РОССИЯ И ГЛОБАЛЬНЫЕ ВЫЗОВЫ
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕЖДУНАРОДНАЯ ЖИЗНЬ

XII Международный форум

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

Москва. Издается с марта 1922 г.

РОССИЯ И ГЛОБАЛЬНЫЕ ВЫЗОВЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

XII Международный форум

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

Гармиш-Партенкирхен, Германия
16–19 апреля 2018 года

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

Ответственный редактор:
Заместитель главного редактора -
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:
М.С.Тюрина

Материалы, публикуемые в специальном выпуске журнала «Международная жизнь»
«Россия и глобальные вызовы в области информационной безопасности»,
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 «Диамант-принт»
РФ, 394036, Воронежская область, г. Воронеж, ул. Трудовая, д. 50, кв. 10
89586495331@mail.ru тел. 89586495331

Тираж 1000. Цена свободная.
Дата выхода в свет 28.12.2018.
Компьютерный набор, верстка и дизайн редакции.

МЕЖДУНАРОДНАЯ ЖИЗНЬ

СОДЕРЖАНИЕ

XII Международный форум

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

Пленарное заседание

Семинар - «круглый стол» №1

«Актуальные проблемы информационной безопасности в контексте развития цифровой экономики»

Семинар - «круглый стол» №2

«Механизмы реализации государственно-частного партнерства в области обеспечения безопасности критической информационной инфраструктуры»

Шестнадцатая научная конференция Международного исследовательского консорциума информационной безопасности (МИКИБ)

Семинар - «круглый стол» №5

«Проблемы обеспечения «цифрового суверенитета» государств»

XII Международный форум

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

Гармиш-Партенкирхен, Германия

16-19 апреля 2018 года

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

Пленарное заседание

Шерстюк В.П., сопредседатель Оргкомитета форума, советник секретаря Совета безопасности Российской Федерации, директор Института проблем информационной безопасности МГУ им. М.В.Ломоносова: Уважаемые коллеги, уважаемые дамы и господа, позвольте мне открыть заседание очередной, XII сессии Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Еще раз хотелось бы высказать слова искренней признательности руководству Администрации города Гармиш-Партенкирхен, другим представителям Федеративной Республики Германия, которые уже 12 лет радушно принимают нас и создают благоприятную обстановку для работы.

За это время форум превратился в уникальную международную внеблоковую дискуссионную площадку по вопросам информационного общества и цифровой экономики, обеспечения безопасности и использования информационных и коммуникационных технологий.

Наше заседание проходит в период очередного обострения международной обстановки, связанного в первую очередь с различием в трактовках современной мировой политики, желанием некоторых государств доказать свою правоту с помощью силы. Международное право как регулятор отношений между государствами начинает давать сбой. Это обусловлено целым рядом новых явлений, сопровождающих развитие глобального информационного общества.

Речь идет прежде всего об использовании социальных сетей для распространения политической информации, в частности информации о виртуальных политических событиях, об активном манипулировании международным и национальным общественным мнением, использовании этих событий для угрозы силой суверенным государствам.

Прошедший год показал, что данный вызов миру становится все более осязаемым. В этих условиях особую опасность приобретает возможность распространения фейковой поли-

тики, фейковых новостей на глобальную информационную инфраструктуру. Это повышает актуальность всей нашей деятельности по укреплению международной информационной безопасности.

Мы здесь собрались, чтобы свободно и открыто обсудить наиболее острые вопросы обеспечения национальной и международной безопасности, предложения по противодействию угрозам злонамеренного и враждебного использования информационных технологий, в том числе террористическими и другими преступными организациями.

Уважаемые участники форума, мне хотелось бы проинформировать вас о значительном, на мой взгляд, событии. 10 апреля 2018 года в Москве, в главном здании Московского университета, проведено учредительное собрание Национальной ассоциации международной информационной безопасности. Кроме Московского университета, учредителями выступили Московский государственный институт международных отношений МИД России, Дипломатическая академия МИД России, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Институт современных проблем безопасности (эта организация создана ГМК «Норильский никель») и Редакция журнала «Международная жизнь». Учредители определили основные цели деятельности ассоциации. К ним, в частности, относятся:

- содействие федеральным органам исполнительной и законодательной власти РФ в их деятельности по реализации государственной политики в области международной информационной безопасности, а также российским коммерческим и некоммерческим организациям и гражданам, участвующим в реализации государственной политики в указанной области;

- содействие объективному информированию и разъяснению гражданам и организациям гражданского общества РФ и зарубежных государств основных положений государственной политики России в области международной информационной безопасности.

На наш взгляд, создание ассоциации будет способствовать укреплению как безопасности Российской Федерации, так

и международной безопасности. Усилия ассоциации будут направлены на координацию исследований в области гуманитарных и технических проблем обеспечения международной информационной безопасности, проводимых в научных центрах и высших учебных заведениях. Ассоциация будет в упреждающем режиме проводить проработку проблемных вопросов обеспечения международной информационной безопасности в интересах формирования переговорных позиций государственных органов. Таким образом, ассоциация должна стать национальным центром научных и методических компетенций в сфере информационной безопасности, который будет вырабатывать экспертные рекомендации для органов принятия решений. Не сомневаемся в ее активном участии в работе нашего форума.

В рамках сегодняшнего «круглого стола» планируется обсудить проблемы международного сотрудничества и обеспечения международной информационной безопасности в условиях цифровизации глобальной экономики. Значимость развития цифровой экономики в настоящее время сомнений не вызывает. Так, по оценке некоторых российских экспертов, объем цифровой экономики в Российской Федерации к 2025 году может составить примерно 65 трлн. рублей.

В условиях роста опасности злонамеренного использования информационных технологий для нанесения ущерба экономическим интересам граждан, госорганизаций и частного бизнеса существенно возрастает актуальность развития системы международного сотрудничества в области противодействия данной угрозе. Достижению этой цели, как представляется, может способствовать принятие международной конвенции по обеспечению международной информационной безопасности, а также универсальной конвенции ООН о сотрудничестве в области информационной преступности. Проект такой конвенции был представлен в мае 2017 года на VIII Международной встрече высоких представителей, курирующих вопросы безопасности, а также на «полях» XXVI сессии Комиссии по предупреждению преступности и уголовному правосудию ООН. Наш форум мог бы внести свой вклад в разработку позиции по этому вопросу.

На «круглом столе» №2 завтра в первой половине дня будет организовано обсуждение механизмов реализации государственно-частного партнерства в области обеспечения безопасности критической информационной инфраструктуры. В рамках данного обсуждения внимание участников будет сосредоточено на вопросах правового регулирования международных отношений в области безопасности критической информационной инфраструктуры. За последние годы опасность нападений на такие объекты меньше не стала. Становится все более актуальной тематика взаимодействий государства с частным бизнесом, собственниками соответствующих объектов критической инфраструктуры.

С этой точки зрения заслуживает серьезного внимания инициатива, выдвигаемая представителями бизнеса. Так, на XI форуме в Гармиш-Партенкирхене российская компания «Норильский никель» выступила с инициативой разработки хартии информационной безопасности критических объектов промышленности. «Норильский никель» в нашей стране является глобальной и системообразующей компанией. Она вносит значительный вклад в социально-экономическое развитие регионов России. Достаточно перечислить направления ее деятельности, чтобы оценить масштабы находящихся под ее управлением объектов критически важных инфраструктур. Это геологоразведка, производство, сбытовая сеть, транспорт, включая морской и авиационный, энергетика, информационная структура и научные коллективы. По оценкам экспертов компании, в среднесрочной перспективе уровень автоматизации производственных процессов превысит 80%. Поэтому компания в полной мере осознает значимость процесса обеспечения безопасности глобальной инфраструктуры.

За прошедший год представителями компании проделана большая работа по разработке проекта хартии, подготовке ее обсуждения заинтересованными лицами и организациями. Выдвигая эту инициативу, «Норильский никель» четко обозначает свое представление о том, какое поведение в информационном пространстве бизнес-сообщества должно приветствоваться, а какое - осуждаться. Компания исходит из того, что любой, кто использует информаци-

онные технологии для недобросовестной конкуренции, приготовления технологических процессов кражи чувствительной информации у коллег-конкурентов, должен быть осужден бизнес-сообществом.

В рамках «круглого стола» будут обсуждаться вопросы практической реализации положений хартии в деятельности бизнес-сообщества. Информационное пространство не делится на пространство для государственных структур и для бизнеса, оно у нас общее. И проблемы здесь общие.

Надеюсь, что мы сегодня значительное внимание также уделим рассмотрению концепции «Цифровой женевской конвенции». На форуме мы заслушаем доклады ее авторов - представителей «Microsoft».

Завтра после обеда предполагается рассмотреть проблемы противодействия враждебному использованию информационных и коммуникационных технологий в военно-политических целях. Спектр использования информационных технологий для достижения военно-политических целей значительно расширился. Все больше внимание специалистов привлекают исследования путей применения систем искусственного интеллекта в системах вооружения и военной техники. Активно исследуются методы создания и боевых роботов на суше, на море, в воздухе, информационных инфраструктур в космосе.

Информационные технологии применяются и для повышения эффективности средств ведения вооруженной борьбы на всех стадиях развития конфликта. Одновременно значительно расширяется множество объектов инфраструктуры государства, поражение которых угрожает существованию самого государства. Теперь к таким объектам часто относят не только объекты военной инфраструктуры государства, но и объекты экономического и социального характера. По мнению экспертов ОБСЕ, около 50 государств активно реализуют программы создания боевых вредоносных программ. В число этих стран входят десять государств, обладающих самыми внушительными военными бюджетами. Развитие средств ведения силовых действий в среде информационных технологий не способствует укреплению международной безопасности.

При подготовке форума мы исходили из того, что в обсуждении существующих в данной области проблем примут активное участие представители военных структур заинтересованных государств. Нас на это настраивало продвижение данной идеи нашими американскими и канадскими коллегами. Однако буквально накануне открытия форума заявка на участие военных экспертов нашими партнерами была отозвана. Такое обстоятельство наряду с фактом срыва Госдепартаментом США российско-американских консультаций по вопросу международной информационной безопасности в марте 2018 года в Женеве дает основание предположить, что зарубежные партнеры пока не готовы к серьезному обсуждению данной тематики. Это обстоятельство вызывает очень глубокое сожаление.

Утро среды мы посвятим обсуждению механизма выполнения норм, правил и принципов ответственного поведения государств в ИКТ-среде. Этот вопрос является одним из наиболее важных в информационной безопасности. В 2015 году принятие доклада Группой правительственных экспертов ООН, включавшего добровольные нормы, правила и принципы ответственного поведения государств в среде информационных технологий, стало настоящим прорывом. Последующие годы авторитетные эксперты по всему миру занимались научной проработкой возможностей их практической реализации.

В Институте проблем информационной безопасности МГУ в 2016 году были разработаны комментарии к нормам, принципам и правилам ответственного поведения. В 2018 году международной группой экспертов под руководством присутствующей на форуме доктора Энекен Тикк сделан очередной шаг в данном направлении: подготовлен сборник комментариев, отражающих мнение ведущих зарубежных специалистов международного права по этой теме, что, как нам представляется, создает условия для следующего шага в направлении практического применения выработанных правил.

Следующий вопрос - обеспечение цифрового суверенитета государств. Он будет вынесен на обсуждение в среду во второй половине дня. В нашем институте в течение последних лет с различных точек зрения изучается проблема наполнения правовым содержанием понятий «цифровой суверенитет» и

«разграничение зон ответственности государств в информационном пространстве». Решение этой проблемы, на наш взгляд, является важным условием для практического применения норм, принципов и правил ответственного поведения в среде информационных технологий. Все правила ответственного поведения государств базируются прежде всего на выполнении государствами международных обязательств по соблюдению ограничений в области использования силы для решения межгосударственных споров. В результате исследований, выполненных применительно к глобальной информационной инфраструктуре, нами отмечено, что с технической точки зрения идея разграничения зон ответственности государств в сфере информационных технологий является реализуемой.

В рамках нашего форума состоится заседание Международного консорциума информационной безопасности. На обсуждение будут вынесены вопросы выполнения решений консорциума, состоявшегося в декабре 2017 года, а также предложения по новым совместным исследовательским проектам, наполнение которых можно было бы начать в 2018 году.

В работе нашего форума принимают участие ведущие ученые и специалисты из 13 государств мира: России, США, Китая, Великобритании, Японии, Республики Корея, Австрии, Белоруссии, Канады, Киргизии, Швейцарии, Эстонии, Финляндии, а также представители двух международных организаций - ICANN (Корпорации по управлению доменными именами и IP-адресами) и компании «Технологии против терроризма» под эгидой Конференции ООН по торговле и развитию.

В заключение хотел бы поприветствовать руководителей организаций, которые ежегодно оказывают поддержку нашему форуму. Это вице-президент - руководитель Блока корпоративной защиты ПАО «ГМК «Норильский никель» Владислав Иванович Гасумянов и научный руководитель АО «НИИАС», ОАО «Российские железные дороги» Владимир Георгиевич Матюхин.

Уважаемые коллеги, желаю плодотворной работы нашему форуму.

Слово для оглашения приветствия ректора МГУ им. М.В.Ломоносова В.А.Садовничего предоставляется заместителю

директора Института проблем информационной безопасности Соколову Владимиру Викторовичу.

Соколов В.В., заместитель директора Института проблем информационной безопасности: «Организаторам и участникам XII Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Уважаемые коллеги,

Приветствую вас от имени коллектива Московского государственного университета и поздравляю с началом работы очередного, XII по счету, Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Уже не первый год гостеприимный Гармиш-Партенкирхен становится местом обсуждения наиболее актуальных проблем международной информационной безопасности. Московскому университету вместе со своими партнерами удалось создать уникальную площадку, где международный, междисциплинарный коллектив ученых, специалистов и политиков может не только высказывать и выслушивать разные точки зрения, но и предложить свой интеллектуальный и экспертный потенциал для поиска ответов на общие проблемы.

Начавшийся более 20 лет назад процесс массового освоения информационного пространства не замедляется. Сейчас уже более половины населения планеты являются пользователями глобальной сети Интернет. Непрерывно возрастает число предприятий, которые включаются в реализацию концепции «цифровой экономики». Идет развитие шестого технологического уклада и индустрии 4.0. Появляются даже специализированные ИКТ-инструменты реализации национальных интересов. Человечество только начинает широко использовать в своей деятельности такие инновации, как большие данные, квантовые вычисления, дополненная и виртуальная реальность, блокчейн, но при этом зачастую не задумывается о связанных с ними угрозах и рисках.

Нам необходимо фундаментальное научное осмысление и понимание происходящих процессов и прогнозирование их последствий. Нет неоднозначного ответа на вопросы: как человеку и обществу защититься от фейковых новостей, политических манипуляций и влияния деструктивных идеологий? Как способствовать равноправному стратегическому партнерству в глобальном

информационном пространстве? Как обеспечить устойчивый рост и развитие «цифровой экономики», не принося в жертву безопасность?

Долг университетской корпорации и экспертного сообщества выработать и представить человечеству ответы на угрозы не только сегодняшнего дня, но и будущего. Эффективная работа на этих направлениях невозможна без объединения усилий научных коллективов различных государств. Уникальность форума в том, что именно здесь уже собран такой международный состав экспертов, который не только способен ставить перед собой актуальные задачи, но и успешно их решать.

Желаю всем участникам форума плодотворной работы, достижения значимых результатов.

Ректор Московского государственного университета им. М.В.Ломоносова академик Виктор Антонович Садовничий».

Шерстюк В.П.: *Слово предоставляется сопредседателю Оргкомитета, начальнику Департамента аппарата Совета безопасности Российской Федерации Бойко Сергею Михайловичу.*

Бойко С.М., начальник Департамента аппарата Совета безопасности Российской Федерации: Мне бы хотелось озвучить приветствие участникам и гостям нашего форума со стороны сопредседателя Оргкомитета, заместителя секретаря Совета безопасности Российской Федерации Олега Владимировича Храмова:

«Уважаемые коллеги,

Позвольте приветствовать организаторов, участников и гостей XII Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

В этом году ведущие эксперты в области международной информационной безопасности из 13 стран мира в 12-й раз собрались в Гармиш-Партенкирхене, чтобы обсудить наиболее актуальные проблемы противодействия современным вызовам и угрозам в информационной сфере. Программа форума традиционно включает в себя обсуждение ключевых вопросов обеспечения информационной безопасности, международного сотрудничества в данной области. В том числе применительно к условиям активно развивающейся «цифровой экономики».

В центре внимания, как всегда, будет дискуссия, посвященная проблемам противодействия использованию ИКТ во враждебных военно-политических

целях, включая обсуждение проблематики предотвращения опасной деятельности в информационном пространстве. Полагаю, что участники форума смогут представить новые идеи, новые инициативы, нацеленные на выработку превентивных мер в отношении подобных угроз. Важно сделать все возможное для недопущения конфликтов в информационной сфере.

Отличительной чертой форума в Гармиш-Партенкирхене является включение в повестку дня вопросов, касающихся безопасности всего мирового сообщества. И в этом году впервые планируется обсудить механизмы выполнения норм, правил и принципов ответственного поведения государств в информационном пространстве. Такая дискуссия в условиях, когда потребность мирового сообщества в подобных правилах становится не просто очевидной, а жизненно необходимой, приобретает особое значение.

Предлагаемые участниками форума подходы к обеспечению международной информационной безопасности находят свое отражение в документах, которые впоследствии принимаются в Организации Объединенных Наций, ОБСЕ, Региональном форуме АСЕАН по безопасности и в формате других международных структур. Практическая ориентированность тематических «круглых столов», заинтересованное обсуждение наиболее острых проблем в указанной области стали по праву визитной карточкой конференции в Гармиш-Партенкирхене и сделали ее одной из самых заслуженных, авторитетных международных экспертных площадок.

Уверен, что и в этом году форум будет нацелен на сближение позиций его участников в поиске оптимальных путей формирования системы международной информационной безопасности. Желаю всем успешной и плодотворной работы.

Сопредседатель Оргкомитета, заместитель секретаря Совета безопасности Российской Федерации Олег Храмов».

Уважаемые коллеги, хотел бы перейти к выступлению в рамках пленарного заседания. Как вы видите, в названии нашего форума сосредоточена триада составляющих борьбы с угрозами в информационной сфере: государство, бизнес и гражданское общество.

Остановлюсь на первой составляющей как представитель государственной структуры. Все основные намерения Россий-

ской Федерации и ее политика в этой области сформулированы в вполне конкретном документе «Основы государственной политики РФ в области международной информационной безопасности на период до 2020 года», которые были утверждены Президентом нашей страны в июле 2013 года. Цель, которая сформулирована в этом документе, предельно ясна: «Содействовать установлению международно-правового режима, направленного на создание условий для формирования системы международной информационной безопасности».

Как достигнуть этой цели? Как прийти к тому, что заявлено государством на самом высоком уровне? Ответ - в конкретных, практически ориентированных шагах, инициативах, идеях в рассматриваемой области. Причем, спектр этих инициатив и идей может быть достаточно широк. Это и правовое поле, и организационные вопросы, различные другие виды обеспечения, вопросы сотрудничества и т. д.

В целом предназначение такой системы можно рассматривать в двух аспектах. Первый аспект - это противодействие угрозам стратегической стабильности в информационной сфере и стратегической стабильности миропорядка в целом. И второй аспект - это способствование равноправному стратегическому партнерству в глобальном информационном пространстве. Вот два вектора, на которые нацелена государственная политика России в данной области.

Поэтому на передний план выходит сотрудничество с государственными структурами, научным, экспертным сообществом, деловыми кругами всего мира для достижения этой цели. Политика нашей страны нацелена на взаимодействие по всем ключевым направлениям такой деятельности. Безусловно, мы говорим о системе международной информационной безопасности. Как любая система вообще, эффективная система должна строиться на единой платформе во имя достижения единых целей. Только тогда можно достичь конкретного конечного результата, на котором она основана. Мы в начале пути. Что же может, по мнению России, выступить основой, платформой для построения этой системы, системы международной информационной безопасности? Безусловно, это совокупность норм и подходов, которые должны быть закре-

плены в ключевых международных нормативно-правовых документах, прежде всего, как нам кажется, в документах Организации Объединенных Наций. А международно-обязывающий документ на площадке ООН - это ее конвенции. Но, конечно, путь достаточно непростой и далеко не быстрый.

Оглянемся назад - 1998 год. По инициативе России вносится резолюция Генассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Первый шаг на этом направлении нашей страной при поддержке ее партнеров был сделан 20 лет назад, то есть осознание угрозы состоялось еще тогда, понимание опасности новых вызовов и угроз уже было ранее. Поэтому мы не в начале пути, мы на этом пути уже сейчас находимся, но мы буксуем, мы делаем шаг вперед, а затем - несколько шагов назад.

Вместо того чтобы, засучив рукава, вместе работать и сотрудничать, мы начинаем апеллировать к каким-то различиям в подходах, тем самым оголяя свои тылы, обнажая свою критическую инфраструктуру, поскольку наши оппоненты в лице международного терроризма, международного криминала не ждут. Они совершенствуют свои формы и способы, пока мы пытаемся договориться по понятийному аппарату. Давайте мы еще лет десять подождем, тогда и собираться не придется, и обсуждать будет нечего.

Мы начинали в 2004 году первое заседание Группы правительственных экспертов ООН, а эта площадка в Организации Объединенных Наций также была создана по инициативе Российской Федерации в одной из резолюций, о которой я уже упоминал. Это первая экспертная площадка по тематике международной информационной безопасности в Организации Объединенных Наций, и группа уже собиралась пять раз. Так вот, первая работа группы закончилась ничем, потому что не сошлись в понятиях. А мировой криминал шел вперед, и ему, простите, наплевать на то, что у нас нет совпадения во взглядах. У него с этим проблем не бывает. Но вот поэтому вопрос достаточно остро и стоит. И Россия вновь остается приверженцем тех инициатив, с которыми выступала ранее. Мне хотелось бы остановиться на трех ключевых, которые мы имеем сейчас.

Несмотря на то что Группа правительственных экспертов 2016-2017 годов не смогла выйти на консенсусный доклад, у нас есть хороший задел предыдущей группы, которая по итогам своей работы привнесла в мировое сообщество рекомендации по правилам, нормам и принципам ответственного поведения государств в информационном пространстве.

Есть фундамент, и сегодня Россия предлагает этот «кирпич». Плюс основой нового документа могут стать и станут правила поведения в области обеспечения международной информационной безопасности - это инициатива стран Шанхайской организации сотрудничества, представленная в ООН в январе 2015 года. Уже есть консенсусный документ в виде этой инициативы, в виде доклада Группы правительственных экспертов 2015 года, часть доклада 2013 года, то есть уже все предпосылки созданы.

Россия предлагает принять резолюцию Генеральной Ассамблеи ООН нового формата, документ, в котором были бы сконцентрированы консенсусные результаты в области правил поведения, в области обеспечения международной информационной безопасности. На каких постулатах можно построить эту работу?

В основе этих правил - ряд главных подходов. Отмечу некоторые из них:

1) информационно-коммуникационные технологии должны применяться исключительно в мирных целях;

2) международное сотрудничество в этой сфере должно быть направлено на предотвращение конфликтов в информационной среде, а не на их регулирование. Очевидная потребность сегодня - поставить барьер в правовом плане, в организационном плане, в плане сотрудничества государственного и негосударственного секторов;

3) необходимость поиска новых международно-правовых регуляторов ИКТ-среды. Действующее международное право не позволяет охватить весь спектр вызовов и проблем;

4) государства должны обладать суверенитетом над своей информационной инфраструктурой. Никто не вправе посягать на этот суверенитет. Любые обвинения в адрес государств в деструктивном применении информационных технологий

должны быть доказаны. И это доказательство - не сообщение в средствах массовой информации. Государства, безусловно, не должны давать возможности кому-то использовать свои территории для вредоносной деятельности в информационном пространстве;

5) обязанность государств бороться с внедрением и использованием скрытых вредоносных функций и программных уязвимостей в IT-продукции, добиваться ее безопасности для простых пользователей.

Что же позволит принять такую резолюцию? Конечно, это начало конкретной практической работы по новому составу Группы правительственных экспертов, к которой можно было бы приступить уже в следующем, 2019 году.

Вот в целом идея этой инициативы, но системный подход России к формированию архитектуры международной информационной безопасности подчеркивает другая инициатива. Вы знаете, что осенью прошлого года на 72-й сессии Генассамблеи ООН Россией в качестве официального документа сессии был внесен проект конвенции о сотрудничестве в области противодействия информационной преступности. Есть потребность в этом документе или нет? Давайте говорить сухим языком цифр. По оценкам экспертов, в 2006 году ущерб мировой экономике от криминального использования ИКТ составил практически 450 млрд. долларов. Уже в следующем году можно ожидать увеличения этого ущерба до 2 трлн. долларов, а буквально спустя год-два - выход на трехтриллионные рубежи.

Конвенция, которая была представлена ООН, - это результат многолетней работы российских экспертов по созданию универсального, всеобъемлющего документа, нацеленного на противодействие подобным преступлениям. Документ учитывает современные реалии, основывается на принципах суверенного равенства сторон и невмешательства во внутренние дела.

Каковы цели? Во-первых, необходимо содействовать принятию и укреплению мер, направленных на предупреждение ИКТ-преступлений и иных противоправных деяний. Во-вторых, в основу положена борьба с использованием технологий

в преступных целях путем обеспечения наказуемости таких деяний. Содействие всем процедурным вопросам по их расследованию, преследованию, как на внутригосударственном, так и международном уровнях. И третий посыл - развитие международного сотрудничества, повышение его эффективности.

В чем отличие от предыдущих документов? Проект документа включает широкий понятийный аппарат, рассматривает вопросы технического содействия, регламентирует порядок оказания взаимной правовой помощи и ряд других механизмов.

Нельзя не упомянуть о третьей инициативе России на этом направлении. Она направлена на решение проблем безопасности функционирования и развития сети Интернет. Это концепция, соответствующая конвенции Организации Объединенных Наций. Основные задачи: содействовать дальнейшему развитию Сети, повышать ее безопасность и обеспечивать гарантии прав и свобод ее пользователей; более эффективное управление сетью Интернет на основе равноправного международного сотрудничества. Проект являет собой своеобразный правовой фундамент, ориентированный на исключение права какого-либо государства или группы стран создавать помехи для функционирования сети Интернет, возможности манипулировать доступом в Сеть для влияния на другие суверенные государства.

Естественно, возникает вопрос: готово ли сейчас мировое сообщество к подобным реформам? Пока такой готовности в полной мере нет. Конечно, наиболее проблемными являются вопросы создания международных норм и правил, регулирующих отношения в этой сфере под эгидой институтов ООН. Представленная редакция в нынешнем виде - это, конечно, пища для размышления.

Таковы основные инициативы России в рассматриваемой области, направленные на формирование системы международной информационной безопасности.

Шерстюк В.П.: *Спасибо, Сергей Михайлович. Хочу предоставить слово специальному представителю Президента Российской Федерации по вопросам международного сотрудничества в области информационной*

безопасности Чрезвычайному и Полномочному Послу Российской Федерации Крутских Андрею Владимировичу.

Крутских А.В., специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, посол по особым поручениям МИД РФ: Уважаемые коллеги, мы только что вместе с вами пережили острый военно-политический кризис с Соединенными Штатами. Итог кризиса - не погибли ни один россиянин, ни один американец. Давайте спросим себя: как такое может быть? Сотни ракет летают, самолеты подняты, флот. При любом другом раскладе мы с вами могли бы и не встретиться. Мир мог пойти по совершенно другому пути. Почему это произошло? Не собираюсь анализировать военно-технические детали. Но задаю вам вопрос: а если бы не был заключен в свое время Договор о запрете на испытания ядерного оружия в трех средах? Если бы не был заключен Договор о нераспространении ядерного оружия? Если бы не был создан режим предотвращения распространения ракетных технологий? Если бы не было Соглашения о предотвращении инцидентов в открытом море и в воздушном пространстве над ним? Если бы не было Соглашения о предотвращении опасной военной деятельности? Если бы не было российско-американского опыта ведения переговоров? Если бы наши военные не говорили напрямую друг с другом? Если бы наши президенты не говорили друг с другом? Исход этого кризиса был бы другой.

Ничего этого нет в сфере кибербезопасности. Хотелось бы упомянуть Р.Рогозинского, который выступал в Москве 14 декабря 2017 года на конференции по киберстабильности, организованной «Международной жизнью», с докладом «Назад к безопасности: опасная запутанность между ядерным и кибероружием». Наши силовики обратили внимание, что эта тема сейчас поднимается все чаще и чаще, прежде всего американцами, западниками.

Суть - ИКТ как приводной ремень к обычной «горячей» войне и войне ядерной. Поэтому, если мы более-менее смогли предотвратить глобальную катастрофу сейчас в Сирии, то мы ее не сможем предотвратить, если вдруг политики захотят

использовать не флот, не самолеты, не танки и пушки, а информационно-коммуникационные средства воздействия друг на друга.

В этом году мы будем отмечать 20-летие резолюции об информационной безопасности. 20 лет назад Россия оказалась прозорливее изобретателей Интернета, и именно мы внесли этот проект. Он поначалу был весьма жестким: мы называли вещи своими именами. Но впоследствии он претерпел серьезные изменения, смягчился благодаря западному сообществу в ООН.

Когда мы внесли резолюцию, многие в ООН просто не понимали, что это за текст и зачем он нужен. Все думали, что это футуризм. Никто не осознавал ни угроз, ни проблем. Но это непонимание очень быстро ушло. В том числе и благодаря распространению ранее закрытой информации о возможностях ИКТ, например о системе «Эшелон», которая контролирует каждый телефонный звонок в Европе; благодаря Э.Сноудену, который рассказывал всему миру о глобальной системе контроля за киберпространством и про которого стали уже забывать. Сегодня во многом благодаря и нашим усилиям пришло осознание значимости фактора ИКТ в вопросах безопасности, стабильности и развития.

Естественно, американцы решили, что мы слишком перехватываем инициативу на этом треке, и проголосовали «против». А все практически единодушно поддержали нас. Мы установили рекорд этой резолюцией. Из 84 стран 80 проголосовали «за».

Второй момент. Как вы знаете, работа по Группе правительственных экспертов закончилась в прошлом году неудачей. Мы предвидели эту ситуацию. Встречались с американцами, решали, кто будет председателем. Сразу бросилось в глаза, как негативно были настроены американцы по отношению к немцам. Они все время хотели, чтобы председателем были, конечно же, англосаксы, австралийцы, канадцы. Мы настояли, чтобы были немцы, рассчитывали, что немцы обеспечат нужный уровень доверия западных участников Группы, чтобы объективно вести переговоры и достигнуть компромисса. Потом мы поняли, что американцы и англи-

чане решали другую задачу. Они не были заинтересованы в позитивном исходе этой группы. И если уж Группа «заваливается», пусть она «утонет» вместе с немецким председателем. Так и получилось.

Но есть и позитивный результат. В ходе работы образовалась так называемая группа из государств БРИКС, ШОС, нейтральных, развивающихся стран. Эти группы стали продвигать близкие нам идеи, а именно: бороться за свою кибербезопасность.

Многие из предложений уникальны и перспективны. К примеру, Сенегал выступил с идеей создания третейского киберсуда. Если пойдут фейковые или нефейковые обвинения, к кому должны апеллировать государства? ООН и Совет Безопасности этой темой не занимаются. Устав ООН кибертему не рассматривает, потому что в статье 51 сказано, что только вооруженное нападение дает право на самооборону.

