УПРАВЛЕНИЕ ИНТЕРНЕТОМ И БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ: ГЛОБАЛЬНЫЕ УГРОЗЫ И РОССИЙСКИЕ ИНТЕРЕСЫ

*

Международная динамика событий в сфере регулирования информационно-коммуникационных технологий и глобального управления интернетом за последнее время дает основания говорить о том, что эти вопросы превращаются в один из центральных нервов мировой политики. Особую значимость приобрел вопрос о будущих путях развития и трансформации глобальной архитектуры управления интернетом.

Как оценить итоги и каков общий дальнейший вектор трансформации архитектуры глобального управления интернетом с учетом неоднозначных итогов конференции Международного союза электросвязи в Дубае (ВКМЭ) в 2012 г.? Какие концепции отвечают интересам российского и мирового сетевого сообщества? Какие задачи в сфере ГУИ должны стать приоритетом российской повестки дня в рамках саммита G8 в Сочи и Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО+10) в 2015 г.? Насколько официальная повестка дня отвечает интересам иных стейкхолдеров? Эффективна ли сама нынешняя модель управления Сетью в свете разоблачений Эдварда Сноудена? Как бороться с трансграничной киберпреступностью?

Для рассмотрения этих вопросов ПИР-Центр провел в Москве[1] ряд международных экспертных обсуждений, в которых приняли участие программный директор Национального форума информационной безопасности Инфофорум *Елена* ***Волчинская****, заместитель директора Департамента регулирования радиочастот и сетей связи Минкомсвязи РФ Георгий* ***Грицай****, советник по правовым вопросам посольства США в России Люк* ***Дембоски****, координатор программы ПИР-Центра Международная информационная безопасность и глобальное управление интернетом Олег* ***Демидов****, советник по развитию законодательства и регулирования* Microsoft Russia *Ульяна* ***Зинина****, заведующая кафедрой международного частного права Дипломатической академии МИД России Мадина* ***Касенова****, заместитель Посла Великобритании в России Дэнис* ***Киф****, директор Координационного центра национального домена сети интернет Андрей* ***Колесников****, вице-президент* ICANN *по взаимодействию с заинтересованными сторонами в Российской Федерации, странах СНГ и Восточной Европе Вени* ***Марковски****, член Совета Координационного центра национального домена сети интернет Михаил* ***Медриш****, генеральный директор* Group-IB *Илья* ***Сачков****, советник Экспертной группы № 2 Сектора стандартизации электросвязи (МСЭ-Т) Международного союза электросвязи Ричард* ***Хилл****, председатель Совета ПИР-Центра Михаил* ***Якушев.***

ЯКУШЕВ: Сегодня, после ВКМЭ–2012 в Дубае, перед нами стоят вопросы управления интернетом в глобальной перспективе: произошел ли раскол интернета, стала ли конференция шагом на пути к более совершенной модели управления

или же главным ее результатом стало отсутствие реальных изменений? Кроме того, речь идет о процессе формирования российской позиции в сфере глобального управления интернетом после ВКМЭ–2012. Мы попытаемся понять, в чем состоят стратегические национальные цели и определяющие ценности РФ при подготовке к ВВУИО+10 в 2015 г.

Еще один важный момент — различия в подходах России и ее западных партнеров к вопросам глобального управления интернетом. Где пролегает путь к устранению ключевых противоречий и какова возможная цена консенсуса? Наконец в рамках дискуссии невозможно обойти стороной вопрос о том, какую роль сегодня играет управление интернетом в контексте международной безопасности и глобального развития, как технологические и геополитические сдвиги в архитектуре Сети влияют на ее безопасность и устойчивость, а также на стимулы к дальнейшему развитию частного ИТ-сектора.

Надо отметить, что все эти вопросы обсуждались на площадке Рабочей группы по вопросам международной информационной безопасности и глобального управления интернетом (МИБ и ГУИ) при Экспертно-консультативном совете ПИР-Центра, однако сегодня они будут рассматриваться в рамках более широкого и представительного экспертного формата.

ИТОГИ ДУБАЯ–2012: *SKYPE* И ПРОБЛЕМА СУВЕРЕНИТЕТА

ЯКУШЕВ: На конференции в Дубае и после нее периодически возникали вопросы в отношении того, кто участники процессов, составляющих *глобальное управление интернетом*. К сожалению, поведение российской делегации на встрече в Дубае и те события, которые происходили до и после Конференции, свидетельствовали о превалировании упрощенного подхода, дихотомии, в основе которой лежит противопоставление двух структур: специализированного учреждения ООН — Международного союза электросвязи (МСЭ) и организации, отвечающей за адресное пространство интернета, — Корпорации интернета по присвоению имен и адресов (*ICANN*). Вопрос ставился таким образом, что одна из этих организаций якобы должна была *победить* другую в борьбе за рычаги управления интернетом, и ключевой задачей в рамках такой логики было определение, кого должна поддержать Россия и в чем в этой связи должны заключаться российские интересы.

Этот подход представляется существенно упрощенным, потому что у каждой из этих двух организаций имеется достаточно узкое функциональное наполнение и четко очерченный круг компетенций, которые они реализуют в соответствии со своими уставными задачами. Сводить все глобальное управление интернетом к конфликту между МСЭ и *ICANN*, на мой взгляд, некорректно. Существуют другие международные организации и глобальные дискуссионные площадки. Помимо них на глобальную картину влияют интересы национальных государств, региональных и страновых организаций. В результате ландшафт и проблематика управления интернетом оказываются намного более сложными и гетерогенными, чем бинарная оппозиция двух крупных структур, как зачастую пытались представить итоги ВКМЭ–2012.

Однако в то же время нельзя не приветствовать тот факт, что российская делегация в Дубае и выступления ее представителей уже после конференции в значительной степени подчеркивают важность и значение *мультистейкхолдерского* подхода (*multistakeholder approach)*. Это предполагает участие всех заинтересованных сторон, включая государственные органы, бизнес и гражданское общество, и сегодня к этому перечню все чаще добавляют научно-экспертные организации и сообщество интернет-пользователей. Возникает вопрос: насколько полно этот подход воплощается в практической деятельности российского государства, на площадках вышеупомянутых международных организаций, а также в рамках глобальных дискуссий в сфере управления интернетом.

Важное политическое значение имеет вопрос о коалиционных подходах к управлению интернетом. Позиция, которую отстаивала Россия на конференции в Дубае, не была поддержана большинством участников встречи. Тем не менее совершенно очевидно, что по многим вопросам современной повестки дня Россия не столько солирует, сколько исполняет роль лидера в рамках разнообразных внешнеполитических коалиций: как естественных, т. е. определенных географически, так и тех, которые связаны с определенным уровнем экономического развития, причем оба типа комплементарны друг другу.

В этой связи нельзя не упомянуть страны БРИКС — активный и перспективный для России формат, который, безусловно, нужно дополнить странами СНГ, государствами–членами ОДКБ, а также иными интеграционными объединениями, в которые входит РФ. Однако насколько наши партнеры по таким объединениям понимают и готовы поддерживать то, что Россия предлагает, насколько совпадают их цели и тактические подходы с нашими и, самое главное, насколько наши партнеры готовы отстаивать эти подходы вместе с Россией?

От ответов на эти вопросы зависит объем того внешнеполитического ресурса, которым Россия может располагать при выстраивании собственной линии в рамках глобальной повестки дня в сфере управления интернетом, в том числе в рамках ускоряющегося процесса подготовки ВВУИО+10 в 2015 г.

