространяться.

Если, условно говоря, один пригласит военного, он возьмет большую бомбу «взрывать» свою большую аудиторию, это будет дорого. А у меня будет фея, такая маленькая фея, которая будет летать с пипеткой и капать отравленными каплями на мозги моей целевой аудитории, я потрачу гораздо меньше сил и меньший бюджет. И вот именно так была устроена кампания Трампа, именно так устроен механизм воздействия на аудиторию в соцсетях, то есть нужно понять, где образуются сгустки нашей целевой аудитории, надо понять, в каких еще группах активны эти же люди, надо выделить среди них лидеров мнений и именно туда впрыскивать информацию.

В завершение еще два красивых примера, как эти технологии использовать на стороне добра.

Пример первый: как мы боролись с пиратами. В последний четверг прошлого года вышел очень популярный в России фильм «Елки-5». Его тут же украли пираты, тут же выложили на торренты, но кроме этого какой-то парень начал звонить в студию Т.Бекмамбетова и шантажировать, что он сейчас сделает так называемую «посевную», то есть начнет разбрасывать по Интернету ссылки с этим пиратским контентом.

Они пробовали обратиться к юристам и правоохранителям, что-то с ходу не получилось, они обратились к нам. Что мы сделали? Первое - мы запустили ботов, которые стали распространять по Интернету точно такой же текст, как у этого парня, такие же заголовки, такие же хештеги, но ссылка была неправильная, ссылка вела или на порнушку, или на старые фильмы, или на платный контент. У меня ребята еще хотели поставить ссылку на приемную ФСБ, но я им не разрешил. И атака самого этого парня стала незаметной, то есть его ссылки уже были не видны. Второе - мы сделали встречную атаку: стали распространять информацию о том, что не надо нажимать на эти ссылки, хештеги, потому что это вирус «троян», который заразит компьютер. И третье, мы сделали бота-юриста, который «ходил» по социальным сетям, находил этот противоправный контент, нажимал на кнопку «пожаловаться» и заполнял форму «пожаловаться».

В итоге активности этого парня хватило на полдня, потом он понял, что бесполезно, с ботами сражаться человек не может.

И последний пример. 25 января в Оптиной пустыне сгорел женский монастырь. Большой проблемы бы не было, потому что их духовник, отец Илий, является духовником Патриарха - деньги на ремонт нашлись бы мгновенно. Но в Интернете образовалось порядка 50 сайтов-мошенников, где начали собирать деньги вроде как на ремонт, на восстановление обители, а надо сказать, что наша церковь крайне неумело работает с интернет-аудиторией.

К нам обратились за помощью. Что мы сделали? Первое - мы сделали бота, который находил все места размещения про-

тивоправного контента и верхним комментарием писал: «А ведь это мошенники. Вас хотят обмануть. Сами мошенники, и счет мошеннический. Если хотите помочь, переводите деньги вот на этот счет», и показывал правильный счет. Естественно, мошенники это видели, тут же комментарий стирали. У бота стоял регламент 15 минут, он через 15 минут заходил, говорил: «А ведь это мошенники и счет у них неправильный, мошеннический». Человек не может каждые 15 минут бороться с железным ботом. После этого мы сделали еще встречную атаку, стали распространять ссылки с правильными реквизитами, ну и сделали бота-юриста, который «бродил» по Интернету, находил вот этот противоправный контент, нажимал кнопку «пожаловаться».

Итак, резюмирую. Технологии, о которых я хотел рассказать, сейчас стали реальностью. Нам очень помогло, что именно они использовались при выборах Президента Трампа и «наши» победили. Поэтому сейчас эта тема привлекает внимание и, надеюсь, будет востребована и представителями правоохранительных, силовых и государственных структур разных стран во имя добра.

Обеспечение информационной безопасности - одна из составляющих стратегической стабильности

Наталья Ромашкина, Институт мировой экономики и международных отношений им. Е.М.Примакова РАН: Хотелось бы поблагодарить организаторов форума за то, что проблема обеспечения стратегической стабильности стала темой столь авторитетного мероприятия. Уже много лет я занимаюсь проблематикой стратегической стабильности и в качестве математика, и в качестве международника, поэтому для меня это просто подарок. Предлагаю вашему вниманию результаты наших исследований по теме информационная безопасность как часть проблемы стратегической стабильности.

В первую очередь надо отметить, что, к сожалению, проблема обеспечения стратегической стабильности уже очень много лет не обсуждалась с Россией на международном уровне. Россия

была исключена из дискуссий по этим вопросам. Это привело к тому, что современный период, который можно назвать периодом ракетно-ядерной многополярности, характеризуется крайней степенью неопределенности, что существенно усложняет процесс обеспечения необходимого и достаточного уровня стабильности. Многие эксперты считают, что сегодняшний уровень стратегической стабильности приблизительно такой же, какой был в период Карибского кризиса, то есть самый низкий за всю историю существования ядерного оружия, за всю историю существования человечества.

Авторитетные ученые-атомщики совсем недавно переставили свои символические часы на время без двух минут до полуночи, где вот та самая полночь означает начало широкомасштабной ядерной войны. Как так получилось? На мой взгляд, это было предсказуемо. Безусловное исключение России из обсуждения проблем стратегической стабильности должно было привести именно к такому положению.

Немного о термине «стратегическая стабильность». Появился этот термин после того, как было создано ядерное оружие. И до сегодняшнего дня Россия и Соединенные Штаты обладают самыми большими запасами военных ядерных арсеналов. Поэтому не соглашусь с тем, что влияние ядерного оружия не столь значительно. Безусловно, ядерное оружие продолжает играть очень важную роль в процессе обеспечения стратегической стабильности и в оценке ее уровня.

На сегодняшний день в научной литературе существует очень много определений стратегической стабильности, от самых расплывчатых (например, таких, что все государства в равной степени должны строго соблюдать международные соглашения и договоры - хотя это совершенно невыполнимо, никогда не выполнялось и выполняться, вероятно, не будет) до более четких, более конкретных определений, которые уже касались непосредственно военных арсеналов и т. д.

С учетом тех изменений, которые произошли после холодной войны, мы предлагаем определение стратегической стабильности военно-политической системы, как состояние мира,

то есть отсутствие широкомасштабной войны в рамках этой системы, которая поддерживается даже при постоянно действующих возмущениях тех самых дестабилизирующих факторов, которые необходимо и очень трудно оценивать, в течение определенного, заданного периода времени. Вот эта заданность определенного периода времени как раз говорит о том, что понятие стратегической стабильности, безусловно, меняется в процессе изменения системы международных военно-политических отношений.

Структура понятия стратегической стабильности сегодня охватывает не только количественные и качественные уровни военных потенциалов. Она уже связана с уровнем экономического развития акторов, участников обеспечения стратегической стабильности, во многом зависит от договорно-правовой базы, причем не только в отношении ядерных вооружений.

В настоящее время отсутствие единого для всех ключевых субъектов современных международных военно-политических отношений закрепленного в документах определения стратегической стабильности, на мой взгляд, существенно затрудняет выработку международных практических мер по обеспечению ее необходимого и достаточного уровня.

Опыт показывает, что процесс разработки критериев оценки уровня стратегической стабильности и основанные на этом конкретные планы по ее обеспечению должны происходить с учетом как общих для любого исторического периода характеристик, так и особенностей, которые свойственны различным этапам.