В итоге темой заинтересовались все, поступила масса подобных предложений: «Давайте создадим организацию типа Комитета ООН по космосу, но в киберпространстве. Давайте создадим третейский суд. Давайте уполномочим Совет Безопасности». Натовцы промолчали, против выступили Англия и Соединенные Штаты. Несмотря на противодействие, дискуссия по этой теме набирает обороты.

И в данном процессе бизнес обгоняет политиков: предприниматели в числе первых, кто хочет договориться о правилах игры. Потому что они, как никто другой, понимают, что в условиях киберанархии огромные состояния становятся заложником ИКТ. Отсюда и наше предложение создать новую Группу правительственных экспертов в ООН таким образом, чтобы она могла рассматривать не только политические решения, но и вопросы бизнеса.

Наконец, финальный аспект. Как, в том числе с помощью диалога по кибербезопасности, укрепить стратегическую стабильность, улучшить взаимоотношения между Россией и США? Мы выдвинули целый ряд тем: по предотвращению кибервойны между Россией и США, о расширении мер доверия, о предотвращении опасной военной деятельности, о создании постоянно действующего механизма переговоров по киберпро-

странству. Предлагали заключить межправительственное соглашение о предотвращении инцидентов в киберпространстве.

Ответ с американской стороны мы все знаем - поток фейкньюс о вмешательстве в выборы, о российских хакерах. Но так мы никуда не продвинемся. Нам нужен нормальный диалог профессионалов.

Шерстюк В.П.: *Хочу сейчас предоставить слово старшему вице-президенту, главному техническому директору Корпорации по управлению доменными именами и IP-адресами (ICANN) Дэвиду Конраду (David Conrad).*

Дэвид Конрад, старший вице-президент, главный технический директор Корпорации по управлению доменными именами и IP-адресами (ICANN): Не буду говорить о глобальной политике или военных действиях. Мое выступление затронет деятельность моей компании в контексте обеспечения безопасности и устойчивости в киберпространстве.

Я работаю в сфере Интернета с 1983 года, занимался многими вещами, включая запуск стартапов в Кремниевой долине, также я основал Азиатско-тихоокеанский информационный центр в Токио, который впоследствии переехал в Брисбен (Австралия). По большей части я техник, поэтому если у вас будут вопросы, связанные с политикой, то не смогу на них ответить.

Наша корпорация ICANN была создана в 1998 году в результате консультаций правительства США с представителями экспертного сообщества. Был контракт до октября 2016 года с Министерством торговли США и национальной администрацией по делам связи и информации, затем был заключен контракт по исполнению функции IANA (Администрация адресного пространства Интернет) об управлении доменными именами, IP-адресами и интернет-протоколами, используемыми Инженерным советом Интернета. Сейчас нас около 600 человек в разных уголках мира, у нас есть офисы в Сингапуре, Стамбуле, Вашингтоне, штаб-квартира в Лос-Анджелесе, также офисы в Кении, Монтевидео и Брюсселе. Наш бюджет около 140 млн. долларов, он покрывает затраты на персонал. Значительная

часть уходит на выплаты членам нашего сообщества для посещения заседаний ICANN, которые проводятся трижды в год по всему миру. ICANN состоит из трех частей: сообщество заинтересованных лиц, совет, который избирается из сообщества, а также орган, который может быть по функционалу приравнен к секретариату. Мы обеспечиваем поддержку и приветствуем дискуссии в сообществе.

Мы управляем одним из 13 рут-серверов, ранее известным как L, теперь мы его называем «ICANN managed server», мы работаем с доменом .int, где регистрируют имена международные организации. NATO.int находится в среде .int. И мы управляем DNS trust anchor, механизмом, устанавливающим виртуальное доверие. Если говорить о работе IANA, мы отвечаем за изменение доменных имен верхнего уровня: .com, .ru, .de. Каждый раз, когда кто-то желает внести изменения, они связываются с ICANN и мы выполняем для заказчика эту задачу. Мы выделяем большое количество IP-адресов для региональных интернет-регистраторов, их всего пять по всему миру.

Как ранее упоминал, я помогал в создании Азиатско-тихоокеанского информационного центра, который охватывает АТР. В Европе эти функции выполняет RIPE NCC, основанный в 1993 году. Он охватывает Европу, страны бывшего СССР, Ближний Восток и др. ARIN охватывает Северную Америку, LACNIC - Южную Америку и Карибский бассейн, AFRINIC охватывает Африку. Инженерный совет Интернета - это орган, который создает протоколы для Интернета, ведет учет реестров, в которых хранится информация об этих протоколах, есть уникальные идентификаторы, которые используются в протоколах, к примеру, вы можете знать port 80 для Всемирной паутины (worldwide web), число 80 зарегистрировано в реестре, управляемом ICANN.

Какова же позиция ICANN по поводу обеспечения безопасности и устойчивости в киберпространстве? Одной из первых строчек общей концепции деятельности компании является «Обеспечение стабильной и безопасной работы систем уникального идентификатора». Это означает, что мы избегаем любых действий, способных поставить под угрозу структуру Интернета. Для безопасности мы обеспечиваем

целостность и доступность систем. Большая часть людей знает о ICANN по доменным именам, но мы также занимаемся IP-адресами и параметрами протоколов. Но пока чаще всего о ICANN говорят в контексте доменных имен.

В нашем регламенте (документ порядка 300 страниц) зафиксированы обязательства и основные ценности ICANN. В первом параграфе написано: «Сохранять и улучшать администрирование DNS и стабильность работы, надежность, безопасность, глобальную совместимость, устойчивость и открытость DNS и Интернета; поддерживать способность координировать DNS на общем уровне и работать для поддержки единого, глобально совместимого Интернета».

Говоря о стабильности, одним из вызовов, с которым и мы сталкиваемся, является создание конкуренции. На заре Интернета было три домена верхнего уровня, но большинство регистрировалось в .com. Люди думали, что существует некая монополия, и одной из причин возникновения ICANN было создание свободной среды, которая позволила бы доменам верхнего уровня конкурировать с .com. Однако стабильные системы минимизируют изменения созданием новых доменов верхнего уровня. Так что ICANN приходится соблюдать баланс между стабильностью и изменениями, необходимыми для создания конкуренции.

О безопасности DNS. Мы нацелены на сохранность и доступность. В DNS нет конфиденциальности, по крайней мере сейчас. Существуют предложения от Инженерного совета Интернета по добавлению конфиденциальности, но на данный момент это находится на стадии эксперимента и не было как-либо имплементировано. Говоря о сохранности, ICANN отвечает только за корневые серверы DNS, только домены высокого уровня. Мы сопоставляем опубликованное и полученное, используя DNS SAC на основе криптосистемы с открытым ключом, чтобы генерировать подписи, которые позволяют признавать действительной информацию, которую они получили, и что она не была изменена во время передачи.

Говоря о доступности, как я уже заметил, мы управляем одним из 13 корневых серверов, в таком рут-сервере дублируются около 200 инстанций по всему миру. Есть еще 12 других

рут-серверов, и всего инстанций на данный момент около 600, их число постоянно растет, чтобы дать большую доступность.

Мы делаем рут-зону доступной и другими средствами. Если вы интернет-провайдер, то вы можете заполучить рут и сделать его доступным для ваших клиентов, повышая устойчивость и производительность вашей сети.

Другие органы ICANN, ответственные за безопасность, - это Консультативный комитет по вопросам безопасности и стабильности (SSAC), в который входят 36 экспертов по безопасности. Также обеспечением безопасности занимается Консультационный совет по управлению корневыми серверами (RSSAC), в этом органе состоят только операторы серверов, IANA. В рамках ICANN функционирует также система WHOIS - регистрационная база данных, доступная по всему миру. Возможно, кто-то из вас сталкивался с ней в связи с Общим регламентом по защите данных (GDPR), принятым Европейским союзом. Это децентрализованная база данных, которая используется для идентификации того, кто владеет интернет-ресурсом, что применимо как к доменам, так и IP-адресам.

На данный момент региональные интернет-реестры делают нечто похожее для адресов. Но все поменяется со вступлением в силу GDPR 25 мая, пока идет обсуждение о замене системы WHOIS, но, вероятно, это приведет к уменьшению количества информации, доступной исследователям и органам правопорядка.

Информация о том, кто использует IP-адрес или домен во время, скажем, кибератаки, из-за ограничений, вводимых GDPR, больше не будет доступна общественности. Доступ будет осуществляться ограниченно посредством системы аккредитации или предъявления соответствующего ордера или иных документов для получения доступа.

Мы также стараемся помогать бороться с кибератаками. Мы участвовали в уничтожении ботнета Avalanche и других, предоставляя информацию органам правопорядка, иным силовым структурам и помогая налаживать контакты между ними.

О наращивании потенциала. Это работа по информированию органов правопорядка о том, как использовать разные ин-

струменты, чтобы выследить нападавших или другие криминальные элементы. Все эти данные мы предоставляем бесплатно.

ICANN не контролирует Интернет. Многие ошибочно представляют нашу организацию как инструмент, при помощи которого правительство или другие структуры воздействуют на Интернет. ICANN этим не занимается. Интернет - это децентрализованное объединение сетей, и каждая сеть работает независимо. У ICANN нет механизма, чтобы заставить кого-либо что-либо делать. ICANN не контролирует корневые серверы, 13 рут-серверов управляются 13 организациями, ICANN является лишь одной из них. Мы содействуем улучшению связи между остальными 12 структурами, но мы их не контролируем.

Мы не можем удалить домены из Интернета. Единственное, что мы можем сделать, так это удалить домен по запросу администратора этого домена, к примеру, если страна изменила свое название. Когда Восточный Тимор изменил свое название на Тимор-Лешти, мы изменили их домен высокого уровня с .tp на .tl. Мы не предпринимаем действий в одностороннем порядке. ICANN также не может блокировать домены, не существует механизма, который сделает домен недоступным, это относится к любому уровню DNS.

Шерстюк В.П.: *Уважаемые коллеги, я хотел бы предоставить слово вице-президенту, руководителю блока корпоративной защиты ГМК «Норильский никель» Гасумянову Владиславу Ивановичу.*

Гасумянов В.И., вице-президент, руководитель блока корпоративной защиты ГМК «Норильский никель»: За прошедший 12-летний цикл форум вырос из ординарного тематического мероприятия в области информационной безопасности в уникальное движение, которое мы называем «гармишевский процесс». Показательно, что наш форум также получил неофициальное название «электронный Давос».

Присоединившись к гармишевскому процессу, компания «Норильский никель» рассматривает данную площадку в качестве пространства возможностей для непосредственного участия в формировании устойчивой системы международной информационной безопасности. Главную цель своего высту-

пления вижу в том, чтобы привлечь внимание бизнеса к обсуждаемым здесь острым проблемам.

«Норильский никель» - это лидер горнометаллургической промышленности России, крупнейший в мире производитель палладия, входит в топ-пять мировых производителей никеля, платины, кобальта и родия. Доля компании в объеме промышленного производства страны составляет около 3%. В объеме металлургического производства - около 10%. В мировом производстве никеля компания занимает второе место, в производстве палладия - первое.

Свою миссию «Норникель» видит в том, чтобы, плодотворно используя природные ресурсы и акционерный капитал, обеспечивать человечество цветными металлами, которые делают мир надежнее, помогают воплощать надежду людей на развитие и технологический прогресс. Для решения поставленных задач мы опираемся на ценности, сформировавшиеся за десятилетия нашей деятельности: это, конечно, надежность, способность принимать любые вызовы, сохраняя успешность своей деятельности; ответственность, готовность выполнять обязательства, принимать решения и отвечать за их результат; эффективность, умение достигать поставленных целей в срок и при оптимальных затратах; профессионализм, способность выполнять свою работу с высоким результатом; развитие, эффективный рост и обновление производства, внедрение самых современных технологий, повышение профессионального уровня сотрудников; сотрудничество, готовность и способность совместно достигать поставленных целей, делиться опытом, знаниями и ресурсами. Указанные этические императивы, сформулированные в корпоративном манифесте ценностей, в современных условиях тотального проникновения информационно-коммуникационных технологий в бизнес и социальную сферу приобретают особое значение.

На этом форуме мы будем неоднократно возвращаться к теме доверия между партнерами, между странами, предсказуемости поведения всех участников - государств, бизнеса и представителей гражданского общества. По нашему мнению, развитие информационно-коммуникационных технологий, систем обеспечения информационной безопасности в усло-

виях отсутствия доверия может замедлиться и даже привести к деградации. В качестве примера хотел бы проиллюстрировать такой момент. Развитие трансграничных облачных платформ, когда оператор облака как юридическое лицо вынужден действовать в юрисдикции одной из стран, может быть затруднено. Пользователи в широком смысле - частные лица, бизнес, государства из других юрисдикций по соображениям безопасности будут вынуждены использовать «классические» сервисы и инфраструктуру на своей территории, хотя это может быть менее выгодным с экономической точки зрения или менее эффективным.

Сегодня под управлением нашей компании сосредоточено значительное число критически важных информационных инфраструктур, связанных как с бизнесом ее предприятий, так и с социальной составляющей ее деятельности. Не секрет, что ведущие российские корпорации зачастую выступают драйверами экономического роста и социального развития территорий. К «Норникелю» это имеет самое прямое отношение, поскольку его основные производственные единицы находятся в моногородах, расположенных в экстремальных географических и климатических условиях. Этот фактор является для нас важным побудительным мотивом для активного и деятельного участия в процессах формирования системы обеспечения безопасности критически важных объектов информационной инфраструктуры России.

В современных условиях глобализации успех деятельности по обеспечению безопасности национальных, критически важных инфраструктур немыслим без выстраивания справедливой, надежной и устойчивой структуры международной информационной безопасности, основанной на уважении прав и интересов всех вовлеченных в этот процесс сторон. Это непростой путь, но мы вместе должны его пройти. Часть данной задачи, касающейся крупного промышленного бизнеса России, последовательно реализует «Норильский никель». В этом сложном деле нам импонирует мудрый принцип - малыми шагами идти к великой цели. Ровно год назад здесь, в Гармише, мы выступили с инициативой разработать проект хартии информационной

безопасности критически важных объектов промышленности. Документ был подготовлен нашими специалистами и представлен на конференции Международного исследовательского консорциума информационной безопасности в декабре прошлого года в Москве.

В хартии мы сформулировали свое представление о том, какое поведение в информационном пространстве бизнес-сообщество приемлет и приветствует, а какие вещи определенно осуждает. Проект был в целом одобрен и рекомендован к представлению на международном уровне в рамках настоящего форума. В качестве ключевых интеллектуальных центров развития и реализации этой хартии мы предлагаем следующие структуры.

Первое, это Международный исследовательский консорциум по информационной безопасности, очередная конференция которого проходит в рамках нашего форума. Второе, созданная в прошлом году по инициативе «Норникеля» автономная некоммерческая организация «Безопасность информации в промышленности» - БИП-клуб. Членами клуба на сегодня являются руководители подразделений информационной безопасности крупнейших промышленных предприятий России, таких как «Северсталь», «АЛРОСА», «Евраз», компания «Полюс», «Лукойл» и др. Клуб открыт для всех присутствующих и ваших коллег, партнеров. Мы вас приглашаем вступать в члены клуба, еще одной открытой площадки для обсуждения наших проблем.

Полагаю, было бы полезно и целесообразно обсудить и одобрить предложенную хартию на заседании консорциума и предложить пути продвижения этой хартии. Это могут быть международные структуры бизнеса, отраслевые и научные объединения, международные организации. Мы примем определенные принципы, как продвигать хартию.

В связи с этим от имени компании «Норильский никель» хочу выступить еще с одной инициативой - мы объявляем о своей готовности финансово поддержать в форме грантов научные исследования по вопросам формирования отдельных элементов системы международной информационной безопасности. В первую очередь наше предложение обращено к

членам консорциума, но не ограничивается этим. В качестве стартовых направлений для исследовательских проектов предлагаем рассмотреть следующие общие темы, вынесенные на обсуждение тематического «круглого стола», который состоится в рамках нашего форума.

Это проблема международно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры, а также политические, юридические, технические проблемы выстраивания механизмов взаимодействия центров реагирования на компьютерные инциденты; проблемы, угрозы и вызовы монополизма поставщиков IT-систем и решений в области информационной безопасности по отдельным направлениям; защита национальных рынков и свобода торговли предпринимательства применительно к проблематике информационной безопасности.

Соискатели гранта обязаны будут в течение года подготовить журнальную публикацию по заявленной теме, представить результаты своих исследований как минимум на двух международных конференциях, одной из которых должна быть конференция консорциума. Дополнительную информацию можно будет получить в секретариате БИП-клуба - полномочного органа по приему заявок по работе с соискателями. Я не хотел бы сейчас подробно говорить об условиях, думаю, что все это будет в средствах массовой информации, в Интернете, поэтому приглашаю принять участие. Для получателей грантов будут оплачены расходы, проезды, проживание, взносы, связанные с участием в конференциях, на которых представляются результаты исследований. И будут выплачены гонорары, размеры которых определятся позднее. Не сомневаюсь, что данная инициатива придаст свежий импульс научным исследованиям и позволит перейти к конкретным действиям по формированию элементов системы международной информационной безопасности.

Уверен, что на это обязательно откликнется наша молодежь, и, у нее будет свежий взгляд на те проблемы, которые мы пытаемся решить. Первые результаты данного эксперимента мы вместе сможем обсудить здесь же, на гостеприимной

баварской земле через год в ходе очередного международного форума информационной безопасности.

Шерстюк В.П.: *Слово предоставляется директору Центра киберправа Университета Корё, Республика Корея Ноюну Паку.*

Ноюн Пак, директор Центра киберправа Университета Корё, Республика Корея: Наш центр (The Cyber Law Centre at Korea University, CLC) был основан в 2012 году. В дополнение к исследованиям и обучению мы консультируем корейское правительство по разным профильным вопросам. К примеру, по поводу первого и пятого заседания Группы правительственных экспертов ООН (UN GGE), по составлению национальной стратегии кибербезопасности и законов о защите данных.

CLC участвует во втором треке диалога по вопросам кибербезопасности между экспертами из Китая, Японии и Кореи. Эти встречи должны способствовать развитию объективного понимания проблем, которые обсуждаются представителями органов власти.

Шерстюк В.П.: *Впервые на нашем форуме присутствуют и выступают представители крупнейшего российского банка - Сбербанка России, и я предоставляю слово заместителю председателя Правления Сбербанка России Кузнецову Станиславу Константиновичу.*

Кузнецов С.К., заместитель председателя Правления Сбербанка России: Мы впервые принимаем участие в работе форума, для нас это большая честь. Хотел бы поблагодарить организаторов за возможность донести наше видение сложившейся ситуации, поделиться нашим богатым опытом, озвучить выводы, которые могут быть полезны для всех участников форума.

Тема моего сегодняшнего сообщения - глобальная киберпреступность и вызовы для международного сотрудничества.

Прежде всего позвольте несколько слов о том, что из себя представляет Сбербанк. Это уже не просто традиционный банк, не сберегательная касса. По сути, сегодня это мощная высокотехнологичная компания. У нас работают 325 тыс. со-

трудников, мы присутствуем в 22 странах мира. В Сбербанке сегодня 146 млн. активных клиентов. Из них 38 миллионов используют информационные технологии, чтобы управлять своими счетами. В 2017 году Сбербанк стал первой компанией России по капитализации.

В начале осени 2015 года мы пришли к выводу, что нам для поддержания высокой степени безопасности всех наших технологических систем требуется совершенно другой уровень защиты. В этой связи с учетом международного опыта мы разработали систему, которая позволяет сегодня достаточно надежно обеспечивать безопасность банка и его клиентов.

Это масштабная система, объединяющая механизмы защиты и оперативного многоуровневого взаимодействия с нашими коллегами из других компаний, правоохранительными органами и профильными международными структурами.

Мы имеем два мощных центра: Операционный центр кибербезопасности, защищающий систему Сбербанка, и Центр мониторинга, который защищает наших клиентов от различного рода атак.

Уровень киберрисков настолько высок, что банки должны обеспечивать защиту клиентов даже в той ситуации, когда они сами не в состоянии распознать посягательство на свои интересы. Мы совместно с нашими коллегами устанавливаем на девайсы, телефоны, андроид-платформы собственные антивирусы, работающие автономно и не создающие помех и сложностей клиентам.

Мы сегодня имеем около 3 млрд. различного рода рисковых событий, которые происходят ежедневно. Было около 400 тыс. попыток заразить наши системы вирусами. Из примерно 100 млн. различных транзакций от 5 до 10 тысяч блокируются клиентами с помощью наших систем.

Для России особенно проблемными являются преступления, совершенные с использованием так называемых методов социальной инженерии, когда преступники, например, звонят клиентам и вымогают у них различные пароли, секретные слова, информацию о карточках, о пин-кодах.

У Сбербанка около 300 дочерних компаний, и одна из них под названием «Безопасная информационная зона» («БЕЗОН») занимается защитой системы Сбербанка, тестиру-

ет наши продукты, участвует в расследованиях и очень тесно взаимодействует с правоохранительными органами по расследованию разных инцидентов.

Несколько слов о центральных элементах нашей инфраструктуры безопасности. Это упомянутый выше Операционный центр, задача которого защищать все системы Сбербанка, в том числе в тесной координации и при поддержке партнеров, таких как «Ростелеком». Его сотрудники выявляют различного рода вредоносную активность, анализируют и передают информацию в компетентные органы.

Важно, коллеги, посмотреть на другой центр, о котором я также упомянул, - Центр мониторинга, элементы инфраструктуры которого работают на стороне клиента. Я люблю приводить пример, что, если какая-то бабушка, проживающая в Саратове, вдруг неожиданно во Владивостоке снимает все деньги со своей карточки, механизмы в нашей инфраструктуре безопасности автоматически останавливают транзакцию, мы связываемся с клиентом и предотвращаем любые попытки несанкционированного перевода денег. Масштаб проблем в этой связи достаточно высокий, и я хотел бы подчеркнуть, что если в 2016 году спасенных клиентских средств было чуть больше 270 млн. долларов, то в 2017 году эта цифра превысила уже 660 млн. долларов.

Наши системы достаточно успешны. Если в мире считается эффективной система, распознающая 83-84% атак, то наши сегодня детектируют фактически 97% любых атак и автоматически устраняют риски.

Надо сказать, что киберпреступления трансграничны. Достаточно очевидно, что национальные границы нам в этом смысле мешают. Если у преступников нет границ, а мы вынуждены спотыкаться о различного рода препоны, то мы испытываем большие проблемы для противодействия преступникам. В этой связи мы достаточно осознанно приняли решение активно развивать сотрудничество на международном уровне. У нас налажено взаимодействие с рядом американских компаний. Установлены прямые контакты с коллегами и сделаны попытки перенять лучший опыт, который был наработан.

Гармиш-Партенкирхен, Германия

Компания «БЕЗОН» в сентябре прошлого года после длительного конкурса организации «Свифт» победила в тендере и стала аудитором систем безопасности всех банков, которые входят в «Свифт». Мы активно участвовали в начале 2017 года во всех мероприятиях Давосского экономического форума. Взаимодействуем с Интерполом, подразделением INTERPOL Global Complex for Innovation. Это современная структура, которая сегодня занимается расследованиями компьютерных преступлений. Мы поддержали создание Global Centre for Cybersecurity на уровне Давосского форума, считаем, что это новый шаг возможностей для сотрудничества всем нам вместе.

Хотел бы поддержать тезис А.В.Крутских, что у нас сегодня недостаточно развита юридическая основа для сотрудничества. По сути, в мире сложилась пагубная ситуация, когда общих правил взаимодействия не существует. Нельзя не отметить, что площадка ООН здесь сегодня немножко проигрывает. Мы за то, чтобы на площадке ООН появились глобальные решения, глобальные документы, глобальные подходы к формированию единых правил, по которым будут работать и государство, и бизнес.

У нас достаточно большой рост потерь в мировой экономике от киберпреступлений. В 2017 году эта сумма достигла уже около триллиона долларов. Наш прогноз: в этом году будет рост еще на полмиллиарда. Меняется ландшафт, архитектура. Каждая компания сегодня в среднем в два раза больше испытывает DDoS-атак. Увеличилось не менее чем в два раза число хакерских группировок, которые достаточно активно атакуют прежде всего финансовый сектор. У нас ежедневно рождается 285 тыс. новых «зловредов», и около 100 млрд. долларов сегодня тратят различные компании в различных странах мира для того, чтобы поддерживать достаточный уровень своей безопасности.

Последние годы искусственный интеллект сам порождает разнообразные вирусы, адаптирующиеся к средствам защиты. У нас уже появляются преступления с криптовалютой. В 2018 году рост воровства криптовалюты был фантастическим. И атаки осуществлялись на самые современные системы, в том числе и на блокчейн.

Какие мы видим вызовы в 2018 году? Мы считаем, что финансовый сектор будет постоянно в фокусе. Ключевые отрасли экономики также будут в фокусе внимания злоумышленников. Сегодня киберпреступления вплотную приближаются к той самой черте, за которой начинается кибертерроризм.

Как бы могла выглядеть архитектура сотрудничества? Как объединить усилия элементов архитектуры защиты на государственном уровне, в том числе и в сфере бизнеса, профильных структур правоохранительных органов, Интерпола? Ответить на этот вопрос - наша с вами, коллеги, задача.

Мы сделали такую попытку. Все отрасли, все крупные компании должны построить собственные системы противодействия и минимизировать риски. Сведения о рисках должны передаваться в отраслевые центры, которые будут обмениваться информацией. Из миллиардов событий всего несколько инцидентов или рисков, которые представляют действительно интерес и которые после такого многоуровневого анализа могут представлять интерес для правоохранительных органов, автоматически передаются по нужному адресу. Возникает несколько центров, которые могли бы помогать в расследовании, содействовать международному сотрудничеству.

Приведу только один пример. Джим Снабе, руководитель компании «Маерск» («Maersk»), выступал в ноябре 2017 года в Женеве. В первые три дня, когда атаковали вирусы WannaCry и NotPetya, он потерял около 300 млн. долларов. Три дня они не знали, что делать.

Что было на нашей стороне? Сбербанк тут же собрал группу, изучил ситуацию и создал утилиту, которая блокировала распространение вируса. И мы этой утилитой поделились со всеми. Если бы компания «Maersk» в первый день знала бы об этом, уверен, что ее потери можно было бы снизить на несколько сотен миллионов долларов.

Мы видим сегодня зарождающуюся инициативу Global Centre for Cybersecurity на уровне Давоса. Почему она вызывает интерес у нас? Потому что это единение позиций бизнеса, государственных институтов, правоохранительных органов на одной площадке. Мы ее поддерживаем.

По взаимодействию с Интерполом. Мы посетили отделение Интерпола в Сингапуре, которое специально создано для расследования киберпреступлений. И по просьбе Интерпола мы даже направили своих сотрудников для оказания помощи в расследованиях. Вскрыли сеть хакеров, которая базировалась в Китае, за что я получил большое благодарственное письмо от генерального секретаря Интерпола. Мы заключили двусторонний договор с Интерполом.

Но вот на уровне ООН, структур глобального уровня у нас такого сотрудничества пока не получается. Наши консультации с партнерами говорят о том, что представители различных стран приветствуют подобные подходы, но проявляют при этом осторожность. Мы хотели бы, чтобы на уровне ООН можно было бы развернуть дискуссию в отношении некой конвенции по кибербезопасности. Интерпол мог бы нам в этом помогать. В будущем мы не исключаем, что на уровне ООН могли бы появиться новые правоохранительные органы, которые бы прозвучали, например, как Киберпол (Cyberpol).

Завершая свое выступление, не могу не сказать, что по инициативе и при поддержке Сбербанка, Ассоциации банков России, государственной программы «Цифровая экономика» 5 и 6 июля в Москве будет проходить Международный конгресс по кибербезопасности. В его рамках 5 июля мы также организуем тренинг по противодействию кибератакам у себя в Операционном центре. Полагаем, что в нашем конгрессе примут участие руководители различных министерств и ведомств, и ожидаем, что будут представители руководства страны. Хотел бы всех вас пригласить в Москву 5-6 июля принять участие в нашей конференции.

Шерстюк В.П.: *Слово главному редактору журнала «Международная жизнь», члену президиума Национальной ассоциации международной информационной безопасности Армену Гарниковичу Оганесяну.*

Оганесян А.Г., главный редактор журнала «Международная жизнь», член президиума Национальной ассоциации международной информационной безопасности: Сегодня

международное сообщество уделяет значительное внимание политическим, военным и экономическим аспектам информационной безопасности. Выведение из строя критической инфраструктуры, кибершпионаж, хакерские атаки на крупный бизнес и банковский сектор - действительно острейшие вопросы современности.

Однако давайте поговорим о не менее важном аспекте информационной безопасности - гуманитарном, а именно о безопасности детей и подростков в Интернете. «Дети - наше будущее». Никакого устойчивого развития государства, да и всего международного сообщества в целом, не может быть, если детям и подросткам как наиболее уязвимой социальной группе не будут предоставлены должная защита и права в информационном пространстве. Напомню, по оценкам экспертов, каждый третий из всех пользователей сети Интернет в мире сегодня моложе 18 лет. Это существенная цифра.

Современные дети, получив доступ к Интернету, открыли своего рода ящик Пандоры. Нельзя сказать, что его содержимое - это лишь опасности и угрозы, отнюдь нет. Всемирная паутина открывает широкие возможности доступа к развивающей информации, общению, онлайн-обучению, установлению социальных связей и простору для творческого самовыражения.

Однако виртуальное пространство таит для детей и подростков немалое число угроз. Первая и, пожалуй, наиболее серьезная опасность для детей - интернет-зависимость, или, другими словами, своеобразная «цифровая наркомания». Согласно исследованию, проведенному «Kaspersky Lab» в 2016 году, практически постоянно в Сети находятся около 56% всех опрошенных несовершеннолетних пользователей России. В США цифра чуть ниже - 51%, в Европе - 40%. Дети, ежедневно проводящие огромное количество времени в Интернете (по три-восемь часов в сутки), неизбежно дистанцируются от социума и, таким образом, перестают полноценно развиваться. Подобный образ жизни ведет к проблемам с физическим и психическим здоровьем, депрессии, бессоннице. А по словам итальянских ученых, интернет-

зависимость для некоторых людей даже способна изменить личные представления о пространстве и времени, а также повлиять на бессознательное «я», что приводит к нейробиологической патологии. Это тем более актуально для неокрепшей психики детей. Словом, «цифровая наркомания» - чрезвычайно серьезная проблема.

Вторая проблема заключается в том, что киберпространство используют в своих далеко не гуманных целях различного рода злоумышленники. Здесь можно отметить и кибербуллинг (киберхулиганство), и сексуальное преследование детей, и деструктивный контент (порнография, призывы к экстремизму, суициду через «группы смерти»).

Вышеперечисленные проблемы повсеместны, они коснулись не только США, стран Европы и России, но и стран Ближнего Востока, Азии.

По мнению известного специалиста в области современных информационных угроз Б.Мирошникова, наибольшего размаха, как и опасности, достигает деятельность трансграничных организованных преступных групп. Как правило, они работают на территории нескольких государств: изготавливают порнографические материалы на территории одной страны (иногда нескольких стран), порносайты размещают на информационных ресурсах других государств, а денежные расчеты осуществляют через банковские структуры третьих стран. В таких криминальных структурах существует четкое распределение ролей: одни лица осуществляют подбор «моделей» и изготовление порноматериалов, другие обеспечивают их рекламирование и распространение в сети Интернет, третьи обналичивают и распределяют денежные средства, поступившие в качестве оплаты. Данные обстоятельства существенно затрудняют розыск преступников, так как требуют организации расследований силами правоохранительных органов нескольких государств.