У меня также есть один специфический вопрос к Ричарду Хиллу. Сегодня огромное количество пользователей по всему миру используют сервисы IP-телефонии, такие как *Skype*. Как вы оцениваете изменение парадигмы телекоммуникаций, которое нам дает развитие технологий, подобных *Skype*, но в то же время влечет огромное количество вопросов экономического толка, проблем, связанных с обеспечением безопасности и т. д.? Поднимались ли эти вопросы в Дубае в формате выработки новых международных документов и если да, удалось ли участникам ВКМЭ продвинуться в их решении? Если же прогресса не последовало, как Вы оцениваете последствия этого факта именно для регулирования телекоммуникаций?

ХИЛЛ: Официально вопросы, связанные с безопасностью сервисов IP-телефонии, в том числе в связи со *Skype*, в Дубае не обсуждались; они лишь затрагивались косвенно в статье нового Регламента международной электросвязи (РМЭ), посвященной безопасности. С другой стороны, финансовые аспекты сервисов вроде *Skype* были предметом обсуждения в рамках ВКМЭ. Стратегического решения по поводу, что делать с вопросами IP-телефонии, принято не было, однако было решено обсуждать эти вопросы в дальнейшем, что указано в Резолюции № 5 ВКМЭ.

Как Вы справедливо отметили, *Skype* и подобные ему сервисы являются предметом оживленных споров, связанных с позицией телекоммуникационных операторов. Дело в том, что сервисы IP-телефонии не платят государственные сборы за право оказания телекоммуникационных услуг (*permission fees*), чем обеспечивают себе конкурентное преимущество по сравнению, например, с операторами GSM-телефонии. Но другие участники рынка, помимо операторов услуг IP-телефонии, имеют резон думать иначе: как и зачем я буду создавать инфраструктуру, если я не получаю денег в обмен на ее создание от субъектов, которые ее используют? Эту позицию активно отстаивали в последнее время европейские телекоммуникационные операторы, и она вызвала и продолжает вызывать много вопросов. Несомненно, отсутствие решения этих вопросов в ходе ВКМЭ–2012 перекидывает мостик к их уже более серьезному и основательному обсуждению в будущем, в том числе, возможно, в рамках ВВУИО+10.

Однако данные вопросы не находились в центре повестки дня в Дубае. Возможно, нам всем здесь будет полезно общее, панорамное освещение повестки дня ВКМЭ, которое планируют сделать коллеги.

ДЕМИДОВ: Господин Хилл, спасибо, я как раз хочу представить некую общую панораму дубайской встречи с международно-политической точки зрения.

Прежде всего надо ответить на вопрос, следует ли рассматривать итоги дубайской конференции Международного союза электросвязи как некий водораздел, рубеж в истории глобального управления интернетом? С одной стороны, это так. С другой стороны, процесс глобального управления интернетом слишком диверсифицирован и включает множество игроков, площадок, параллельно развивающихся событий и встреч, в том числе самого высокого международного уровня. Например, мы ждем Всемирную встречу высокого уровня по вопросам информационного общества в 2015 г., являемся свидетелями регулярных конференций *ICANN*, Всемирного форума по политике в области телекоммуникаций МСЭ в Женеве в мае 2013 г., региональных форумов наподобие Европейского диалога по управлению интернетом (EuroDIG).

В этом смысле ВКМЭ–2012 не была чем-то исключительным. Да, произошло такое значимое в рамках относительно недолгой истории интернета событие, как пересмотр РМЭ. Однако существует всем известная карта со всем известным разделением голосов по итогам Дубая. Особенность ее в том, что она разделена на лагерь сторонников новых инициатив по внесению проблематики интернета в сферу компетенций МСЭ и группу противников таких инициатив. Это было интерпретировано экспертами, СМИ и некоторыми официальными лицами в России и за рубежом как ситуация политического характера, выходящая за рамки технических споров и дискуссий в рамках повестки дня ВКМЭ. И в центре данной политической тематики оказалась Россия как игрок, который инициировал процесс более радикального пересмотра существующего Регламента международной электросвязи, не включавшего ранее даже упоминания интернета.

Политическим моментом здесь является то, что деятельность РФ и поддержавших ее стран (ряд государств Персидского залива и Африки и Китая) стала попыткой через площадку МСЭ закрепить в международном документе идею суверенитета в интернет-пространстве. Это означало бы переформатирование нынешнего подхода к управлению Сетью на основе участия всех заинтересованных сторон в пользу примата государств в части принятия решений.

Такое видение российской позиции и содержания дискуссии в Дубае положило начало тезису о том, что дубайская конференция и ее итоги стали шагами международного сообщества к так называемой *холодной войне онлайн.* Это понятие возникло в первую очередь в западных оценках и в западной прессе.

Но проблема состоит в том, что площадка МСЭ вряд ли подходит для того, чтобы рассматривать вопросы управления интернетом в международно-политическом ключе. Регулирование телекоммуникаций, которое осуществляет МСЭ, это прежде всего комплекс мер сугубо технического характера, которые не подразумевают возможности ухода в плоскость определения суверенитета, определения полномочий государств в области регулирования национального сегмента интернета, поэтому не стоит чрезмерно драматизировать итоги Дубая и скатываться в радикальный спектр оценок.

Мы все знаем, что итоговые изменения, которые отразились в измененном Регламенте международной электросвязи, во многом носят косметический характер по сравнению с теми предложениям государств-участников, которые выдвигались изначально, еще в преддверии ВКМЭ. Со стороны ряда африканских государств поступали предложения о пересмотре принципа тарификации трансграничного трафика, в свою очередь от РФ поступали предложения о введении понятий *суверенитета в интернете* и утверждении права национальных государств на суверенный контроль над системой имен DNS, распределением IP-адресов и т. п.

Эти предложения были сняты на предварительном этапе конференции и не вошли в итоговую повестку 12–14 декабря 2012 г., когда обсуждались самые важные вопросы и утверждался проект обновленного РМЭ. Иными словами, в целом

в ходе конференции работал нормальный механизм согласования позиций; он дал сбой в последний день ВКМЭ, когда принцип принятия решений консенсусом был впервые нарушен в истории МСЭ. Но в течение всего периода подготовки конференции, сбора проектов поправок в РМЭ и большей части самих заседаний в рамках ВКМЭ этот механизм позволял отфильтровать самые радикальные, технически спорные и самые не поддающиеся согласованию консенсусом предложения.

Каковы отсроченные итоги дубайской конференции и почему они вызывают интерес не только у представителей интернет-сообщества, но и у экспертов в области международных отношений? Один из сценариев, который может реализоваться в ближайшей временной перспективе — усиление борьбы за перенос контроля и полномочий в сфере глобального управления интернетом с *мультистейкхолдерских* площадок на межправительственные площадки, где мнения простого или квалифицированного большинства официальных представителей государств будет обладать решающим значением. Неожиданный, но достаточно четкий и мощный импульс этой тенденции придали разоблачения Эдварда Сноудена, которые уже побудили президента Бразилии Дилму Русеф с трибуны ООН призвать к передаче контрольных полномочий по управлению Сетью от *американской ICANN* к структурам ООН.

Вопрос здесь в том, какими путями согласования пойдут и к какой конфигурации консенсуса придут государства в будущем? Удастся ли определить устраивающую всех площадку, которая позволила бы сохранить *мультистейкхолдеризм* как главный принцип глобального управления интернетом и одновременно обеспечить государствам должную степень контроля и полномочий — так, чтобы это негативно не отразилось на процессе управления Сетью и на экономике интернета?