Для современного этапа характерно ускоренное развитие информационно-коммуникационных технологий, и это на сегодняшний день является одним из дестабилизирующих факторов. Сейчас мы постараемся это доказать. Итак, что же это за дестабилизирующие факторы, которые сегодня определяют состояние и уровень стратегической стабильности? Это существующие потенциальные очаги локальных войн и вооруженных конфликтов, как было и в период холодной войны. Это возможность подрыва стратегической стабильности в результате нарушения международных договоренностей в области ограничения и сокращения

стратегических вооружений. Это отсутствие или неустойчивое состояние договоренностей по противоракетной обороне и обычным вооружениям, которые в определенных условиях также могут носить стратегический характер.

Кроме того, это возможность подрыва стратегической стабильности в результате нарушения режима нераспространения ядерного оружия, то есть создание современных видов вооружения, новых технологий военного производства в сочетании с попытками отдельных государств получить доступ к ядерному оружию, чтобы использовать его для реализации военных и политических целей. Еще один дестабилизирующий фактор - это создание широкомасштабной системы противоракетной обороны США, в которую вовлечены более 20 государств, и распространение баллистических ракет и ракетных технологий. Число государств, которые обладают баллистическими ракетами разной дальности, сегодня составляет более 30.

Следующий дестабилизирующий фактор - это возрастание роли и мощи неядерных, то есть высокоточных, высокоинтеллектуальных видов оружия в стратегическом планировании. Сравнительно новый дестабилизирующий фактор, который оказывает все большее влияние на уровень стратегической стабильности, - это развитие черного рынка ядерных материалов, технологий и экспертизы. Сюда же можно отнести международный терроризм, организованную преступность, которые способны использовать новейшие военные технологии, элементы ядерного оружия.

И на все эти указанные дестабилизирующие факторы на сегодняшний день влияют информационно-коммуникационные технологии. Каждый из приведенных факторов усугубляется использованием этих технологий, внезапностью воздействия информационно-психологических вредоносных средств.

Таким образом, к числу современных дестабилизирующих факторов и угроз, которые влияют на уровень стратегической стабильности и способы его снижать, конечно, сегодня уже можно отнести ускоренное развитие средств ИКТ, киберпреступность, кибертерроризм, кибервойны.

Еще один важный вопрос - понятие «киберугроза», для которого, как и для термина «стратегическая стабильность», пока не существует единого, общепринятого определения. Известно, что в России и еще в некоторых других странах больше используется термин «информационная угроза», в западных странах - «киберугроза». Мы применили самую широкую трактовку понятия «киберугроза», чтобы оценивать уровень стратегической стабильности. Это и хакерство, и вывод серверов из строя, и хищение, и шпионаж, и саботаж, и стратегические атаки, и противоборство государств в сфере ИКТ.

Каким же образом можно классифицировать эти киберугрозы в военной сфере? Мы выделили несколько классификаций. Это кибернападение на объекты военной и связанной с ней гражданской инфраструктуры, это физический вред, нанесенный программно-аппаратным средствам, элементной базе, линиям связи или сетям, которые обеспечивают функционирование военного объекта, или логический вред, наносимый дистанционно, с помощью вредоносных компьютерных программ, логических бомб и т. д.

К киберугрозам мы также отнесли атаки на военные объекты с целью шпионажа и создания киберагентурных сетей или саботажа. И фактически реальный вред от кибернападения или психологическое восприятие угрозы, то есть создание неуверенности у лиц, принимающих решения в процессе управления и контроля над ядерным вооружением.

Это очень важный аспект, потому что действительно это психологическое восприятие, психологический фактор, всегда игравшее очень большую роль в оценке уровня стратегической стабильности и восприятии ядерных вооружений. Все связанные с этими угрозами проблемы можно отнести к различным элементам военной организации инфраструктуры, но совершенно понятно, что самым важнейшим в данном контексте является блок киберугроз в сфере ядерного оружия. Мы выделили несколько проблем, которые существуют в этом отношении.

Хотела бы сказать, что в настоящее время существуют различные точки зрения в отношении вероятности и последст-

вий вредоносного кибервоздействия на систему командования, управления и контроля над ядерным оружием - от полного отрицания этой возможности до тезисов о резком увеличении такой вероятности в последние годы.

Мы исходили из реальности самых страшных вариантов. В качестве первой проблемы мы выделили возможность несанкционированного запуска баллистических ракет, а также влияние на принятие решения о применении ядерного оружия. Чем продиктована такая возможность? Ложной информацией от системы предупреждения о ракетном нападении, о запуске баллистических ракет с ядерным оружием со стороны потенциального противника. Это продиктовано возможностью внедрения и управления коммуникационными системами в командных пунктах ракетных войск для создания ситуаций несанкционированного пуска. А также непосредственным внедрением в электронные системы командования и контроля над ядерным оружием.

Итак, вторая проблема, которую мы выделили, заключается в том, что при анализе информационных угроз возникла необходимость оценивать разницу между акторами вредоносного воздействия с применением ИКТ - это государство, террористы и другие какие-то третьи лица. В этом случае кибернападения государств друг на друга, вероятно, могут быть направлены на шпионаж, выведение из строя системы командования и контроля над ядерным вооружением или элементов самого ядерного оружия противника, а также создание неуверенности у лиц, принимающих решения, в том, что системы будут работать эффективно.

В качестве третьей проблемы мы выделили следующее: анализ целей различных акторов, о которых мы говорили в рамках второй проблемы, привел к необходимости учета отличий между типами кибератак, открывающих доступ и блокирующих доступ к соответствующим системам. Открывающие доступ атаки могут быть направлены непосредственно на ядерное оружие, чтобы спровоцировать его применение, в том числе путем обмана так называемой Системы предупреждения о ракетном нападении (СПРН). Второй тип кибератак - блокирующие, они

могут быть направлены на намеренное повреждение систем вооружений для нарушения их работы или вывода из строя, в том числе повреждение коммуникационных сетей и СПРН, которые не дадут возможности получить приказ о запуске ядерного оружия, а также хищение секретной информации.

Еще одна проблема, которая сегодня стоит очень остро. Должно ли ядерное оружие играть какую-то роль в предотвращении информационных нападений на социальные, военные и другие критически важные объекты инфраструктуры? Этот вопрос представляется достаточно актуальным в связи с тем, что НАТО рассматривает сегодня кибернападение как военное нападение.

В качестве пятой проблемы мы выделили влияние роста вероятности вывести из строя или уничтожить ядерное оружие посредством ИКТ на будущее процессов ядерного разоружения и нераспространения. Налицо очень интересная дилемма. Возможны два пути, какими будет развиваться это влияние. В принципе это может послужить поводом для ускоренного процесса сокращения таких вооружений. С другой стороны, и, к сожалению, такой путь более вероятен, он может стать причиной для масштабной модернизации ядерного оружия, развития более сложных защищенных систем и, таким образом, приведет к созданию предпосылок для качественной и/или количественной гонки ядерных вооружений и как следствие - к дальнейшему снижению уровня стратегической стабильности.

На мой взгляд, России и США необходимо продолжать переговоры по ограничению сокращения стратегических ядерных вооружений. Исходя из вышесказанного, становится совершенно понятно, что продолжение этих переговоров неизбежно приведет к необходимости учета информационного фактора. Таким образом, вопросы обеспечения информационной безопасности будут включены в переговоры по ядерным вооружениям и стратегической стабильности на многосторонней и двусторонней основе с участием РФ.