Существует огромное количество всевозможных фондов, которые занимаются надуманными проблемами с использованием надуманных методов, не приносящих никакой пользы. Создаются какие-то дорогостоящие программы по распознаванию и сопоставлению образцов. Где-то они внедряются.

Но где результаты? Никто не задает вопроса об эффективности расходования этих денег.

Еще одна очень опасная проблема касается домашних гаджетов, а именно интернет-игрушек. Эксперты отмечают, что такие игрушки сегодня легко могут взломать злоумышленники и получить доступ к домашней сети Wi-Fi, а также получить данные о ребенке или отправить ему сообщения от лица близких. Проблема заключается еще и в том, что дети, ничего не подозревая, общаются со своими интернет-куклами и другими игрушками как с обычными, а хакеры шпионят и собирают информацию. Инциденты уже были. Например, американская фирма «VTech», производитель электронных игрушек, недостаточно поработала над безопасностью приложения «Kid Connect», которое было связано со многими обучающими игрушками. В итоге оно было взломано. В руки хакеров попали даты рождения детей, их имена и имена их родителей, почтовые и электронные адреса. Утечка затронула всего около 3 млн. детей. От нее пострадали пользователи из США, Австралии, Великобритании, Китая, Германии, Франции и других стран Западной Европы, Азии и Латинской Америки. В итоге компания была оштрафована на 650 тыс. долларов.

К сожалению, и сами дети нередко переходят на «темную сторону» интернет-пространства. Громкая история произошла с 15-летним британским мальчиком-аутистом Кейном Гэмблом, который умудрился проникнуть в компьютеры высших чинов американских разведслужб. Он не только терроризировал семьи госслужащих различными сообщениями, но и разместил в Интернете данные 20 тыс. сотрудников ФБР.

Взвешивать «за» и «против» использования детьми Интернета - занятие бессмысленное. Цифровизация общества - процесс необратимый. Как сказал известный американский экономист и трейдер Нассим Талеб: «Само по себе развитие благотворно и неизбежно, вопрос лишь в том, как мы к нему адаптируемся. Если общество недостаточно быстро приспосабливается к изменениям, его ждет коллапс». Причем в самых чувствительных областях.

Гармиш-Партенкирхен, Германия

Семинар - «круглый стол» №1

«Актуальные проблемы информационной безопасности в контексте развития цифровой экономики»

Кузнецов С.К., заместитель председателя Правления Сбербанка России: Хотел бы особо отметить, что в 2018 году в России усилиями нескольких ведомств была разработана программа «Цифровая экономика», и летом было принято решение на уровне Правительства Российской Федерации дать старт ее реализации. Параллельно с программой «Цифровая экономика» ведущими компаниями страны была учреждена автономная некоммерческая организация «Цифровая экономика», чтобы уже совместными усилиями обеспечивать экспертную оценку профильной деятельности федеральных ведомств.

Было создано пять направлений, и по согласованию с Советом безопасности России пятым направлением как раз стала «Информационная безопасность». На данном направлении задействовано два органа: Центр компетенций и рабочая группа. Центр компетенций доверили возглавить мне, а рабочую группу возглавляет моя коллега Наталья Касперская, которая еще является владельцем компании InfoWatch. Почему правительство применило эту схему?

На наш взгляд, решение является достаточно уникальным, потому что правительство привлекло к широкому обсуждению экспертное сообщество, бизнес-сообщество в нашей стране. Центру компетенций было предложено составить некую программу, в рамках которой должны по согласованию с различными федеральными министерствами и ведомствами реализовываться ряд мероприятий с конкретным финансированием на период до конца 2018 года.

В первом большом нашем совещании приняло участие около 450 экспертов из 230 компаний. Мы договорились сначала

сделать диагностику отрасли информационной безопасности в целом - ее состояние, проблемы, успехи и неудачи. В течение месяца была проведена такая диагностическая работа. В итоге был собран достаточно объемный материал, который мы систематизировали и затем заложили в основу первого плана мероприятий по информационной безопасности.

В ходе работы выявилось отсутствие единой архитектуры построения информационной безопасности. При этом активная роль и широкие полномочия в ее разработке были предоставлены бизнес-сообществу. Такого, по сути, никогда не было. Это уникальный опыт. И мы с большой благодарностью восприняли это доверие.

Для нас принципиально важно поддержать запуск программы «Информационная безопасность» в рамках «Цифровой экономики» в России, в том числе и посредством обмена опытом с зарубежными структурами, запустить на этом треке механизмы международного взаимодействия, выработать общие правила.

К слову о проектной работе, наша компания, Сбербанк России, объявила о строительстве умного города, так называемого Смарт Сити, который будет построен в двух километрах от МКАД, в местечке, которое называется Рублево-Архангельское, на площади 460 га земли. Именно в этом городе мы планируем применить самые современные технологии, и что важно - другие отношения между людьми, между людьми и машинами в том числе. Мы видим, что и правоохранительная сфера должна быть совершенно другой и построена по другим принципам. И в этом смысле даже нашли поддержку в МВД, которое готово испытать в умном городе (Смарт Сити) ряд пилотных инициатив. Каким будет город, пока еще вопрос открытый, и мы приглашаем всех к этой дискуссии подключиться.

В контексте расширения взаимодействия по нашей тематике есть важный тезис, который хотелось бы озвучить: крупные компании сегодня научились защищаться, научились противостоять киберугрозам, но что делать средним и малым компаниям? Их бюджет не позволяет тратить деньги на дорогостоящие системы, а уровень риска не ниже. Может быть, есть

необходимость создать некую единую платформу, подключение к которой даст новую гарантию безопасности для таких экономических структур. Это вопросы и для нашей сегодняшней дискуссии.

Информационные риски глобальной цифровой трансформации: взгляд из России

Смирнов А.И., Национальный институт исследований глобальной безопасности: Уважаемый коллеги, у меня будет несколько иной взгляд на проблему, поскольку цифровая экономика, ИКТ, технологии двойного назначения несут в себе существенные риски. Постараюсь очень кратко их «пролистать» с комментариями.

Для начала - несколько цитат для осмысления моего подхода. Например, Герберт Маршалл Маклюэн, известный канадский социолог сказал, что «смена исторических эпох определяется сменой информационных технологий». Мы за 20 лет прошли четыре исторических эпохи, если считать веб-1, веб-2, веб-3 и когнитивный веб. Далее, конечно, Клаус Шваб: «История войн - это история технологических прорывов». И, наконец, хочу процитировать Президента России насчет искусственного интеллекта: «Это не только будущее человечества, но и колоссальные угрозы. И тот, кто станет лидером, тот будет властелином мира».

Мы переживаем непростые времена: ломка существующего миропорядка, информационная революция, цифровизация экономики, гибридные войны - они порождают и новые вызовы, где ИКТ-составляющая является доминирующим или, как минимум, неотъемлемым элементом.

Информационный нарратив сегодня резко расширился. Это документы ООН, БРИКС, ШОС, СНГ, ОБСЕ и решения на национальных уровнях. И в этом плане хотелось бы еще подчеркнуть, что у нас в Стратегии национальной безопасности четко изложено, что информационная сфера - это сфера, где мы должны максимально быть сконцентрированы. То же и в других документах, которые появились у нас, - «Доктрина информационной безопасности», «Стратегия на-

учно-технологического развития», «Доктрина экономической безопасности».

Клаус Шваб написал замечательную работу, уходя с поста президента Всемирного экономического форума в Давосе. И мы видим, что Германия первой в 2011 году разработала программу «Индустрия 4.0» и что заявил немецкий министр иностранных дел, когда выступал на ее презентации через два года. Он сказал, что все замечательно, но только сети биг-дейт, которые собирают данные всей цифровой экономики Германии, почему-то принадлежат четырем фирмам, которые базируются в Калифорнии, в Силиконовой долине.

Наконец, следующий момент, который хотелось бы подчеркнуть. Вот в «Стратегии нацбезопасности» 2017 года термин «кибер» употреблен 45 раз, в прошлой «Стратегии» было 30 раз, я подсчитал специально. И плюс подчеркивается, что ревизионистские силы Китая, России используют технологии пропаганды и принуждения. Кто, собственно, автор термина «гибридная война»? Джеймс Мэтис. Статьи по этой теме он опубликовал еще в 2006 и 2009 годах. Сами из гибридных войн не вылезают и при этом вовсю обвиняют Россию. Активно раскручивают тезисы, что «Россия приблизилась к военным базам НАТО», «Россия хочет войны», а сами первыми создают информационную и киберинфраструктуру наступательного характера: Рижский центр, Таллинский центр, Вильнюсский центр, сейчас появился центр «противодействия» гибридным угрозам в Хельсинки.

Евросоюз тоже не хочет отставать от США и НАТО. В условиях «Индустрии 4.0» Евросоюз уже с 2011 года начал заниматься стратегией кибербезопасности. Много очень разработал документов, директив. Мы в России отстаем. Нам бы хотелось сотрудничать с Евросоюзом, видимо, и европейцы не против. Но старший брат из-за океана сказал: «Нельзя».

Если посмотреть в целом на события в мире, то человечество идет к войнам нового поколения. Информационная составляющая в современных гибридных конфликтах начинает превалировать над боевой, военно-дипломатической, экономической. Информационный и киберпрессинг неизбежно влияет на целевую аудиторию в другой стране. Новые

технологии давно уже вышли за рамки технической сферы и стали фактором геополитической конкуренции. Нам нужно максимально объединять усилия, по крайней мере в нашем формате, идти к цифровому Вестфалю.

Вопросы международного сотрудничества при обеспечении информационной безопасности в организациях кредитно-финансовой сферы

Сычев А.М., Банк России: Если позволите, хотел бы пару слов сказать как представитель регулятора.

Мы пытаемся здесь заниматься каким-то смешением понятий, не учитывая, что на сегодняшний день во всех юрисдикциях существует достаточно обширное законодательство, связанное с обращением информации.

Например, в любой стране есть понятия «банковская тайна», «персональные данные», - они закреплены, как правило, на уровне федеральных законов, где в каждом законе установлен свой режим обработки той или иной информации. То, о чем вы говорите, очевидно не относится к этому типу данных. Речь идет, скорее, об обработке тех данных о себе, которые граждане достаточно спокойно размещают в информационном пространстве, не задумываясь о последствиях.

Действительно это бесценный массив данных, который можно использовать как в маркетинговых, так и в противоправных целях. Но обращу внимание, что это не имеет никакого отношения к законодательным инициативам, которые мы здесь с вами пытаемся обсудить. Это немножко другая тема. Если мы говорим с вами о законодательстве, то вопрос обмена этой информацией на государственном уровне все-таки решен. Он регулируется в том числе и законодательными актами, и межправительственными соглашениями.

Например, что касается банковской тайны, то ЦБ РФ участвует в наблюдении за сетью передач финансовых сообщений СМИ, и в рамках этой процедуры он имеет возможность получать конфиденциальную информацию о деятельности организации. Или если мы с вами говорим о платежной информации, то это регулируется соглашениями между двумя

субъектами. Поэтому говорить о том, что на сегодняшний момент в передаче информации и ее правовой защите есть правовой вакуум, наверное, не совсем правильно.

Можно говорить о том, что какие-то сферы обращения этой информации действительно требуют дополнительной проработки. Да, я с вами согласен, насчет обращения той информации, которая свободно размещается нашими гражданами в социальных сетях, на других ресурсах в сети Интернет. Она обрабатывается и дальше распространяется, вне зависимости от их желания. Это действительно требует обсуждения.

Но все-таки режим защиты информации установлен, он определен и национальным законодательством, и межправительственными соглашениями и далее технически обеспечивается в соответствие с тем, какого рода эта информация.

Возвращаюсь к вопросу о том, что же такое сайдер секьюрити и занимается ли этим кто-нибудь или никто не занимается. На самом деле на международных площадках, помимо ООН, существует достаточно большое количество организаций, которые тем не менее занимаются этой проблемой - киберустойчивостью.

На сегодняшний день мы можем говорить о трех составляющих. Во-первых, то, что касается инфраструктуры. Во-вторых, это требование к безопасности организаций, которые предоставляют аутсорсинговые услуги. В-третьих, ситуационная осведомленность.

Почему мы выделяем процессы, связанные со сторонними организациями? Вся финансовая отрасль не сама переводит деньги. Она использует для этого достаточно большую инфраструктуру, на которую влияния оказывать не может. В качестве примера приведу ситуацию двухлетней давности, когда вся Скандинавия лишилась в один «прекрасный» момент всей банкоматной сети только потому, что один-единственный провайдер связи производил у себя на оборудовании ремонтные работы. В результате того, что все работы были произведены неправильно, три государства остались без банкоматов. Хорошо, что это длилось недолго, но тем не менее такая ситуация стала возможной.

Если говорить о Российской Федерации, мы на самом деле не так далеко ушли от скандинавов. У нас, конечно, диверсификация операторов связи побольше будет, но были ситуации, когда несколько банков не могли проводить транзакции только потому, что их обслуживал один аутсорсинговый партнер.

С точки зрения выправления данной ситуации ЦБ РФ работает по ряду направлений. Прежде всего, это внесения изменений в законодательство для того, чтобы можно было обеспечить эту самую киберустойчивость, включая все работы, связанные с обменом информацией о лицах, через которые выводят ворованные деньги или которые осуществляют воровство денег.

Хотел бы обратить внимание, что российские банки, включая Сбербанк, живут не только по требованию европейского законодательства, но в первую очередь по требованиям регулятора - Центрального банка. Ситуационная осведомленность для нас - это один из ключевых моментов в обеспечении киберустойчивости финансовой отрасли. С точки зрения регуляторных актов и того, что на сегодняшний день мы имеем, это достаточно серьезная масштабная работа, проведенная в Банке России.

Два стандарта серии ГОСТ, которые будут обязательны к применению в российских финансовых организациях, формировались не только на основе российского опыта, но и зарубежного, с учетом мнения не только регулятора, но и достаточно большого круга участников финансового рынка.

Ныне как государственный стандарт такие документы существуют. Один из них - это «Общие требования и технические требования к процессам обеспечения информационной безопасности в кредитно-финансовой сфере для обеспечения устойчивости», и второй - это «Методика оценки соответствия тем требованиям к тому, что реализовано на самом деле».

По ситуационной осведомленности. Существуют некоторые результаты работы того самого центра мониторинга реагирования на компьютерные инциденты кризиса в финансовой сфере, что называется finCERT. Могу похвастаться тем, что количество участников информационного обмена, из которых около 70% сейчас являются активными, у нас

максимальное по отношению даже к крупнейшим мировым CERTам. Количество информационных бюллетений, которые мы направили, - это только о таргетированных атаках, которые были сделаны в момент их выявления и которые имеют действительно серьезные последствия.

В отличие от большинства государств кредитно-финансовой системы Российская Федерация в прошлом году и в этом достаточно хорошо выглядела применительно к атакам. По вирусам-шифровальщикам, которые хорошо ходили по миру, одна-единственная кредитная организация имела проблемы на полдня, и все.

Не скажу, что это заслуги ЦБ, но те требования, которые представляет, соответственно, ЦБ, и ситуационная осведомленность, которую мы предоставляем компаниям, способствуют тому, что большинство из них готово к таким ситуациям.

Мы по-прежнему считаем, что взаимодействие с участниками рынка, информационное взаимодействие с другими участниками финансовой системы, не банками, для нас является крайне важной задачей. Безусловно, все это может быть понятно только тогда, когда есть вполне осязаемые экономические показатели.

Расчет на сегодняшний день это пять тысячных процента потерь от общего финансового оборота электронных денег в России. Считаем мы этот показатель по двум основным направлениям.

Это по официальной статистике, которую мы получаем от других организаций. Возможно, наша статистика не всегда отражает реальную ситуацию, именно поэтому мы ее совершенствуем и выходим на перепроверку данных через балансы кредитных организаций. Следовательно, говорить о том, что мы не можем перепроверить реальную статистику, тоже будет неправильно.

Показатель доверия, то есть как население доверяет финансовым технологиям с точки зрения безопасности. Это показатель, который измеряется путем социологических опросов. Причем двумя путями, чтобы опять же была перепроверка этих данных. Это запрос непосредственно у населения, и это запрос у самих кредитных организаций, а дальше идет собственно сложная процедура математической выверки двух этих показателей.

К международному сотрудничеству. В рамках Евразийского экономического союза у нас есть договоренность между четырьмя центральными банками об оперативном обмене информацией о тех проблемах информационной безопасности, которые возникают у нас в рамках своих юрисдикций. Мы готовимся к переходу на обмен информацией в том числе о тех счетах, через которые выводятся ворованные деньги. Там есть проблемы на уровне юрисдикции некоторых наших коллег, например в Белоруссии крайне жесткое законодательство в плане банковской тайны, и им еще придется проделать некоторые шаги для того, чтобы его немножко либерализовать. Но тем не менее работа такая есть, соглашения такие есть и такой обмен ведется.

В рамках ЕАЭС основная проблема в том, что каждое из наших государств считает правильным использовать свою родную криптографию, а уполномоченные органы не могут договориться о самых элементарных вещах. Этот вопрос здесь почему-то не обсуждается, а зря. Например, по результатам расследования инцидента, связанного с группой сайдеров Кобальтстрайк, мы имели информацию о банках, которые эта группа собиралась атаковать. В других юрисдикциях эта информация была передана в соответствующие CERTы. Надо сказать, что мы получили от них благодарность, потому что оперативно было отработано. Кстати, швейцарские банки тоже «попали под раздачу».

Напоминаю, что в плане обмена информацией существует такая замечательная организация, как IOSCO (International Organization of Securities Commissions), в рамках которой есть свой информационный обмен, который точно так же позволяет нам оперативно выходить на остановку денежных средств и предотвратить непосредственное попадание денежных средств, похищенных у наших клиентов, в руки преступных сообществ, которые находятся в других юрисдикциях.

У нас еще много чего не хватает в международном праве, но, может, имеет смысл подумать о том, как использовать имеющиеся механизмы, которые сейчас закреплены в праве каждой из юрисдикций для того, чтобы обеспечить ту самую кибернадежность.

Андреас Кюн, Институт Восток - Запад, США: *Китай принял новый закон с жесткими требованиями, которые касаются банков. Видите ли вы аналогичное развитие событий в России?*

Сычев А.М.: *Если речь идет о регулировании криптовалют, то в Российской Федерации сейчас есть два законопроекта, касающихся обращения криптовалют, - это Закон о краудфандинге, то есть Закон ICO, и Закон о цифровых активах. Они достаточно жесткие. Но позиция ЦБ однозначна - обращения на территории Российской Федерации криптовалют как денежного средства и средства платежа нет и не будет в ближайшей перспективе. Если же вы говорите о вопросах, связанных с обеспечением безопасности, на самом деле требование к информационной безопасности в Российской Федерации гораздо жестче, чем в Китае. При этом мы мягче подходим к требованиям информационной безопасности, чем в Сингапуре. Там коллеги достаточно твердо выстраивают свою политику по отношению к информационной безопасности поднадзорных организаций, включая и вновь появляющиеся финтехкомпании. Мы считаем, что здесь пока «закручивать гайки» рано. Надо делать это постепенно.*

Почему важны правила в глобальной цифровой экономике?

Рафал Рогозинский, SecDev Group, Канада, Международный институт стратегических исследований, Великобритания: В прошлом году я был удостоен чести стать экспертом Всемирного банка, работал с правительством России по развитию программы для цифровой экономики, так что достаточно знаком с работой Банка в сфере реализации госспроектов с привлечением частного капитала. Меня поразило, насколько правительство России готово сотрудничать с частным сектором.

В своем коротком выступлении затрону ряд насущных проблем кибербезопасности и киберзащиты, которые касаются развития национальных программ и стратегий. Эта презентация предлагает некоторые статистические данные, необходимые для понимания важности цифровой экономики для национального развития.

Гармиш-Партенкирхен, Германия

Почему цифровая экономика важна для национальной экономики - это довольно просто. Из 107 трлн. долларов всемирного ВВП в следующем году, по предположениям Всемирного банка, около 26% будет относиться к цифровой экономике. Если вы понимаете, что 107 трлн. долларов включают перемещения всех товаров и услуг, то 26% - это крайне значимая сумма, и это объясняет, почему защита данного сектора так важна для стран. Другая цифра, важная для понимания, - это то, что за следующие пять лет примерно 1 трлн. долларов в год будет потрачен на обеспечение кибербезопасности. Почему? Ответ прост. В прошлом году был рост киберпреступлений до 2,2 трлн. долларов, что в пять раз превзошло статистику 2015 года. С каждым годом, согласно статистике Всемирного банка, рост количества кибератак составит примерно 26%. Крупные корпорации потеряют 11,3 млн. долларов на последствия преступлений против их инфраструктуры. Как уже было сказано, количество вредоносных программ увеличивается в разы по всему миру. Довольно интересно, что самые подверженные киберпреступности страны - это Россия и Китай.

В чем главные причины проблем с кибербезопасностью? Они лежат на поверхности и заключаются в том, что на основном техническом уровне созданные нами системы проектировались как эластичные, а не безопасные. Другими словами, совместимость технических особенностей Интернета не подразумевает уровня контроля, необходимого для того, чтобы иметь высокую степень уверенности в доступности и целостности информации. Несмотря на то что частным сектором были потрачены триллионы долларов на кибербезопасность, она все еще находится в зачаточном состоянии. Это не развитая наука, где интересы бизнеса и обязательства государства расходятся.

Есть наиболее прозрачный ряд данных, который покажет, что индустрия кибербезопасности находится в зачаточном состоянии. 92% всех вредоносных программ используют один механизм контроля - DNS. В прошлом году в США только 30% из списка Fortune 1000 имеют техническое представление о DNS. Если 92% всех вредоносных программ используют один канал управления и только треть из наиболее

дорогих компаний США имеют представление об этом, то у нас есть пропасть между проблемой и ее техническим пониманием.

90% самых больших индустриальных концернов в мире не доверяют безопасности системы интернет-управления приборами (Internet of things), хотя эти самые компании будут инвестировать во внедрение IOT, во много раз увеличивая количество компьютеров - в пять или шесть раз от того, что есть сейчас. Причина, почему они не доверяют безопасности IOT, состоит в том, что сегодня самыми эффективными способами определить вредоносные программы и проникновение хакера является использование аналитики пользователей. Это означает анализ взаимодействия между человеком и устройствами, выявление аномального поведения.

IOT построен на сообщении компьютеров, и эта уязвимость существует лишь потому, что у нас нет опыта и понимания этой технологии. Последние 90% - самые важные. 90% всех успешных проникновений в банки или корпорации использовали человеческий фактор для попадания в организацию. Другими словами, они используют человеческую слабость для проникновения в систему, вместо того чтобы использовать технологическую брешь.

Несколько лет назад в США оборонным предприятием был проведен эксперимент. В эксперименте флеш-накопители оставили на стоянке этого оборонного предприятия. Удивительно, но 60% сотрудников данного учреждения подняли эти флешки и вставили в свои рабочие компьютеры. Когда этот же эксперимент был проведен с CD-диском с названием компании на нем, 90% вставили их в свой компьютер.

Интересно отметить, что такие уязвимости, как WannaCry, могли быть предотвращены. WannaCry использовал тот канал управления, о котором я говорил ранее. Если бы компании, включая российские, следили бы за DNS и блокировали DNS, WannaCry бы не имел таких серьезных последствий. На самом деле комбинация использования человеческого фактора с брешами в коде программ является одной из главных проблем для корпораций. В прошлом году Maersk потерял 99% своей инфраструктуры. Они были

вынуждены прекратить работу в 73 грузовых портах по всему миру. Если бы у них не было шести компьютеров в Нигерии, которые не были подключены к сети, то они бы не смогли восстановить свои финансовые и логистические системы. Потери Maersk составили более 1 млрд. долларов, они потеряли 10% своего международного бизнеса, а они являются самой большой транспортной компанией в мире. Это больше не может восприниматься как помеха, это вопрос существования.

Что делать? Первое и самое важное - изменение менталитета, понимание, что кибербезопасность - это не только технологический вопрос.

В чем разница между информационной безопасностью и кибербезопасностью. В Северной Америке или в англоязычном мире есть разница между кибербезопасностью и защитой киберпространства. Кибербезопасность - это ряд практик, которым стоит следовать. Защита киберпространства - это комплексный подход к пониманию отношений, подразумевающий, что у вас есть обязанности, которые вы должны выполнять.

Вопрос лишь в скорости реакции и плане обеспечения устойчивого функционирования. Защита киберпространства в отличие от кибербезопасности на сегодняшний день является ключевым словом. Она требует комплексного подхода, чтобы отреагировать на меры, которые комбинируют технический и функциональный компоненты и подразумевают стратегический подход к проблеме.

На национальном уровне это означает, что государство должно предоставить общие принципы защиты киберпространства на долгосрочную перспективу. В Соединенном Королевстве это вылилось в подход, который различает три категории: защита, сдерживание и развитие. Защита сетей и ресурсов, которые в этом нуждаются, сдерживание субъектов, действующих противоправно, и развитие возможностей, которые могут быть применены в будущем.

В категорию защиты входит создание активного подхода к защите киберпространства, который в равной мере относится к обороне и наступлению как к единому целому и не во

всяком случае начинает процесс обороны с периметра сети. Он включает распознавание целостности государственных сетей как основного приоритета, не только техническую целостность, но и информационную целостность сетей. Он включает обеспечение охвата и реагирование для обеспечения безопасности инфраструктуры. Один из примеров - это создание Национального центра кибербезопасности как основы для защиты национальных предприятий от киберугроз, использующего возможности правительства по отслеживанию сигналов. Второй компонент - это кампания по осведомлению общественности о киберугрозах. Другими словами, создание основных правил для пользователей, начиная с школьного периода и до того, как они устраиваются на работу.

Сдерживание подразумевает работу с целью снизить уровень киберпреступности, создать возможности противостоять влиянию враждебно настроенных иностранных субъектов, включая террористов, развивать военные кибервозможности, чтобы отвечать иностранным субъектам, угрожающим национальной инфраструктуре.

Приоритетами в сфере развития являются оттачивание кибернавыков в рамках национальной экономики, стратегическое инвестирование в кибербезопасность, поддержка исследований и разработок, инвестирование в начальное образование.

Несколько заключительных мыслей. Только сейчас мы начинаем видеть значимость цифровой экономики и появляющиеся для нее угрозы. Важно понимать, что сам Интернет, те, кто им пользуется, очень молоды. Глобально средний возраст пользователей до 25 лет - это молодые люди, только вошедшие в самые продуктивные годы своей жизни, которые, скорее всего, изменят положение вещей. Они экспериментируют, и некоторые эксперименты приводят к киберпреступлениям. Их поведение больше не контролируется так, как это было с нашим поколением: семьей, школой, институтом, вместо этого они напрямую взаимодействуют с интернет-ресурсами. Это приводит к изменению в культурной среде, что как на Западе, так и в России привело к новым формам политики и нестабильности. Такой порядок останется еще, по крайней мере, на ближайшие 20 лет.

Также нужно отметить, что доступ в Интернет значительно увеличивается, но глобально только 30% населения пользуются ресурсами, на которых мы строим свою модель. Что́ следующий миллиард пользователей сделает, чтобы изменить эту среду, будет крайне важным.

Правительство России осознало во время создания национальной программы, насколько глобально важна роль Евразии в этом процессе. На данный момент 70% Интернета находится в Евразийском регионе: Россия, Китай и другие. Более того, благодаря этому региону инфраструктура ICT увеличилась на 50%. На самом деле именно данный регион будет задавать направление остальному миру, так что решения, которые вы принимаете, как вы формулируете путь вперед, будут крайне важны.

Цифровизация экономики и обеспечение информационной безопасности: опыт Республики Беларусь

Курбацкий А.Н., Белорусский государственный университет: Мы - небольшая страна, молодое государство. У нас, можно сказать, и не выработались стабильные традиции управления страной - и это в эпоху глобальной цифровизации, наверное, не так уж и плохо. Можно строить некоторые новые модели и схемы без особого сопротивления чиновников. Где-то в традиционных сферах мы притормаживаем, где-то в новых сферах мы можем двигаться вперед без оглядки на традиции. Собственно, как некоторый экспериментальный полигон цифровых страновых инноваций мы можем быть интересны, особенно для евразийского пространства.

Многие тренды глобальной цифровизации (особенно негативные) в небольшой стране можно раньше заметить, чем в больших традиционных странах, - у нас меньший запас прочности по многим параметрам, мы более чувствительны к угрозам. Но для анализа таких тенденций нужна хорошая экспертиза, профессиональное экспертное сообщество. И здесь начинаются проблемы. Мы часто в дискуссиях говорим: вот нужно собрать экспертов, пообсуждать, чтобы не попасть под

фейковую волну СМИ, которые, как образно выразился в докладе на форуме Гармиш - 2018 С.М.Бойко, стали ведущей движущей силой, за которой выстроились традиционные руководящие силы. Что мы можем противопоставить фейковой волне? В первую очередь мнение экспертов. А где взять экспертов? Система образования, университетская среда все меньше справляются с их подготовкой. Потенциальные эксперты массово уходят в бизнес, особенно цифровой, и не сильно стремятся работать на страну. Относительно независимое экспертное сообщество резко сокращается. В небольшой стране, как Беларусь, это особенно заметно.

С этим связана и наша недооценка процессов, происходящих с молодым поколением, которое быстро погружается в цифровой мир, по сути, живет в нем. И, конечно, система образования медленно адаптируется к таким реалиям. В частности, мы мало задумываемся о проблеме идентичности молодежи в небольших странах, особенно новых странах. Мы вроде бы и понимаем, что, если нет молодежи, у страны нет будущего. Но действуем зачастую без серьезного учета современных тенденций. Как воспользоваться глобальной цифровизацией, чтобы обеспечить стабильную среду и общество для молодого поколения? Как бы мы ни критиковали процесс цифровой глобализации, мы его не остановим. Но есть смысл активно в нем участвовать, находя компромиссные решения и формируя цифровой суверенитет стран, тем самым их же и сохраняя.

У небольших стран стоит проблема своей идентификации в глобальном мире. Многие молодые государства не оставляют попыток сформировать национальные государства по некой как бы традиционной схеме: этнос - язык - культура и т. д. Наверное, в наше динамичное время они точно уже опоздали. Тогда зачем нам загонять себя в прокрустово ложе этнонации? Сейчас эта модель практически не работает или работает в направлении регресса. Тогда зачем экспериментировать над целыми странами, если можно попробовать пойти «другим путем». Сложно для новых молодых поколений, формирующихся в рамках глобальных инициатив, сформировать на основе идеи этнонации некие основополагающие жизненные

ориентиры. Разве что для некоторых периферийных недостаточно образованных, совсем без всяких ориентиров, либо для той части, которая сознательно участвует в разрушении государства и страны за внешние гранты.

С нашей точки зрения, чтобы сохранить страну и государство, интереснее было бы формировать у молодого поколения понятие цифровой нации. Если уж мы привыкли к термину «нация», то можно его использовать с новым содержанием и контекстом. Можно сказать и так: в возможной паре «этно+цифра» поменять местами (поменять приоритеты) «цифра+этно». Наверное, для молодежи такое сочетание будет гораздо понятнее.

Можно, конечно, настаивать на уточнении: что мы понимаем под цифровой нацией? Но пока, возможно, достаточно и следующего объяснения. Ну нравится многим термин «нация», хочется ощущать себя особенным, отличным от других, не раствориться в глобализации, быть полноценной страной - так и идем на разумный компромисс. Как это сделать? Если не затрагивать прямолинейно политические аспекты, то можно сказать, что один из основных механизмов - это образование. Нужно срочно формировать эффективное образование, соответствующее текущей цифровой трансформации общества.

Есть ли предпосылки для формирования такого образования? Одним из опорных процессов может стать стремление к цифровому суверенитету.