Если консенсус окажется недостижим, возможны достаточно негативные сценарии, которые маловероятны сейчас, но могут актуализироваться в будущем. Один из таких сценариев — *цифровая Вестфалия*. Предполагается фрагментация системы глобального управления интернетом до уровня взаимодействующих, но вполне автономных сетей национальных государств и региональных структур. Такой путь действительно поможет реализовать контроль государств над интернетом и приблизит воплощение концепции суверенитета в информационном пространстве, но при этом пострадают трансграничное взаимодействие и процессы становления глобальной интернет-экономики как мотора глобального экономического развития.

Спрогнозировать, просчитать и проанализировать варианты развития тренда, в том числе исходя из итогов развития Дубайской конференции — одна из задач неправительственного доклада — *Белой книги ПИР-Центра*, мы прорабатываем эту идею в рамках Рабочей группы при Экспертно-консультативном совете ПИР-Центра.

МНИМЫЙ *РУБИКОН* И ВЕКТОРЫ РЕАЛЬНОГО ДВИЖЕНИЯ

КОЛЕСНИКОВ: Я хотел бы коснуться более широкой проблематики, связанной с конференцией МСЭ в Дубае и последующими событиями. Мой более чем 20-летний опыт работы с различными интернет-технологиями дает мне четкую уверенность в том, что сегодня политический процесс и развитие технологий необходимо разделять, потому что технологический прогресс движется на порядок быстрее, чем его политико-административное и нормативно-правовое регулирование. Вместе с тем право, структуры и политические практики тоже неумолимо меняются под влиянием глобальной передачи информации, идей и концепций.

Говоря о холодной войне в контексте интернета и ВКМЭ–2012, моя позиция рискует показаться несколько маргинальной, однако я считаю, что холодная война в интернете в достаточной степени стимулирует и подстегивает к движе-

нию вперед инженерное и техническое сообщество. Такое сообщество в ответ на любой политический вызов, связанный с ограничением прав и свобод в интернете придумывает новые технологии, основанные на самых современных решениях и математических формулах, которые позволяют с успехом обходить противоестественные ограничения на доступ и поиск информации в Сети, но это позиция инженера.

В целом же вокруг интернета существует некая *экологическая гармония*, которая с каждым годом всех нас движет в сторону прогресса — вот такое позитивное утверждение я хотел бы озвучить. На этом фоне представляется, что дубайская ВКМЭ не развернула общую тенденцию и ни в каком смысле не стала *Рубиконом* для управления интернетом.

Второй вопрос, который я затрону — суверенный интернет, который на самом деле есть явление не политическое, а техническое. Можно долго говорить о суверенитете, который необходим различным странам в интернете, а можно проводить активную государственную политику, которая позволяет такую систему реализовать и учитывать национальные интересы в области информационно-компьютерных технологий (ИКТ) в рамках отдельно взятого государства.

Например, Китай не особо ярко и активно выступает в защиту своей концепции *китайского интернета* на международных мероприятиях. Однако количество и объем совершенных КНР технологических прорывов поражают воображение: Китай — единственная страна, где принята государственная стратегия перехода на протокол IPv6. Наблюдая за тем, как развивается IT-экономика в КНР, западные эксперты и комментаторы теряют дар речи, даже не сказав ни слова о защите прав и свобод. Я говорю это к тому, что в практике мировой политики обычно выигрывают страны, которые меньше *болтают* и больше делают — это и есть самая эффективная защита национальных интересов, в том числе по вопросам управления Сетью.

Впрочем, нужно отметить позитивные сдвиги в этом направлении, которые сегодня демонстрирует наша страна уже после спорной по своим итогам дубайской ВКМЭ. В 2012 г. РФ вошла в тройку стран мира, обладающих наибольшей *связностью* интернета, т. е. количество входящих и выходящих трансграничных каналов интернет-коммуникации позволяет говорить о том, что наша страна максимально устойчива к флуктуациям и сбоям работы Сети, и нашу сеть каналов невозможно выключить из одного центра. Об этом можно говорить и этим фактом можно гордиться.

Дальше весьма интересная вещь имела место в мае 2013 г. в Женеве на Пятом всемирном форуме по политике в области электросвязи МСЭ. Россия впервые на моей памяти с трибуны крупной межправительственной организации провела комплексную презентацию своей позиции, показала цифры, представила подробную статистику, тенденции и динамику развития национального ИКТ-сектора. Делегация Минкомсвязи РФ озвучила российские планы по развитию информационного общества, что было весьма интересно услышать, а также оценить подробные данные по российским реальным достижениям в ИТ-индустрии.

Этот тренд мне кажется весьма позитивным и правильным, ведь для эффективного продвижения своей позиции и инициатив слова необходимо подкреплять цифрами, а у России они сейчас такие, что их совсем не стыдно предъявлять всему миру. В области ИТ-сектора Россия сейчас — успешная европейская страна, на равных конкурирующая с ведущими зарубежными партнерами. Вот в чем я вижу один из ключевых приоритетов и сильных аргументов РФ в дискуссиях по вопросам управления Сетью. И на подобный ракурс полезно ориентироваться, не замыкаясь на вопросах мнимой *холодной войны онлайн* и *конкуренции ICANN* с МСЭ.

ГРИЦАЙ: Обозначу основные выводы, а также дальнейшие планы внутренней работы Минкомсвязи РФ, когда дубайский саммит остался в прошлом и мы уже сосредоточились на повестке 2014 г.

Во-первых, в подобных МСЭ широкоформатных организациях голос стран, мнения которых ранее обычно не учитывались, сегодня становится слышен и важен. Более того, традиционные и достаточно примитивные методы манипулирования голосами стран-членов и принуждения их к голосованию более не работают.

Во-вторых, четкая политика принятия решений, ее открытость и понятные средства осуществления — это обоюдоострый инструмент. В рамках именно такого механизма на ВКМЭ–2012 явно проявились промахи российской стороны при подготовке и участии в Конференции, но и промахи делегаций США и европейских стран. Все эти проблемы вскрылись в последний день ВКМЭ — 13 декабря 2012 г., когда был нарушен принцип принятия решений консенсусом государств-членов на площадке МСЭ и проект обновленного РМЭ был вынесен на экстренное голосование по инициативе иранской делегации.

В-третьих, при подготовке к любому масштабному мероприятию в области управления интернетом необходимо учитывать более широкий контекст, нежели тот, которым изначально оперировала российская делегация на саммите в Дубае. В частности речь идет о необходимости учитывать тенденции, инструменты и обязательства, которые принимались нами ранее в рамках других международных форматов, в том числе решения по присоединению России к Всемирной торговой организации (ВТО) и работы по присоединению к ОЭСР.

Связанный с этим вывод, который также надо учитывать при международной работе: в области интернета на самом деле не существует единого подхода, и *мультистейкхолдерский* подход, который пропагандируется и активно защищается странами Запада, не является единственно возможным. Для 89 стран, которые в итоге проголосовали за обновленный РМЭ, более актуален подход государственного административного регулирования, а не регулирования по методу *снизу вверх* (*bottom-up approach*) — и это их суверенный выбор, с которым следует считаться.

Ключевая идея, с которой российская делегация прибыла в Дубай — это начало процесса по получению правовых гарантий равноправного участия государств в управлении интернетом, или, по крайней мере, гарантий учета голоса РФ в вопросах глобального управления Сетью. На данный момент можно констатировать, что такие гарантии в ситуации *status quo* невозможны. Более того, они невозможны и в двустороннем формате, так как ни одно государство по отдельности не управляет интернетом, включая США, несмотря на все технологические и юридические преимущества этой страны. Соответственно, достижение правовых гарантий в многостороннем формате тоже пока невозможно, потому что консенсус между большим количеством государств труднодостижим, что и показала ВКМЭ в Дубае.