В качестве еще одного пункта хотелось бы обратить внимание на то, что государствам - обладателям ядерного оружия

целесообразно активизировать работу по более эффективной подготовке персонала. Это должно начинаться еще с обучения в вузе и продолжаться в ходе переподготовки и дополнительной подготовки уже профессионалов-специалистов.

И наконец, хочу обратить внимание на необходимость активизировать научное исследование по разработке теоретических и методологических подходов к общепринятому понятию стратегической стабильности. Одним из очень серьезных стимулов для этого может послужить тот опыт, который был у США и СССР в свое время, когда речь шла об обеспечении стратегической стабильности еще до столь глобального влияния информационных средств.

Деэскалация роботизированной войны

Филипп Бомард, Политехническая школа Парижа (Франция): Я работаю в составе высокого совета по стратегическому образованию и исследованию. Это аналитический центр, созданный при Президенте Саркози, и, надеюсь, он сохранится при следующем Президенте Макроне. Наш центр охватывает несколько министерств, учебных заведений, Политехническую школу Парижа и несколько компаний. В его составе присутствуют отставные и действующие военнослужащие. Мы сами финансируем наши исследования, за последние десять лет реализовали 60 проектов.

У нас есть программа национальной обороны «DJ», это аналог американский DARPA. Имеется программа направленного финансирования стартапов, в первую очередь инвестиционных фондов, инновационных, исследовательских, ИКТ. Создан специальный банк, который специализируется на финансировании научно-исследовательских проектов в области ИКТ, искусственного интеллекта, его бюджет составляет 6 млрд. евро.

Мы осознаем, что все эти инновации могут интегрироваться в военную сферу, и поэтому мы должны разработать нормы, сдерживающие, или, как мы называем, деэскалирующие воз-

можность применения современных ИКТ-технологий, достижений в области искусственного интеллекта в военных целях.

Давайте попытаемся оценить степень автоматизации боевого управления. Чем больше автоматизации, тем меньше человеческого фактора. При этом надо учитывать и плюсы, и минусы. Плюс - в экономии человеческих ресурсов. Минус в том, что меньше возможности у человека вмешаться в какое-то внештатное развитие событий и пресечь его, в частности за пределами страны.

Вот такой забавный пример. Четыре года назад во Франции два подростка-хакера решили использовать автономных ботов, о которых мы сегодня слышали уже, обвалив сайт «Орандж». «Орандж» - это крупный оператор мобильной связи во Франции. Они же устроили «блэкаут», на два часа, полностью лишив район Парижа электричества. Мы их поймали, погрозили пальцем, потому что, собственно говоря, они подростки, что с них спросишь. Тем не менее такие возможности существуют сейчас, и как от этого застраховаться?

Любопытно, но на той же неделе, когда Президент России подписал российскую Концепцию обеспечения информационной безопасности, в то же самое время у нас была утверждена последняя версия доктрины информационной безопасности, не знаю, это совпадение или нет? Не думаю, как говорится. Французская кибероборона использует понятие «хэк бэг», то есть, если элемент суверенитета оказывается объектом кибервоздействия, объявляется условное состояние чрезвычайного положения. После введения ЧП вступает в силу принятый в 2015 году закон, предполагающий очень широкие полномочия для спецслужб в контексте угрозы со стороны хакеров. Если мы говорим об искусственном интеллекте, он не такой уж искусственный, откровенно говоря. Это набор инструментов вполне человеческого происхождения. Говоря об эволюции искусственного интеллекта, системы постоянно усложнялись, сначала появилась способность к обучению под управлением человека, потом возникло самообучение. Stuxnet - первый пример атаки с возможностью автономного обучения.

Другой пример с чатом «Тайм», в который был запущен бот, взаимодействовавший с участниками две недели и превративший его в вульгарную площадку неонацистского толка. Чат пришлось отключить. Это было PR-катастрофой с точки зрения «Майкрософт».

Сейчас все отрасли ИКТ активно вкладываются в разработку и развитие искусственного интеллекта, не для военных целей, для той же рекламы, как «Гугл», «Дипмайнд» например. Какая задача? Создать искусственного «друга» среди целевой аудитории, чтобы продавать продукты, отслеживать интересы пользователей.

Давайте посмотрим на динамику эволюций развития искусственного интеллекта. Логические бомбы в 1990-х, потом началась кампания по фишингу, потом «Triggered switch», «DNS». Центр Демократической партии в 2016 году тоже стал жертвой фишинговой кампании именно на уровне логической бомбы. Далее - украинцы использовали тоже фишинговый инструмент.

Следующий этап - это манипуляции на основе глубокого изучения (deep learning). Многие военные организации используют как раз системы национальной обороны, израильтяне например. Все эти технологии сейчас являются объектами активных экспериментов.

Последний момент - инъекция искусственного интеллекта в систему контроля боевого управления, разведки, связи и т. д. Там применяются не боты, не ботнеты. Это уже автономные, дистрибутивные атаки, которые предполагают достаточно изощренный инструментарий, позволяющий внедрять сложные вредоносные программы, которые самостоятельно способны эскалировать свои привилегии, и управлять, и проводить «соушл инжиниринг», сами создавать подсистемы, которые соответствуют их целям. Если такие атаки совершаются, то вам не нужно никакого надзора.

Искусственный интеллект может применяться в качестве оружия, не оставляя возможности человеку вмешаться. Связи с центральным пультом боевого управления уже не будет. Можете противопоставить друг другу два искусственных интеллекта, которые будут бороться сами, занимаясь эскалацией в соответствии с той моделью, которой мы их обучили. Можно получить конфликт такого уровня, который выходит из-под контроля и бумерангом бьет по нам же.

Правовая база направлена на деэскалацию автоматизированных операций с использованием ботнетов, но мы не говорим, что добились совершенства, тем не менее какие-то подвижки имеются. Нам нужно определить пути того, чтобы не допустить каскадирующего эффекта, распространения автоматизированных роботов, которые могут быть использованы в военных целях. Поверьте мне, в ближайшие годы будет очень много ситуаций, когда политическое руководство потеряет контроль над сценарием.

В Лос-Анджелесе на прошлой неделе, в Сан-Франциско, в Нью-Йорке на несколько часов целые районы были лишены электричества, вроде это было в результате пожаров, но тут очень много странных совпадений. Ладно, в Сан-Франциско это произошло от пожара, который вызвал отключение электричества, утром он начался, но, представьте себе, это неслучайно, не совпадение. Что произошло в Сан-Франциско? Финансовый район полностью пострадал и был лишен электричества. Интересно, что пострадал тот квартал, где живет

Марк Цукерберг, учредитель «Фейсбука». Именно тот район, где он живет, был отрезан от электричества на несколько часов.

Анатолий Стрельцов: *У меня такое ощущение, что классическое право, которое существует уже 2 тыс. лет, а может и больше, применительно к тем условиям, которые мы обсуждаем, становится все менее и менее эффективным в том виде, в каком мы привыкли его использовать. Для того чтобы обеспечить или повысить эффективность использования этого права в новых условиях, необходимо подумать о том, как обустроить IIKT-мир, чтобы в нем можно было успешно применять правила и нормы, потому что они в нынешних условиях в данной сфере становятся все большей и большей фикцией. Мы можем выпускать сколько угодно прокламаций о том, что надо «запретить это, давайте контролировать это, давайте делать то», но если у нас нет инструментов решения данных задач, если у нас нет инструментов, которые позволили бы нам проконтролировать выполнение нормы и найти того, кто занимается противоправной деятельностью, тогда право становится бессмысленным.*

II меня даже больше волнует не просто сам искусственный интеллект, а следующий этап, связанный с нанотехнологиями. Он будет значительно более серьезным по последствиям, потому что, если мы сейчас не видим, но догадываемся, то там мы можем и не видеть, и не догадываться, что именно происходит и в какую сторону мы идем. Просто надо подумать на эту тему.