Проблемы информационной безопасности подталкивают власть к тенденции обеспечить цифровой суверенитет (как свойство самосохранения, хотя, конечно, не все это ясно понимают). И идея цифрового суверенитета может послужить хорошим стимулом для перестройки образования. Понятно, что этот процесс долгий, но лучше его начинать, чем все время находиться в ожидании, что что-то станет лучше.

Один из известнейших философов современности (весьма популярный в молодежной среде) Нассим Талеб сказал: «Само по себе развитие благотворно и неизбежно, вопрос лишь в том, как мы к нему адаптируемся. Если общество недостаточ-

но быстро приспосабливается к изменениям, его ждет коллапс. Но и слишком быстрое приспособление превращается в регресс: общество начинает терять то хорошее, что у него было до того, как начались перемены… Патология нашего времени - потеря контакта с реальностью». Не нужно впадать в эйфорию, которая достаточно заметна в мировом сообществе, в первую очередь благодаря бизнесу, от цифровизации, искусственного интеллекта, блокчейнов, будущего образования и т. д. Бизнес утверждает, дайте нам свободу и мы изменим к лучшему экономику, политику, образование и общество в целом. Но так ли это?

Сейчас много говорят о социальной ответственности бизнеса. Конечно, было бы идеальным, если бы бизнес был более социально ответственен за свою цифровую продукцию. Но, к сожалению, слишком раскрученная (иногда заведомо искусственно) конкуренция в цифровой сфере за прибыль не даст решения этой проблемы за приемлемый срок. Гонка за прибылью, как правило, не сопровождается анализом, насколько цифровая продукция полезна и безопасна для общества, - ведь такой анализ слишком затратен.

Обычно, когда мы говорим о киберпространстве, то в первую очередь ассоциируем его с интернет-пространством, хотя понимаем, что киберпространство - это не только Интернет, это государственные, банковские, ведомственные, частные сети во всех взаимосвязях. Развитие ИКТ происходит столь стремительно, что даже эксперты не в состоянии осознать всех рисков, которые несет за собой такая интеграция. На базе данных сетевых инфраструктур идет стремительный процесс интеграции финансовых, торговых, промышленных систем, систем жизнеобеспечения, СМИ.

Новые ИКТ порождают новые глобальные инициативы в виде комплексных глобальных проектов, которые включают целый ряд интегрируемых ИКТ. Мы часто не можем гарантировать безопасность и надежность в рамках одной ИКТ, что уж говорить, если они еще интегрируются. И если на прогнозирование функциональности таких проектов затрачиваются большие ресурсы и средства, то безопасность и надежность исследуются по остаточному принципу.

Нужен разумный компромисс между радикальными тенденциями от бизнеса и достаточно консервативной ролью государства. Для разумного компромисса опять же нужна экспертная среда. А такая среда - это прямое следствие эффективного образования, в первую очередь университетского.

Быстрая цифровизация мирового сообщества резко обострила проблемы и, пожалуй, даже кризис традиционного университетского образования. Эти проблемы носят мировой характер. Будущее традиционных университетов под вопросом. Даже мировые лидеры образования не могут быть уверены в завтрашнем дне. По сути, многие университеты живут чуть ли не в парадигме средних веков (когда массово появились европейские университеты). Сейчас, конечно же, нужна новая парадигма университетов. Ведь что ценно было в традиционном университете: преподаватели и эффективный доступ к информации. Основное информационное хранилище - библиотека. Попросту говоря, хорошие преподаватели и хорошая библиотека и определяли качество университета. Интернет «разрушает» традиционные библиотеки и создает конкуренцию преподавателям.

Если говорить о Беларуси, то у нас было действительно хорошее высшее образование, которое готовило технократическую элиту. Благодаря этому мы и имеем сегодня Парк высоких технологий (ПВТ), удачные стартапы. Но, к сожалению, советский запас прочности мы исчерпали. Нужны «новые университеты» для технократов. Как их построить? Только через эксперименты. При этом нельзя разрушать то, что есть, - БГУ, БГУИР, БНТУ и другие. Но нужно дать возможность проводить эксперименты в образовании. Естественной площадкой для таких экспериментов может стать ПВТ. На основе удавшихся экспериментов можно в дальнейшем создавать совершенно новые образовательные структуры и мягко модифицировать уже существующие.

Собственно, по такому пути экспериментов идут и мировые лидеры образования. Сначала ведущие американские университеты (в первую очередь Массачусет, Стенфорд, Гарвард), затем в процесс включились передовые университеты ЮВА (Китая, Японии, Южной Кореи, Сингапура), сейчас уже и не-

которые европейские и российские университеты. Один из самых значимых трендов - это быстрое развитие дистанционного образования в виде образовательных онлайн-платформ. Самая известная такая платформа Coursera - это стартап в сфере онлайн-образования, основанный профессорами Стенфорда, который позволяет пройти полный интерактивный курс университета пока бесплатно. Например, в 2016 году обучалось более 15 млн. человек.

Традиционно в Беларуси было неплохое ИТ-образование. Но в 1990-х годах в университетской среде уже стало понятно, что если не предпринимать никаких шагов, то мы будем готовить ИТ-специалистов для внешних стран, пока не исчерпаем запас прочности университетов. Поэтому за три года университетским экспертам удалось убедить государство предпринять определенные шаги. В 2001 году появился указ Президента РБ о создании научно-технологической ассоциации «Инфопарк БГУ». Примерно четыре года убеждали бизнес поверить в эти процессы. Как следствие, в 2005 году появился декрет президента о ПВТ. Основной вид деятельности - разработка программного обеспечения. Массовый процесс оттока ИТ-мозгов остановили. Но активно развивалась в основном модель аутсорсинга. Это ускорило, однако, и исчерпание продуктивного ИТ-образования.

Большая часть компаний работает по следующей схеме. В основном заказы из Северной Америки и Западной Европы и, соответственно, оттуда же и спецификации на разработку программного обеспечения (ПО) и информационных систем (ИС). В итоге - в ПВТ в основном центры разработки. При этом зарплата программистов в такой модели существенно выше, чем на внутренних проектах. Но во внутренних проектах поддерживаются все этапы жизненного цикла разработки программного обеспечения и информационных систем, а на зарубежных только несколько этапов.

Соответственно, под эту же схему медленно, но подстраивалась и система ИТ-образования (а это как раз и опасно для страны). Мы потихоньку скатываемся к образованию по эксплуатации ПО и соответствующих систем. В ведущих университетах, которые готовят ИТ-специалистов, много

учебных центров и классов по Microsoft, Oracle, Cisco, SAP и т. п. Но это не центры R&D, а банальные центры навыков, компетенций по простому кодированию, тестированию, внедрению и эксплуатации. Конечно, это может быть и не плохо, если бы это в итоге не подменяло бы основные университетские курсы. Студенты видели, что для работы в центрах разработки не нужна серьезная математика, физика. Терялась мотивация. Наиболее интересные молодые специалисты плавно перетекали из центров разработки в Парке в центры вне страны, туда где более интересные этапы жизненных циклов разработки. И далее, как правило, не возвращались. Учитывая, что страна небольшая, это существенные потери. Часто в такой эмиграции даже не заработки главное, а возможность творчества вместо ремесла и промышленного программирования.

По сути, такая деятельность ПВТ еще ускорила разрушение инженерного, конструкторского, общесистемного образования. Ускорилось разрушение мотивации к изучению математических, физических, сложно-системных дисциплин. Действительно, зачем студенту тратить время на их глубокое изучение, если достаточно получить навыки по кодированию и тестированию программного обеспечения на основе несложных технологических платформ и легко получить работу на одной из компаний ПВТ. Похожая ситуация и с выбором направления обучения после окончания средней школы. Зачем толковым школьникам идти на инженерные, естественно-научные, конструкторские, сложно-системные специальности, если можно быстро вписаться в «технологический конвейер» ПВТ и гарантировано получать среднюю зарплату по ПВТ (которая намного выше зарплаты инженеров, конструкторов, проектировщиков сложных систем).

Достаточно массово средний программист превращается в банального ремесленника с примитивным знанием промышленной сборки ПО. Из-за такого оттока мы в итоге получаем посредственные решения на внутреннем рынке.

Но тем не менее был создан достаточно масштабный ИТ-бизнес. За 11 лет в ПВТ зарегистрировалось более 150 компаний.

К 2015 году стало понятно, что текущая модель ПВТ уже почти не развивается. И наконец-то удалось убедить бизнес, что с образованием у нас не все хорошо. И уже не только профессура вузов стала говорить о плохом образовании - присоединился бизнес.

И в середине декабря 2017 года руководство страны приняло новый декрет развития ПВТ. Существенно расширены виды деятельности. Особое внимание уделено возможностям развития образования. Это уже начало приносить плоды. За несколько месяцев в ПВТ вступило более 100 компаний. Активнее стала развиваться продуктовая модель. Сложнее, конечно, с трансформацией образования, но определенные предпосылки появились.

У айтишников пользуется популярностью понятие «прототипирование», то есть процесс построения функционирующего прототипа (макета) реальной системы (программного продукта). Так, по-видимому, и нам необходимо быстро создавать прототипы «университетов будущего». К сожалению, наши традиционные университеты в силу как объективных, так и субъективных причин вряд ли сегодня могут стать инкубаторами таких инициатив. Даже достаточно простые модели университетских технопарков у нас практически не прижились. Что уж говорить о кластеризации с бизнесом. Пожалуй, только экосистема ПВТ способна стать инкубатором для быстрого создания прототипа «университета будущего».

Нормативное регулирование цифровой экономики России и вопросы информационной безопасности

Якушев М.В., Вымпелком Европа: Цель - привлечение вашего внимания к тем аспектам программы «Цифровая экономика», которые не были освещены в выступлении Станислава Константиновича. Обращаю ваше внимание на те моменты, которые касаются создания нормативной базы цифровой экономики и при этом имеют отношение к информационной безопасности.

Были определены так называемые сквозные технологии. Это такие вещи, о которых еще лет пять назад мало кто слышал и потреблял. Это и большие данные. Это и квантовые технологии, и система распределенного реестра, то, что называется блокчейн, и промышленный Интернет, и технология виртуальной дополненной реальности - это сквозная программа «Цифровая экономика».

Я работаю в рабочей группе по нормативному регулированию. И здесь хотелось бы привлечь ваше внимание, что по всем показателям программы есть некоторые количественные критерии, которые могут выглядеть несколько странными. Остановлюсь на информационной безопасности. Два показателя - доля субъектов, использующих стандарт безопасного информационного взаимодействия, 75% и доля внутреннего сетевого трафика российского Интернета, маршрутизированного через иностранные серверы, 5%. Если эти два показателя будут достигнуты, то у нас с информационной безопасностью в цифровой экономике должно быть хорошо. Это вызывает определенное если не сомнение, то желание подискутировать.

По нормативному регулированию также был определен целый набор результатов. Один из главных - снять ключевые правовые ограничения, то есть тут у нас есть много вещей, которые препятствуют в правовом отношении развитию цифровой экономики, цифровых технологий. Про управление программы уже было сказано. У нас достаточно сложная схема, но она в принципе позволяет каждому желающему в этих вопросах поучаствовать. Соответственно, по нормативному регулированию приглашаются все заинтересованные коллеги поучаствовать в 14 подгруппах по направлениям работы. Среди них - опять-таки нерусские слова, такие как «Финтех», Киберфизические системы, - это не что иное, как фактически беспилотные транспортные и прочие средства.

Вы видите, что здесь очень большой разброс тем, которые связаны с правовым регулированием, нормативным регулированием цифровой экономики. Поэтому был утвержден план порядка 70 мероприятий. В декабре была создана рабочая группа и так же, как по информационной

безопасности, центр компетенции. Нашу группу возглавил мой коллега из компании МТС. И вот обратите внимание, приведу несколько примеров того, чем мы должны заниматься. Это и какие-то точечные изменения, различные акты и законодательство, касающиеся, например, такой темы, как электронный документ. Это и утверждение национальных стандартов в области информационной безопасности. И глобальный проект по созданию так называемого инфокодекса, а именно - направление среднесрочного регулирования инфокоммуникационной отрасли.

По снятию ключевых правовых ограничений есть три основные поднаправления. Во-первых, создание единой цифровой среды доверия: это идентификация, упрощение требований по идентификации и расширение возможностей по идентификации всех, кто так или иначе участвует в информационных отношениях.

Во-вторых, формирование сферы электронного гражданского оборота. Здесь есть все возможности вот этих распределенных реестров, блокчейны и т.д. Но появляются новые электронные формы сделки. Почему это важно? Потому что в конечном итоге под такого рода новыми сделками будет подразумеваться и обмен эсэмэсками, то есть не ходить подписывать друг к другу какие-то договоры, ставить печати, а сделка может быть заключена и закреплена просто обменом даже не эсэмэсками, а сообщением, например, в WhatsApp или в каком-то ином мессенджере.

И, наконец, обеспечение правовых условий для внедрения использования инновационных технологий на финансовом рынке. Это как раз то, что говорили коллеги из банковской сферы, из регулятора, то, что называется финтех, блокчейн, криптовалюты.

Совершенствование механизмов стандартизации. Это то, что имеет непосредственное отношение к теме нашего обсуждения, - утверждение национальных стандартов в области информационной безопасности. Ведомство, которое за это отвечает, называется Росстандарт. Сомневаюсь, что здесь кто-то присутствует из Росстандарта, кто мог бы рассказать, что они планируют. Но за все, что связано с информационной безопасностью, отвечает Росстандарт.

Следующее такое поднаправление - это определение позиций Российской Федерации по вопросам, требующим гармонизации подходов в этой сфере на пространстве ЕАЭС. На мой взгляд, это одна из очень важных тем, которой не уделяется надлежащего внимания. Мне, например, было очень интересно выслушать выступление коллеги из Белоруссии, потому что это как раз та страна, где люди чрезвычайно похожи на нас, но они повторяют наши ошибки и делают свои. И нам было бы очень важно понять, что мы делаем не так, чтобы не повторять этих ошибок. И также прозвучала справедливая мысль, достаточно, на мой взгляд, обидная для всех присутствующих, что на пространстве ЕАЭС существует недоверие друг к другу со стороны органов, обеспечивающих информационную безопасность.

Действительно, никто не доверяет российской криптографии, никто не хочет особенно связываться с тем, что рекомендует ФСБ. В свою очередь, не очень-то интересуемся и мы, что происходит в Казахстане или Белоруссии, где есть уникальные и реально работающие механизмы, обеспечивающие все необходимое, но без оглядки на российский опыт. Если мы говорим, что строим единое пространство в рамках ЕАЭС, то поставил бы это в числе наиболее важных для нас приоритетов.

И последнее. Впервые, видимо, в таком документе появляются вопросы правового регулирования применения искусственного интеллекта. Пока что только для целей социально-экономического планирования, в каком-то прикладном значении, но, безусловно, именно искусственный интеллект - это то, что нас ждет в плане регулирования.

Обеспечение безопасности интернета вещей

Андреас Кюн, Институт Восток - Запад, США: Во время усиленной напряженности как в киберпространстве, так и за его пределами нам кажется крайне важным продолжать диалог и держать наши каналы связи открытыми. Во время подготовки своей речи я с интересом прочел о российской программе «Цифровая экономика», в которой особое внимание уделяется интернету вещей, умным городам и кибербезопасности.

Интернет вещей соединяет информационно-коммуникационные технологии с реальным миром, создает киберфизические системы. Интернет вещей - инфраструктура соединенных объектов, людей, систем и информационных ресурсов, а также служб разведки, позволяющая обрабатывать информацию реального и виртуального миров и реагировать. Обычные физические системы подключены к виртуальной среде, и это переходит критический барьер. К примеру, мы думаем о подключенной к Интернету машине, в которой киберугрозы и риски не ограничиваются вопросами кибербезопасности, в этом случае возможны угрозы безопасности в реальном мире.

Существуют прогнозы, что к 2020 году 25 млрд. устройств будут подключены к Интернету, что приведет к появлению множества угроз безопасности, некоторые предрекают «цунами» уязвимостей как результат массового внедрения интернета вещей. Одна из угроз - создание ботнетов из IOT-устройств для последующих DDOS атак, что было продемонстрировано печально известным ботнетом Mirai.

Но мы также видим в IOT угрозу увеличения способов манипуляции данными в критически важных инфраструктурах путем вмешательства в системы контроля. Устройства IOT имеют очень слабую систему защиты, что ставит безопасность пользователей под угрозу, и у многих устройств IOT нет базовой защиты каналов связи путем шифрования. IOT увеличивает совместимость и взаимозависимость, что усложняет контроль за этими устройствами, их защиту и предотвращение каскадных сбоев.

Нынешнее законодательство не подразумевает штрафов за небезопасные устройства как для продавцов, так и для пользователей. В то же время экономика растет и технологии совершенствуются, что позволяет оснащать устройства нижнего ценового сегмента Ethernet-портами с пропускной способностью в 1 гигабит, что в случае их заражения вредоносными программами делает их «пушками, стреляющими трафиком».

Кибербезопасность IOT подразумевает ответственность. Для защиты IOT от множества угроз требуется совместная

работа всех участников экосистемы Интернета как на локальном, так и на международном уровнях. Ни одна организация в одиночку не справится с обеспечением информационной безопасности. Необходимы комплексная многоуровневая коалиция, состоящая из продавцов, пользователей, провайдеров, регулирующих структур, а также гражданское общество. Основным вопросом является: кто должен нести ответственность за безопасность IOT?

Как мы знаем, IOT все еще развивается, как и структуры, контролирующие информационную безопасность. И мы можем только предположить, в каком векторе будет происходить развитие, но мы знаем, что со временем это изменится и будет отличаться в зависимости от страны.

Постараюсь показать потенциальные варианты развития. Во-первых, законодатели могут искать пути решения этого вопроса, к примеру, утверждая обязательную возможность устанавливать обновления на устройства и совершенствовать их, обязывать производителей устранять уязвимости прежде, чем устройство попадет к покупателю, а также давать пользователям возможность менять дефолтные пароли. Правительства также могут устанавливать стандарты используемых IOT-устройств и инфраструктур. Власти могут проводить «круглые столы» и совместные проекты с фирмами, о чем ранее компании просили, особенно когда речь заходила о проведении курсов цифровой безопасности и обеспечении цифровой безопасности во всем мире.

Частный сектор посредством отраслевых объединений может лучше выработать методы работы. Один из обсуждаемых подходов - это публикация рейтинга безопасности, который даст пользователям рекомендации по покупке IOT-устройств, что может стать частью сертификации IOT-устройств.

В то же время группы реагирования на инциденты, связанные с компьютерной безопасностью, могут быть задействованы в работе с IOT. Премирование за обнаружение уязвимостей в программном обеспечении может быть другим подходом для выявления уязвимостей в коде.

Производители IOT-устройств включились в обеспечение их безопасности, меняя подходы к архитектуре. К примеру,

облачные сервисы начали использовать систему управления идентификационными данными Nexus именно для IOT.

Хотел бы выделить одно действующее лицо - интернет-провайдеров, которых часто забывают в таких дискуссиях. Имея более полную картину использования Интернета своими клиентами, провайдеры могут взять на себя важную функцию по наблюдению за поведением IOT-устройств, наблюдению за аномалиями в трафике, предоставлять данные о поведении устройств, определять устаревшее ПО на этих устройствах, а также сообщать о наличии вредоносных программ. Также провайдеры могут применить различные техники выявления ботов, например «входное фильтрование» (ingress filtering), чтобы распознать блок или часть трафика, взаимодействуя с другими провайдерами, прежде чем вредоносный трафик попадет в сеть. Более того, страховые компании предлагают страховые решения для IOT.

Мы должны задаться вопросом, кто несет ответственность за эти меры: правительство или частный сектор? Должна ли безопасность IOT обеспечиваться силами рынка, зависеть от инвестиций корпораций или должно ли правительство регулировать безопасность посредством законов.

Важность концепции состоит в том, что киберустойчивость не является предупреждением сбоя, а это фактор, благодаря которому, несмотря на продолжительную дестабилизацию, система продолжает нормально работать. Нам надо подумать, как сделать IOT устойчивым. Киберустойчивость не ограничивается техническими аспектами, требуется всеобъемлющий подход в отношении основных компонентов и других систем в рамках более широкой экосистемы.

Завершая свое выступление, хотел бы огласить две идеи. Во-первых, международное сотрудничество необходимо в IOT, это подразумевает обмен информацией об угрозах и способах борьбы с ней. Во-вторых, угрозы IOT не распространяются в равной степени по миру, сотрудничество провайдеров в фильтровании и исключении вредоносного трафика необходимо для борьбы с источниками киберугроз.

Гармиш-Партенкирхен, Германия

Семинар - «круглый стол» №2

«Механизмы реализации государственно-частного партнерства в области обеспечения безопасности критической информационной инфраструктуры»

Кульпин А.А., ГМК «Норильский никель», Россия: Мне очень приятно от лица «Норильского никеля» поблагодарить организаторов за возможность вести эту встречу. Тема для нас как для крупной промышленной компании очень важна. И речь идет не только о традиционном понимании этого. Например, в городе Норильске, где расположены основные наши активы, сейчас минус 16 градусов, а ощущается как минус 24. Поэтому в городе, где отопительный сезон начинается уже в августе, все жизненно важные, даже бытовые инфраструктуры - как водоснабжение, электроснабжение - становятся критичными. С точки зрения нас как бизнеса, как эксплуатантов этих критических инфраструктур и с точки зрения выстраивания государственно-частного партнерства те отношения, которые сейчас складываются у компании с представителями государств и с регуляторами, по крайней мере в периметре России, для нас крайне важны, демонстрируют рост и положительную динамику.

Хотел бы, в частности, привести пример принятого Федерального закона «О безопасности критической информационной инфраструктуры» и дальнейших действий регулятора, который сформировал требования, правила категорирования. Эта работа строилась действительно по принципу государственно-частного партнерства. Были приглашены представители крупного бизнеса и большое число представителей государственных структур, что действительно помогло выработать четкие правила поведения: каким образом государство будет регулировать, какие требования будут выставляться, какие информационные инфраструктуры будут причислены к критичным, какие - нет, какой масштаб ущерба должен быть, чтобы категорировать в ту или в другую сторону.

Все было обсуждено и уже принималось с учетом требований бизнеса для того, чтобы в дальнейшем для

нас была прозрачность и понимание, как это будет развиваться. Когда ситуация может быть прогнозируема, тогда действительно - это большая помощь, что позволяет нам планировать работу, выделять необходимые ресурсы. Угрозы, которые вчера мы подробно обсуждали, не неизменны, так как технологии развиваются. Не хотел бы сейчас заострять внимание на трендах, таких модных сейчас словах, как блокчейны, Internet of Things, все это, несомненно, внедряется. Для нас, как производственной компании, внедрение Internet of Things в промышленность носит не только совершенно очевидные преимущества в плане экономики, мы сразу начинаем просчитывать те угрозы, которые возникают при столь масштабном внедрении и повышении автоматизации производства.

Еще несколько моментов. На многих мероприятиях все очень любят говорить о сформированной экосистеме. Она предполагает некий баланс, но в случае прямых столкновений с угрозами и реальными инцидентами информационной безопасности совершенно четко появляется ситуация, когда продукты не «секьюр бай дизайн», «дизайн фор криминалс», то есть не безопасны по своему дизайну, а только помогают злоумышленникам нападать или негативно воздействовать на информационную инфраструктуру.

Эта проблема очень серьезная. И хорошо, что на нашем «круглом столе» присутствуют также и производители средств защиты информации, и производители крупного программного обеспечения, которое все используют. Для промышленности серьезную угрозу представляют те тренды и те киборы, которые делают крупные производители программного обеспечения. Могу пояснить, что большинство крупных западных компаний постепенно свое решение переводят в «облака», то есть по сути, вы покупаете уже не продукт, а сервис. И для нас, когда мы сталкиваемся с санкциями и тому подобными вещами, ситуация просто переворачивается с ног на голову. Неделю назад мы столкнулись с тем, что к нам как к пользователям обратились крупные западные компании с вопросом: «А что вы будете с нами делать»? А у нас не то что нет

ответа. У нас есть встречный вопрос к этим производителям: «А что вы будете делать, если случится час X и мы не сможем пользоваться вашим облачным программным обеспечением, когда мы, по сути, покупаем только сервис?»

Поэтому сейчас мы совершенно четко видим конфликт, вызванный тем, что вендоры идут в сторону «облаков», а мы хотим обезопасить себя, мы хотим, по крайней мере, иметь продукт у себя на борту и в случае чего совершенно спокойно продолжать пользоваться, да, может быть, без техподдержки, да, может быть, без еще чего-то. Но для нас это совершенно не праздный вопрос. Это прямая угроза производственным цепочкам, производственным процессам.

Мы выступили с инициативой создания Клуба безопасности информации в промышленности. Сегодня тут присутствуют два соинициатора этой инициативы - учредители VIP-клуба Борис Николаевич Мирошников и компания «Северсталь». Оба представителя сегодня здесь, поэтому мы могли бы обсудить те достижения, которые есть на «поляне» VIP-клуба.

Это такой неформальный механизм, который нам позволяет - и уже были совершенно конкретные результаты от этой работы при набивших оскомину атаках - в режиме реального времени обмениваться реальными сигнатурами, событиями, которые помогают нам обезопасить нашу инфраструктуру. Подчеркну, что, не умаляю значимость финансового сектора, но, когда дело идет о безопасности IT-инфраструктуры в промышленности, в первую очередь это затрагивает жизни людей: системы вентиляции, водоотведения, подъема-спуска людей в шахты и т. д. Эти системы представляют прямую угрозу безопасности людей.

Передаю слово моему коллеге Чарльзу Барри, который сегодня выступает в роли независимого эксперта.

Перспективы международного сотрудничества по защите критической инфраструктуры

Чарльз Барри, Институт национальной стратегии Университета национальной обороны США: Я бы хотел

поговорить не только о концепции государственного-частного партнерства, а о его концепции в контексте защиты критически важной инфраструктуры.

Концептуальная модель государственно-частного партнерства основана на государственных органах, деловом сообществе и гражданском обществе. Государственные органы должны предоставлять правовую защиту и обеспечивать безопасность своих граждан, а деловое сообщество предоставляет товары и услуги, о некоторых из которых уже говорили. Для гражданского общества важно вовлечение как государственных органов, так и делового сообщества, и именно об этом партнерстве я буду говорить сегодня.

Последние атаки сильно повлияли на наши предприятия, и бороться с ними следует не только самим предприятиям, государство также должно помогать в этой борьбе, ввиду того что стоимость борьбы требует совместных усилий. Хочу привлечь ваше внимание к некоторым из атак. Первая атака Stuxnet произошла в 2010 году, а вторая - на энергетические компании Украины в 2015 году. Обе эти атаки были направлены не только на информационные сети, но и на техническую составляющую, влияющую на функционирование этих предприятий. Данные атаки очень сложные, потому что им надо не только обойти защиту информационной сети, но и внедриться в фактические технологии, а также знать, как они работают.

Другие атаки, такие как Aramco, вирусы Shamoon и WannaCry в прошлом году, более направлены на сами информационные сети, но также атакуют важную инфраструктуру. В случае с WannaCry атаке была подвержена инфраструктура британской системы здравоохранения. Проблема заключается в том, что большинство следующих значительных атак будет направлено на важную национальную инфраструктуру, в которой всё взаимозависимо. К примеру, от выработки электроэнергии зависит телекоммуникация. Всеобъемлющий Интернет также усилит вектор атак.

Что такое критически важная инфраструктура? Существует множество определений, наиболее интересная из них:

«В случае, если на стадионе собралось достаточное количество человек, он считается критически важным». Некоторые национальные символы являются критически важными. Есть о чем поразмыслить. В США под критически важной инфраструктурой мы подразумеваем ту инфраструктуру, уничтожение которой ставит под угрозу национальную безопасность, экономическую безопасность, здоровье населения и его безопасность.

В ЕС разделяют национальную критически важную инфраструктуру, определение которой схоже с определением США, и инфраструктуру критически важную для ЕС, перебои в которой затрагивают двух или более членов ЕС. В результате взаимозависимости, о которой говорилось, перебои в снабжении электроэнергией могут повлиять на грузоперевозки, управление уличным движением и, возможно, системы кондиционирования в высотных зданиях.

Сильными сторонами считаю тот факт, что основные игроки киберпространства преуспели в организации отношений между государственным и частным секторами. Но поддержание этого сотрудничества является сложной задачей ввиду того, что компании не желают делиться информацией по поводу атак. А ведь пользователь должен знать, как не попасть под удар. Мы должны инвестировать в обучение. Многие наши старые системы не защищены, в то же время существует интернет вещей, привносящий новые незащищенные системы в результате того, что фирмы пытаются как можно скорее вывести на рынок незащищенные продукты.

Быстро пройдемся по тому, как совершаются атаки. В 2011 году Lockheed Martin представил модель под названием «Цепь киберубийств», в которой отмечалось, что хакеры сначала изучают программы и вероятные данные, к которым они хотят получить доступ. Получив доступ, они устанавливают вредоносное программное обеспечение (ПО) и впоследствии получают контроль над системой. Они могут как извлечь данные, так и продолжить исследование сети, а также использовать сеть с целью проникновения в другую сеть. Мы пытаемся научиться тому, что угрозу

проникновения надо предотвращать еще на стадии изучения хакерами системы. В 2011 году институтом SANS была представлена более совершенная модель, в которой также говорилось о том, что минимизация количества рабочих станций с доступом к сети и уменьшение количества программ благоприятно влияют на общую безопасность.

Плохим аспектом является то, что у нас все еще много незащищенных систем, которые в будущем должны быть заменены, а системы контроля - усовершенствованы. Другим аспектом является то, что системы в большинстве случаев перестают работать не из-за кибератак. Несколько лет назад в Вашингтоне, столице одной из главных держав мира, были перебои в электроснабжении, виной которых стала снежная буря, которая повалила деревья на провода. И мы должны помнить, что защита важной инфраструктуры необходима и в физическом плане.

Как же мы можем обезопасить инфраструктуру? Нужно сделать так, чтобы компании делились уязвимостями систем, работали над техническими решениями, но можем сделать еще больше, применяя искусственный интеллект. Если преступники работают с искусственным интеллектом, то следователи тоже должны иметь возможность им пользоваться. Нам надо озаботиться с законодательной точки зрения распространением интернет вещей, а именно - незащищенных устройств.

Возможно, нам не стоит начинать с больших соглашений, а стоит прийти к ним, но не начинать с них. Существует много организаций, которые стоит привлечь. Следует изучить модель НАТО, организации использующей полностью свои сети и управляющей ими, единственной организации, занимающейся этим на основе консенсуса 29 стран. В мире почти 200 стран, 29 - не такое большое число, но это пример того, как управление, нормы, стандарты, протоколы могут действовать вместе для функционирования сетей с высоким уровнем безопасности ради единой цели.

Мы работаем в морском пространстве уже долгое время, на данный момент насчитывается около 60 тыс. коммерческих су-

дов и 6 тыс. военных судов в мире, и все они следуют букве морского права. Не важно, в открытом море или в территориальных водах, все следуют одним правилам, однако путь к этому занял долгие годы.

Быстрее шел процесс с авиацией. За 100 лет мы добились формирования Международной организации гражданской авиации, хотя не все страны в нее входят, лишь 170. Мы уже 50 лет находимся в космическом пространстве, и был заключен один, но объемный договор. А вот, несмотря на то, что мы находимся в киберпространстве уже более 20 лет, где нет тысяч судов или самолетов, имеем дело с миллионами пользователей, но у нас нет законодательной базы. На данный момент единственное, что у нас есть в глобальном плане, - это Группа правительственных экспертов ООН. Но цифры говорят о том, что существует срочная необходимость в какой-либо законодательной базе.