Все управление интернетом зиждется на консенсусе между всеми заинтересованными сторонами — в этом заключается и сила Сети, и основные риски, связанные с ее функционированием, поэтому нет никаких гарантий от появления альтернативной системы работы корневых серверов DNS. Теоретически нет никаких правовых гарантий от нарушения консенсуса между *ICANN* и теми организациями, которые занимаются распределением адресных ресурсов в сети интернет.

Отсюда же следует еще один вывод: в отсутствие международно-правовых гарантий равноправного участия в управлении интернетом государства могут иметь лишь некие технические гарантии, которые могут быть получены путем более серьезной работы с теми неправительственными игроками, которые участвуют в саморегулировании интернета. Опять же сила и слабость этих организаций заключаются в наличии открытой политики принятия решений и следовании этой политике.

Интересный пример в этом смысле связан с Инженерным советом интернета (*Internet Engineering Task Force, IETF*) и Советом по архитектуре интернета (*Internet Architecture Board, IAB)* — речь идет о декларации, согласно которой в сферу компетенции этих организаций не входит стандартизация в сфере фильтрации и блокирования интернета. Однако учредительные документы этих организаций равным образом не предусматривают формальных оснований для отказа от рассмотрения этих планов. В частности, компанией *Huawei* и рядом других компаний сейчас прорабатываются проекты, связанные с техническими решениями в сфере фильтрации и блокирования контента в глобальной сети. Момент истины для такого рода организаций — следование принципам принятия решений и правильно организованная работа. Здесь основной вопрос состоит в том, будет ли доведена такая работа до конца и будут ли приняты такой организацией соответствующие документы.

Со стороны российских организаций также прилагаются усилия в этой области, в частности с целью популяризации российских криптографических алгоритмов для различного применения, в том числе в рамках протокола DNSSEC. Также ведется работа над архитектурным принципами интернета, в том числе разрабатываются протоколы глобальной адресации и маршрутизации в Сети и внедрения в них передовых механизмов защиты. В рамках этой деятельности Россия придерживается позиции, согласно которой в интернете на архитектурном уровне должны отсутствовать единые *точки контроля* и единые *точки отказа*, а также должен исповедоваться принцип децентрализации.

РФ в целом и Минкомсвязи в частности, равно как и ряд поддерживаемых министерством организаций, включая представителей интернет-отрасли, ведет работу с *ICANN* и другими организациями по согласованию и выработке политики в сфере управления интернетом. Обсуждаются и готовятся предложения по проверке данных тех лиц и организаций, которые регистрируют ресурсы, доменные имена и адресные диапазоны. Также готовятся предложения по принципам раскрытия таких данных для различных запрашивающих лиц, в том числе для правоохранительных органов, по принципам реагирования на запросы правоохранительных органов в части отзыва регистрации или блокирования соответствующих сайтов.

Отдельная тема — активно развиваемая *ICANN* программа новых доменных имен (nGTLDs), которая нарушила сложившийся баланс между принципами регистрации доменных имен в отношении страновых доменов (ccTLDs) и доменов общего назначения (gTLDs). Если ранее при создании новых доменов верхнего уровня предполагались согласования с национальными администрациями, то в рамках программы nGTLDs этот процесс отсутствует. Тем не менее в рамках программы могут регистрироваться домены, содержащие географические названия-топонимы, а также названия единиц административно-территориального деления или другие названия, в контроле над которыми естественным образом заинтересовано государство.

Ярким примером коллизии, к которой может привести реализация этой программы, стала недавняя дискуссия по поводу домена *.amazon*. Получив запрос на регистрацию такого домена от организации в США и столкнувшись с яростными протестами представителей стран бассейна Амазонки, *ICANN* после долгих дебатов отказала в регистрации домена.

Мы получили сообщение от западного сообщества о том, что его ключевые *стейкхолдеры* готовы работать по достаточно чувствительной тематике защиты детей от информации, приносящей вред их развитию и здоровью, и такая работа должна вестись в рамках ОБСЕ и ОЭСР. В то же время тематика кибертерроризма должна обсуждаться на площадке ОБСЕ, а также в *Большой восьмерке*, площадками для работы по вопросам защиты персональных данных выступают Совет Европы и ОЭСР. Аналогичные площадки возникают и по вопросам контрафактной продукции.

Внутри России необходима концентрация ведомственных усилий, в частности привлечение Минэкономразвития и Минкультуры РФ к выработке консолидированной позиции на соответствующих международных площадках. Позиция Минкомсвязи может быть сформулирована следующим образом: нам очевидно, что интернет является основным на сегодня *проектором* социально-экономического развития с инновационным уклоном, что российский сегмент интернет-экономики, по данным на 2012 г., составил 4,5–5% ВВП, причем темпы роста в этом сегменте были и остаются гораздо выше, чем в иных секторах национальной экономики.

Мы понимаем потребности государства в сфере информационной безопасности, однако политические и технические решения в области информационной безопасности, как правило, обречены быть неким тормозом для развития интернета. Такие решения создают дополнительную нагрузку на бизнес, на операторов, на поставщиков интернет-сервисов. Исходя из этого Минкомсвязи РФ объективно заинтересовано в поиске баланса между запросами государства и интересами бизнеса. Работая по направлению информационной безопасности, мы не хотим разрушить эту сбалансированную конструкцию.

Есть *домашнее задание*, которое должно быть выполнено РФ для содействия глобальному развитию Сети, оно касается повышения внутренней связанности сетей, увеличения точек перехода границы. Важно проводить работу по переносу на российские площадки зарубежных поставщиков контента и сервисов, важно развивать национальных поставщиков контента и различных услуг, не менее существенной задачей является увеличение доли международного транзита в российских сетях. Однако вопросы, связанные с обеспечением безопасности и дополнительной нагрузки на бизнес в данном случае особо чувствительны.

Работа по вышеперечисленным направлениям — основной гарант устойчивости российского интернета, а также залог того, что голос России будет услышан на международной арене в вопросах управления интернетом, в том числе на ключевой площадке ВВУИО+10.

КАСЕНОВА: Очень важным вопросом является компетенция участников международных дискуссий по вопросам управления Сетью, а также сами площадки и форматы решений, которые участники могут принимать. Сегодня в МСЭ, который имеет статус специализированного учреждения ООН, входят 193 государства-члена, и никакие иные *стейкхолдеры* в нем участвовать в принятии решений не могут.

Соответственно, тот обновленный Регламент международной электросвязи, по которому велись обсуждения и голосование в Дубае, должен соблюдаться проголосовавшими за него государствами-членами, а не абстрактным сообществом. Вместе с тем в процесс глобального управления интернетом включены другие площадки, где ситуация может отличаться.

Существует и активно действует площадка Всемирного форума по управлению интернетом (IGF), которая действует с 2006 г. в рамках ООН в соответствии с планом реализации решений Тунисского этапа ВВУИО.

Обратной стороной широкого и равного участия является то, что принимаемые в рамках *мультистейкхолдерских* форматов решения не создают прецедентов и новых норм международного права и в основном носят рекомендательный характер. Суть позиции России заключается в том, что она как суверенный субъект международного права проводит самостоятельную внутреннюю и внешнюю политику в этой сфере, и не делает скидок на специфику информационного пространства в реализации своих суверенных прав. Степень осознания и согласия государства со своей ролью в качестве одного из равноправных участников *мульстейкхолдерской* модели существенно разнится в западных стран и таких государствах, как Россия, Китай, Куба.