Мы действительно находимся перед кризисом современного права, и в том числе международного права. Но если внутри себя каждое государство старается за счет разных технологий, за счет использования или усиления возможностей спецструктур, правоохранительных органов как-то эту ситуацию сгладить, то во внешнем мире, где у нас нет верховного судьи, где у нас нет каких-то общих силовых структур, системы объективного наблюдения, мы становимся перед совершенно новой ситуацией. II, наверное, это одна из тех проблем, которые тоже требуют и обсуждения, и внимательного изучения, особенно на уровне международного права.

Наталья Ромашкина: *Говоря об искусственном интеллекте и автономных вооружениях, если это делать ответственно, мы должны доказать поведенческие характеристики этой технологии в отношении конкретных целей, конкретных сред. Мы должны знать, что будет делать система. Насколько нам известно, по искусственному интеллекту система работает в микросреде, но в открытой среде мы не знаем, как она будет себя вести.*

Если мы вводим различные виды логики в системах машинного обучения, то невозможно доказать наличие плана для решения конкретной проблемы. То есть по аналогии с тем, что мы сделали в области военных, прецизионных вооружений, есть нормы, определяющие те или иные действия. Возникает проблема других субъектов, которые не обладают такими аналитическими и криптографическими средствами, возникает проблема обеспечить исполнение тех или иных норм.

Анатолий Стрельцов: *Уважаемые коллеги, предложу вам возможные варианты выводов из нашей работы.*

Во-первых, совершенно очевидно, что работу надо продолжать. В этом нет сомнений.

Во-вторых, в основу работы следует заложить в том числе и обсуждение глоссария или терминов - здесь тоже договорились. У нас есть определенный задел, который был создан ИИнститутом Восток-Запад совместно с МГУ. Давайте его дополним, посмотрим, насколько он соответствует сегодняшнему дню, тем задачам, которые перед нами стоят. Будем ее поддерживать в актуальном состоянии, для того чтобы потом политики смогли ею воспользоваться.

Следующий вопрос. Можно не ждать, чем закончится встреча группы правительственных экспертов 2017 года. Мир настолько динамичен, что тот пик доверия, который был в 2015 году, трудно поддерживать на этом же уровне в течение следующих трех-четырех лет.

Если удастся сделать решение резолюцией Генеральной Ассамблеи ООН - прекрасно. Если удастся вынести это на Совет Безопасности и принять его решение по этим правилам - прекрасно. Но прежде чем такое решение Совет может принять, неплохо было бы, чтобы члены СБ понимали, чем чревато принятие данного решения. Потому что если Генассамблея может, так сказать, в абстрактном плане сказать:

«Да-да-да, очень хорошо», то члены СБ должны понять, сколько это будет стоить и кто это будет реализовывать.

Должны быть проработаны хотя бы некоторые организационные, технологические вопросы и некоторые стандарты. Давайте сделаем эту работу, может частично, в зависимости от того, какие будут средства и кто будет ее заказчиком. Если будет, например, встреча высоких представителей США, России, Франции, Китая, то почему бы на этих встречах не проработать данные вопросы и не принять соответствующие решения о том, что этим надо заниматься?

Когда будет поставлена задача, тогда в каждом государстве органы власти, имеющие свой бюджет, специалистов, могут эту работу поручить сделать и задействовать ее результаты.

Мы как эксперты можем записать себе, что считаем это важным. А дальше каждый из нас донесет до наших руководителей решения, может, и средства массовой информации нам в какой-то мере помогут. И тогда уже мы в следующем году будем исходить из того, что основной задачей на перспективу будет разработка методического руководства. Его можно делать по частям, там, по-моему, 15 правил. Давайте выберем три-четыре правила, которые являются ключевыми.

Таковым элементом являются ИКТ-инциденты, как их определять, что с ними делать вообще, и как мы должны координировать свою деятельность в процессе обсуждения ситуации, возникшей в связи с каким-то инцидентом.

Не менее важный вопрос: за что отвечает государство, где границы, пространственные границы суверенитета государств, в пределах которых они несут ответственность за безопасное использование ИКТ?

И третий вопрос: что такое безопасное использование ИКТ, за что они отвечают? Безопасное использование ИКТ - это такая абстракция. Это как строительство коммунизма в отдельно взятой стране. Да, вот, красиво, хорошо, здорово, но непонятно.

Если мы хотя бы эти три вопроса начнем обсуждать и по ним двигаться вперед, то дальше мы выйдем все равно на все остальные вопросы.

Гармиш-Партенкирхен, Германия

Семинар - «круглый стол» №3

Проблемы обеспечения информационной безопасности критически важных объектов промышленности

Чарльз Барри, Институт национальной стратегии Университета национальной обороны США: Сектор коммерческих предприятий можно разделить на небольшие элементы: СМИ, медиа, кинопроизводство и другие. Несколько лет назад была атака на «Sony». Атакуют места общественных сборов, скоплений. Помним теракты в Беслане, на Дубровке («Норд-Ост»). Такие объекты не всегда оснащены системами АСУ, но тем не менее они тоже относятся к критически важной инфраструктуре.

Мы разработали значительную нормативную базу для регулирования этого сектора. Важно отметить, что́ мы в США рассматриваем прежде всего как экономическую проблему. Нормативы систем промышленного управления в основном составляются Министерством торговли. Действительно, все больше и больше атак совершается на системы диспетчерского управления и контроля, на распределенные системы управления производством. Мы знаем о таких атаках, как Stuxnet, это нападение на подобные промышленные системы.

Но есть и другие угрозы. Угрозы физического характера. Это очень важно, и это становится фактором риска для систем производственного управления и контроля. Особенно в местах с тяжелыми погодными условиями, как, например, Заполярье.

Такие системы являются встроенными, обладают различными компонентами, их очень трудно вывести из состояния рабочей готовности.

В США мы построили подобную модель. При анализе рисков мы разработали методы устранения проблем и угроз. В результате возникла система предупреждения о нападении или, например, природном бедствии. В этом случае у нас уже есть заранее разработанный план ликвидации последствий или снижения остроты последствий, реагирования и восстановления работоспособности той или иной системы.

Еще один элемент нашей программы: государственные и частные партнерства. В числе крупных компаний они являются владельцами систем, однако обычно государство несет ответственность за обнаружение угроз и реагирование на различные опасности. В рамках американского «плана защиты национальной инфраструктуры» 2013 года значительное внимание уделяется государственно-частным партнерствам, чтобы операторы и владельцы были вовлечены в этот процесс обмена информацией. Представители финансового, частного и государственного сектора взаимодействуют на этой основе. Чтобы они понимали, разбирались в вопросах коммерчески чувствительной информации, например ценообразований на фондовом рынке и т. д. Эта работа не закончена, мы пока не достигли желаемых целей, но пытаемся действовать максимально инклюзивно.