Мирошников Б.Н., группа компаний «Цитадель»: Если вы готовы делиться информацией, то вы - зрелая компания, а если вы не готовы делиться информацией о своих киберинцидентах, то вы - незрелая компания. Но это и вопрос зрелости государства. Банковская система, фирмы, которые окружают те самые критические инфраструктуры, и просто владельцы огромного количества информационных ресурсов на сегодняшний день, а практически все у нас в государстве сегодня, включая магазины и киоски, обладают информационными ресурсами, в том числе и подлежащими защите. Все они внимательно смотрят: заслуживает ли государство того, чтобы с ним делиться своими проблемами? И это, между прочим, не шутка, не ирония, а весьма серьезная вещь. Потому что я, когда делюсь, должен обладать тем, что очень важно в нашей сегодняшней жизни как внутри любой страны, так и на международной арене, - это доверие.

Есть у меня это доверие, созрело ли оно? Как правило, к сожалению, нет. Именно поэтому, прежде всего банкиры, как наиболее чувствительная сфера, не хотят показать свою уязвимость, не хотят показать, что их ресурсы слабо защищены. Это их бизнес и выживание. Но существует и

другая сторона. Как ведет себя регулятор, который требует информировать об инцидентах? Оказывается, информация об инциденте становится уязвимым моментом для финансового учреждения еще и с точки зрения государства. Оно попадает в какой-то «черный список» оттого, что у него недостаточно защищены ресурсы. Попадает в список очередных проверочных действий со стороны регулятора, попадает в разряд тех, кого будут завтра наказывать и подвергать каким-то санкциям.

Все это не способствует обмену информацией с государством. Кроме того, у государства - я говорю о нашем российском обществе - есть еще одна очень важная функция, которую оно недостаточно успешно выполняет. Например, я как банкир знаю о некой проблеме. Хочу поделиться со своим соседом, являясь членом некого банковского сообщества. Но регулятора не устраивают такие правила, по закону я не имею права передать эту информацию соседу. Таким образом, я оказываюсь владельцем информации, которая могла бы предотвратить развитие какого-то преступления, в частности о вирусе, но я не имею права этого сделать, потому что регулятор мне установил такие правила.

Есть еще проблема, когда мы знаем, как ведет себя преступник. И я тоже, зная признаки этого преступника, обладая информацией о нем, мог бы передать соседу эту информацию, чтобы его защитить. Однако регулятор и здесь заставляет меня притормозить с этим обменом, потому что применяется положение закона о персональных данных, что, на мой взгляд, совсем нелепо, когда речь идет о преступнике. Но тем не менее эти узкие места до сих пор неразрешены, хотя этой проблеме уже не один год.

И в этой связи я поддерживаю моего друга и коллегу Чака, который говорит: «Время не на нашей стороне», намекая на то, что мы здорово опоздали. И вместе с тем через 15 минут он нам говорит: «Все надо делать тихо, постепенно, последовательно». Здесь видно некоторое противоречие. Я настаиваю, что мы в долгу и здорово опаздываем. Наши теоретические размышления, которые иногда тянутся годами, для того чтобы отточить мысль, приводят к накапливанию

жизненных проблем, а количество жертв в результате нашего бездействия ежегодно растет.

Приведу пример. Еще 20лет назад мы сформулировали одну из больших бед - анонимность. Анонимность в сетях - фактор, поощряющий преступника. Безумное количество симкарт, розданных просто так под любые имена, безумное количество псевдонимов сегодня наполняют интернет-пространство нашей планеты и взаимодействуют друг с другом, переписываются, атакуют друг друга. Это какие-то псевдонимы, какие-то номера. Огромное число преступлений самого разного масштаба, самого разного качества совершается с помощью анонимности. Ни у одного бандита, когда мы вели войны на Северном Кавказе, не было телефона, оформленного на его имя. Это огромная анонимная масса. Мы находили ящики, картонные коробки, в которых навалом лежали симкарты, с помощью которых они выходили в эфир по телефонам, по каналам, по IT-телефонии, с помощью этого работали на любых каналах связи.

Борьбу с подобным явлением государство должно взять на себя. И только одно это резко снимет уровень угроз, о которых мы говорим. 20 лет назад мы обозначили эту проблему, и только в 2018 году наши политики в Госдуме заговорили о том, что надо бы принять закон. 20 лет они «созревали». Мы за это ответственны. Мы лишь говорили, но не кричали, а об этом нужно было кричать и стучать кулаками по столу, потому что за это время мы потеряли очень много человеческих жизней, потеряли огромное количество финансовых средств. Потрачено огромное количество человеческих усилий на борьбу с тем, на что не нужно было бы тратить время, а тратить на другие, более полезные дела.

Еще один тезис о роли государства. О том, что бизнес прекрасно занимается своим делом. Нам сегодня это показали «Норильский никель» и «Северсталь». Их много, замечательных компаний, которые эксплуатируют то, что называется критическими инфраструктурами. Печально, что до сих пор мы обсуждаем, а что же есть критические инфраструктуры, и признаем, что определений их очень много. Завтра мы будем говорить, что такое гибридная война.

И определений тоже найдется пара сотен. Это печально, потому что на фоне того, что существует, как сказали мы здесь, до 40 определений критических инфраструктур, мы пытаемся между тем сформулировать законы, сформулировать стандарты для области критических инфраструктур.

Как это возможно? Закон, где должны быть очень точные юридические формулировки, где очень строгие определения, - мы ведь и сами требуем от юристов однозначности понимания. И при этом 40 определений критической инфраструктуры? Согласитесь, что это нонсенс. Это задача, наверное, науки и юристов - избавить нас от этой нелепости - в 40 определений и одновременно разработать закон. Так вот, функция государства состоит еще в одном, мне кажется, очень важном. Мы не первый год собираемся в этом зале, много лет общаемся друг с другом на разного рода конференциях. И я напомню, по крайней мере русскоязычной аудитории, прекрасный фильм «Место встречи изменить нельзя», цитату из которого бесконечно тиражируют: «Вор должен сидеть в тюрьме».

Преступник должен сидеть в тюрьме за решеткой, так спокойнее обществу. А где эти усилия с нашей стороны? Я имею в виду того самого регулятора - государство, которое участвует в этом процессе? Мы с вами который год очень хорошо говорим о борьбе с преступностью и киберпреступностью, о борьбе со злоумышленниками, борьбе с теми, кто очень много нам досаждает. Но мы говорим о преступнике как о каком-то марсианине, который находится где-то далеко. И мы не говорим о том, что он должен сидеть в тюрьме. Он должен быть наказан за свои деяния, о которых мы тоже очень много говорим. 26% прироста киберпреступности ежегодно! Разумеется, такими же темпами растет ущерб от киберпреступности всех мастей.

Мы сейчас говорим о войне в киберпространстве, которая влечет сумасшедшие потери. При этом мы не знаем, когда она начнется. Потому что кибервойна будет прикидываться киберпреступностью. Но ущерб-то растет. И то, что сегодня делают производители информационных продуктов, можно сравнить с построением высоких заборов и крепких зáмков. Нападение на преступника, его поиск, разоблачение,

задержание его, нейтрализация и изоляция от общества - об этом мы не говорим.

Мы говорим только о заборах и замках. Хочу привести аналогию. Наша компания тоже этим занимается, мы говорим: «Мы сегодня создаем продукты, которые вас защищают от атак, от вирусов, от всякого рода нападений, но одновременно мы создаем продукцию, которая позволяет зафиксировать действия преступника». На юридическом языке, на процессуальном языке, это называется формированим улик, доказательств. Потому что мы понимаем: некая сила должна существовать в государстве, которая бы поймала, разыскала преступника и в законном судебном порядке привела его в тюрьму, к положенному ему наказанию.

Это очень важная функция, о которой мы не говорили сегодня. И очень печально, что в нашем зале не присутствуют те, кому нужно осуществлять эту функцию. Потому что обеспечить безопасность критических информационных инфраструктур, безопасность наших государств, нашего общества и наших граждан невозможно без осуществления этой очень важной, государственной силовой функции - привлечения преступника к ответственности. Согласитесь, если у нас хотя бы половина преступников сядет в тюрьму, то вторая половина значительно сократит свою преступную активность и мы почувствуем себя в значительно большей безопасности. Если мы не будем ограничиваться словами, а действовать, то, стало быть, мы достигнем конкретных успехов в этой деятельности.

Платформенные решения для безопасности критических информационных инфраструктур

Тихонов А.И., «Лаборатория Касперского»: Очень сложно говорить после таких авторитетных ораторов и добавить что-то новое к уже сказанному, тем не менее я постараюсь.

Первое, к чему хочу привлечь ваше внимание, это то, что появление цифровых инфраструктур и цифровой экономики происходило достаточно быстро и многие из присутствующих пережили разные поколения информационных технологий.

Некоторое время назад все было довольно примитивно, сегодня же нас окружает интернет вещей, все находится в облачных сервисах и т. д. И в скором времени мир вновь изменится. В этом мире машины будут общаться между собой, будут применяться новые методы, новые правила. Исторически в нас заложена некоторая база, и изменения происходят настолько быстро, что большая часть этой базы уже неверна. Мы привыкли к умным вещам вокруг нас, но мы не рассматриваем их как угрозу. И эта угроза все еще недооценена.

К примеру, умные системы. На данный момент мы окружены умными городами, умным транспортом, умной энергией, но мы не предполагаем, что эти системы являются очень сложными киберфизическими системами, в которых основное понятие безопасности уже изменилось. Я имею в виду инфраструктуру национального института стандартов и технологий, у которой подразумевается наличие трех сред: физической, аналоговой и кибер, соединенных между собой, и пяти аспектов безопасности. Конфиденциальность, надежность, безопасность и устойчивость также важны для данной структуры. Это приводит нас к очень сложной инженерной дисциплине. Лидирующие интернет-консорциумы, такие как Консорциум промышленного интернета (IIC), используют новые методологии, чтобы справиться с новыми угрозами. Также стоит иметь в виду, что у атак разные источники и сами по себе они могут быть очень сложными. Это то, что мы сейчас наблюдаем.

Другой значительной частью эволюции является эволюция доверия. Некоторое время назад все было сравнительно просто ввиду того, что все было централизовано. На данный момент мы работаем с децентрализованными сетями, социальными сетями, с которыми довольно сложно работать. В скором времени мы будем работать с разделенным доверием, с такими вещами, как блокчейн и ему подобными.

Механизмы обеспечения доверия и гарантии доверия становятся все более сложными, а также более уязвимыми. Ранее обсуждалось, что кибератаки можно приравнять к стихийным бедствиям. Почему? Киберфизическая природа этих комплексов может спровоцировать технические

катастрофы. Десять главных целей для цифровой безопасности - это те, у которых есть киберфизическая природа, а именно: транспорт, энергетика и подобное им. Изучив это, многие страны на данный момент принимают законы, связанные с критически важной информационной инфраструктурой, и у каждой из стран они специфичны. К примеру, в Великобритании призывают к государственно-частному партнерству, но было четко оговорено, что в случае если данное партнерство не заработает в течение года, то его примут на законодательном уровне. Если я правильно понял, то закон находится на стадии подготовки.

Разные страны в разной степени готовы к принятию законов, связанных с кибербезопасностью, и это применимо к национальным центрам, органам власти. Все страны в той или иной степени решают эту проблему. Существует большой знак вопроса над моделью управления «закручивания гаек». Эти процессы должны происходить довольно деликатно. Во многих странах на данный момент это происходит благодаря общим действиям различных структур, вместо того чтобы централизованно управлять данной системой. Регулятивный орган должен работать с обществом, индустрией и другими промышленными регуляторами. Общим является то, что каждая из стран защищает свои интересы и имеет свои традиции и другие аспекты. Но также существуют и общие для всех понятия.

И в первую очередь - это обеспечение безопасности, с чем согласны все.

9 апреля было объявлено о документе Security Maturity Model интернета вещей, который мы разработали совместно с «Майкрософт». Мы применили интернет вещей для инфраструктур, включая критически важные инфраструктуры. Мы хотели определить, как измерить уровень защищенности. Как подготовленность инфраструктуры, так и сервисы должны быть применены для работы в этом направлении, чтобы обеспечить безопасность.

Другим важным аспектом является применение архитектур, которые будут способствовать усилению безопасности. К примеру, архитектура MILS. Мы являемся частью EURO-MILS,

эти мероприятия проходят в Европе при финансовой поддержке ЕС и других участников. Мы сталкиваемся с тем, что архитектуры, использованные для создания самолетов или ракет, космических кораблей и т. д., приходят в нашу среду, и архитектура умных домов сейчас схожа с ранее упомянутой.

Мы находили и изучали множество вредоносного ПО в индустриальных и IT системах, а именно в таких сферах, как энергетика, транспорт и им подобное. Мы видим уязвимость, и, по нашему мнению, от этой уязвимости надо избавиться. Многие из проблем, включая последние с самым известным вредоносным ПО, могли бы быть решены при помощи обновления инфраструктуры, так как нам были известны уязвимые места. Обновление инфраструктуры может решить 80% наших проблем.

Новым аспектом является то, что мы должны быть готовы к вещам, о которых еще не знаем, так как количество вредоносного ПО растет по экспоненте и довольно скоро искусственный интеллект сможет создавать вредоносное ПО, вместо того чтобы бороться с ним. Мы должны быть готовы к более сложной ситуации с критически важной инфраструктурой. С этим не удастся бороться обычными методами, которыми мы пользовались ранее. И даже если мы улучшим наши методы, это все еще будет проблемой. Уязвимости интернета вещей повсюду. Изучив это довольно детально, можно сказать, что они равно распределены во всех частях интернета вещей: в облаке, шлюзах, устройствах и во всем остальном.

Надо сказать, что атаки на устройства интернета вещей довольно сложны сами по себе, мы знаем о большей части проблем, но следует заметить, что из-за киберфизической природы физический домен, которому можно было беспрекословно доверять, уже не является таковым, так как проникновение в физическую инфраструктуру также может быть одним из сценариев кибератаки. И это тоже должно быть принято во внимание во время разработки методов обеспечения безопасности. Интернет вещей проникает во все критически важные инфраструктуры, и безопасность этой сферы должна быть значительно улучшена. Полтора года назад ботнет MIRAI заставил говорить о безопас-

ности, и именно тогда все поняли, что безопасность не шутка и что новая волна грядет. Этот ботнет не атаковал владельца инфраструктуры, он атаковал других. И это означает, что если атака была произведена с определенного домена, это еще не говорит о том, что владелец домена виноват в этом, он виноват в безграмотности.

Шлюзы интернета вещей являются самой незащищенной частью, которая соединяет облачную среду с устройствами. Не хочу называть все векторы, но их много. У нас есть решение для этого. Более опасным является роутер, весящий больше тонны. Производители автомобилей уделяют много внимания обеспечению безопасности своих автомобилей. Однако каршеринг, к примеру, использует телематические решения, некоторые из которых могут без проблем заглушить двигатель на скорости в 100 км/ч. Это чудовищно, это на самом деле пугает.

Разработчики назвали безопасность своим основным предметом озабоченности, но никто ничего с этим не делает. Это не находится в списке их приоритетов. Они хотят, чтобы кто-то обеспечил безопасность за них. Мы в состоянии это сделать, но они могут к нам не обратиться, что подтверждает мое утверждение, что безопасность должна быть применена ко всему комплексу. Мы – «Лаборатория Касперского» - имеем линейку продуктов, которые позволяют полностью обезопасить инфраструктуру, но вся архитектура довольна сложна. Мы открыты для сотрудничества.

Обзор практик взаимодействия государства и бизнеса в области SOC

Чаплыгин Роман, компания «PricewaterhouseCoopers»: Мой доклад связан с двумя поднаправлениями кибербезопасности. Это операционные центры кибербезопасности и центры расследования инцидентов кибербезопасности. Немного поговорили об анализе этого вопроса в различных странах. Есть определенное различие между двумя типами данных структур. Первый направлен на постоянный мониторинг, превентивное обнаружение различных угроз. Второй сфо-

кусирован на устранении и расследовании уже случившихся инцидентов.

История СЕРП, компании, которая занимается расследованиями, начинается с конца 1980-х годов, когда появились отдельные центры, потом стали появляться государственные центры расследования инцидентов, и уже в 2003 году появились первые партнерские центры. Так, путем государственно-частного партнерства создается организация, предоставляющая свои сервисы различным структурам, как коммерческим, так и государственным. Тенденции создания Секьюрити Оперейшн центров очень похожи.

Действительно, в том числе и в России, появились вначале коммерческие центры, стали появляться операционные центры кибербезопасности в конкретных компаниях. Сейчас тенденция идет к тому, чтобы появлялись и государственные центры кибербезопасности, и партнерские. По нашему представлению, общая структура, некая целевая картина национального центра расследования киберинцидентов, выглядит таким образом. Мы предполагаем, что наша госструктура будет играть роль платформы и координационного центра, будут центры по отраслям, по направлениям. Есть место для коммерческих поставщиков услуг в области кибербезопасности, так как не все организации способны экономически построить внутренний операционный центр кибербезопасности.

Но очень важный момент, что в такой архитектуре должен заработать долгожданный активный обмен информацией. Очень быстрый оперативный обмен, направленный на устранение, а может, даже предотвращение для некоторых киберкомпаний инцидентов и атак. С точки зрения практики, которая сейчас сложилась в России, есть коммерческие центры, группа IT-компаний, неплохо работает финансовая индустрия, Финсерф, созданный при Центральном банке. Вчера мы слышали выступление представителя Сбербанка, где также есть центр кибербезопасности и расследования киберинцидентов.

Все это преимущественно сфокусировано в банковской отрасли. Также мы знаем, что «Касперский» («Лаборатория Касперского») является поставщиком индустриального центра по

расследованию инцидентов. И, конечно, несколько государственных центров, которые сфокусированы на взаимодействии с крупными компаниями, также решают вопросы правительственных и федеральных структур. Немного хочу сказать, какие мы видим различия в подходах установления этих практик в России и Европе.

Сейчас в России прослеживается такая тенденция по формированию некой общей платформы, причем выстраивается некий технический инструмент для обмена информацией об инцидентах и немного - для регулирования, в том плане, как этот обмен должен быть. В то же время в Евросоюзе мы наблюдаем более системный подход. Есть определенный базовый стандарт, базовые правила, и все компании, как государственные, так и коммерческие, стараются максимально приблизиться к уровню, заданному этим стандартом. Чрезвычайно важно, что такой стандарт включает разные направления. Не только технические, но и организационные и более комплексные, что является преимуществом.

И также есть уже примеры созданного государственно-частного партнерства, которое должено быть достаточно успешным на поле противодействия киберпрестуности. Также сделали сравнительный анализ по странам, чтобы понять общие тренды, общие тенденции. Наличие базового законодательства в области защиты критичной информационной инфраструктуры существует во всех странах. Вопрос в том, что не во всех странах законодательство имеет инструменты внутреннего контроля и проверок, в частности аудиты за соблюдением этого законодательства. Мы отметили, что большинство стран уже обладает созданными национальными центрами расследования и реагирования на киберинциденты, а Россия сейчас активно участвует в этом процессе. Операционные центры кибербезопасности на национальном уровне тоже стали появляться.

Видимо, это уже следующий шаг в развитии противодействия киберпреступности. В то же время хочу отметить, что на практике мы видим, как коммерческие компании уже решают подобные вопросы. И им не требуется особого законодательства, чтобы включить в пункты договора правила по защите, обмену информацией, обязательства по сообщениям об инцидентах

между партнерами, контрагентами, а также проведение независимых аудитов, самостоятельных для сверки уровней безопасности. Эти вещи уже работают между различными компаниями и, мне кажется, дают свои плоды.

Актуальные потребности частного бизнеса в области обеспечения безопасности критической информационной инфраструктуры

Гусев С.Б., АО «Северсталь-Менеджмент»: С точки зрения частной производственной компании-лидера в области экономики и индустрии в Российской Федерации - компании «Северсталь», верхнеуровневые - то, что называется корпоративными системами, защищены достаточно неплохо, есть правильные средства защиты, которые позволяют выявлять и пресекать точки атак, но производственные системы, системы автоматизации производственных процессов находятся еще на незрелом уровне с точки зрения системы защиты. По прогнозам экспертов, на 2018 год на первое место ставятся атаки на инфраструктуру, которые затрудняют дальнейшее выявление штатными средствами атак интернет вещей.

К относящейся тематике - это атака на посредников, на те доверенные ресурсы, с которыми выстроены взаимодействие и интеграция, от которых ожидается, что идет правильная и защищенная безопасная информация. Прошлый год нам показал, что много атак было проведено через те самые доверенные ресурсы. На первом месте, наверное, атаки на технологии. Все хотят быстрого внедрения новейшей технологии, быстрой отдачи от вложений. Но скорого результата достигнуть не всегда получается, хотя вроде бы и функционал найти удается подходящий. А хотелось бы видеть «секьюрити бай дизайн» - защиту систем на всем жизненном цикле - от момента создания до момента утилизации. На практике этого не происходит. На мой взгляд, до сих пор отсутствуют качественные решения, которые позволяют выявлять декларированные возможности. Атаки вредоносов, которые мы выявили в прошлом году, доказывают, что заявленный цикл

безопасной разработки программного обеспечения пока явно не на том уровне, который позволял бы использовать и останавливаться только на техническом «бай дизайн» решении, опять же - тратить ресурсы.

И еще глобальный тренд, который начался еще года три назад, - мы выявляли как клауд-технологии, которые к нам приходят, то есть «облачные», дальше вместе с ними стали появляться лэйки для анализа и учета данных. Это привело к тому, что системы нижнего уровня стали более связаны с верхними уровнями и за счет этой связанности ландшафт угроз и воздействие мошенников, умышленных и неумышленных атак увеличивают риски. Внешняя среда. Наблюдается до 300 тыс. новых кодов вредоносов ежедневно. Кто эти люди, которые тратят колоссальное количество времени на их создание? Значит, это кому-то надо.

Точно видим неоднородный уровень безопасности внешних сервисов и новых технологий. И облачные решения, и облачные сервис-провайдеры обладают разным уровнем зрелости, но явно находятся под давлением.

По инфраструктурной части. Здесь явно во многих системах страдает гигиена базовой информационной безопасности. Связано это с устареванием, с производственным циклом, необходимо подстраиваться под плановые ремонты. Явно прослеживается пренебрежение требованиями информационной безопасности подрядчиками, которых мы выбираем. Это касается и наших подрядчиков, и зарубежных. Что-то вырабатывается хорошо, но есть случаи, когда подрядчик приходит налаживать систему с внешним носителем на компьютер, где явно нет гигиены. Если у нас какие-то лицензионные требования идентифицированы, то, с точки зрения внешних поставщиков, IT решений таких нет.

Остановлюсь отдельно на людях. Это как персонал компании «Телеком», так и обслуживающие сотрудники, которые оказывают услуги, - явно здесь у нас есть белые зоны. Ну, и немножко по ожиданиям. Говорили уже про доверие. Доверие в средствах защиты, которое имеется на рынке, надо как-то растить. Пока явно есть ощущение, что доверяешь только собст-

венному, родному. Ему доверяешь лучше, чем «облакам» со стороны. Наверное, потому что нет механизмов, подтверждающих сертификацию, а атаки, проходившие в 2016-2017 годах, демонстрируют отсутствие доверия, отсутствие контроля над ней.

Даже должной защиты доверенных ресурсов, особенно уровня государственных, точно не ожидаешь. А информация оттуда должна приходить безопасная. Наш форум полезен с точки зрения оценки работ, проводившихся ранее, экспертных сетей, базы знаний, методов защиты и обнаружения атак, понимания текущей картины и т. д. Но есть еще потребность в технических вещах. Мы вместе с одним из государственных вузов проводим работу, преподаем студентам, делимся знаниями, вовлекаем их в работу, в написание каких-то вещей для того, чтобы не абстрактно, а на практике будущие специалисты по защите информации получали практические знания на современном уровне.

В этом году компания «Северсталь» стала активно смотреть в сторону инноваций, и одной из инноваций могут стать какие-то секьюрити решения, которые позволили бы бизнесу удобно и безопасно использовать системные решения для дальнейшего продвижения и роста. СЕРП на сегодняшний день, конечно, есть, но, с другой стороны, пока с его стороны получаешь непривычную, сервисную модель, когда понятны договоренности об уровне услуг, а получаешь просто уведомление. При этом с точки зрения угроз всю ответственность несет владелец информационной инфраструктуры. Здесь надо подумать над некими правилами игры, чтобы это было обоюдно интегрировано и с точки зрения государственных интересов, и с точки зрения других структур. Большие надежды возлагаются на помощь в борьбе с массовыми атаками, потому что они преодолевают фильтры провайдеров и сетей связи, доходят до конечной цели, и уже приходится работать внутри компании. Ну, и точно рассчитываем на помощь в расследовании преступлений. Мы свою доказательную базу собираем, но вот из-за анонимности Интернета зачастую преступления, которые выявляются, уходят в никуда.

Гармиш-Партенкирхен, Германия

Семинар - «круглый стол» №3

«Проблемы противодействия использованию ИКТ во враждебных военно-политических целях»

О военно-политических аспектах применения существующего международного права в информационной сфере

Юниченко С.П., Генеральный штаб Вооруженных сил РФ: Уважаемые коллеги, в последнее время мировое экспертное сообщество много внимания уделяет военно-политическим аспектам применения существующего международного права в информационной сфере. Наибольшее количество споров вызывает обсуждение возможности применения права на самооборону и международного гуманитарного права. Эксперты западных стран во главе с США ратуют за безусловное применение права на самооборону, а также норм международного гуманитарного права применительно к ведению военных действий в информационной сфере.

Российский подход к этим вопросам ранее не раз доводился до международной общественности в ходе различных международных форумов. Последний раз он прозвучал в выступлении заместителя секретаря Совета безопасности РФ О.Храмова на международной конференции ОБСЕ по кибербезопасности в ноябре прошлого года. Его суть в том, что возможность применения существующего международного права в информационной сфере обусловлена необходимостью учета уникальных особенностей современных информационных технологий. Речь идет о необходимости решения таких базовых вопросов, как определение понятий «информационное оружие и вооруженное нападение в информационной сфере», «возможность использования права на самооборону в ответ на враждебное нападение в ней», «международно-правовая квалификация таких нападений, нейтралитет, избирательность и пропорциональность применения силы в информационном пространстве», «вероломство и военная хитрость в ходе военных операций», «статус

Тезисы доклада подготовлены коллективом авторов в составе: И.Н.Дылевский, К.О.Песчаненко, В.В.Карнаух, С.А.Комов, С.П.Юниченко

гражданского персонала, привлекаемого к информационным операциям», «запрещение отдельных видов оружия» и др.

Кроме того, необходимо искать пути преодоления анонимности и повышенной скрытности действий в информационной сфере, которая не позволяет достоверно определить национальную принадлежность, мотивы действий и географические координаты источников информационных атак. Если в процессе применения права на самооборону или международного гуманитарного права всего этого не учитывать, можно получить обратный результат. Например, неверное определение источника агрессии и последующее применение в соответствии с правом на самооборону военной силы против невинного государства может поставить жертву агрессии в положение агрессора.

Объем вопросов, связанных с развитием международного права, очень велик. Остановлюсь на вопросах применения права на индивидуальную и коллективную самооборону в информационной сфере. Суть российской позиции в том, что это право может быть применено только в том случае, если информационные технологии и средства используются в качестве оружия. Кроме того, такое использование информационной технологии и средств должно привести к нанесению ущерба, сопоставимого с ущербом от применения традиционных видов оружия. При выполнении этих двух условий можно считать, что совершено вооруженное нападение, по смыслу 51-й статьи. Здесь следует сделать два дополнительных уточнения.

Во-первых, в существующих универсальных документах международного права, к сожалению, не закреплено определение самого родового понятия термина «оружие» или его аналога «вооружение». Вместо этого применяется подход, основанный на том, что под оружием, как правило, понимают некие технические устройства или предметы, предназначенные для нанесения физического ущерба каким-либо объектам и/или живой силе противника. Например, в договоре о торговле оружием, вступившем в силу в декабре 2014 года, перечислены отдельные виды вооружений, подпадающие под его юрисдикцию: боевые танки, боевые бронированные машины, артиллерийские системы большого калибра, боевые самолеты, боевые вертолеты, военные корабли, ракеты и ракетные установки, стрелковое оружие и легкое

вооружение. Руководствуясь методом аналогий, можно утверждать, что нанесение ущерба, сопоставимого с ущербом применения перечисленных видов оружия при использовании какого-либо вида информационных технологий и средств, также позволяет квалифицировать их в качестве оружия.

Во-вторых, в действующем международном праве не существует однозначных критериев вооруженного нападения. Вместе с тем имеется определенная аналогия между терминами «вооруженное нападение» и «агрессия». Содержание агрессии раскрыто в резолюции Генеральной Ассамблеи ООН 1974 года. По смыслу резолюции «вооруженное нападение» представляет собой акт агрессии, который ведет к нанесению видимого физического ущерба. В статье 3 резолюции приведен перечень возможных актов агрессии, одним из которых может являться «вооруженное нападение». В частности, вооруженным нападением будут использоваться информационные технологии для осуществления нападения вооруженными силами государства на сухопутные, морские или воздушные силы другого государства.

Например, проведение вооруженными силами одного государства компьютерных атак на информационную инфраструктуру вооруженных сил другого государства, которое привело к ущербу, сопоставимому с применением традиционных видов оружия, может быть признано вооруженным нападением. Вооруженным нападением также будет применение информационных технологий специальными подразделениями армии, флота и авиации одного государства для поражения информационных ресурсов или информационной инфраструктуры, размещенных на территории другого государства. При этом также должен быть нанесен сопоставимый физический ущерб.

Кроме того, с использованием информационных технологий может быть осуществлено и вооруженное нападение одного государства на другое государство с территории третьего государства, которое последнее представило в распоряжение первого для совершения акта агрессии. Под действие этой нормы могут попасть все государства, на территории которых расположены прокси-серверы, используемые государственными агрессорами с разрешения их хозяев для проведения анонимных компьютерных атак, завершившихся нанесением физического ущерба объекту атаки.

И наконец, под актом агрессии может пониматься засылка государством или от имени государства вооруженных банд, групп и регулярных сил или наемников для вооруженного нападения с применением информационных технологий на другое государство, наносящее столь серьезный урон, что равносильно перечисленным выше актам. Упомянутая резолюция дает Совету Безопасности ООН возможность не ограничиваться приведенным в ней перечнем. В статье 4 указывается, что приведенный выше перечень актов не является исчерпывающим и Совет Безопасности ООН может определить, что другие акты представляют собой агрессию, согласно положениям Устава ООН.

Поэтому конкретные акты агрессии с использованием информационных технологий могут по мере необходимости дополнительно быть сформулированы Советом Безопасности ООН. Хочу еще раз подчеркнуть, что неправомерно имеющее место утверждение о применимости статьи 51 Устава ООН к действиям государств в ответ на использование в отношении их информационных технологий, повлекших нанесение любого ущерба.

Необходимым условием применимости права на самооборону будет совершение вооруженного нападения, то есть нанесение физического ущерба, сопоставимого с применением традиционного оружия. В заключение хочу подчеркнуть, что, несмотря на различие национальных подходов, не существует альтернативы объединению усилий всего мирового сообщества для достижения единой цели - предотвращения военных конфликтов, которые могут стать следствием агрессивного или иного враждебного применения информационных технологий.