ПОЛИТИКА НА ГРАНИ СХОЛАСТИКИ

КАСЕНОВА: Вместе с тем не стоит игнорировать тот факт, что на протяжении практически всей 40-летней истории интернета финансирование его развития велось и ведется преимущественно за счет правительства США. Дело в том, что *ICANN* — американское юридическое лицо, которое было создано в качестве некоммерческой корпорации, и мы имеем дело с ситуацией, когда американское юридическое лицо в своей структуре имеет Политический консультативный комитет (*ICANN Government Advisory Committee*), в который входят представители государств. Это уникальная композиция, но она все равно не меняет статус этой организации.

Сразу после дубайской конференции Россия оказалась в ситуации выбора: сохранить *мультистейкхолдерский* подход, который есть сегодня, либо пытаться перевести организационно-правовую модель глобального управления интернетом на рельсы межправительственной международной организации вроде МСЭ, чтобы утвердить примат государства в процессе выработки глобальной политики в этой сфере.

Вопрос до сих пор открыт, и простого решения не может быть хотя бы по той причине, что эта альтернатива построена на сопоставлении площадок с различными компетенциями. Вообще, смешивание интернета и телекоммуникаций в единую проблематику может быть заложено в российском подходе уже на уровне терминологии и самой концепции.

Характерно, что на Западе говорят об *информационных и коммуникационных технологиях*, а в России во всех документах приводится официально принятая формулировка *информационно-коммуникационные технологии*, что содержательно меняет смысл. С 2005 г. Верховный Суд США определил, что если в контексте тематики ИКТ речь идет об информации, то это вопросы услуг и сервисов, а если речь идет о коммуникации — то это вопросы связи и соответствующих регулирующих норм.

Из этого подхода во многом вытекает политика США на международной арене. Если в рамках международных дискуссий рассматриваются вопросы телекоммуникаций — Вашингтон готов обсуждать их на площадке МСЭ, если же речь идет непосредственно об информации, то это вопросы информационных сервисов, и тогда мы иначе подходим к правовому регулированию этого вопроса. Каждое государство, являющееся членом МСЭ и ООН, обладает суверенитетом, и его право поступать так, как оно сочтет необходимым.

Мне кажется, что создавать один документ для интернета на международном уровне бессмысленно. Однако нужно также учитывать исторический контекст ВКМЭ в Дубае в 2012 г. Предыдущая версия РМЭ была принята в 1988 г., поэтому к моменту проведения ВКМЭ он естественным образом не отражал сегодняшние реалии и нуждался в *апдейте*. Прежний РМЭ имел статус, приближенный к международному договору, соответственно и новый РМЭ будет обладать аналогичным статусом для тех государств, которые его подписали или подпишут. Иными словами, подводя итоги ВКМЭ–2012, следует говорить о конкретных пунктах, зафиксированных в договоре международной организации.

Подчеркну, не следует придавать встрече в Дубае излишнее значение — это просто новый этап осознания международным сообществом, что такое интернет.

МАРКОВСКИ: Да, *ICANN* — это юридическое лицо США, основанное именно в Калифорнии, так сложилась история. Здесь нет противоречия и тем более попыток как-то искусственно уместить процесс глобального управления интернетом в правовое поле США. *ICANN* ни в коем случае не претендует на монополию или исключительность. А еще до основания компании американские представители в 1995 г. обратились к руководству МСЭ с вопросом, хотел бы МСЭ взять под свой контроль вопросы управления системой DNS, а также системой IP-адресов. На это от МСЭ был получен следующий ответ: «На данный момент мы не видим целесо-

образности и необходимости в принятии на себя таких функций, поскольку будущие перспективы развития интернета в целом представляются сомнительными». Видимо, ситуация значительно изменилась.

Однако Дубай не является каким-то водоразделом — все главное нас ждет впереди. Как справедливо отметил Георгий Грицай, в мире есть еще площадки для согласования подходов к управлению интернетом, не говоря уже про процесс подготовки к ВВУИО+10. Также работает комиссия ЮНКТАД по вопросам цифровых технологий и развития интернета, — там тоже участвуют не только государства, но и другие *стейкхолдеры*. В общей сложности насчитывается минимум 7–8 крупных глобальных площадок, на которых идет международное обсуждение вопросов, пересекающихся с дубайской повесткой дня в части управления интернетом.

Главную позитивную тенденцию и залог конечного успеха я вижу в том, что обсуждение идет, пусть и в формате конфликтного голосования, как на ВКМЭ. Вот если диалог застопорится, тогда есть риск, что число подписантов и сторонников нового РМЭ будет шириться и тенденция не обратится вспять.

Приведу любопытную деталь. Как участник ВКМЭ–2012 могу подтвердить, что на дубайской площадке велась широкая и активная дискуссия внутри делегации Евросоюза, и если бы не ряд предложений, внесенных в последний момент, ЕС мог бы согласиться на поддержку большинства тех инициатив, которые были озвучены в начале конференции, возможно, вопреки собственным принципам и интересам.

ЯКУШЕВ: Если возвращаться к совместной позиции монархий Персидского залива, Ирана, Китая и России, то, *во-первых*, суть их предложений — изменение принципа тарификации с учетом трансграничного трафика и введение Международным Союзом электросвязи понятий и определений, связанных с интернетом и регулируемых интернетом. Правда, в финальной версии российских предложений этих понятий было не так уж и много.

Во-вторых, надо понять, ради чего эти предложения выносились. Есть много конспирологических теорий, что в реальности это было сделано ради распространения принципа национального суверенитета в интернете и введения жесткой цензуры в Сети. Подведение вопросов, связанных с инфраструктурой интернета, под национальное регулирование означает закрепление права государств по собственному усмотрению регулировать в соответствии с национальным законодательством контент в интернете.

Из-за этого разгорелся принципиальный спор, так как речь идет о странах, которые известны достаточно жесткой системой цензуры в интернете как по произвольным принципам, что мы видим в Иране, так и по юридически закрепленным принципам, что мы видим в КНР. В России подобного рода цензурные ограничения были введены начиная с ноября 2012 г., но пока они не имеют политического характера.

В-третьих, надо определить, насколько эта позиция отражает интересы стран, которые в том числе являются партнерами России? Казахстан поддержал предложения России, а Белоруссия и Армения выступили против. В этой связи возникает вопрос: насколько эффективно Региональное содружество в области связи (РСС), которое должно было согласовывать позиции своих членов по таким вопросам? К слову, РСС зарегистрировано под российской юрисдикцией как частное предприятие, т. е. как и *ICANN*, в строгом смысле слова не является международной организацией.

В-четвертых, насколько все предложения поддерживаются не только сотрудниками МИДа и Минкомсвязи, но и российским бизнесом и интернет-сообществом? Здесь возникают большие проблемы с соблюдением принципа *мультистейкхолдеризма* и признанием этой позиции как отражающей интересы всех российских граждан и всех пользователей интернета. Да, представители *Координационного*

центра национального домена сети интернет были в составе российской делегации в Дубае и принимали участие в работе конференции, но они не участвовали в выработке российской позиции. В России есть площадка, представляющая интересы бизнеса, — Российская ассоциация электронных коммуникаций (РАЭК), но и сюда представители государственных органов ни разу не обращались для формулирования российской позиции в Дубае.