Понимаю, что частный сектор является не только собственником, но и обладает всеми необходимыми экспертными знаниями. 16 секторов - это так называемые центры анализа и обмена информацией, созданные для каждой отрасли, каждого сектора. Это, скажем так, верхний уровень государственно-частного партнерства.

Возьмем финансовый сектор в качестве примера. Он сыграл важнейшую роль в обмене информацией по борьбе с некоторыми нападениями с целью выкупа. В нефтегазовом секторе была проведена оценка нападения на украинскую электросеть в 2015 году. Доклад имеется в открытых источниках в Интернете, очень хороший документ. Это, как я уже сказал, высший уровень частно-государственного партнерства и обмена информацией между этими отраслями. Работа пока не закончена.

Министерство торговли создало соответствующий нормативный документ. Он обновляется чаще других в силу меняющегося характера систем, а также сбора новой информации о возможностях защиты сектора. Создана специальная группа реагирования (CIRT) для систем автоматического управления производством.

Для тех, кто эксплуатирует эти системы, предусмотрена соответствующая программа подготовки персонала. Если есть технические данные, они хранятся отдельно от данных коммерческой бизнес-информации, чтобы подобные данные не были одинаково доступны в случае попыток манипуляция какими-то системами управления производством.

ВПН, двухфакторная идентификация - это все средства защиты систем, которые мы пытаемся встраивать не только у нас в стране.

Уязвимости и новые угрозы для критически важной инфраструктуры

Андрей Ярных, «Лаборатория Касперского» (Россия): Расскажу про защиту критически важной инфраструктуры на примере тех проблем, тех видений специфики, с которыми мы столкнулись при разработке продукта «Касперский индастриал кибер секьюрити».

О промышленной специфике. Первое, с чем мы столкнулись: промышленность и критически важная инфраструктура - это далеко не то же самое, что обычная, корпоративная сеть, относящаяся к бизнес-структурам. Здесь значительно перераспределение тех ценностей и тех приоритетов, которые мы видели раньше в корпоративной сети в виде конфиденциальности, целостности и доступности. Они выстраивали угрозы именно в таком порядке, применительно к индустриальным продуктам.

Доступность, целостность вышли на первые места, и только третьим пунктом явилась конфиденциальность. Компаниям, даже большим, индустриальным, энергетическим, необходимо меняться, интегрировать новые технологии. В противном случае они либо теряют долю в капитале, либо приобретаются другими более успешными компаниями, либо просто разоряются. Это тоже в определенной степени последствие того, что компания не успевает модернизироваться и внедрять новые технологии.

При этом новые технологии достаточно динамичны. Очень много подключений к сети Интернет, интернету вещей, который более привычно звучит в контексте частного сектора, частного пользователя. Схема проникновения вещей в домашний быт работает и на уровне промышленных предприятий, конечных устройств, на уровне включения в схемы автоматизации. Сегодня это уже достаточно актуальный тренд, который в дальнейшем будет увеличиваться.

О рисках. В ранжире рисков 2013 года киберугрозы занимали 13-е место, в 2015-м они уже на пятом месте. С развитием технологий, с большим включением IT-устройств в промышленное производство поднимается значимость этого аспекта как киберугрозы и выводится практически на передовые позиции. По результатам 2017 года, возможно, этот риск будет оцениваться еще выше, на уровне четвертого места, возможно, даже третьего.

Что касается кибератак на АСУ ТП. Все происходит очень быстро. Я показывал, как проводилась учебная атака на линию электропередач и рассказывал, что неподготовленным хакерам - для того чтобы изучить и провести успешную атаку - потребовалось порядка четырех-пяти часов знакомства с инфраструктурой. После чего они смогли обнаружить уязвимость и осуществить успешную атаку. Речь идет буквально о часах, а не днях, которые необходимы вирусописателям для того, чтобы провести все пять необходимых шагов, чтобы осуществить успешную атаку на критически важную инфраструктуру, внести необходимые изменения, получить, соответственно, результат и зачастую даже скрыть следы своего проникновения.

Потому что иногда целевые атаки осуществляются до определенного результата, после чего следы заметаются и очень сложно что-либо обнаружить, и только по произведенному эффекту можно сказать, что это было вмешательство на уровне программного кода.

Суммируя то, что прозвучало, около 14 часов - это среднее время развития атаки в промышленных сетях, вот эти все пять стадий вирусописатели умудряются пройти за довольно короткий период.

В чем сложность защиты? Есть совокупность факторов, которые затрудняют защиту структуры промышленных предприятий. Зачастую приходится иметь дело с устаревшими системами, которые при написании не учитывали необходимость защиты, ну и в дальнейшем уже не поддерживаются обновлениями. Фактически те уязвимости, которые находятся в них, не закрываются производителями, операционными системами. В таких критических объектах не проводятся обновления операционных систем.

Одной из самых существенных угроз, сложностей является персонал, который зачастую не понимает все риски и угрозы, с которыми сегодня приходится сталкиваться. Уязвимости градируются от беспечности до целенаправленного злого умысла - оставления лазеек для атаки хакеров.

Вот кратко указаны причины инцидентов. Они касаются вредоносного программного обеспечения в 35%. В значительной степени, как уже говорил, они касаются ошибки в базовом ПО, это в том числе отсутствие обновлений, ну и человеческий фактор, ошибки операторов и другое. Никакой код не совершенен, все равно находятся в нем уязвимости, которые необходимо выявлять.

Что касается людей. Традиционной уязвимостью является нарушение регламента. То есть существуют процедуры безопасности, которые необходимо соблюдать, тем не менее халатность и небрежность ведут к тому, что вирусописатели и хакеры получают шанс для атаки. Большой ущерб могут нанести действующие сотрудники, но еще больший ущерб могут нанести бывшие сотрудники, особенно недовольные, ушедшие со скандалом или по какой-то причине, например потере доверия. Они могут проявлять большую активность и предоставлять для вирусописателей и хакеров возможности атаки на инфраструктуру, причем делают это умышленно, целенаправленно и тем самым становятся более опасными источниками проникновения.

Ну и, естественно, внешние подрядчики и зарубежные исполнители. Тут тоже есть угрозы для периметра безопасности

просто в силу того, что, если подрядчики часто меняются, бывает, что новый подрядчик не всегда учитывает регламент работы и, соответственно, у хакеров появляются шансы пробить периметр защиты.

Еще раз приводя общие риски и киберугрозы, можно сказать, что это начинается от действий сотрудников и заканчивается кибероружием, нечестной конкурентной борьбой, киберхулиганством.

В принципе, целевые атаки - они в значительной степени потому и целевые, что создаются специально под определенное предприятия, иногда даже определенный сервер на предприятии. И отразить такие атаки крайне сложно, если нет специальных инструментов защиты.

Например, с точки зрения вирусописателя, было вмешательство в программный код и, соответственно, в бензовоз наливалось большее количество бензина, то есть была взломана система автоматизации и, соответственно, неучтенное топливо заправлялось в бензовоз с небольшой поправкой. И на эти 2%, которые там были указаны, злоумышленники и жили, имели свой дополнительный доход от взлома системы учета АСУ ТП в данном случае нефтеналивной компании.