Крутских А.В. *Внутреннее мое впечатление, что государства - я не говорю, какие - хотят переложить ответственность на военных за ведение кибервойны. Правильно ли это? Кибервойна может вестись в политических целях, что, в частности, неоднократно обсуждалось и в Белом доме. Как измерять, после чего война станет войной от нанесенного ущерба? Но ущерб-то могут нанести не военные. Значит ли это, что войны после этого не будет? Возникает очень интересный вопрос: если не военные будут своими действиями виноваты в том, что начнется кибервойна? А кибервойна - в Группе правительственных экспертов ООН мы договорились об одной важнейшей норме - звучит так: «Государство несет ответственность за все кибердействия, которые происходят на его территории в рамках его информационного*

пространства». Там ни слова не говорится о военных. Государство несет ответственность за все действия. А если эти действия нанесены не военными, а уголовниками или террористами? Государство-жертва не должно применять ответную силу для наказания государства, с территории которого последовали эти действия? Мы должны ждать, чтобы этот ущерб нанесли обязательно военные, чтобы считать это вооруженным нападением. Вдумайтесь! Это страшная вещь. Потому что это легализует войну без объявления войны. Это легализует действия, наносящие ущерб без привлечения военных. А война тем не менее со всеми разрушительными последствиями будет происходить. А нападение на бизнес-корпорации? Приведу пример, на который хотел сослаться еще вчера. Представитель «Maersk», этой триллионной компании, насколько я понимаю, - американской, которая несет ответственность за 15% всех глобальных контейнерных перевозок, сообщал, что она этим летом подверглась кибернападению со стороны уголовников. Корабли этой компании, каждый из которых перевозит по 20 тыс. контейнеров, стали входить в резонанс, и, как мне сказал глава сингапурского агентства по кибербезопасности, такой корабль мог перевернуться.

Вопрос ко всем вам: если бы этот корабль перевернулся, вы же лучше меня знаете, мировая страховка возросла бы в десятки раз, а вместе с ней - цена мировых перевозок возросла бы в 100 раз. Это был бы мировой экономический кризис. Это война или нет? Как на это реагировать? Я спросил руководителя компании «Maersk», а американское правительство после этого как-то реагировало на этот инцидент, помогло поймать преступников? А оно объективно не могло этого сделать. Это ситуация не только с США, не только с Россией, не только с Китаем - мы все живем в такой ситуации.

Так как мерить войну? Если военный, полковник, нажимает на кнопку - это война. А если я, частный гражданин, нажимаю на кнопку и вызываю мировой экономический кризис - это что? Следовательно, изменилось лицо войны. лицо ущерба и лицо конфронтации. Но для таких стран, как Австрия, для таких стран, которых 99 на планете, это означает конец света, и без войны формальной ни ОБСЕ, ни НАТО, ни Устав ООН там становятся неприменимы. Так что мы сегодня обсуждаем? Как ведут себя наши военные? Или мы обсуждаем новые формы войны? Ответьте мне на этот вопрос, потому что мне приходится с российской стороны вести переговоры по этим нюансам, вот здесь мы не можем договориться.

А когда наши военные встречаются с американскими военными или с китайскими военными в ходе двусторонних переговоров, у нас нет проблем. Они говорят на своем языке, и все понимают, им все ясно. Но в докладе

полковника Российской армии заданы те вопросы, которые к армии не имеют отношения. Это политические вопросы. И они не решены.

ИКТ-угрозы в военно-политической сфере: сотрудничество или конфронтация мировых держав?

Ромашкина Н.П., Институт мировой экономики и международных отношений им. Е.М.Примакова Российской академии наук: В настоящее время военные все большего количества стран считают сферу информационно-коммуникационных технологий (ИКТ) частью комплексного пространства боевых действий. Сегодня в него входят уже не только суша, море, воздушное, околоземное космическое пространства, но также и информационные и кибероперации.

Включение ИКТ-сферы в интегрированное поле боевых действий создает новую логику развития событий в процессе противостояния государств. Эта логика заключается в следующем: с одной стороны, в ходе противоборства государства стремятся использовать свои конкурентные преимущества, в том числе преимущества в ИКТ-сфере; с другой стороны, если одна из сторон не обладает преимуществом в какой-либо из частей пространства боевых действий, она будет использовать свои сильные возможности в других сферах. То есть, другими словами, сторона, проигрывающая в ИКТ-среде, может и будет задействовать другие пространства боевых действий. Таким образом, если в ходе острой конфронтации одна из стран использует свои исключительные ИКТ-средства во враждебных целях против другой страны, но без применения прямой военной силы, то в ответ может последовать удар с использованием всех имеющихся военных средств, в том числе оружия массового уничтожения.

Это формальная логика противоборства, нормальная для условий острой конфронтации, когда военно-политические отношения переходят от взаимодействий, характерных для мирного времени, к действиям, принятым во время ведения войны. Это очень опасная ситуация, когда ИКТ могут спровоцировать развязывание межгосударственного военного конфликта, в первую очередь из-за возможности несоразмерного использования методов реагирования на угрозы и атаки: пострадавшая сторона мо-

жет применить в ответ реальное оружие. Кроме того, конфликт может возникнуть по ошибке, так как в настоящее время отсутствует универсальная межгосударственная методология идентификации «нарушителей правопорядка» в ИКТ-пространстве, не выработаны критерии отнесения кибератак к вооруженному нападению, не сформированы универсальные принципы расследования инцидентов. Все эти угрозы только усиливаются с учетом решения НАТО о применении статьи 5 Устава альянса в ответ на кибернападения.

При этом в современных конфликтах прослеживается тенденция исчезновения границ между мирным состоянием государств и переходом их в состояние войны. А это значит, что вышеописанная логика противоборства с применением ИКТ становится еще более опасной.

Кроме того, расширяется состав участников военных конфликтов. Наряду с регулярными войсками в военных действиях используются внутренний протестный потенциал населения, а также террористические и экстремистские формирования. Растут масштабы военного применения ударных роботизированных средств с дистанционным управлением, искусственного интеллекта в военных целях и т. д.

Все эти особенности современной системы военно-политических отношений приводят к необходимости поиска ответов на целый комплекс острых вопросов.

Насколько велика вероятность угрожающих последствий от применения современных ИКТ в военно-политической сфере?

Что необходимо сделать, чтобы снизить эту вероятность?

Насколько значима сегодня угроза дестабилизации глобального баланса сил и интересов в связи с развитием ИКТ?

Приведет ли осознание взаимной стратегической уязвимости в ИКТ-сфере к необходимости взаимодействия мировых держав или неизбежна дальнейшая нарастающая конфронтация?

Под ИКТ-угрозами в военно-политической сфере в настоящее время понимаются и информационно-технологические (кибер) угрозы (хакерство и хактивизм, вывод сервера из строя, хищение и шпионаж; саботаж и разрушение, стратегические атаки и информационное противоборство), и информационно-психологическое воздействие, и вмешательство во внутренние дела

государства, и террористическая и экстремистская деятельность в этой сфере - все, что связано с вызовами внутри ИКТ и от ИКТ.

Уровень угроз можно наглядно представить в рамках модели деления противоборства на три вида: борьба влияния, вооруженная борьба и борьба с инфраструктурами.

Высшей формой противоборства является борьба влияния, цель которой - привести противника к принятию решений, выгодных для воздействующей стороны. Это считается наиболее рациональным в силу относительно малых затрат и высокой эффективности. В случае недостижения цели в рамках «чистой» борьбы влияния традиционным вплоть до последнего времени оставался переход к вооруженной борьбе. В результате противник с помощью военной силы приводился в состояние, когда его политическое руководство вынуждено принимать выгодные для воздействующей стороны решения. Однако сегодня ситуация изменилась. В рамках новой реальности силовое обеспечение борьбы влияния может осуществляться без развязывания вооруженной борьбы, но посредством борьбы с инфраструктурами.

Почему это стало возможным? В связи с лавинообразным ускоренным развитием ИКТ. В связи с глобальной компьютеризацией, оказавшей огромное воздействие на эффективность борьбы влияния. В связи с так называемым сетецентрированием техносферы; появлением средств кибернетического и киберкинетического воздействия (в случае, если технологии применяются по отношению к информационным объектам, говорят о кибернетическом воздействии на них, если по отношению к материальным - о киберкинетическом воздействии), способного выводить из строя целые сегменты критически важных объектов государственной инфраструктуры. Это предоставляет новые возможности в рамках борьбы с инфраструктурами. При этом ущерб от воздействий на инфраструктуру могут понести также и социумы, которые входят в объект борьбы влияния, но жизнедеятельность которых зависит от объектов инфраструктуры.

Какие же исключительные, уникальные возможности предоставляют сегодня ИКТ в рамках борьбы влияния? Одной из самых эффективных является так называемая «мягкая сила», создателями и теоретиками которой являются США. Соединенные Штаты стали также общепризнанным мировым лидером

и в практическом применении «мягкой силы». Использование этой стратегии напрямую связано с важнейшей современной ИКТ-угрозой - вмешательством во внутренние дела государств. Успешные для авторов стратегии «мягкой силы» операции с применением ИКТ (финансовая, организационная, материально-техническая, информационная и идеологическая деятельности) позволяют с высокой степенью вероятности прогнозировать дальнейшее совершенствование и использование подобных методов в будущем.

Уникальные возможности предоставляют ИКТ и в рамках борьбы с инфраструктурами. Речь идет о вредоносном воздействии на критически важные государственные объекты инфраструктуры. Страны с наиболее развитой ИКТ-сферой в ходе борьбы с инфраструктурами реализуют комплекс мер, направленных, с одной стороны, на минимизацию возможностей своих оппонентов по деструктивному воздействию на свою критическую инфраструктуру (КИ), а с другой - на заблаговременную скрытую подготовку глобальных систем (киберагентурных сетей) для контроля и реализации аналогичных воздействий на ключевые объекты критических инфраструктур других государств.

В настоящее время более 30 стран обладают программным обеспечением (ПО) для нападения на объекты КИ. При этом средний ущерб от целевой кибератаки на КИ составляет 1,7 млн. долларов, а потери промышленной компании от кибератак - более 0,5 миллионов в год. При этом растущая сложность оборудования и ПО КИ ведет к росту вероятности ошибок и уязвимостей. Вредоносному воздействию ИКТ подвергались в последние годы правительственные органы, системы водоснабжения, жилищно-коммунальные, финансовые и налоговые, энергетические, топливные, атомные и транспортные системы, крупные производственные предприятия и т. д. Их количество в последнее время исчисляется десятками миллионов в год. При этом очень многие инциденты происходят с участием сотрудников предприятий.

Безусловно, наиболее важными являются проблемы, связанные с влиянием ИКТ на безопасность военных объектов как части критически важной инфраструктуры государства. При этом особого внимания требует защита стратегических вооружений, системы предупреждения о ракетном нападении, системы

командования и контроля над ядерным оружием, системы противовоздушной и противоракетной обороны.

Возвращаясь к нашей модели противоборства, отметим, что в условиях острой военно-стратегической обстановки возможен сценарий заблаговременно подготовленного, скрытого, масштабного, разрушающего ИКТ-воздействия на объекты КИ, от функционирования которых зависит боеготовность и боеспособность армии и флота. После этого в условиях результатов борьбы с инфраструктурой методами борьбы влияния с угрозой применения военной силы может осуществляться нарастающее давление на руководство государства с целью принятия им решений, составляющих цель агрессии.

Однако еще одной уникальной особенностью ИКТ является взаимная, или даже равная уязвимость крупных государств. Во-первых, государства с наиболее развитой ИКТ-сферой являются наиболее уязвимыми. Во-вторых, при отсутствии каких бы то ни было ограничений существуют стимулы для создания и взаимного применения ИКТ в военно-политических целях для враждебных действий и актов агрессии всеми мировыми державами. В-третьих, для страны-лидера ИКТ-противоборства существует серьезная опасность, связанная с возможностью контроля, дезинформации и манипулирования со стороны компетентного противника. Это возможно, если компетентный противник выявит киберагентурные сети лидера, будет их эксплуатировать и наблюдать за лидером, не затратив при этим никаких усилий (кроме усилий на выявление).

И наконец, самая серьезная угроза связана с серьезным снижением уровня стратегической стабильности посредством вредоносного применения ИКТ. Эта проблема важна для всех участников международных отношений. И если в прошлом году в этом зале я говорила, что уровень стратегической стабильности приблизительно равен уровню Карибского кризиса 1962 года, то сегодня я считаю, что уровень стратегической стабильности ниже. Нынешняя ситуация отличается еще большей, чем в 1962 году, неопределенностью, непредсказуемостью, отсутствием каких бы то ни было общих правил в международных военно-политических отношениях.

Реальная оценка всех этих угроз, безусловно, позволяет сделать вывод о том, что в создании международных механизмов снижения ИКТ-угроз в военно-политической сфере, в расши-

рении сотрудничества крупных ИКТ-держав «промедление смерти подобно».

Искусственный интеллект, автономные боевые системы и угрозы мирного времени

Дэниел Штауффахер, Регина Сурбер, фонд «ICT4Peace» (Швейцария): Тема нашего доклада «Искусственный интеллект, автономные боевые системы и угрозы мирного времени» немножко отличается от тем предыдущих докладов и может служить скорее как основа для дальнейших дискуссий.

Начнем с некоторых терминов и понятий. Сегодня искусственный интеллект (ИИ) быстро развивается и широко применим, например, в переводческих программах, беспилотных автомобилях или в медицинских целях. Исследователи разделяют ИИ на развитый и неразвитый. Под первым подразумевается, что ИИ способен выполнять те функции, которые способен выполнять и человек. Второй тип ИИ предполагает выполнение некоторых функций, которые машина иногда способна выполнять лучше, чем человек. Если ИИ способен выполнять функции лучше человека, то ИИ может потенциально заменить его.

Сегодня некоторые технологии ИИ способны самостоятельно, без участия человека, адаптироваться к складывающейся ситуации. Такой ИИ получил название автономного ИИ. Можно программировать такой ИИ для помощи спасателям в ликвидации последствий катастрофы, в медицинских целях. Они являются примерами использования технологий во благо. Однако их можно использовать и для автономных видов вооружений, таких как самонаводящаяся пушка, беспилотные дроны или воздушно-космические самолеты, способные самостоятельно выбирать цель и принимать решение об использовании оружия. Такие технологии часто называют летальными автономными системами вооружения. На протяжении последних четырех-пяти лет они являлись темами для обсуждения в ООН, женевских переговорах по конвенционным вооружениям и в неформальных дискуссионных группах. Около 20 стран, в том числе Китай, выступают за запрещение такого вида вооружений.

Наиболее серьезной проблемой является использование законодательных актов по запрещению данного класса вооружений

в военное время в рамках гуманитарного права. Эта тема привлекла внимание множества организаций, НПО и гражданских обществ. Использование автономных систем вооружений ставит важный вопрос: в какой момент наступает человеческая ответственность за использование автономных систем? Более того, дебаты в рамках ООН не рассматривают использование автономных систем во время полицейских операций, а также автономное кибероружие. В ООН концентрируются только на законодательстве в отношении развивающихся технологий, а не анализируются угрозы, связанные с использование автономных технологий вместе с уже существующими.

Тем самым технологии с ИИ представляют угрозу не только, когда используются в системах вооружений, но и для глобальной безопасности в целом. Такие риски менее очевидны, более системны и различны. Что мы подразумеваем под угрозами в мирное время? Что если, например, автономный ИИ будет генерировать «фэйк-ньюс»? Сегодня больше ботов, которые способны создавать ложную информацию, чем тех, которые помогают нам ее выявить. Существуют и технологии, создающие видео и изображение высокого качества с фэйковым контентом. Автономный ИИ используется для принятия судебных решений и помогает в сборе информации по потенциальным преступникам. Однако это ставит под угрозу принцип презумпции невиновности, так как потенциальный преступник выявляется по набору характеристик. Более того, в мире ограниченных ресурсов может ли ИИ принять решение о том, кто должен продолжать жить, а кого можно принести в жертву ради жизни других?

Наконец, мы стоим на пороге изменения парадигмы, когда человек больше не будет единственным разумным существом. Что если возможности автономного ИИ позволят изменить современную структуру человеческого общества или даже человечества, человека как биологического вида.

Что же нам нужно делать? Мы должны понять, что происходит. Нам необходимо комплексно изучать данный вопрос, нам нужны специалисты в области ИИ, информационных технологий и безопасности. Мы должны начинать с университетов, шаг за шагом. Нам необходимо целостное представление.

Гармиш-Партенкирхен, Германия

Семинар - «круглый стол» №4

«Механизмы выполнения норм, правил или принципов ответственного поведения государств в ИКТ-среде»

Энекен Тикк, независимый эксперт (Финляндия): Некоторые мысли о том, как мы можем развить нашу дискуссию об ответственном поведении государств. Мне кажется, что необходимо взглянуть сначала, на каком мы этапе, и проанализировать то, чего мы достигли и кто помогал на этом пути.

Хотела бы вернуться к деятельности не только Группы правительственных экспертов ООН, но и Первого комитета Генеральной Ассамблеи ООН в этой сфере, которой в этом году исполняется 20 лет. Если мы посмотрим на численность и состав стран, то поймем, как государства и международное сообщество должны подходить к проблемам международной информационной или кибербезопасности.

На протяжении последних лет заметен большой интерес к обмену мнениями по данной проблеме. Многие страны присоединяются к обсуждению. Что касается Группы правительственных экспертов ООН, которая созывалась пять раз, то ее состав значительно увеличен уже, но не включает все страны, желающие принять участие в ее работе. Мы видим, что в течение последних лет идет борьба за членство в данной группе. В целом готовность не только участвовать в дискуссии, но и переходить от теории к практике довольно высока.

Буду говорить о том, как совместить все точки зрения, потому что на предыдущих встречах мы слышали разные инициативы, в том числе и от частных компаний. Полагаю, что существует множество вариантов дальнейшего развития дискуссии. Однако мы еще в фазе обсуждения наиболее оптимального пути развития. Первый путь - всеобъемлющее изучение вопроса. На этом направлении Группой не было достигнуто значительных успехов. Второй - «Дорожная карта»

по реализации того, что было достигнуто в обсуждении. И наконец, создание нового консенсуса, новых принципов международного права.

Также хотела бы поделиться последними результатами нашей работы. На конференции в Эстонии в 2016 году, созванной для обсуждения рекомендаций отчета Группы правительственных экспертов ООН, выработанных в 2015 году, г-н Стрельцов дал свои комментарии по рекомендациям и призвал других исследователей сделать то же самое. Позже этот проект был взят под эгиду УНОДА. И буквально вчера я получила подтверждение, что материалы данного проекта будут опубликованы на сайте организации.

Что же далее? Думаю, у нас еще не было возможности изучить все предложения, представленные Группе, особенно тех стран, которые недавно включились в работу структуры. Полагаю, что хорошей моделью было бы изучение киберпреступности и использования ИКТ террористами. Важно учитывать взгляды всех стран, которые вносят свой вклад. Работа Группы заключается не только в обеспечении нашей безопасности, но и в развитии доверия и понимания, культуры информационной безопасности.

Основываясь на своем опыте, могу сказать, что результаты работы Группы в первую очередь направляются в министерства иностранных дел или даже министерства внутренних дел, но не в министерства и структуры, занимающиеся информационной безопасностью на более низком уровне. И это нужно изменить.

Институт киберполитики уже начал изучение возможности реализации инициатив, что позволит нам понять, как можно реализовать идеи, какие дальнейшие шаги предпринять, как можно усовершенствовать международное право. Необходим консенсус в понимании всеми сторонами преимуществ и недостатков международного права в этой сфере. Важно понять, какие страны могут сделать наибольший вклад в тот или иной вопрос. Важную роль играют и принципы, на которых государства готовы выстраивать деятельность и на которых страны могут двигаться вперед. И все это необходимо учитывать в подготовке последующих материалов.

Гармиш-Партенкирхен, Германия

Основные проблемы применения международного права в ИКТ-среде

Стрельцов А.А., Институт проблем информационной безопасности МГУ им. М.В.Ломоносова: Группа правительственных экспертов, начиная с 2004 года и заканчивая 2017-м, провела титаническую работу по разъяснению всем, в чем заключается угроза, которая возникает в ИКТ-среде, что такое ИКТ-среда, кто является основным источником этих угроз, как государству смотреть на всю эту ситуацию. И апофеозом этой титанической работы стал доклад, который был подготовлен в 2015 году Группой правительственных экспертов ООН. В нем были сформулированы результаты исследования норм, правил или принципов ответственного поведения государств в информационном пространстве.

Уверен, что далеко не все понимают, что там написано, а если понимают, то каждый по-своему. И еще более точно: те эксперты, которые работают на Группу по-разному понимают то, что там написано, а ведь они будут помогать или формировать мнение Группы, как голосовать, за что голосовать, в каком направлении двигаться. Поэтому, на мой взгляд, очень полезно было бы продолжить обсуждение того, как можно трактовать ИКТ на базе принципов международного права, которое, как зафиксировано в 2015 году, применимо к тем отношениям, которые формируются или реализуются в ИКТ-среде.

Вместе с тем в 2015 году здесь, в Гармише, была высказана идея: чтобы дальше заниматься этими принципами, правилами и нормами, нужно сформировать группу, в которую вошли бы юристы, инженеры, военные, представители спецслужб, и таким заинтересованным коллективом попытаться понять, куда и как нужно двигаться дальше. Это было реализовано отчасти при подготовке таллинского руководства. Но вместе с тем у меня сложилось впечатление, что специалисты-юристы, которые работают в международном праве, не слышат инженеров или не понимают, что они говорят, а инженеры плохо понимают, что говорят юристы. А без понимания этого очень трудно сказать, в чем те проблемы, которые мы имеем.

Что меня озадачивает? Две группы правительственных экспертов говорят о том, что международное право применимо как

минимум лет десять. Все говорят о том, что кто-то на кого-то нападает, и за десять лет нет ни одного случая консультаций по поводу конкретных атак. Ни одного случая обращения в суд. Вопрос: почему? Что же это за право такое, которое применимо, и в то же время применить его нельзя, поскольку никто не знает, что делать.

В чем проблема, с которой сталкивается любой юрист, пытающийся заняться этой проблематикой? В основе международного права лежит понятие суверенитета, а суверенитет всегда имеет пространственные границы. Всегда. Пространственные границы суверенитета всегда определяются некоторыми международными договорами между основными субъектами международного права, и эти субъекты берут на себя обязательства. При выполнении этих обязательств исходят из того, что они устанавливают некий режим государственной границы, который позволяет им обеспечить реализацию своих международных отношений, - торговля, борьба с преступностью и т. д.

В ИКТ-среде нет этих границ. Кто за что отвечает?

Говорят, к примеру, что Россия напала на кого-то. Возникает вопрос: откуда это взяли? За что Россия отвечает в этой ИКТ-среде? Где хоть один документ, где написано, что Россия отвечает за такие-то IP-адреса? Да, наши граждане получали эти адреса. Но они могут жить и работать, где угодно. Кто это отслеживает? Каким образом? Это первое.

Второе, не менее важное. Государства в рамках принципов и норм ответственного поведения взяли на себя добровольное обязательство не допускать враждебного использования информационных технологий. Какие у них есть средства реализации данного обязательства, если нет границ. Если непонятно, в каком порядке могут применить те специфические для каждого государства средства, которые позволяют этому государству обеспечить единство власти на всей территории страны и в рамках этого государства обеспечить соблюдение гражданами и лицами без гражданства, но пребывающими на территории этого государства, выполнение тех требований, которые государство формулирует. Если нет ничего, как мы все это будем делать?

Мне кажется, когда мы говорим о том, что международное право применимо, мы исходим из двух основных положений.

Мы согласны с тем, что те международные обязательства, которые государства взяли на себя, должны быть реализованы, в том числе и применительно к деятельности ИКТ-среды. Но при этом необходимо четко понимать, что должны существовать некоторые методы идентификации и авторов, и событий, которые в ИКТ-среде существуют и которые потенциально или реально могут рассматриваться как нарушение международных обязательств того или иного государства.

Как мне видится решение проблемы? В соответствии с международным правом каждое государство самостоятельно решает свои проблемы. А правоохранительные и правоприменительные органы государства обеспечивают реализацию тех правовых режимов, которые установлены на территории государства, и в рамках реализации этого установленного режима они готовят предложения политическим лидерам по оценке тех или иных событий, происходящих в ИКТ-среде. То есть, по сути, спецслужбы и правоохранительные органы применительно к ИКТ-среде готовят этот справочный материал. Потому что, кроме них, никто не имеет доступа к тем устройствам, событиям, которые поражены или захвачены каким-то непонятным действием.

Еще раз скажу. У нас нет оснований в ИКТ-среде доверять кому бы то ни было, потому что - это моя личная позиция - все международное право основывается на некоторых базовых положениях. Первое положение: мы видим те субъекты, которые между собой вступают в отношения. Неслучайно нам нужны свидетели, видевшие, как те или иные акторы, принимавшие участие в каких-то действиях, совершали эти действия и в связи с этим вступали в некоторые правовые отношения с другими лицами.

Следующее. Мы совершенно точно должны уметь собирать и фиксировать факты, говорящие о совершении правонарушения.

И третье. Нужно иметь возможность доказать, что между событием и наступившими последствиями существуют причинно-следственные связи. Если мы это не умеем делать, то право не действует.

Что у нас есть в ИКТ-среде? В ИКТ-среде есть данные, которые мы не видим и не можем видеть. У нас есть информационно-коммуникационные технологии, реализующиеся посред-

ством программного обеспечения на технических средствах, и мы не видим, что они делают. Мы не можем наблюдать этот процесс. И уж тем более мы не видим, какая есть связь между тем, как выполнялась та или иная программа, и наступившими негативными последствиями.

Что нужно сделать для того, чтобы право было применимо? Нужно создать условия для ИКТ-среды. Надо научиться определять акторов, фиксировать следы и факты, говорящие о том, что было какое-то событие, которое может иметь негативные последствия. Нужно договориться, каким образом будут фиксироваться события. Надо научиться выстраивать логическую цепочку от тех или иных событий до наступивших негативных последствий. Если мы научимся это делать, то многие вопросы отпадут.

Как мир всегда выходил из такой ситуации? Через доверие к третьей стороне. Судья - это третья сторона, которая независима, которая не заинтересована в поддержке интересов одной из конфликтующих сторон и с объективных позиций исходя из норм права может формировать свое мнение по поводу того, кто соблюдает нормы права, а кто не соблюдает, и как правильно разрешить конфликтную ситуацию.

Также первоочередная работа, без которой очень трудно будет продвигаться вперед, - разработка проекта руководства по применению принципов, норм и правил ответственного поведения государств в киберпространстве. Я говорю: руководство, так как сейчас уже понимаю, что в английском языке есть много слов, отражающих статус этого документа, который может родиться в процессе деятельности некоторой группы. Как я понимаю, мы хотим, чтобы у нас сформировалась некая позиция специалистов по тем вопросам, с которыми мы полностью согласны, по тем вопросам, которые требуют дополнительной проработки, и по тем вопросам, по которым мы не согласны в силу тех или иных причин. Например, вопрос атрибуции - есть такая проблема. Если нет атрибуции, значит, мы создаем условия для произвола.

В 2016 году в Женеве я высказал свою позицию, что проект международной конвенции по международно-правовой ответственности государств за нарушение международных обязательств - очень опасная вещь для применения в ИКТ-среде. Мы все знаем,

что этот проект не одобрен Генеральной Ассамблеей ООН. Он 16 раз возвращается на доработку в комитет, и в 2019 году будет опять обсуждение данного проекта.

Мне кажется, опасность в том, что в соответствии с этим документом, как представлялось юристам, которые работали еще в том комитете, каждое государство, если видит нарушение международных обязательств, может приписать ответственность за это нарушение тому или иному государству и применить к нему международно-правовую ответственность. Это то, что мы видим сейчас в Сирии. Придумали, на мой взгляд, химические атаки, распространили информацию через СМИ, убедили себя в том, что это все было, после этого решили применить международно-правовую ответственность и нанесли бомбовые удары по Сирии. Было? Не было? Неясно. Но есть конкретный ущерб, конкретные последствия, с которыми еще придется разбираться.

Так применительно к ИКТ-среде - еще хуже. Если относительно химических атак у нас есть международная организация, которая может поехать, посмотреть, написать заключение, - хоть какая-то иллюзия того, что мы создаем объективное мнение о том, что там было, - то применительно к ИКТ-среде у нас ничего нет. У нас нет договоренностей. Непонятно, кто будет это делать.

Коллеги, в качестве приоритета на данном этапе предлагаю сформировать совместную группу для подготовки материала, который условно можно было бы назвать «Руководство по применению норм, правил и принципов ответственного поведения государств в киберпространстве».

Трансформация права в условиях новых вызовов и угроз информационной безопасности

Полякова Т.А., Институт государства и права РАН: Анатолий Александрович блестяще охарактеризовал ситуацию с правом. Сегодня никто не понимает, куда двигаться международному праву. Достаточно ли тех принципов и норм, которые заложены в Уставе ООН. Все знают, что это десять принципов. Многие говорят, что на сегодняшний день они применимы и в информационном пространстве. Но существует совершенно разное восприятие самого этого пространства.

Мы говорим об информационной среде и информационном пространстве, и это достаточно широкие определения. Некоторые определения нашли свое отражение в нормативных актах, которые являются указами президента. Но в любом случае, если мы говорим о разных правилах, то надо понимать, что это право, потому что это нормы, без которых сегодня нам трудно договориться. Абсолютно согласна с коллегами, которые говорят о необходимости сотрудничества, а без этого нельзя договариваться о нормах и правилах в международном праве.

Происходит трансформация права, связанная с развитием национального законодательства любого государства. В целом ряде международных актов есть такие нормы. А мы должны говорить о том, как активно развивается сегодня информационное право и в России. У нас вообще это самостоятельная отрасль. И вопросы информационной безопасности, и международной информационной безопасности, и международного сотрудничества относятся к информационному праву. Фундаментальные исследования в этой области тоже проводятся, и как бы мои коллеги ни говорили, что сегодня первичными являются задачи достижения договоренностей, сотрудничества, нам всем, представителям разных государств, надо быть готовыми и с позиции права отстаивать свое мнение, свою точку зрения.

Настроены мы на то, чтобы эти исследования позволили нам найти сегодня очень важные точки соприкосновения, потому что понятно, что решение политических задач без обоснования наших правовых позиций сейчас весьма затруднительно. Согласна, что международники сегодня не могут найти оптимального решения, речь идет в рамках трансформации права, и одним из методов является аналогия. Так, границы в информационном пространстве могут проводиться по аналогии с Арктикой, Антарктикой, по аналогии с космосом. А космическое право активно развивается. Юрий Батурин, наш космонавт, работает в МГУ, возглавляет кафедру компьютерного права и информационной безопасности. Он еще в 1987 году написал работу о праве в группе компьютерной информации. Многие вопросы, затронутые там, и на сегодняшний день остались неразрешенными, хотя уже прошло 30 лет с момента написания этой работы.

Важна и тема правового регулирования отношений, связанных с робототехникой и искусственным интеллектом. Здесь тоже проявляется определенная трансформация. Мы пытаемся понять: это объекты или субъекты права? Может быть, не юристам данная тема скучна и это надо обсуждать на юридических профессиональных площадках. Но я абсолютно согласна с А.Стрельцовым, который сказал, что надо, чтобы это были совместные группы, потому что юристы без специалистов в области информационной технологии не смогут это написать. Но у нас уже появляются проекты, один внесен в Госдуму, связанный с тем, что возникают цифровые деньги как объект гражданских прав. Есть предложение признать сегодня робота тоже субъектом информационных прав и т. д. Нам на перспективу нужно обсуждать и эти темы.