Все вышеприведенное однозначно отвечает на вопрос о том, насколько российская официальная позиция отражает интересы российского экспертного сообщества и российского бизнеса и как она согласована даже в рамках тех коалиционных международных объединений, участником которых является Россия. Даже по БРИКС мы видим *разноголосицу* в отношении РМЭ.

ГРИЦАЙ: Хотел бы вмешаться и сделать ряд уточнений. Во-первых, Бразилия, как и Россия и Китай, подписала обновленный РМЭ. Во-вторых, Индия, хотя и не голосовала, также не может считаться оппонентом предложенных нововведений, поскольку она зарезервировала время для обсуждения своей позиции на правительственном уровне, т. е. *разноголосица* не такая уж существенная.

Возвращаясь к поддержке Россией модели многостороннего участия в принятии решений; здесь вопроса нет: Россия участвовала в подготовке и подписании документа ВВУИО, где эти принципы декларируются, и Россия их поддержала. Россия также неоднократно выражала свою поддержку данной модели, например, в Довильской декларации *Группы восьми* в 2011 г., и обязалась ему следовать в части разработки своей национальной интернет-политики.

При этом мы разделяем государство в целом и его государственный аппарат. На уровне государственного аппарата решения принимаются и реализуются *сверху вниз*, а на уровне государства в целом работает модель *снизу вверх*. В то же время консолидированная позиция российских ведомств в полной мере не обеспечена, и здесь есть задел для работы, которая пока ведется медленно. Соглашусь также, что в рамках координационных и совещательных органов Минкомсвязи и МИД РФ отечественные неправительственные организации не участвуют, но в рамках экспертных рабочих групп при этих ведомствах участвует значительное число российских специалистов из других организаций.

ХАКЕРЫ: МЕЖДУ КРИМИНАЛОМ И ПОЛИТИЧЕСКИМИ УСЛУГАМИ

ДЕМИДОВ: В контексте управления интернетом и международных усилий в этой области остро стоит проблема киберпреступности. Как здесь обстоят дела и какие проблемы, в том числе проблемы политические, проблемы международные, стоят на пути борьбы с ней?

САЧКОВ: Ежегодно российская компания *Group IB* проводит исследования совместно со 153 партнерами по всему миру и приблизительно оценивает реальный ущерб от компьютерной преступности. Кстати, я хотел бы отметить, что мы специально вводим два понятия: русский и российский рынок. Российский рынок — это хакеры и иные преступники, которые действительно являются гражданами Российской Федерации. Русский рынок шире и соответствует пониманию слова *русский* на Западе, где оно употребляется в адрес любого человека, который может быть гражданином Латвии либо бывшим россиянином, живущим в Таиланде.

Российский рынок весьма не маленький, однако он не является лидирующим в мировом масштабе. Если за 2010 г. рынок российской киберпреступности составил 1,3 млрд долл., то в 2011 г. этот рынок вырос в 1,5 раза и составил 2,055 млрд долл. В то же время русский рынок киберпреступлений — это 4,5 млрд долл. В 2012 г. российский рынок киберпреступности стагнировал и дошел до отметки в 1,938 млрд долл. — такие деньги были похищены со счетов российских и иностранных граждан, а также со счетов корпораций. Кроме того, эти цифры включа-

ют *внутренний рынок* киберпреступности, когда один киберпреступник оказывает услуги другому.

Существенное обострение ситуации с киберпреступностью в РФ пришлось на 2010 г. и последовало во многом из-за чувства безнаказанности и быстрого выхода организованного криминала на этот рынок, а также из-за *дыр* в российском законодательстве. Пробелы в законе в части компьютерных преступлений существуют во многих странах мира, но у нас они достаточно заметны и, увы, никуда не исчезли даже с изменением в декабре 2011 г. главы 28 Уголовного кодекса. Соответственно, никуда не исчезли и сверхприбыли киберпреступников, что обусловливает достаточную сложность этой проблемы в России в настоящее время.

Например, два русских хакера из группы *Carberp*, пользуясь платежной системой *WebMoney*, украли за полтора месяца 24 и 26 млн долл. соответственно. Другой россиянин в возрасте 16 лет первым в мире создал ботсеть, предназначенную для сдачи в аренду, и за полтора года заработал 1,7 млн долл. И это не является исключением из правил — рынок киберпреступности достиг размаха традиционного криминала и стал достаточно опасным. Оборот российской киберпреступности соизмерим с оборотом марихуаны и гашиша.

Характерно, что сейчас многие преступные элементы, которые в 1990-е гг. занимались оружием, наркотиками, торговлей людьми, сейчас переходят в область киберпреступности по причине того, что если торговля оружием и наркотиками сегодня вызывает серьезную озабоченность правоохранительных органов и общественности, проблема организованной киберпреступности все еще игнорируется.

В России также существует понятие *гонки вооружений* в области компьютерной преступности. У нас ежегодно тратятся огромные деньги на информационную безопасность, но при этом количество атак и инцидентов растет. Это происходит, потому что без привлечения людей к ответственности начинается *пинг-понг* злоумышленников и специалистов по ИТ-безопасности.

В группе *Carberp* программист получал 35 тыс. долл. в месяц. Это мировой рекорд по заработку для человека, который занимается разработкой программного обеспечения. Именно по этой причине талантливые молодые люди, к сожалению, становятся на путь совершения киберпреступлений.

В истории российской криминальной хроники не так давно возникли два персонажа: г-н Аникин, российский хакер, укравший у Королевского банка Шотландии 10 млн долл., и г-н Блинников, взломавший рекламный монитор на Садовом кольце. Первый получил пять лет условно, и его СМИ назвали *героем*, второй — шесть лет колонии. Я не понимаю, в чем состоит его *героизм*. После таких случаев люди понимают, что заниматься киберпреступностью выгодно — вряд ли вы получите реальные сроки лишения свободы.

Еще один пример — это Леонид Куваев. Несмотря на действующие в США обвинительный приговор и штраф в 37 млн долл. с возможностью отбывания тюремного заключения до 25 лет, в России его могли посадить только за преступление против несовершеннолетних. Первоначально суд дал ему 20 лет лишения свободы, а потом смягчил до 10 лет лишения свободы.

Основным в России является мошенничество, связанное с интернет-банками, потому что рост электронных платежей в России составляет примерно 200% в год, и хакеры, раньше воровавшие деньги в западных странах, сегодня вернулись в Россию. Во многом трудности борьбы с этим явлением обусловлены отсутствием понятия *место совершения преступления*. Верховный суд говорит, что это место, где злоумышленник получил возможность распоряжаться денежными средствами, но каждый территориальный орган МВД это трактует по-разному — там, где был заражен компьютер, либо где были деньги обналичены, либо где находился расчетный счет и так далее. Это тоже проблема.

Возьмем пример ботнета, созданного для кражи денег у юридических лиц. В своей практике наша компания сталкивалась со многими десятками случаев ботнетов, поражающих тысячи бухгалтерских компьютеров практически всех российских платежных систем. На форумах киберпреступников хакеры, выставляя ботнеты на продажу или продавая доступ к взломанным данным, указывают, сколько денег и в какой валюте находится на счету. Миллионы рублей уходят в теневой оборот.