Хочу остановиться на двух таких больших аспектах. Во-первых, кибербезопасность - это постоянный процесс. И действительно, казалось бы, проведя полный комплекс, завершив этот круг, получили определенный результат, но появляются новые угрозы, новые возможности у вирусописателей и хакеров, появляются уязвимости. Это требует постоянной оценки рисков, проектирования, защиты, внедрения, поддержки и - опять по кругу. Поэтому мы скорее оцениваем кибербезопасность как некий цикличный процесс постоянных ответов на вновь возникающие угрозы.

Второй пункт, который мог бы привлечь особое внимание. Вы видели, что персонал является повышенной уязвимостью. Не дать ответ на эту угрозу мы, конечно, тоже не могли и создали определенные бизнес-игры, в которых моделируются ситуации атаки на промышленные предприятия. Мы показываем

персоналу уязвимости, которые могут быть, и в рамках деловой игры, в рамках такого тренинга, стараемся обучить персонал для того, чтобы, по крайней мере, небрежность, халатность и пренебрежение регламентами не являлись уязвимостями. Поэтому большое значение мы уделяем именно обучению людей.

Обзор юрисдикций государств в киберпространстве: вызовы для IT-бизнеса

Томас Ламанаускас, Вымпелком Европа: У меня более широкая тема, которая касается не только защиты критической инфраструктуры, она касается общих проблем, с которыми сталкиваются цифровые, компьютерные, телекоммуникационные компании в такой сложной ИКТ-среде.

Во-первых, бизнес-императивы. Почему мы, технологические или цифровые компании, должны участвовать в дискуссии по этим темам, которые традиционно не были в сфере внимания телекоммуникаций? Потому что бизнес-модель телекома сейчас под ударом и необходимо меняться. Несколько фактов, подтверждающих следующее: хотя объемы данных растут, выручка не поспевает и это оказывает воздействие на общую рентабельность, прибыльность этих компаний вызывает необходимость менять бизнес-модель.

С другой стороны, глядя на инвесторов, деятельность которых проявляется в заголовках и финансовых результатах, мы видим, что деньги больше не поступают в инфраструктуру, а поступают цифровым игрокам. За последние несколько лет мы видим изменения в капитализации, цифровые игроки растут, а традиционные компании телекома стагнируют или даже снижают свою капитализацию. Поэтому мы и решили заняться этим. Мы больше не называем себя «телекоммуникационная компания», да, мы по-прежнему обладаем 13 операторами телекома различных рынков, включая Россию, Евразию, Восточную Европу, Центральную Азию, у нас восемь из 13 находятся на этих рынках, у нас несколько миллионов подписчиков. Одновременно мы также становимся провайдером других цифровых услуг

на основе платформы мессенджера «Veon». Это наше будущее, и данная платформа мессенджеров интегрирует также финансовые и другие цифровые услуги, которые предоставляются с использованием нашей платформы.

Не буду ее подробно представлять, хочу лишь дать вам общее впечатление о том, как эти изменения в отрасли затрагивают не только вас, но и других операторов телекома. Сейчас уже невозможно четко разделять эти две отрасли или два направления, они очень тесно взаимосвязаны, я буду говорить не только о прямых киберугрозах.

Усложняющаяся геополитическая ситуация неизбежно воздействует на телеком-бизнес. Повышается чувствительный характер общей среды телекома. Инциденты возникают в этих сферах, проходят расследования, они все связаны с определенными цифровыми элементами. «Apple», «Sanbernardina» после лондонских терактов обсуждают вопрос шифровки мессенджеров, любая национальная безопасность все больше и больше связана с тем, как мы представляем себе регулирование телекоммуникационных бизнесов и цифровых компаний.

Конечно, усложняется характер угроз в киберсреде. Видно, что тенденция продолжается, она растет, доклад сыска в 2013 году зарегистрировал некое замедление, но это скорее исключение из правил, сейчас опять наблюдается рост опасности и угроз. Ну и не в последнюю очередь люди обеспокоены частной сферой. Все больше обсуждается вопрос защиты личных данных. Это воздействует на политику, это также отражается в фактическом бизнесе, в коммерческой деятельности. Компания не только теряет деньги в результате таких угроз и инцидентов, но и теряет пользователей и абонентов, и это очень важно. Для нас это очень существенный аспект подобной деятельности.

Мы, как компания, должны найти равновесие, баланс интересов и возможностей и в то же время развивать новые бизнес-модели, которые должны отражать наиболее успешные модели существования и работы бизнеса в мире, приспосабливаться, корректировать нашу деятельность.

Кроме того, политическая сторона пока не решена, не отрегулирована, она поспевает за кибераспектами, об этом говорили и другие ораторы. Возникают конкретные вопросы, связанные с трансграничным характером операций и деятельностью таких глобальных компаний, как наша. Политики не всегда понимают, как решать вопросы передачи данных, трансграничного сотрудничества, обмена данными и т. д.

Также наблюдается дефицит определенной нормативной базы. Не во всех странах есть законы о защите данных. Опять же это плохо для бизнеса. Нам нужна четкая нормативная база. Отсутствие регулирования не всегда хорошо для бизнеса, потому что приходится искать неопределенные решения, не знаешь, как будет этот вопрос регулироваться в будущем.

Некоторые страны резко переходят от отсутствия регулирования к очень строгому регулированию, так как возникает риск, возникает нажим с точки зрения национальной безопасности. Таким образом, политическая среда начинает усложнять нашу деятельность, поскольку нет глобальных, общемировых ответов, каждый регион ищет свой собственный ответ.

Одна тенденция распространения юрисдикции: страны говорят, что не важно, где это происходит, это в моей юрисдикции. Пример - США. Они пытаются получить доступ к информации «Майкрософта» в Ирландии, идут обращения в бельгийские суды, суды других государств Европы. Если вы - европейская компания, работающая в Европе, то это применимо к вам, где бы вы ни работали, если вы обрабатываете данные европейских граждан, где бы вы ни находились, это тоже к вам применимо. То есть очень широкая юрисдикция.

Что это означает? Если одна страна выходит за пределы своей юрисдикции - это один момент, но если все будут так делать, это означает, что раньше, в качестве глобальной компании, надо было соблюдать много правил, но правил конкретных стран, в которых вы работали. Сейчас, как только мы выходим за пределы нашей юрисдикции, даже работая в конкретной стране, иногда вы попадаете под действие законов различных стран, иногда противоречащих друг другу, потому что все эти страны пытаются распространять свою

юрисдикцию на другие регионы. Одно из решений находится в области двусторонних соглашений, они немного помогают.

Еще один негативный подход - некоторые политики говорят, что нет глобальных правил, мы не доверяем друг другу в этих сложных условиях, давайте, мол, закрываться, изолироваться, отгораживаться. Очень трудно работать в условиях, при которых страны изолируются друг от друга.

О локализация данных. Политики говорят: мы не хотим, чтобы данные выходили за пределы, мы хотим хранить данные в стране, закрываться и т. д. Что это означает? Возникают барьеры для торговли в общем и для данных в частности, вы видите статистические данные, конкретно свидетельствующие о препятствиях для ведения бизнеса не только для нас, но и для других компаний. Это ограничивает рост ВВП и ведет к повышению издержек для телекоммуникационных компаний.

Ну и не в последнюю очередь соотношение интересов безопасности и защиты частной сферы. Силовые структуры высказывают законные опасения на предмет угроз, требуют сотрудничества и взаимодействия со стороны бизнеса, но бизнес также заинтересован в обеспечении частной сферы. Как сбалансировать эти противоречивые интересы, особенно в условиях противоречивых законодательных данных? США требуют данные, а законы Европейского союза требуют защиту частных данных Европейского союза.