Согласна с тем, что нужно готовить разносторонних специалистов, чтобы не просто одни понимали технические вопросы, а другие - юридические. Исследования должны проводиться на постоянной основе и, безусловно, только в сотрудничестве.

Мика Кертуннен, Институт киберполитики (Эстония): у американцев есть выражение «разведка поля боя». Это не сухие какие-то академические изыскания, это то, чем занимается государство в реальной жизни.

Итак, я рассмотрел различные национальные стратегии кибербезопасности с нормативной точки зрения, прочитал почти все. Несколько основных положений. Исходная ситуация. Всего 70, примерно, стратегий по информационной и кибербезопасности. Это не синонимы, но для целей данного исследования использую их как синонимы. У 113 стран пока нет четкого представления о кибербезопасности.

Каковы общие разделы с точки зрения государств: информационное общество, информационная безопасность, противодействие киберпреступности, осведомленность, международная киберполитика, дипломатический уровень, нормативное развитие. Чего не хватает? Практически отсутствуют ссылки на оборонный сектор. Тем, кто ссылается на это, говорят, что оборонный сектор может поддержать гражданское общество в кризисные времена. Может быть, создается полный спектр.

Хочу сказать, что страны не слишком зациклены на обсуждении применения или неприменения права вооруженного конфликта. Они занимаются повседневными вопросами функционирования общества. Кибертерроризм упоминается в контексте защиты критической инфраструктуры. Это очевидная вещь. Террористическое использование Интернета для пропаганды, вербовки и финансирования - достаточно общая формулировка во всех этих стратегиях. Несколько уточнений. Когда я применяю терминологию «принципы и нормы», под первыми я понимаю факты, под вторыми - ожидания поведения.

Стратегии, доктрины, концепции информационной безопасности являются совокупностью мероприятий и инструментов, которые имеют последствия на всех уровнях. Мы говорим о скучных вещах. Это государственное администрирование. Это стратегия примерно 80 стран. Для 13 стран - это то, к чему нужно стремиться. Надеюсь, что это необходимо и для других государств, и для нас тоже.

Только две страны в своих стратегиях упоминают рекомендации Группы правительственных экспертов ООН, а именно Нидерланды и Австралия. Однако и они не подтверждают свою приверженность нормам.

Может быть, эти нормы проникают в регуляторные фундаменты и основы, меняют домашний юридически-правовой ландшафт и при этом наполняют их эффектом страха, так как рекомендации «Группы 20» могут дать вызов сложившимся нормам этих стран. Далеко не все к этому готовы. И при этом необходимо возвращать мир в равновесие в отношении онлайн и офлайн. И поэтому создаются двойные стандарты, подрывается доверие. Снижается уровень легитимности государств. Особенно сложно в развивающихся странах, где нет достаточных ресурсов.

Далее, нет альтернативы мировому порядку, основанному на нормах и правилах. Мы не можем допустить беспорядок. Поэтому мы должны медленно, но верно продвигаться в этом направлении. Необходимо убеждать государства имплементировать эти нормы. Можно отметить, что происходит универсализация этих явлений на национальном уровне (Финляндия, Эстония).

Итак, есть общий ряд знаменателей, которые мы выявили. И это говорит о том, что мы продолжаем данный процесс и предстоит еще многого добиться. Проект, который инициировал МГУ, а именно кодекс ответственного поведения государств, имеет много общего с нашим представлением. Не упуская из вида расхождения, нельзя допустить, чтобы эти расхождения помешали нам продвигаться вперед в поисках общих знаменателей и переходе к формулированию общих норм и правил общественного поведения. Ведь когда речь идет об информационной и кибербезопасности, у нас много общих моментов. Почему бы не материализовать их?

Крутских А.В.: *Хотел бы поздравить Мику с его докладом, это лучшее, наверное, что я услышал сегодня. Но хотел бы задать вопрос: Десять заповедей Господних являются международным правом? И было бы нам легче жить на планете все это время, если бы не было десяти заповедей Господних? Может быть, можно было бы провести аналогию с тем, чем нужно заняться юристам. Может быть, не обязательно называть все это международным правом? Но нужен какой-то моральный кодекс поведения государств, чтобы государства четко знали: что можно, что нельзя. И хотелось бы напомнить всем, что, когда мы сочиняли ооновскую резолюцию, то в разделе, где обговаривались нормы (это будет интересно юристам), нормы были поставлены на третье, и самое последнее, место. На первом месте были правила, принципы и только потом нормы ответственного поведения государств.*

Вы спросите: а почему так получилось? Я это сделал под огромным давлением США и западных стран, и особенно Великобритании. Именно их юристы в Группе правительственных экспертов объясняли, что нормы - это самое безответственное, что только может быть в английском языке. Вот почему они хотят мягкое право. Они хотят добровольное право. Они хотят самое-самое неприменимое право. Поэтому русское слово «правило», на чем настаивали первоначально мы, хотя и стоит первым, но о нем сейчас мало кто вспоминает. А ведь наш документ изначально назывался «Правило». Принципы тоже оказались слишком серьезными. Вследствие чего мы пошли на компромисс и согласились со словом «нормы», мягкое право. Вот сегодня предлагаю назвать это заповедями, конечно, не Божьими, но нашими заповедями, международного сообщества, потому что сейчас этих заповедей в киберпространстве в принципе нет.

Этика как инструмент обеспечения стабильности в контексте международной информационной безопасности

Бирюков А.В., Московский государственный институт международных отношений МИД России: Нам надо создать человеческие заповеди. А это особая и очень серьезная и сложная задача. Мы приехали сюда в пятницу 13 апреля, а в субботу, 14-го числа в ночь состоялся удар по Сети. И это означает, что человечество еще на один шажок приблизилось к «красной черте», за которой, к сожалению, находится варварство и все, что с ним связано. Поэтому тема этики, на мой взгляд, особенно актуальна и сегодня, и в принципе, тем более в условиях возрастающего влияния научно-технического прогресса на международные отношения, в частности возникновения цифровой эпохи. Современность востребует людей знающих, много знающих, творческих, устремленных в будущее и одновременно высокоморальных. Потому что им в руки вложены такие инструменты, которые могут нанести колоссальный ущерб прежде всего биосфере Земли.

Проблема заключается в том, что, во-первых, в мире доминируют цели, несовместимые с глобальным приоритетом и справедливостью, и во-вторых, несмотря на разнообразные препятствия, знания и творчество, все активнее проникают в общественную жизнь ряда стран. Однако результаты такого проникновения на данном этапе развития человечества вовсе не всегда приближают его к безопасному благополучию, к которому мы все стремимся. В условиях перехода к многополярному миропорядку эти проблемы обостряются, а глобальная нравственная революция, о которой так много говорят ученые, к сожалению, пока не становится реальностью. В мире наблюдается целый ряд противоречивых тенденций, связанных с этикой.

Хотел бы сказать о следующем. Продолжает работать созданная в 1998 году Всемирная комиссия по этике научных знаний и технологий при ЮНЕСКО. Ее эксперты акцентируют внимание на человеке, благополучие и интересы которого приоритетны по отношению к науке и технологии. По их мнению, человек несет ответственность за принимаемые им самим

решения, и применение новых знаний и технологий возможно только с согласия человека. Свободная воля человека должна опираться на адекватную информацию и может проявляться в возможности изменить решение в любое время без объяснения причин.

Эти идеи вошли в доклад о принципе и уважении уязвимости человека и целостности личности. А соблюдаются ли эти заповеди в мире, в том числе в информационном кибернетическом пространстве? Со второй половины XX века растет понимание, что человек берет на себя ответственность не только за судьбу общества, но и биосферы как таковой. Создав качественно новые производительные силы, он вовлекает нарастающим темпом запасы энергии вещества, накопленные этой самой биосферой за сотни миллионов лет, став, по существу, основной биологической силой планеты.

Так вот, одна из центральных задач научно-технического прогресса заключается в том, чтобы снизить антропогенное и техногенное давление на биосферу Земли, на гомеостат биосферы Земли, если быть точнее. Это означает, что возникает основа этики ноосферы, когда человек не имеет права перейти границы, необратимой деградации природы. Осмысление человеком себя как составной части биосферы, от которой зависит все живое на планете, является важнейшим шагом в понимании собственной ответственности. Вполне закономерно, что к числу этических принципов, зафиксированных в документе, посвященном изменению климата, отнесены обязательства по ненанесению вреда другим людям и окружающей среде, осуществлению устойчивого развития, интеллектуальной и моральной солидарности человечества, общей, но идентифицированной ответственности стран в связи с влиянием на климат.

Еще одна важная тенденция в области этики связана с развитием так называемых социально ответственных инноваций. Казалось бы, все это несколько в стороне от развития информационно кибернетического пространства. Однако, если вдуматься, все это вписывается в данное пространство, отражает тенденции, развивающиеся на этом пространстве. Так вот, социально ответственные инновации предполагают сплав социальной ответственности и инновационного прорыва. В Европе, которая

с точки зрения осмысления данного феномена на корпус опережает другие страны, другие регионы, исходят из того, что социально ответственные инновации должны быть ориентированы на получение общественно значимой выгоды и находятся в поле зрения общества и, следовательно, должны быть открытыми, прозрачными и доступными.

То есть общественная значимость, дополненная общественным контролем, является достаточной гарантией того, что рыночная сущность инновационной деятельности всегда будет корректироваться в позитивном направлении. Хотел бы в связи с этим явлением ответственных инноваций обратить ваше внимание, что инициаторы идеи и последователи, люди, превращающие ее в реальность, огромное внимание уделяют этике и морали, по существу клятве Гиппократа, но применительно к ученым, которые занимаются наноиндустрией или биотехнологиями, или большими данными, - все они принимают своеобразную клятву Гиппократа, то есть руководствуются правилами и общественно признанными нормами.

К сожалению, в современном мире господствуют негативные тенденции, связанные с деградацией человеческих ценностей, об этом мы много говорим в том числе в дискуссиях «на полях» данной конференции, расцветом однополого существования, нарушениями Божеских заповедей, культивированием двойных стандартов, исключающих единство этических норм - основ человечества.

На информационно-кибернетическом пространстве также наблюдаются весьма негативные феномены, один из которых получил название «квадратура Интернета», означающий, что на первом этапе оптимального функционирования Интернета сетевой статус участника виртуального пространства потребовал открытости, анонимности, ответственности поведения и информационной безопасности. И все эти понятия сплелись в единое целое и только в таком качестве могли играть позитивную роль.

Однако реальные противоречия достаточно быстро проникли в виртуальный мир и нарушили упомянутую целостность. Причем речь идет не только о каких-то злонамеренных действиях, не о результате рыночных обстоятельств и даже не о психологических

особенностях общения в Сети. В итоге открытость превратилась в прозрачность доступа к личной информации. Анонимность полностью утратила смысл, трансформировавшись в цинизм и полное неуважение к другим. Ответственность поведения в условиях отсутствия дамоклова меча осталась благим пожеланием, и, наоборот, здесь наблюдается полная безответственность, чреватая самыми негативными последствиями. А информационная безопасность стала уделом богатых, которые могут себе позволить купить ее. И, соответственно, она не гарантирована всем остальным.

На этой конференции в предыдущие дни основное внимание уделялось обсуждению различных правил и норм, то есть праву и деятельности, связанной с обеспечением международной информационной безопасности. Оказалось, в частности, что были достигнуты определенные результаты, например в Группе правительственных экспертов. Согласованы правила ответственного поведения, но, к сожалению, эти правила стали жертвой политических обстоятельств. И несмотря на то что они относятся именно к мягкому праву, они не должны стать жертвой различного рода фобий и предрассудков, которые процветают в международных отношениях. В этой связи, если наша конференция имеет право голоса, хотелось бы где-то зафиксировать необходимость большей решительности и большей ответственности в продвижении хотя бы мягких правовых форм.

Крутских часто говорит о политико-правовом беспределе, который царит на международном информационном пространстве. А Небензя, наш представитель в ООН, недавно в связи с «делом Скрипалей» заговорил даже о запределе, то есть мы доходим до такого состояния, когда нам надо срочно, быстро, эффективно, дружно создавать те самые основы ответственного поведения на этом пространстве.

И еще. Вчера завершилась сессия об искусственном интеллекте. И это достаточно скорое будущее. А в условиях, когда человек уже не сможет адекватно и полно фиксировать все изменения, которые происходят при социально-экономическом и научно-технологическом прогрессе, вопросы этики абсолютно возрастают. Человек должен быть главной фигурой на Земле, иначе будет царить искусственный интеллект, а это реальная угроза в будущем.

Шестнадцатая научная конференция Международного исследовательского консорциума информационной безопасности

Шерстюк В.П.: *Мы начинаем работу Шестнадцатой научной конференции Международного исследовательского консорциума информационной безопасности (МИКИБ).*

В 2010 году 11 организаций из девяти стран мира сочли необходимым объединить свои усилия для изучения основных проблем в сфере международной информационной безопасности. Мы организовали консорциум для того, чтобы обеспечить непрерывность работы в течение года. В какой-то мере нам это удается. Силами консорциума мы выполнили ряд проектов, которые получили высокую оценку международного экспертного сообщества. В частности, был разработан глоссарий по международной информационной безопасности. Мы с вами определились с 50 терминами для межгосударственного и межэкспертного общения по нашей проблематике. Глоссарий существует на русском и английском языках, переведен на китайский, корейский, японский и широко используется нашими экспертами. Сегодня в состав консорциума входят 28 организаций из Азербайджана, Белоруссии, Германии, Болгарии, Великобритании, Индии, Израиля, Казахстана, Канады, Киргизии, Китая, Республика Корея, России, США, Швейцарии, Эстонии и Японии.

Подобная политическая география дает возможность представить на заседании консорциума весьма широкий спектр взглядов позиций по обсуждаемым вопросам. Члены консорциума практикуют и многосторонние и двусторонние встречи. За прошедший год под флагом консорциума состоялись двусторонние консультации между Россией и Японией, стороны провели подробное обсуждение проблем в сфере международной информационной безопасности. В декабре на площадке МИД России мы провели Пятнадцатую научную конференцию нашего консорциума. Организаторами этого заседания консорциума выступили журнал «Международная жизнь» и Институт проблем информационной безопасности. В конференции участвовали представители Академии наук Белоруссии, ГМК «Норильский никель», Института Восток - Запад, одного из канадских фондов, Международного института стратегических исследований (Великобритания), «Лаборатории Касперского», Института электроники и телекоммуникаций Кыргызского государственного технического университета им. Раззакова.

Конференция прошла на очень высоком уровне, в частности, на конференции выступили заместитель министра иностранных дел Олег Сы-

ромолотов, представители Совета Федерации, Министерства обороны РФ, Министерства внутренних дел РФ, ряда международных организаций. На прошлом заседании консорциума мы выработали предложения к программе форума, который проводим сегодня. Эти предложения были разосланы всем членам консорциума по электронной почте. Хотел бы предоставить слово секретарю нашего консорциума для того, чтобы он ознакомил вас с резолюцией, которая была принята на предыдущем заседания консорциума.

Шаряпов Р.А., ответственный секретарь МИКИБ: Уважаемые коллеги, по итогам Пятнадцатой научной конференции МИКИБ была принята резолюция. Текст документа был размещен на сайте нашего института и на сайте нашего консорциума на русском и английском языках. И за прошедшие уже более четырех месяцев от членов консорциума не поступало ни одного критического замечания в адрес данного документа. Мы считаем, что все положения этого документа вы приняли и поддержали. Хочу напомнить, какие основные пункты содержались в резюме Пятнадцатой конференции МИКИБ. В документе было сказано, что на обсуждение международного форума, который сейчас проходит в Гармише, мы предложили вынести вопросы: механизмы выполнения норм, принципов и правил ответственного поведения государств в ИКТ-среде, проблемы противодействия использованию ИКТ в политических целях, проблемы реализации государственно-частного партнерства в области обеспечения безопасности важных объектов инфраструктуры общества, проблемы обеспечения цифрового суверенитета государств. Как вы видите, в нашей программе все эти темы нашли отражение.

Далее в проекте содержался пункт о том, что участники консорциума, участники Пятнадцатой конференции поддерживают проект хартии, который предложил ГМК «Норильский никель», - хартии информационной безопасности критических объектов промышленности. И было предложено презентовать этот проект бизнес-сообществу для его широкого обсуждения. Насколько я знаю, еще в конце лета прошлого года всем участникам консорциума проект хартии был разослан и опять же никаких ни критических, ни других замечаний по тексту хартии и ее содержанию ни нам, ни разработчикам «Норникеля» не поступало.

Одним из предложений, которые содержались в резюме, - было предложение представителя Международного института стратегических исследований из Великобритании и группы организаций, заинтересованных в сотрудничестве с консорциумом, о проведении в рамках нашего форума специального «круглого стола», посвященного вопросам военной стабильности в киберпространстве с участием экспертов из России, США и Китая. Могу сообщить, что «круглый стол» в том формате, в котором планировался, не состоялся в связи с тем, что представители США в последний момент оповестили нас, что не смогут принять участие в данном «круглом столе».

Следующий пункт - традиционный - участники выступают и поддерживают потребность в расширении совместных научных исследований, которые проводит консорциум, и механизмов, способов противодействия угрозам международной информационной безопасности, а также создании условий для прогрессивного развития международного права, регулирующего отношения в рассматриваемой области. Участники консорциума согласились, что в качестве одного из приоритетных проектов консорциума может быть разработка проекта руководства по применению правил поведения и норм ответственного поведения государств в ИКТ-среде. Сегодня на заседании консорциума наш коллега представит предложения Института проблем информационной безопасности по этому вопросу.

Проект хартии информационной безопасности критических объектов промышленности был рассмотрен на заседании «круглого стола» секции №2, дискуссия была весьма интересной и плодотворной. Там же мы услышали и предложение компании «Майкрософт» о создании не аналогичного, но близкого по духу документа «Цифровая женевская конвенция». Резюме Пятнадцатой конференции МИКИБ содержало рекомендации всем организаторам форума, который сейчас проходит, активизировать поиск решения проблем расширения участия представителей российского и зарубежного бизнес-сообщества в обсуждении проблем организации государственно-частного партнерства в области ИКТ, а также расширение информирования международного экспертного сообщества о реализации совместных проектов, проводимых консорциумом, и о результатах нашего форума.

Хочу напомнить, что у нас четвертый год работает сайт консорциума. Около месяца назад была полностью обновлена платформа, значительно улучшены качество работы сайта и навигации. Размещены видеоматериалы по нашим предыдущим мероприятиям. И я призываю вас активнее принимать участие в работе по наполнению содержания нашего русско-английского сайта международного консорциума.

Шерстюк В.П.: *Нет вопросов? Тогда мы продолжаем работу. Сегодня хотелось бы предложить вам обсудить одну содержательную тему, которая не запланирована на других «круглых столах», но вместе с тем имеет большую значимость. Этот вопрос был озвучен на пленарном заседании, когда главный редактор журнала «Международная жизнь» А.Оганесян говорил о защите детей и подростков в Интернете. Мы решили в рамках нашего консорциума вернуться к данному вопросу и его обсудить. Предоставляю слово коллегам из журнала «Международная жизнь».*

Защита детей и подростков в Интернете

Толстухина А.Ю., редактор журнала «Международная жизнь»: Сегодня мы растим поколение онлайн. На наших глазах формируется новый тип личности, которой придется жить и работать в цифровом обществе и конкурировать с искусственным интеллектом. В этой связи наша задача - приложить все усилия, чтобы оградить детей от деструктивной информации и киберпреследований. Объяснить, что виртуальное зло ничуть не лучше того, что совершается в реальном мире. И, конечно, не допустить интернет-зависимости. Меры необходимо предпринимать на всех уровнях, начиная с семейного и заканчивая международным. Бесспорно, первый и главный барьер, который ограждает ребенка от пагубного воздействия Интернета, - это его родители. Важность семейного контроля и повышение цифровой грамотности родителей признает большинство экспертов мира. Следующий важный уровень - государственный.

Надо сказать, что в настоящее время многие страны мира активно развивают различные программы, посвященные обеспечению безопасности детей в Интернете. Функционируют горячие линии, оказывающие психологическую помощь детям, которые пострадали от кибербуллинга, от так называемых групп смерти и других угроз.

Во-вторых, в школьную программу вводятся уроки по кибербезопасности. Такие уроки уже введены в Великобритании, в России, готовятся в Индии и других странах. В-третьих, устанавливаются фильтры в образовательных учреждениях, в школах, в библиотеках.

Еще один важный участник в вопросе кибербезопасности, наряду с государством и семьей, это, конечно, бизнес, занимающийся IT-технологиями и интернет-индустрией. На наш взгляд, важно обязывать компании - производители, например, тех же интернет-игрушек, более строгими стандартами обеспечения безопасности конфиденциальных данных детей. Более того, любой производитель интернет-вещей и интернет-сервисов, или интернет-услуг должен учитывать, что, по статистике, один из трех пользователей Интернета - это несовершеннолетний пользователь.

Вообще бизнес - это бесконечный поток разнообразных идей, которые потом могут не только хорошо монетизироваться, но и приносить существенную пользу обществу. Приведем пример с мобильным приложением Холд (Hold), которое не так давно разработали трое студентов, стремящихся победить повсеместную проблему интернет-зависимости. Суть состоит в том, что на мобильное устройство устанавливается приложение и чем дольше студент не пользуется своим гаджетом, тем больше на нем накапливается баллов, которые он потом может обменять на бесплатный поход в кино, бесплатный обед и т. д. И это приложение пользуется популярностью в Скандинавских странах. Сегодня к нему подключено около 120 тыс. человек. Скоро оно будет использоваться в 170 университетах Великобритании. Да, студенты - это другая возрастная категория. Мы сегодня говорим о детях и подростках. Но тем не менее, на наш взгляд, было бы полезным разработать подобные приложения для детей и учащихся в школе.

Теперь перейдем к международному уровню. Интернет - это глобальное явление, и, соответственно, киберугрозы, с которыми сталкиваются дети, имеют международный характер. Поэтому без регионального и глобального сотрудничества здесь не обойтись. Большая работа в данной сфере проделывается Евросоюзом, в рамках которого, например, действует программа «Безопасный Интернет» (Safer Internet Program). Также следует упомянуть и сеть информационных центров «Insafe» (European Safer Internet Network), Международную ассоциацию горячих интернет-линий «INHOPE», в которую сегодня входит более 40 государств

мира, и, конечно, Всемирную организацию по защите детей от киберугроз (COP /Child Online Protection), которая была создана в 2008 году в рамках международной организации ITU. Еще одна организация, занимающаяся вопросами кибербезопасности детей, - «NETmundial initiative», которая была учреждена компанией ICANN, Всемирным экономическим форумом и Бразильским госагентством по Интернету в 2014 году.

Однако при всем изобилии различных международных правительственных и неправительственных организаций и несмотря на предпринятые в последние годы меры международно-правовой регламентации сети Интернет, до сих пор нет согласованного набора принципов, которыми бы могло руководствоваться все международное сообщество в деле защиты детей и прав ребенка в интернет-пространстве. Здесь, конечно, можно упомянуть Конвенцию ООН о правах ребенка, принятую в 1989 году, Рекомендацию Парламентской ассамблеи Совета Европы от 2009 года и Женевскую декларацию по вопросам информационного общества 2003 года, в отдельных статьях которой затрагивается проблема безопасности детей в Интернете. Например, в статье 11 отмечается: «Мы признаем необходимость обеспечить соблюдение прав ребенка, равно как и защиту детей, и их благополучие, при разработке приложений и предоставлении услуг на базе ИКТ».

Тем не менее мы считаем, что этого недостаточно. Универсального документа, посвященного исключительно проблемам безопасности детей в Интернете, практически нет. Общественные отношения в этой сфере еще не получили комплексного правового регулирования на глобальном уровне. В этой связи мы выступаем с предложением разработать проект хартии, посвященной исключительно проблеме безопасности детей и подростков в Интернете, которая представляла бы собой рамочный этический документ, выражающий требования прав детей во Всемирной паутине и их защиты. При этом мы считаем, что к разработке хартии должны быть подключены все заинтересованные стороны, и это не только государства, но и бизнес, общественные организации, и психологи, и юристы, и академические круги, и, конечно, сами дети и их родители. Такой документ впоследствии мог бы гармонично дополнить Конвенцию ООН о правах ребенка и стать неким ориентиром для выработки законодательных актов, как на государственном, так и на международном уровнях.

Солдатова Г.В., профессор психологического факультета МГУ им. М.В.Ломоносова: *Раньше мне казалось неуместным на фоне таких серьезных разговоров включать детскую тему, потому что дети все-таки не являются субъектами активного международного взаимодействия. Но сегодня не являются, а завтра будут. Поэтому мы должны понимать, кто нам приходит на смену и что происходит с поколениями, и именно с подрастающими поколениями, которые сейчас активно осваивают онлайн-пространство. Вообще это первое поколение в истории человечества, которое является передовым отрядом по освоению новых технологий. Такой ситуации никогда раньше не было, и мы, исследователи, пытаемся понять, как же все-таки влияет освоение детьми ИКТ на их когнитивное развитие и личностное развитие. Видим, что такое влияние достаточно существенно.*

По последним данным наших исследований в 2018 году и по статистике, у нас каждый третий ребенок - подросток от 12 до 17 лет проводит в среднем в Интернете восемь часов за электронными устройствами, за цифровыми устройствами. Вот считайте, если восемь часов он спит, то треть своей жизни проводит онлайн. Поэтому он живет в смешанной реальности, 50 на 50 = онлайн/офлайн. Взрослые достаточно мало обращают на это внимания.

Члены консорциума, Фонд развития Интернета к этому вопросу относятся серьезно уже много лет, а Фонд занимается администрированием домена SU. У нас очень много исследований. Из них четыре популяционных, два сделаны в контексте международных исследований программ, о которых упоминала Анастасия Толстухина. Мы с 2009 года издаем журнал «Дети в информационном обществе», который уже имеет большой круг своих читателей. Кроме этого, данные наших исследований мы пытаемся превратить в методические руководства, потому что сегодня это необходимо. Министерство образования и науки Российской Федерации сочло необходимым ввести уроки по кибербезопасности в начальной школе, потому что федеральные государственные стандарты говорят о том, что ребенок уже в начальной школе должен изучать поиск в Интернете. То есть уже нельзя оградить наших детей, как делают некоторые родители, от использования цифровых устройств.

С 2009 года Фонд развития Интернета организовал «горячую линию», линию помощи детям онлайн, там работают профессиональные операторы-психологи. На основании исследований, обратной связи линии помощи детям онлайн у нас выделена и сформирована классификация онлайн-рисков, которая включает пять видов. Это информационные, о которых мы здесь все время говорим; коммуникационные, потому что для детей Интернет все-таки в первую очередь инструмент коммуникации, потребительские -

дети это все осваивают очень хорошо, Интернет давно превратился в рыночную площадку; технические и пятый риск - это риск интернет-зависимости, который мы аккуратно называем интернет-увлеченностью.

Что это такое? Это патология или новый образ жизни? Мы склонны считать, что это новый образ жизни. И я поддерживаю те начинания, которые были предложены. Считаю, что основными задачами здесь являются продолжение создания формирования безопасной онлайн-среды. Для этого в Российской Федерации тоже много сделано, в том числе приняты соответствующие законы, например ФЗ «О защите детей от негативной информации», достаточно чище стал Интернет в этом плане, мы это мониторим.

Но таких усилий недостаточно, они должны быть коллективными. И здесь, я думаю, два основных направления, которые должны развиваться в первую очередь, - это повышение цифровой грамотности, потому что мифы о том, что дети все знают и умеют в Интернете, совершенно не выдержали проверку временем. Мы проводили исследования по изучению этой грамотности и обнаружили, что она на троечку с плюсом. Еще хуже ситуация у родителей. Родители в этом плане оказались вообще безграмотными. Между двумя поколениями огромный разрыв. Это говорит о том, что дети остаются бесконтрольны и в одиночестве в онлайн-пространстве. Второе, на что мы должны направлять наши усилия,- это формирование цифровой культуры в онлайн-пространстве, формирование цифрового гражданина.

Шерстюк В.П.: *Сейчас во исполнение нашей прошлогодней резолюции сессии консорциума, передаю слово Стрельцову А.А. У нас было поручение к сегодняшнему заседанию консорциума внести предложения о разработке руководства по применению правил ответственного поведения государств в ИКТ-среде. Пожалуйста.*

Разработка Руководства по применению правил ответственного поведения государств в ИКТ-среде

Стрельцов А.А., ИПИБ МГУ: Уважаемые коллеги, некоторое представление начала этого проекта было сделано в рамках «круглого стола», на котором мы сегодня обсуждали тематику. Предварительно мы рассылали членам консорциума предложения подумать над тем, целесообразно ли реализовывать такой проект, есть ли перспектива его реализации в современных условиях и как именно можно было бы это сделать, если такая перспектива существует.

Члены консорциума по тем данным, которые у нас есть, поддержали это предложение. Исходя из этого, в рамках подготовки сегодняшнего заседания консорциума мы провели некоторые предварительные консультации с теми членами консорциума, которые проявили наибольшую заинтересованность в реализации данного проекта. Но прежде чем перейти к докладу по поводу участников проекта, хотелось бы сказать о самом проекте.

Доктор Тикк вместе с доктором Микой сделали очень хорошую работу. Они подготовили основу для того, чтобы можно было непредвзятым взглядом и с разных позиций посмотреть на те нормы, которые закреплены в докладе Группы правительственных экспертов. С позиций разных экспертов, разных стран, разных культурных представлений о том, что это такое, попытаться понять, существуют ли здесь вообще какие-то проблемы или все, в общем, ясно и как бы особого предмета для дискуссий нет. То, что сделали наши коллеги, - это достаточно большой том, 270 страниц, которые посвящены обсуждению и изложению взглядов экспертов на 12 принципов, правил ответственного поведения государств, содержащихся в докладе.

Мы предварительно встречались с Институтом Восток - Запад, было предложение наших коллег о том, что вряд ли имеет смысл браться сразу за разработку полномасштабного руководства, охватить все нормы, которые есть, и было предложение выделить одну или две нормы для того, чтобы на них попытаться отработать методику подготовки такого руководства, отработать логистику работы в этом направлении и, самое главное, понять методологию того, как именно нужно подходить к разработке такого руководства.

Считаю, что руководство должно включать три раздела. Первый раздел - это исходные положения на применимость норм международного права к ИКТ-среде, исходя из чего мы смотрим на то, как принципы и нормы, которые сформулированы в докладе, будут применяться к этой среде и как мы трактуем ИКТ-среду как объект реализации международных отношений. Потому что без этого как-то не очень понятен будет переход к изложению тех, может быть, не всегда однозначно понимаемых положений в том документе, о котором я говорил.

Второй раздел - это раздел, посвященный обсуждению возможных подходов к применению этих норм. Ведь, в конце концов, наша цель - не столько разработать руководство как таковое,

сколько дать некоторый дополнительный материал тем людям, которые будут дальше продвигать правила, принципы и нормы ответственного поведения и в рамках Генеральной Ассамблеи ООН и, возможно, в других каких-то региональных структурах. Не исключено, что реализация этих принципов и правил будет иметь какие-то региональные особенности.

И, наконец, завершая свое выступление, хотел бы предложить такую логистику. Совершенно очевидно, что такая группа открыта. Она не содержит каких-то междусобойчиков, каких-то закрытых лакун. Но прежде чем выносить на всеобщее обсуждение какие бы то ни было результаты, было бы неплохо, чтобы какая-то небольшая группа заинтересованных сторон предварительно эти результаты подготовила для обсуждения, сама между собой обсудила и потом уже вынесла как коллективное мнение на рассмотрение и членов консорциума, и, может быть, каких-то других субъектов, заинтересованных в том, чтобы заниматься этими исследованиями.