Современная российская киберпреступность — это люди в возрасте около 25 лет. В 2013 г. были арестованы члены и организаторы самых крупных групп в истории российской киберпреступности, и большинство из них получило реальные сроки. Речь идет о группе *Carberp*, которая действовала против Сберегательного банка Российской Федерации, а также группах *HotPro* и *Hermes*. В каждую из них входили примерно по 20 человек, большинство из них были арестованы, некоторые находились на территории Украины и пытались уйти от ответственности, но в основном все же получили реальные приговоры.

Это пример того, что какие-то позитивные прецеденты в России происходят, но проблем с законодательством, к сожалению, пока еще много. Пример очередного ботнета — 1,4 млн зараженных бухгалтерских машин на территории РФ. Организатор 1987 г. рождения, у других членов преступной группы годы рождения в основном 1983, 1988. Все они долларовые миллионеры.

Есть позитивные сдвиги. В конце 2011 г. благодаря *Координационному центру национального домена сети интернет* мы запустили несколько горячих линий по противодействию *фишинговому* вредоносному программному обеспечению и управлению ботнетами в российских национальных доменах *.ru* и *.рф*. Благодаря этому шагу количество *фишинговых* доменов в России не растет. Это не означает, что люди в России перестанут страдать от *фишинга*, но, по крайней мере, *фишеры* будут аккуратней к этому относиться, к тому же несколько уголовных дел по *фишингу* наша компания во взаимодействии с правоохранительными органами РФ реализовала.

Итак, в России есть проблемы с законодательством и есть проблемы в общественном восприятии кибепреступности. Компьютерных преступников, судя по опросам, которые мы проводили, большая часть населения не считает преступниками, хотя на самом деле они являются уголовниками, а иногда они более опасны, чем *классические* преступные элементы.

Сегодня нам требуется синхронизация международного межведомственного сотрудничества прежде всего в процессуальном аспекте, так как многие преступные группы находятся в странах, которые с Россией в принципе не сотрудничают и могут долгие годы совершать эти правонарушения. На мой взгляд, необходимо ужесточит уголовную ответственность за компьютерные преступления: когда хакеры за кражу 10 млн долл. получают пять лет условно — это не самый хороший пример.

ДЕМБОСКИ: В качестве реакции поделюсь собственным опытом борьбы с трансграничной киберпреступностью. В России я был в качестве дипломата в течение двух лет, но десять лет назад я вел уголовные процессы, связанные с компьютерной преступностью по всему миру. Мой опыт работы в этой сфере гораздо более обширен, нежели на ниве дипломатии, и в ходе обсуждения я вижу, что наши страны имеют точки соприкосновения в плане киберпреступности.

Очевидно, что было невозможно отделить преступления, повлиявшие на финансовую сферу, и рядовые уголовные процессы от проблем в сфере национальной безопасности. Но если мы с вами не в состоянии разделить эти вопросы, если всегда ощущается гигантское присутствие угрозы национальной безопасности, то мы оказываемся парализованы в сотрудничестве по обычным киберпреступлениям.

Соответственно, когда представители российского МИД озвучивают концепцию триады угроз в информационном пространстве, которая подразумевает нераз-

дельность этих угроз, я не могу с ними согласиться. То, что делает интернет успешным, — это степень его подвижности, гибкости, динамичности и рассредоточенности. Если все, что мы обсуждаем сегодня, сводится к тому, что рядовое киберпреступление автоматически становится вопросом национальной безопасности, это сразу все усложняет, и компьютерные мошенники оставляют нас далеко позади по скорости своих действий. Поэтому нужно как можно более четко разделить киберпреступность и национальную безопасность, чтобы мы смогли преуспеть в борьбе с криминалом.

ЯКУШЕВ: Где гарантия, что те же люди за определенное вознаграждение не будут заниматься взломом личных аккаунтов оппозиционных политиков в стране *N*, чтобы предотвратить нормальный избирательный процесс? А после этого те же люди получают деньги и начинают кибератаку против страны *Z*. Фактически они совершают кибернападение. И те методы, тот инструментарий, которым они будут пользоваться, во всех случаях одинаков. К тому же это одни и те же люди. Как можно их противоправное поведение подразделять на разные категории в правовом и процессуальном смыслах?

ДЕМБОСКИ: Методы и каналы, которые они используют в большинстве своем одни и те же, но если вы обратите внимание на хакеров, которые взломали счета Королевского Банка Шотландии, вы увидите, что это преступники и это киберпреступление, а не действия России против США. В Кремниевой долине, когда я веду переговоры с компаниями об инвестировании в Россию, меня не спрашивают о кибервойнах — они заботятся об ответном реагировании российских правоохранительных органов, способности защищать их системы и банковские счета от преступлений.

СЫЩИКИ КАК ДИПЛОМАТЫ

ДЕМБОСКИ: Уголовные дела, которые я возбуждал по всему миру, осуществлялись в самых разнообразных странах, очень сильно отличающихся от США, но преимущественно это были страны из бывшего Восточного блока. Я могу рассказать о трех компонентах в борьбе с киберпреступностью.

Во-первых, вам нужны хорошие законы, но, может быть, не такие хорошие, как вы думаете. *Во-вторых*, вам нужны хорошие технологии, но, может быть, и не самые совершенные. *В-третьих*, и это самое важное, вам нужны очень хорошие личные связи между следователями разных стран. В тех странах, с которыми мы работаем, мы поименно знаем людей, сотрудничающих с нами. Небольшая группа сотрудников правоохранительных органов делает огромную работу по всему миру. Такова моя задача в России: мы хотим выстроить именно такие отношения с нашими российскими партерами.

Возвращаясь к прозвучавшему вопросу, мы на уровне законодательства отделяем киберпреступность как таковую от киберугроз национальной безопасности. Уголовные преступления и сбор доказательств совершенного преступления и преступления против национальной безопасности — это совершенно разные области.

Да, у нас есть уголовное право в этой сфере. Я выступал прокурором в самом большом хакерском деле в истории США в 2010 г., и я прибегал к помощи законодательства о несанкционированном доступе и мошенничестве, которому уже 50 лет. В итоге, я добился приговора о 13-летнем тюремном заключении даже после согласия преступника на сотрудничество со следствием. Все, что было необходимо для этого — это налаженные связи со следователями из других стран.

ЗИНИНА: Хотелось бы задать Илье Сачкову вопрос по поводу утверждения о безнаказанности российских или русских киберпреступников. Вы отметили, что имеются различные проблемы в законодательстве, которые препятствуют расследованиям, а также мешают привлекать преступников к ответственности. Какие

проблемы в наибольшей степени мешают привлечению виновных лиц к ответственности и получению ими реальных сроков?

САЧКОВ: Я уже сказал про мягкость Уголовного кодекса РФ в отношении киберпреступников; мы активно работаем над исправлением этой ситуации. Большинство дел по компьютерным преступлениям подаются в полицию в виде бумажных документов. И если одна преступная группа действует на территории Российской Федерации и совершает 100 преступлений, то до следствия в лучшем случае дойдут один или два эпизода. Были случаи, когда до 20 следователей в разных регионах страны расследовали действия одной и той же преступной группы параллельно, без взаимодействия друг с другом. Такие печальные парадоксы — результат отсутствия синхронизации следственной информации в российской правоохранительной системе. Корень ее заключается в том, что мы пока не можем отойти от бумаги — это проблема технического характера.

Вторая проблема связана с отсутствием четкого механизма определения места киберпреступления. Несмотря на то что существует соответствующий разъяснительный документ Верховного суда РФ и Следственный комитет РФ в случае хищения через систему электронного банковского обслуживания понимает под местом преступления расчетный счет пострадавшего лица, каждый территориальный орган это трактует по-разному. Некоторые дела по киберпреступлениям до двух лет зависают на стадии определения места совершения преступления, от которого зависит, какой орган будет их расследовать.