Как уровнять или согласовать эти противоречивые требования? Мы пытаемся найти свое собственное место в таких сложных условиях, мы, как компания, понимаем вызовы, хотим активно на них реагировать. Мы - глобальная компания, хотим работать глобально, и это помогает развивать инновации и обеспечивает наилучший уровень услуг. Мы выросли из национальной телекоммуникационной компании, поэтому должны, конечно, соблюдать прежде всего местные требования и нормативы. Мы хотим идти на шаг впереди, демонстрируя наши возможности и способности соблюдать требования госорганов и наших пользователей.

Например, мы реализовали программу защиты данных на всех 13 рынках, где бы ни находились эти рынки, мы стараемся

соблюдать самые высокие и жесткие требования защиты данных, где бы ни находились конкретные представительства нашей компании с учетом этих высоких требований.

Если возникнет инцидент, штраф - не самое страшное, самое страшное - это потеря клиентов, абонентов. Доверие наших клиентов - это важнейший фактор, стимул соблюдения нормативных положений.

Разработаны соответствующие программы и стратегии, распространяющиеся на всю нашу зону охвата деятельности.

Чтобы найти бизнес-модель, которая позволила бы бизнесу выжить в новых условиях и соответствовать государственным требованиям, нам нужен глобальный подход. У нас обсуждался национальный Интернет, локализация данных, распространение юрисдикции на другие регионы. Надо обсуждать, как государство и бизнес могут договориться и разработать общее правило ведения бизнеса.

Иногда мы говорим, что у нас выбор, в какую тюрьму идти, то есть правила какой страны мы можем выбирать. Такая ситуация никого не устраивает. Соблюдаешь правила одной страны - другая страна недовольна. Должны быть какие-то базовые стандарты и нормативы с точки зрения национальной безопасности и частной сферы.

Для эффективной работы нам необходимо найти также технологические решения, устраивающие разные страны. Мы постоянно встречаемся с представителями государственных органов и пытаемся выяснить их требования, с тем чтобы разрабатывать наши технические решения с их учетом. Практически невозможно разрабатывать индивидуальные технические решения для каждой страны.

Иногда, для того чтобы соответствовать, приходится идти на какие-то жертвы, скажем коллегами, которые работают в других странах и не соблюдают юридические нормы. Это не очень хороший подход, с нашей точки зрения. Мы хотим соблюдать эти требования, но они должны быть одинаковыми для всех, как и правила игры, равные условия должны быть применимы ко всем игрокам на этом поле.

Обеспечение информационной безопасности объектов промышленности - необходимое условие развития человечества

Александр Баранов, Национальный исследовательский университет «Высшая школа экономики» (Россия): Наши страны практически не имеют особого представления, как бороться с киберугрозами, чтобы использовать потенциал других государств, а также налаживать взаимодействие, по крайней мере в юридической сфере.

А одна из проблем, которая сейчас становится все более реальной, - это как раз информационная безопасность объектов промышленности. Все следующие этапы развития человечества связаны с развитием промышленности именно в этом направлении: информатизация, роботизация и т. д.

Для того чтобы налаживать хоть какое-то взаимодействие, сначала надо договориться о терминах, и эта попытка, надо сказать, уже давно не удается нашим государствам ни вместе, ни по отдельности. Сейчас мы обсуждаем в нашей стране проект закона о безопасности критической информационной инфраструктуры объектов промышленности, и уже появляется много вопросов относительно того, насколько этот проект удачный.

По крайней мере, как показали обсуждения с инициаторами этого проекта, вариант вроде как образовывается. Так вот, по проекту этого закона, объекты критической информационной инфраструктуры промышленности - это автоматизированные системы управления технологическими процессами, функционирующими в основных сферах промышленности, и их информационно-технологические системы. Если вдуматься в это определение, то получается, что практически все обрамление технологического процесса подпадает под этот закон.

А что же такое обеспечение безопасности? Ведь понятие безопасности в каждой стране понимается по-своему, и выводы из этого делаются совершенно различные - от совершенно радикальных, в виде применения военной силы, до безразличных, как это было с Нидерландами, которые этого и не заметили.

Поэтому предлагается следующее определение: «Обеспечение безопасности (я немножко сократил законодательное определение специально для того, чтобы оставить суть) критической информационной инфраструктуры Российской Федерации - это комплекс мер, обеспечивающих устойчивое функционирование в условиях компьютерных атак».

Как только появилось выражение «компьютерная атака», сразу же возникает вопрос: а что это такое? Ну одна из разновидностей этого известна как «вирусы», но в целом, оказывается, тоже есть определение. Компьютерная атака - это целенаправленное воздействие программно-техническими средствами на компьютерные системы, участвующие в технологическом процессе, в целях нарушения их функционирования или безопасности обрабатываемой ими информации.

Как видите, здесь есть два аспекта. Первый - нарушение функционирования самого технологического процесса, а второй аспект - разрушение информации, которая связана с этим процессом.

В заключение возникает совершенно очевидное. Что же такое информационная безопасность? В нашем традиционном представлении это можно найти в любых учебниках, мы этому учим наших студентов, наших магистров, бакалавров - это конфиденциальность, целостность и доступность. Буду придерживаться именно такого понятия, не вдаваясь дальше в то, как эти понятия трактуются в разных странах.

Откуда же возникают компьютерные атаки? По традиции в информационной безопасности есть два вида нарушителей - внешний и внутренний. В первую очередь они направляются на управление бизнес-процессами и техническими средствами, а во вторую - на управление материально-техническим обеспечением. И в меньшей степени, конечно, в технологическую информационную систему, потому что, как правило, все уже научились, и эту часть стараются изолировать. Хотя встречаются случаи, когда некоторые продвинутые, так сказать, компьютерщики, умудряются устроить такое управление технологическим процессом из Интернета напрямую, полагаясь на разного рода демилитаризованные зоны.

Интернациональный характер угроз - возможное последствие планетарного масштаба. Именно по направлению конфиденциальности, целостности и доступности. Нарушение конфиденциальности - это нарушение режима коммерческой тайны или раскрытие технологий контролируемого распространения. Утечка информации о производстве, например, о тонкостях производства химического оружия или тонкостях производства ядерного оружия, конечно, будет являться большой потерей и, без сомнения, может привести к очень тяжелым последствиям.

Нарушение целостности. Это искажение технологического процесса и, как следствие, угроза катастрофических последствий. Так вот, на нарушение целостности процесса как раз и были направлены основные усилия последних атак.

Нарушение доступности - это потеря управления технологическим процессом, что, конечно, приведет к угрозе катастроф.

Как опять же показал опыт последних лет, причем достаточно наглядно и всем, есть еще и внутренний нарушитель, который находится на объекте промышленности, а не только внешний, который вне контролируемой зоны.

Один из самых мощных методов - это изоляция, то есть действенный метод защиты от внешнего нарушителя, совершенно замечательный метод, который, к сожалению, в настоящее время нереален, потому что полная физическая изоляция крупного объекта от общемировой сети практически невозможна. Управление бизнес-процессами, как и управление складскими и прочими возможностями, требует обязательного сопряжения с внешними системами и синхронизации с ними. Вот поэтому взаимодействие с внешней средой необходимо для функционирования этих разделов, и международные контакты тех же самых сфер также требуют своей реализации в силу международного характера производства и международного характера сбыта произведенной продукции.