Исходя из этого, предлагается создать дирекцию проекта в следующем составе: Стрельцов, Институт проблем информационной безопасности МГУ им. М.В.Ломоносова, Андреас Кюн, Институт Восток - Запад, Энекен Тикк, Институт киберполитики, Чухи Пак, Центр киберправа университета Республики Корея, и Дэниел Штауффахер, фонд ICT4Peace, Швейцария. Если вы будете согласны с этим, мы, исходя из этих, уточненных с вашей помощью предложений, попытаемся сформировать ядро команды этого проекта.

Цель сформулирована. Теперь этапы. Очевидно, что вся работа не может быть выполнена достаточно быстро. Но мне представляется, что было бы правильно, если мы к осени подготовили бы некоторые графы документа, в котором попытались бы изложить позицию директората этого проекта, и по одной какой-то норме. И показали бы всем, получили бы от вас какие-то замечания, могли бы вынести на очередное заседание нашего консорциума. Некоторые этот проект еще раз посмотрели бы с применением более пристального анализа и обсуждения того результата, который мы получили, и дальше будем двигаться вперед в зависимости от того, что именно у нас получится. Я не берусь предугадать, но надеюсь, что все будет хорошо. И теперь по поводу собственно норм, которые можно было бы взять в качестве основы для анализа. Предварительно и с доктором Тикк я обсудил, и с Институтом Восток - Запад мы договорились, что дадим им предложения, и они еще подумают.

Семинар - «круглый стол» №5

«Проблемы обеспечения «цифрового суверенитета» государств»

Пилюгин П.Л., Институт проблем информационной безопасности МГУ им. М.В.Ломоносова: Мы сегодня поговорим о суверенитете и о том, как его можно обеспечить, реализовать, с чем связана проблема обеспечения суверенитета, почему он нужен, для каких структур, как его правильно понимать, а также о связи суверенитета и цифровой границы и можно ли реально с этим что-то делать.

Хотел бы остановиться на понятии «цифровая граница». Это просто область в цифровом пространстве, где государство может выполнять свои функции, то есть контролировать осуществление своего национального законодательства. Цифровая граница не преследует цель изолировать государство от Интернета. Вообще, это можно сделать проще, без всякой цифровой границы. Поэтому каждое государство, наоборот, на мой взгляд, настроено на интеграцию в мировую информационную систему, и цифровая граница выполняет чисто утилитарную функцию для обозначения области, где будет соблюдаться цифровой суверенитет. Что из себя представляет цифровая граница? Есть разные подходы: граница виртуального мира, распределение по адресам системы «Интернет» и другие.

Наиболее реальный подход связан сегодня с введением, с представлением через совокупность автономных систем. Совершенно простая логичная связка. Каждая автономная система управляется провайдером, провайдер - это юридическое лицо, оно регистрируется, платит налоги и живет по законам того государства, где оно находится. Поэтому совокупность таких автономных систем можно представить как область, которую контролирует соответствующее государство. И государство здесь выступает как регулятор, оно активно не вмешивается в работу

систем, но определяет некие правила, как они между собой должны взаимодействовать. Мы здесь говорим о технических нормативных регулирующих документах, которые определяют, как между собой должны взаимодействовать эти системы, соответственно и люди, которые их используют.

Вообще, граница - это некая линия, разделяющая государства в реальном, скорее даже так - в политическом пространстве. В этом случае у нас граница стягивается в точку или в множество точек соприкосновения вот этих самых различных групп автономных систем. Как правило, такие точки и множество точек - это провайдеры, которые поддерживают точки обмена трафика. В большинстве случаев они являются точками трансграничных берегов.

Также граница - это не просто линия, не просто множество точек, эта граница предполагает прежде всего режим границы. Для обычной границы есть правила пересечения границы, визовая служба, таможня. Экономика играет там важнейшую роль - стоимость содержания границы, инженерные сооружения и т. д. Какой может быть режим цифровых границ? Здесь прежде всего приходят представления о межсетевом экране, который ближе всего по функциям для контроля за трафиком в месте пересечения границ. Однако, как мы понимаем, в этой узкой точке, когда собирается весь трафик, никакой провайдер, никакая точка обмена трафиком с таким большим потоком трафика справиться не сможет. Более того, глубокий анализ трафика в этой ситуации вряд ли возможен. Поэтому возникает задача распределения этих функций, во-первых, по всей Сети, так как каждая автономная система может контролировать трафик точно так же хорошо, как и точка обмена, с одной стороны. И с другой стороны - мы должны преобразовать линию обороны в цифровую границу, т. е. контролировать как входящий, так и исходящий трафик.

Вторая функция, которая очень важна, на мой взгляд, - это расследование инцидентов, опять как по входящему, так и по исходящему трафику, чтобы понимать, какие, с одной стороны, предъявлять претензии, а с другой - выяснить, что было причиной атаки или этого инцидента. Здесь тоже есть интересное противоречие: с одной стороны, с точки зрения

сложности и нагрузки на точку обмена трафика, а с другой - интересно отметить то, что наиболее полная информация о входящем трафике и об исходящем находится там, где это устройство подключено, в той самой автономной системе, которая ближе всего к цели или к источнику.

По мере удаления этих точек регистрации у нас с вами анализ из глобальной Сети будет затруднен, то есть пропадет прозрачность. Поэтому мы можем построить некое распределение этих систем регистрации, вот она появилась по всем автономным системам, но при этом всю информацию, которая будет на них распределена по мере прохождения входящего и исходящего трафика, надо собрать в цепочки, которые нельзя будет разорвать, подделать. Для этого можно использовать разные специальные технологии, в частности, можно использовать блокчейны, о которых мы сегодня будем говорить.

Ну, и последний пункт, который, на мой взгляд, очень важен, с точки зрения обеспечения режима границы - это протоколы, которые обеспечивают маршрутизацию. Для меня критической точкой является именно маршрутизация Сети, протоколы, по которым она строится, и, соответственно, та функция, которая связана с распределением адресов. BGP (Border Gateway Protocol) определяет маршруты, но, к сожалению, протокол достаточно старый и не очень защищенный.

Сейчас просматриваются различные варианты модификации этого протокола, его развития. В частности, прежде всего его финансовая ориентированность требует новых ролей для пиров, которые в нем участвуют. А с другой стороны, очень интересно расширяется понятие конфедерации. В конфедерацию можно включать группы автономных систем, множество автономных систем с едиными принципами политики маршрутизации, что очень совпадает с идеей того, что мы хотим делать в рамках одного, скажем, государства для обеспечения цифровых границ.

Теперь самый главный вопрос. Дело в том, что классическая система предполагает наличие маршрутизатора, который решает много разных задач. Каждую задачу надо программировать, настраивать, запускать. А сегодня существует программно-коммутированная сеть, она позволяет реализовать, скажем так,

более гибкую систему управления Сетью. При этом решающие правила изымаются из маршрутизатора и размещаются на сервере в качестве решающих программ. Они уже стали соответствующими приложениями, а все маршрутизаторы заменяются простыми коммутаторами. В этих коммутаторах нет ничего, кроме таблиц коммутации, и все возникающие проблемы и задачи, которые вам хотелось бы решать, вы программируете и записываете в этом сервере, в этой сетевой операционной системе, в контроллере, который всем этим управляет.

Так вот, представьте себе, что мы построили нашу глобальную Сеть из сетей, построенных подобным образом. В каждой отдельной сети, в каждой автономной системе каждый маршрутизатор управляется сегодня не общим классическим протоколом BGP, а связывается с неким центром, обычно находящимся в точке обмена трафиком, и откуда он требует и получает все эти маршруты по запросу. Так вот, если у нас эти сети будут построены по такому принципу, то можно организовать второй уровень централизации, уровень управления ими на известном протоколе или его модернизации. Более того, у нас с вами сами эти контроллеры данных локальных сетей будут взаимодействовать с главным контроллером, уточнять маршруты, ну, а самое интересное, у нас возникнет возможность реализовывать и многие функции защиты, межсетевые экраны, фильтрацию, регистрацию на уровне коммутаторов, решая это просто как программируемые задачи, соответственно, для контроллера.

Как бы сложно не выглядели первоначальные задачи обеспечения границы, мы имеем сейчас возможность создания единой политики, но, правда, уже на другой технологической основе. Как определить, вообще говоря, цифровую границу? Мы привыкли определять границу как некую реальную линию на местности, в данном случае мы говорим о точках, где у нас будут провода для налаживания каких-то каналов для передачи информации, - это техника. А второе, что требуется для границы, - двусторонний договор, то есть две стороны договариваются: у нас здесь будут границы. Граница будет с такими и такими параметрами. О чем, по сути дела, можно договариваться? Есть разные свойства, разные особенности границы.

Не буду перечислять известные пять положений. Они написаны не просто так, они соответствуют пятиуровневой принятой модели TCP/IP. Мы можем рассматривать и обсуждать возможности цифровых границ на каждом уровне отдельно. И нам просто решать задачи, когда в каждой стране есть общая граница, реальная точка обмена. Каждая такая граница поддерживает режим границы, и мы можем просто их согласовывать. Может быть, ситуация, когда режим границы есть на четвертом, пятом уровнях, а ниже его нет или вообще нет прямого контакта, а страна-транзитер, которая передает трафик, тоже ничего не поддерживает. Мы все равно можем обсуждать вопросы режима границы как разрешение того же визового режима. Мне проще привести пример из своей практики, как между Россией и Аргентиной, иными словами, мы никогда не пересекаемся, мы находимся на разных континентах, но режим у нас безвизовый, то есть прямое прохождение трафика возможно на более высоком уровне, на уровне TCP (Transmission Control Protocol) или для отдельных приложений, куда мы поднимемся и о чем договоримся.

Еще более сложно, когда другой стороны нет. Вообще в практике определения границ в этих случаях принимается закон о границе в соответствии с некоторыми международными приложениями. Когда вообще ничего нет и приложений нет, в этом случае надо вспоминать, что обмен идет, у нас есть провайдеры, у провайдеров есть между собой соглашения чисто технические, они всегда могут служить основой для дальнейшего переговорного процесса и выработки соответствующего консенсуса, если мы хотим его получить. Таким образом, можем использовать опыт провайдеров для получения таких соглашений. Хотелось бы здесь отметить, что возможно предпринять в этом направлении первую попытку создания правовых оснований для правового обеспечения суверенитета. Не знаю, насколько корректно, с точки зрения юристов, но, во всяком случае, любое действие будет практически реализовано между двумя близко лежащими странами, находящимися между собой в хороших отношениях, но которые хотят контролировать входящий-выходящий трафик и защититься от угроз. Это будет первый шаг в нужном направлении.

Далее, мы говорим о том, что есть, но понятно, что в скором времени все будет совсем по-другому - реально возникает второй Интернет, который очень тяжело сживается с тем, что сейчас есть. Говорю про IP версию 6. Там есть много и замечательных идей, и замечательных наработок, но, к сожалению, есть много и недоработок. Что для нас было бы интересно? Не только просто увеличение адресного пространства, я говорю о структуре адреса, агрегации самого высокого уровня, но она распределяется по старой схеме, то есть с ICANN через IANA и т. д.

Обратите внимание на последнюю строчку. Используется определенный набор, блок адресов для распределения в Сети, все остальное достаточно большое пространство остается в резерве. Такое большое количество адресов позволяет нам с вами реализовать географическое распределение адресного пространства. Это то, о чем мы говорили в самом начале, что в IP версии 4 сделать нам не удалось, чтобы разделить соответственно все устройства по их государственной принадлежности.

Вторая особенность, тоже связанная с адресацией, - это вторая половина данного адреса. Это 64 бита, что превосходит весь существующий Интернет в два в 32-й степени раза. Это ужасно много. Смысл здесь интересен. Дело в том, что по стандарту для IPv6 эта часть заполняется преобразованием MAC адреса, то есть реальный идентификатор интерфейса - это реальный идентификатор физического устройства. Тем самым мы можем полностью уйти от анонимности, т. е. с каким адресом вы пришли, известно, с какого устройства вы пришли.

Если у меня есть полная идентификация, я могу дополнительно проверить, IPv6 мне позволяет заняться отдельно и аутентификацией, и шифрованием через свои дополнительные возможности. Но я идентифицировал этот пакет и дальше могу им пользоваться в своей обычной практике, рассматривать его как паспорт, хотите использовать как визу, для взаимодействия с цифровой границей. На самом деле это не всегда здорово. Более того, может быть, не всегда и нужно. Поэтому есть соответствующие возможности получения

анонимных адресов, есть соответствующие возможности использовать другие адреса для технологических целей.

Вообще, один пользователь может иметь сколько угодно адресов, потому что адресное пространство это позволяет. Но если мы ввели какие-то ограничения цифровых границ, то мы можем пропускать только те потоки, которые хотим, а мы с вами в шестой версии имеем еще одно важное дополнение - идентификатор соответствующего потока, чего не было раньше. Кстати SDN управляет именно потоками, и будем разрешать только то, что нам нужно, запрещать то, что не нужно. Это касается не только трансграничного трафика, о котором мы говорим, там обмен. Сегодня вспоминают «Telegram», который пытались блокировать, но ничего не получилось. Но они это исправят и найдут правильное техническое решение.

А мы говорим, в частности, о тех случаях - мы сегодня будет разбирать вопрос безопасности критически важных объектов, критически важных инфраструктур, - где часто ограничение трафика взаимодействия с ним просто жизненно важно. Прошу задавать вопросы, но, если вы заметили, по каждому пункту, о которых я говорил, у меня есть вопросы, соответственно, к представителю ICANN о географическом распределении адресов. Меня очень интересует мнение юристов: можно ли нам отталкиваться от таких двусторонних и односторонних договоров, чтобы выйти на какие-то правовые основания для создания суверенитета, заработает ли блокчейн в этой ситуации и насколько это будет критично для критически важных объектов?

Дэвид Конрад, ICANN: Многое из того, о чем буду говорить, уже было затронуто ранее, но тем не менее освещу эти вопросы. Некоторые технические проблемы, всплывающие при обсуждении киберсуверенитета или юрисдикции, - это возможность идентификации, мое предположение - а я не адвокат и не пытаюсь им казаться - заключается в том, что для обеспечения суверенитета нужен некоторый контроль, а для его обеспечения должен существовать механизм идентификации входа, должно существовать подобие

паспортов или виз. Интернет - очень хаотичное место. Изо дня в день он продолжает работать, что меня удивляет. Люди находят пути обхода блокировок и делают это очень креативно. При попытках определить источники трафика действующих лиц появляются разного рода проблемы.

Во-первых, настоящая архитектура Интернета ни в коем роде не основывается на географии, геополитической географии, она основана на сетевой топологии, что означает, что сеть получает IP-адреса от генераторов IP-адресов, которыми являются локальные интернет-регистраторы, и эти адреса могут использовать в любом месте, где бы ни находились их владельцы. Это может быть как одна страна, так и весь мир, и это работает благодаря системе маршрутизации. Сегодня с ограничениями системы IPv4 один IP-адрес может быть использован разными организациями, и нет механизма, способного определить, кто в настоящий момент использует этот IP-адрес. Это приводит к тому, что видимый IP-адрес не может быть ассоциирован с производителем трафика. Как отметил Джон, существуют проблемы с VPN, которую легко создать, ею легко управлять, и она позволяет хранить информацию в любом месте, что усложняет идентификацию источника трафика. Я даже не буду упоминать TOR, который представляет собой многоуровневую структуру, состоящую из VPN.

Существуют также ограничения в отношении развития Интернета, а именно - приватности данных и анонимности. После раскрытия Сноуденом данных Инженерный совет Интернета (IETF) начал предпринимать действия по усилению приватности, которые усложнили возможности идентификации пользователей сторонними лицами, что еще более усугубится с введением Общего регламента по защите данных (GDPR), в том плане, что законодательные ограничения будут действовать на определение источника информации. Говоря о доменных именах, если у вас был домен высшего уровня, например, .ru или .us, можно было предположить, что сайт или создатель трафика находился в этой стране. Эти ограничения все больше становятся редкостью. Те, кто хочет продать побольше доменов, уменьшают ограничения для тех, кто может завладеть этими доменами, чтобы им не надо было

подтверждать гражданство для получения почти любого домена высокого уровня.

Сложности добавляет система маршрутизации, которая в своей сущности является небезопасной. Интернет-провайдер может использовать любой IP-адрес в любое время, и эта система работает лишь потому, что существуют нормы и конвенции, без которых система стала бы хаотичной, что привело бы к невозможности адекватно пользоваться Сетью. Существуют предложения по улучшению безопасности системы маршрутизации, но они являются излишне сложными и непопулярными.

Есть также и другие препятствия на пути создания общей правовой базы. Во-первых, это инертность. Существующая на данный момент система маршрутизации всегда основывалась на IP-сетях, а не на геополитических границах. Существуют технические средства, способные изменить это, о чем говорилось ранее, но управляющие структуры, созданные за десятилетия существования Интернета, были образованы вокруг идеи существующих парадигм маршрутизации. ICANN отвечает за 1/8 всей базы IPv6-адресов, которые принадлежат интернет-реестрам и мы не можем присвоить их кому бы то ни было еще. Также преградой на пути изменений может стать бюрократия, сложившаяся за эти годы. Инженерный совет Интернета во многом ответственен за это ввиду того, что он игнорирует какие-либо инициативы по изменению системы.

Еще одним важным аспектом является тот факт, что страны могут единолично блокировать доступ к сетевым ресурсам. Примером этому является великий китайский «Фаерволл». Более того, любая корпорация контролирует входящий и выходящий трафики своей сети, и любая попытка нарушить это повлечет увольнение из данной организации. Но на самом деле каждый раз, когда это происходит, существует риск побочных последствий. Последним примером служит блокировка мессенджера «Телеграмм», который, как известно, был заблокирован на территории России. Приведение блокировки в действие проходило путем блокировки 1,8 млн. IP-адресов, которые относились к провайдерам облачных сервисов, таких как «Гугл», «Амазон» и «Cloudflare».

Проблема заключалась в том, что эти провайдеры предоставляют свои услуги и другим сервисам и организациям, и блокировка IP-адресов делала невозможным использование сервисов других организаций, использующих эти же IP-адреса. Мы также видели примеры, когда страны блокировали Интернет, к примеру, Египет несколько лет назад, Кения, Уганда во время проведения выборов в 2016 году, что обошлось в 2,5 млрд. долларов, и это происходило в странах, не в такой мере завязанных на интернет-сервисах, в странах же, более зависящих от Интернета, эта сумма может возрасти в разы. Результатом ограничения границ Интернета является удар по эффективности Сети, ценность которой заключается в количестве ее участников, и очевидно, что блокируются те, которые являются угрозой, а сопутствующая блокировка неопасных ресурсов влияет на эффективность Сети, которая влияет на ее ценность.

Пилюгин П.Л.: *Доклады все были интересными, но вот блокчейн мы еще с вами не обсуждали.*

Комментарий из зала: *Хотелось бы остановиться на определении сетей. Сеть - это совокупность взаимодействующих объектов, включая правила этого взаимодействия. Если это так, то тогда Интернет, как известно, есть сеть сетей, и, собственно, безопасность Интернета и его надежность - это и есть функционирование этой сети. Все разбивается на объекты, на сети, которые входят в Интернет, а также на правила взаимодействия и обеспечение этих правил взаимодействия. Если такое определение принимается, то тогда становится намного легче жить. Тогда оказывается, что в Интернете есть административная часть - это правила и техническая часть - это и каналы передачи данных, и маршрутизаторы, и DNS серверы. Добавил бы еще: слово «маршрутизация» можно заменить здесь, если касаться Глобальной сети. Интернет - это точки обмена трафика, это могут быть Интернет Exchange, это может быть точка взаимодействия двух или более сетей.*

Если эти определения правильны, то у меня вызывает большое удивление, как формулируются критические инфраструктуры относительно Интернета. Нет, я понимаю, что есть критические инфраструктуры. Атомные станции, электрические станции,

гидроэлектростанции, трубопроводы и т. д. Но подчеркиваю, что говорю сейчас именно об Интернете. Как уже отмечалось, существует более 40 определений критической инфраструктуры, поэтому можно считать, что фактически ее нет. Относительно Интернета вообще на самом деле ничего нет.

Сейчас есть активная путаница. Страна утверждает, что вот такая-то сеть крайне важна для нее, например, финансовая сеть, военная сеть и т. д. и защищает эту сеть государственным образом. Но скажите мне, кто защищает Интернет как интерсеть? На сегодняшний день есть интересное представление, что самой главной в Интернете является ICANN, который управляет Интернетом. Вы не смейтесь, я это слышал не только от наших товарищей, я это слышал от очень-очень многих. Мне это утверждение напоминает, что в Москве есть некоторый офис, где ведется реестр улиц - какие улицы уже есть, а каких еще нет. В этот реестр входят и говорят: «Мы построили улицу, как бы нам ее назвать именем вот такого-то. А, уже есть»?

Так вот, на сегодняшний день, переводя это на Москву, мы получаем, что контора, которая регистрирует имена, управляет Москвой. У меня ощущение, что те товарищи, кто хочет «порулить» Интернетом, как в том анекдоте, ищут не там, где потеряли, а там, где фонарь есть. Другой всемирной организации нет, то же самое в странах. Любое государство говорит: «О! Есть домен сервис CRD, вот им мы будем руководить. Всем остальным руководить необязательно. Но это дело стран. Меня заботит сейчас именно глобальный Интернет. Так вот отвечаю. На сегодняшний день есть какие-то правила в ICANN, это что-то есть, есть организация, хорошая, плохая, но есть. А скажите мне, кто-нибудь регулирует хоть какие-то правила?

Отвечаю: в Европе есть некоторая ассоциация, в которой какие-то правила есть. Больше нигде. А это, извините, тот самый Интернет и есть - точки обмена трафика. Какие-нибудь правила есть, как должен быть организован трафик между этими точками обмена трафика? Не видел. А, может быть, кто видел, скажите, пожалуйста? Так вот, если говорить о критических объектах сети Интернет, то оказывается, что у нас описан, по крайней мере, из трех только один, а ко всем остальным мы не подходили вообще. Что самое интересное? Что то же самое творится во всех странах.

Еще раз: мы путаем понятие Сети и выделенной сети. Конечно же, у Центробанка есть своя выделенная сеть и там есть свои правила безопасности. Никто не сомневается. Но как взаимодействует Центробанк? Ну, Центробанк еще ладно. У нас еще есть Сбербанк, у которого миллионы вкладчиков. Вот у Сбербанка, естественно, своя сеть есть. Внутри там все нормально, все сделано. А вот как эта сеть взаимодействует с сетью Ростелеком? Где-нибудь это прописано? Нет. А если коннективити пропадет, упадет, то, извините, миллионы граждан останутся без операций. Вот хотел бы подчеркнуть, первое, если мы обсуждаем Интернет, то должны обсуждать объекты - это сети, а взаимодействия - это не только DNS, а это точки обмена трафика и взаимодействия этих точек обмена трафика, что касается как глобального Интернета, так и Интернета в странах. Поэтому вот тут обсуждается, где граница, где граница? Уважаемые граждане, если это сети, взаимодействующие сети, то это очень просто. Ну, извините, может быть, я упрощаю. Есть тот, кто управляет этой сетью, его можно причислить к какому-либо государству? Он резидент, гражданин? Понимаю, что юристам это сложно, они привыкли к границам, сколько-то мильная зона и т. д. Ну, значит, сложно.

Криптографические проблемы блокчейна

Федоров С.Н., Институт проблем информационной безопасности МГУ им. М.В.Ломоносова: Мой доклад посвящен такой популярной теме, как блокчейн с точки зрения фундаментальной математики, а точнее, с математической или теоретической криптографии. Можно отметить, что в 1992 году родилась одна из ключевых идей, которая была использована в блокчейне, так называемое «Proof of Work» - доказательство работы.

Сам блокчейн представляет собой цепочку блоков, важно то, что каждый следующий блок содержит хэш-значение всего предыдущего блока. Важно то, что нам нужна функция, которой трудно найти коллизии, то есть она заведомо обладает множеством пар, которые переходят в одну точку, но при этом требуется, чтобы такие пары найти было трудно. И эта же хэш-функция используется для этой самой «Proof

of Work». Надо только пояснить, что это свойство позволяет говорить о том, что у нас есть блок цепочки. И если мы хотим поменять его значение, то, скорее всего, с очень большой вероятностью нам придется пересчитывать следующий блок, за ним - следующий и т. д. Для этого надо потратить определенное количество вычислительных ресурсов и, соответственно, времени.

Как происходит работа? Все пользователи Сети, а Сеть у нас одноранговая, то есть все пользователи Сети равны в правах, причем пользователи могут подключаться или отключаться в любое время. Все пользователи хранят текущее состояние блокчейна. Некоторые из них пытаются генерировать новые блоки. В случае успеха они добавляют этот новый блок в конец цепочки и выполняют ее брогкаст, то есть передают всем пользователям Сети. Здесь еще необходим протокол консенсуса, позволяющий пользователям согласовать состояние хранящихся у них цепочек.

В типичном случае это происходит так. Пользователь получает набор цепочек от других участников, проверяет их (цепочек) корректность и выбирает самую длинную цепочку. Она и будет считаться текущим состоянием. Одна из задач здесь - обеспечить согласованность текущего состояния цепочек у всех честных пользователей. Возможно, за исключением нескольких последних блоков, которые еще не имеют достаточного подтверждения в виде своих значений. А общая цель и, видимо, недостижимый идеал - выполнить два основных требования. Живучесть, которая заключается в том, что если честные пользователи согласны добавить некое сообщение - под сообщениями имею в виду некую полезную информацию - как, например, транзакции биткоин и некое подобное, значит, некое сообщение блокчейн, то рано или поздно это сообщение будет туда добавлено.

И второе свойство - это незыблемость, означающая, что сообщение, добавленное в блокчейн, остается там навсегда. Но уже в задаче согласованности возникает проблема. Пока, даже при условии идеальной хэш-функции, строго доказано лишь то, что сейчас с небольшими задержками передачи данных возможен приблизительный консенсус. В синхронных

сетях доказано, что консенсус вообще недостижим. Приложения на основе блокчейнов бывают двух типов. Один, более распространенный, предполагает, что в Сети есть выделенные участники, или центры доверия, которым другие пользователи доверяют выполнять те или другие действия. Благодаря этому можно решить все проблемы, которые здесь возникают, но в таких обстоятельствах нет, по существу, необходимости в самом блокчейне, потому что, скорее всего, все те функции, которые на него возлагаются, можно обеспечить вот этими доверенными центрами.

Второй тип приложения имеет дело с децентрализованной Сетью. Это тот случай, для которого был разработан блокчейн, но здесь пока остается очень много открытых вопросов. Проблемы, самые очевидные, которые возникают, - одни из самых важных. Во-первых, выбор хэш-функции. Дело в том, что существуют разнообразные стандарты на хэш-функции, но все они были разработаны для других целей и насколько они подойдут для систем на базе блокчейна, непонятно. Потом синхронизация времени - это не совсем математический, а больше технический вопрос, но тоже непонятно, как это делать, а время в блокчейне играет одну из главных ролей. Все определяется на основе того, что ни один из пользователей со средними вычислительными ресурсами не может генерировать блок быстрее, чем за определенное время.

Далее протоколы консенсуса - это довольно большая тема, и там много чего разработано. Я имею в виду протоколы консенсуса в распределенных сетях. Тут проблема в том, что нужен свой протокол консенсуса для каждого конкретного приложения. В последних из перечисленных - может быть самое сложное - это доказательство стойкости против разнообразных угроз со стороны злоумышленных пользователей.

В первую очередь надо задаться вопросом: возможна ли вообще защита от тех или иных действий злоумышленников? Это те цели, которых злоумышленник хочет достигнуть. Но стоит сказать и про то, что возможности злоумышленника могут быть разными. Например, если мы рассматриваем такую модель, где противник, как обычно называют злоумышленника в математической криптографии, имеет

контроль над Сетью в смысле того, что он контролирует передачу данных по каналам в большом сегменте Сети. В этом случае он произвольно может задерживать на сколько угодно долго идущие от одного пользователя к другим блокчейны и таким образом за это время генерировать свои цепочки, которые потом, согласно протоколу консенсуса, будут признаны правильными. Тут уже математика совсем закончилась. Некоторые рекомендации, которые можно было бы сформулировать на основе результатов, полученных в математике. Прежде чем применять блокчейн для решения практических задач, следует ответить на ряд вопросов, среди которых следующие: решены ли вышеописанные проблемы, если нет, то оправданы ли риски, возникающие при использовании такого приложения?

Далее. Нет ли подходящего традиционного решения для данной задачи? Возможно, проще было бы использовать какую-то распределенную базу данных, где все подписывалось бы электронной подписью какого-то доверенного центра, и вполне возможно, что это помогло бы решить все проблемы и не нужно было использовать такой довольно новый объект - блокчейн, еще не изученный, к тому же обладающий рядом известных недостатков, в частности, он требует больших вычислительных ресурсов и большого трафика в Сети.

Не избыточно ли использование блокчейнов в приложении? Есть опасность того, что поскольку это очень модное понятие, то разработчики тех или иных систем вполне могут взять какую-то существующую систему и просто куда-то там вставить этот блокчейн и сказать, что у нас теперь все защищено, потому что у нас используется блокчейн, который выступает в данном случае как некая реклама.

Еще вопрос. Действительно ли важно и возможно не иметь в Сети выделенных узлов или центров доверия? Тут надо заметить, что если мы хотим работать с какими-то физическими объектами с помощью блокчейна, даже необязательно с помощью блокчейна, а вообще, то у нас тут же возникает необходимость в неких сертификационных центрах, которые будут подтверждать связь между физическим объектом и тем виртуальным представлением, с которыми работает данное приложение.

Соответственно, если эти сертификационные центры выступают как центры доверия, потому что им доверяют подтверждать эту связь и, соответственно, у них больше возможностей, то есть если злоумышленник будет контролировать эти центры, то у него возникает больше возможностей взлома системы. И еще один вопрос экологического характера. Стоят ли предполагаемые преимущества блокчейнов тех огромных энергетических затрат, которые они требуют? А необходимость в большом потреблении энергии заложена уже в основу понятия «Proof of Work».

В заключение хочу отметить, что рано пока говорить о каком-то внедрении блокчейна куда бы то ни было, еще нет достаточно прочной научной базы для этого, и даже, если блокчейн обладает всеми теми свойствами, о которых все говорят, это не значит, что нет других уязвимостей, которые пока не изучены. С теоретической точки зрения у блокчейна есть полезное свойство, потому что, говоря о протоколах консенсуса, раньше было решение задачи о согласованности между участниками определенной сети при условии, что злоумышленных участников не больше половины. И там все было нормально.

Здесь, говоря о блокчейне, мы переходим уже на следующую ступеньку, когда речь идет не о количестве участников, а об их вычислительной мощности. Когда я сказал, что раньше проблема была решена, это не совсем правда, если рассматривать стандартные атаки. Но существует такая «атака Сибиллы» (Sybil attack), когда противник может порождать произвольное количество подконтрольных ему узлов, участников Сети, тогда консенсус в традиционном смысле был невозможен.

Видна уже какая-то попытка бороться с этим, поэтому «атака Сибиллы» уже не проходит. Потому что речь идет не о количестве, а о качестве участников, об их вычислительных мощностях. На этом пока завершу. Это, наверное, самый сильный результат о стойкости блокчейна, он был опубликован в прошлом году, авторы Пасс Симон и Шлатт. Не смогу на словах передать, какую стойкость они доказали, но важно, что честные участники Сети согласны насчет текущего состояния блокчейна, за исключением конечного числа блоков, это число тоже зависит от всех этих параметров.

Гармиш-Партенкирхен, Германия