Наконец люди, которые расследуют компьютерные преступления, в абсолютном большинстве не являются следователями по компьютерной преступности и не имеют соответствующей базы знаний. Это следователи, занимающиеся убийствами и автомобильными кражами, аналогичная ситуация складывается с судьями и прокурорами. Поэтому желательно усилить имеющуюся программу обучения либо создать отдельную группу следователей, специализирующихся на рассмотрении дел по киберпреступности. Сегодня следователей, которые могут качественно довести подобное дело до конца, порядка 15 человек во всей стране, а в оперативном подразделении по неправомерному доступу Управления «К» МВД России буквально 10 специалистов на всю Россию.

Соглашусь с вами и по поводу отсутствия цифровых доказательств. Каждый следственный орган изымает данные по-разному, и сейчас появилось целое поколение адвокатов, которые строят свою работу на защите конкретных киберпреступников. Эти адвокаты знают, что специалисты по криминалистике не всегда действуют юридически корректно, не всегда правильно изымают информацию, поскольку нет универсальной методики изъятия компьютерной информации, да и понятие цифровой безопасности отсутствует.

Проблема Уголовно-процессуального кодекса также очень важна. Мы видим, что не работает главная вещь в правосудии — человек после уголовного срока не прекращает заниматься преступной деятельностью. В одной из киберпреступных групп утром человека задержали, вечером привезли в суд, суд постановил подписку о невыезде, а через два дня этот человек находился в соседней республике, где через три дня запустил свой ботнет заново. Причем речь шла о преследовании по делу об атаке на системы Сбербанку, чьи специалисты информировали о преступлении непосредственно министра внутренних дел РФ. Т. е. человек не боится заниматься заново этим делом.

ЗИНИНА: У меня вопрос к Елене Волчинской. Как вы считаете, насколько Европейская (Будапештская) конвенция о киберпреступности 2001 г. сегодня актуальна? Ведь в самом документе содержится достаточно широкий список составов противоправных действий, совершаемых посредством использования ИКТ, которые признаются уголовными преступлениями. И если сравнивать нормы конвенции с Уголовным кодексом РФ, на кажется очень актуальной для нас. Так почему бы не использовать ее для модернизации нашего законодательства?

ВОЛЧИНСКАЯ: Участники Будапештской конвенции уже два года работают над ее новой редакцией. Это свидетельствует о том, что страны Европы признают ее устаревание. Этот документ достаточно узок по своей сфере охвата, в нем нет востребованных механизмов государственно-частного партнерства, там фактически не решены вопросы юрисдикции и т. д., поэтому если говорить о составах преступлений с использованием ИКТ с акцентом на преступления против контента, нормы конвенции здесь узки и недостаточны.

В этом смысле российский УК идет впереди, мы решаем вопросы, с которыми сталкиваемся в сегодняшней практике киберпреступности. Мы не единственные, кто с ними сталкивался в части экстремизма, в части распространения через интернет информации о наркотиках, т. е. с теми типами преступлений, которые связаны с созданием и распространением неприемлемого и противоправного контента.

В целом вопросов сейчас на повестке дня гораздо больше, они очевидны для всех, учитываются *Группой восьми* и поднимаются в рамках международных встреч и саммитов. Иначе говоря, обновление повестки дня и сопутствующее обновление правового инструментария борьбы с киберпреступностью — это объективный процесс. Будапештская конвенция сделала свое дело, и мы должны очень грамотно проанализировать результаты ее работы.

КИФ: Для борьбы с угрозами кибербезопасности, включая киберпреступность, Великобритания инвестирует в 2012–2015 гг. 650 млн фунтов стерлингов в рамках специальной национальной программы. Мы создали структуру по международной информационной политике в рамках британского МИД, чтобы координировать свои усилия в этой сфере. В настоящее время осуществляется тесное сотрудничество между правительственными органами и Агентством по борьбе с организованной преступностью и прокуратурой, а также ведется работа с нашими заграничными представительствами по оказанию содействия международному сотрудничеству в области наращивания потенциала.

Если мы хотим реализовать такое видение киберпространства, при котором мы совместно с другими государствами ликвидируем *тихие гавани* для преступников, а политические дебаты поощряются и инновациям и творчеству позволено процветать, это потребует усилий со стороны государства, бизнеса и гражданского общества.

С осени 2012 г. мы создали новый центр по наращиванию потенциала в сфере глобальной кибербезопасности в Оксфорде. Этот центр сотрудничает с зарубежными правительствами, международными организациями и частным сектором, чтобы способствовать наработке опыта. Мы выделяем полмиллиона фунтов стерлингов в год на его деятельность. Благодаря этим усилиям мы начинаем менять взгляд международного сообщества на киберпространство. Но мы должны идти дальше по этому пути, так как угрозы и вызовы, с которыми мы сталкиваемся, могут стать более серьезными.

В начале 2013 г. преступники использовали предоплаченные карты *MasterCard* и *Visa*, чтобы похитить свыше 42 млн долларов США из банков по всему миру. Этот случай, а также упомянутые российскими коллегами примеры масштабных киберпреступлений убедительно доказывают, если ничего не предпринимать, благополучие каждого из нас будет весьма уязвимо.

Однако возможности киберпространства, расширяющие экономический потенциал во всем мире, так же важны, как и угрозы в интернете. Британское министерство торговли и инвестиции посчитало, что объем глобального рынка кибербезопасности составляет уже более 123 млрд фунтов стерлингов, поэтому мы должны координировать наш опыт в этом секторе, особенно на рынках с высоким потенциалом роста.

Именно поэтому мы создали *стратегию киберэкспорта*, которая стартовала в мае 2013 г. Мы считаем, что акцент на кибернетические знания и опыт будет только

Подробнее с материалами по информационной безопасности Вы можете ознакомиться в разделе «Международная информационная безопасность и глобальное управление интернетом» на сайте ПИР-Центра по адресу: net.pircenter.org

усиливаться, пойдет ли речь о новых возможностях для процветания или необходимости защиты основных прав человека. И я надеюсь, что наша совместная работа поможет пролить свет на ключевые вопросы, связанные с противодействием трансграничной киберпреступности, послужит закладке и укреплению фундамента международного сотрудничества в преодолении вызовов цифрового века и будет способствовать максимально полной реализации его колоссальных преимуществ.

ДЕМИДОВ: Коллеги, в завершении скажу, что материалы и итоги данного обсуждения будут использованы ПИР-Центром для подготовки доклада — *Белой книги по вопросам информационной безопасности и управления интернетом*, которая будет опубликована в 2014 г.

Примечания

[1] При подготовке круглого стола использованы материалы следующих мероприятий:

а) Международный семинар ПИР-Центра *Информационно-коммуникационные технологии в контексте международной безопасности: поиск общих подходов*, который был проведен при поддержке Министерства иностранных дел Великобритании в рамках проекта ПИР-Центра *Международная информационная безопасность и глобальное управление интернетом* 31 октября 2012 г. в Москве, Россия;

б) Международный семинар ПИР-Центра *Управление интернетом после ВКМЭ–2012 в Дубае: определяя ключевые глобальные тенденции и оценивая российские национальные интересы*, который был проведен при поддержке Фонда содействия развитию интернета *Фонд поддержки Интернет* в рамках программы ПИР-Центра *Международная информационная безопасность и глобальное управление интернетом* 30 мая 2013 г. в Москве, Россия.