Защита такого взаимодействия требует применения национальных норм и методов, которые должны сочетаться с международными техническими протоколами и правилами. И вот тут-то начинается большая проблема.

Знаю только одну систему, в рамках которой очень хорошо удалось договориться относительно применения типов шифрования для взаимодействия государств, это область обмена данными в налоговой сфере, в которой предусмотрена такая замечательная программа, как PGP, где возможна реализация различных национальных шифров.

Если с внешним нарушителем с помощью виртуальной изоляции, виртуализации, еще как-то можно бороться, то внутренний нарушитель - это, конечно, самая большая головная боль, которая сейчас наблюдается практически у всех руководителей. Не минула эта напасть и нашу страну. Видимо, в этом и есть особенность человеческой психики. По крайней мере, анализ такого сорта действий внутреннего нарушителя показывает, что за этим стоит, как правило, некий человеческий фактор. Естественно, сразу же возникает вопрос о квалификации нарушителя и об объекте устремления. Как правило, с одной стороны, высокая профессиональная подготовка в области IT характеризует подобного внутреннего нарушителя, а с другой стороны - все, до чего он может дотянуться, оказывается практически в сфере его вредоносного воздействия. Самое неприятное - это возможность отложенного воздействия и управление ситуацией с высокой скрытностью незаконных действий.

Известный мне случай в системе одного из крупнейших банков показал, что воздействие началось через полгода после того, как внутренний нарушитель уволился. Он сделал это просто из мести. При этом удалось зафиксировать, выяснить, кто он и как это сделал, но наказать его не получилось. Потому что законодательной базы оказалось недостаточно, факты, которые получили, были зафиксированы юридически неправильно. Кстати, юридически правильно зафиксировать их практически невозможно, поэтому все эти действия остались ненаказанными.

Как известно, обычно в системах защиты применяются либо апостериорные методы, либо априорные. Апостериорные методы применяются там, где мы не можем полностью положиться на априорные. К сожалению, методы защиты информации отстают от методов развития информатизации.

Поэтому апостериорные методы и системы набирают все большую силу.

Но главное все-таки в них - неотвратимость наказания. Это основной сдерживающий фактор. А вот с ним у нас как раз достаточно сложно.

Теперь мы переходим к международному промышленному терроризму, которому, как очевидно, необходимо противопоставить международную солидарность и взаимодействие. Причем говорю это вполне серьезно, потому что, если мы не выработаем принципов международной солидарности, наша задача по обеспечению стабильности работы технологических систем выполнена не будет.

Можно рассмотреть следующий набор мер. Первое - выработка соглашений по выявлению и наказанию национальными юрисдикциями разработчиков средств компьютерных атак, независимо от географического расположения автора вируса.

Второе - создание международной полицейской системы контроля за управлением и появлением средств компьютерных атак. Ведь есть же Интерпол. Эта полицейская система чрезвычайно эффективна, является большим сдерживающим фактором для преступников, которые, совершив преступление в одной стране, пытаются улизнуть в другую. Почему не попытаться создать некую полицейскую систему контроля и пресечения деятельности тех, кто производит компьютерные атаки.

Третье - организация взаимодействия правоохранительных органов различных государств по координации действий национальных систем противодействия компьютерным атакам. Пожалуй, вот только в этом направлении сейчас можно отметить реальные шаги. Тем не менее без координации в создании системы взаимодействия дело будет двигаться по-прежнему так же плохо, как происходит сейчас.

Четвертое - корректировка и сближение национальных законодательств в области пресечения компьютерных преступлений. За одно преступление в разных странах могут быть совершенно различные виды наказаний. Но когда в одной стране не предусмотрено наказание за распространение вируса, а в

другой предусмотрено, то понятно, что вирусописатель будет стремиться в ту страну, где нет наказания.

В заключение, мне кажется, организация центра по выработке и тестированию международно признанных программно-технических решений защиты критических информационных технологий от компьютерных атак была бы весьма полезной для всех. К сожалению, сейчас складывается такая ситуация, что, несмотря на то что коммерческие средства защиты доступны всем, их тестирование и апробация представляют из себя большую проблему.

Это связано с задействованием огромных ресурсов и необходимостью построения специальных тестовых стендов и тестовых центров. Даже в одиночку отдельным небольшим странам это сложно сделать, да и для больших стран это, кстати, достаточно существенные затраты. Если у нас имеется большое сообщество, которое готово использовать эти возможности, то тестирование подобных средств защиты от компьютерных атак было бы весьма полезно.

Могу привести яркий пример. Так, в области криптографии разработан некий практически международный стандарт, который используется многими странами. Он протестирован, и практика в этой области тоже уже появилась. Почему бы не провести некий аналогичный тендер, конкурс или обсуждение эффективности тех же самых электронных замков или решить проблему визуализации электронной подписи.

Она известна во всех странах, и ни одна страна так до сих пор ее не решила. То, что мы подписываем электронной подписью, на самом деле мы не знаем, что́ мы подписываем, а мы подписываем некий зрительный образ, который вдруг нам показался в той или иной операционной системе. А вы знаете, чем отличаются образы зрительные, подготовленные в «Майкрософте», от тех, что вы смотрите в «Эппле»? Но тем не менее подписываемся, и все мучаются с этой проблемой. Почему, спрашивается, не создать некое одинаковое средство, которое бы потом получило общее распространение? Мне кажется, что реализация подобных мер сказалась бы благотворно, способствовала затем выработке и межгосударственных соглашений.

INTERNATIONAL AFFAIRS

A Monthly Journal of Foreign Policy, Diplomacy and National Security

К СВЕДЕНИЮ АВТОРОВ

С 2009 года журнал перешел на систему рецензирования. Статьи на рецензию представляются в электронном виде. Электронные версии статей следует направлять по электронной почте по адресу редакции: articles@interaffairs.ru с указанием фамилии, имени, отчества (полностью), должности, места работы, ученой степени и звания. Объем присылаемых в редакцию статей - не более 0,6 а.л. Редакция просит авторов прилагать к тексту статей краткую (8-10 строк) аннотацию на русском и английском языках, ключевые слова (не более 10), контактную информацию для переписки (адрес электронной почты). Примечания помещаются в постраничных сносках, источники помещаются в конце текста. Плата с аспирантов за публикацию рукописей не взимается.

РЕДАКЦИЯ РАССМАТРИВАЕТ ФАКТ НАПРАВЛЕНИЯ АВТОРСКИХ РУКОПИСЕЙ ПО АДРЕСУ: articles@interaffairs.ru КАК ПЕРЕДАЧУ ЕЙ АВТОРАМИ ПРАВ НА ИХ ПУБЛИКАЦИЮ.

Правила оформления сносок и библиографии в конце статьи:

[1]Бердяев Н.А. Смысл истории. М.: Мысль, 1990. 175 с.

[2]Putham H. Mind, language and reality. Cambridge: Cambridge univ. press, 1979. P. 12.

[3]Инвестиции останутся сырьевыми//PROGNOSIS.RU: ежедн. интернет-изд. 2006. 25 янв. URL: http://www.prognosis.ru/print.html. id=6464 (дата обращения: 19.03.2007).

[4]Ефимова Т.Н., Кусакин А.В. Охрана и рациональное использование болот в Республике Марий Эл // Проблемы региональной экологии. 2007. №1. С. 80-86.

WWW.INTERAFFAIRS.RU