

**Стенограмма заседания клуба *Триалог*
15 ноября 2006**

**«ИНТЕРНЕТ, ТЕЛЕКОММУНИКАЦИИ И ГЛОБАЛЬНАЯ
БЕЗОПАСНОСТЬ»**

Докладчик: **Михаил Владимирович Якушев**
Директор по правовым и корпоративным вопросам, *Microsoft* (Россия)

В. А. Орлов:

Коллеги, я приветствую наших членов Клуба на очередном заседании, которое мы называем зимним. И я думаю, что, посмотрев в окно, мы убедимся в том, что у нас действительно уже наступает зима. Это последнее заседание в текущем году.

Я хотел бы вместо традиционного нашего начала заседания, когда я рассказываю о деятельности ПИРа, планируемой и завершившейся, использовать несколько минут для того, чтобы поделиться более содержательным материалом с учетом произошедших со времени предыдущего Клуба нескольких событий.

Первое событие – это северокорейские ядерные испытания и их последствия. Второй вопрос – это процесс обсуждения резолюции Совета Безопасности ООН по Ирану. И третье событие – это изменение в Вашингтоне в политической палитре и приход демократов к власти в обеих палатах Конгресса, равно как и смена руководителя министерства обороны США. Ну а в этом же контексте и завтрашняя встреча Буша с Путиным здесь, в Москве.

Хотелось бы высказать несколько соображений, которые как раз подкрепляются моими только что завершившимися поездками. В частности, северокорейскую проблематику приходилось обсуждать в Европейских столицах. А вопросы Ирана и Российско-американских отношений мне приходилось обсуждать, соответственно, в Нью-Йорке на прошлой неделе, когда пришли российские поправки по резолюции. И в Вашингтоне как раз начиная с того вечера, когда стали приходить известия о победе демократов сначала в Палате Представителей, а затем стало ясно, что они возьмут и Сенат. Таким образом, ряд интересных обсуждений предстоит в Соединенных Штатах и в экспертном сообществе.

По Северной Корее принята очень важная резолюция 1718, показывающая, что Совет Безопасности, если захочет, может конструктивно работать над серьезными вопросами нераспространения и более широких угроз международной безопасности, к которым северокорейское испытание, точнее северокорейское поведение, вероятно, относится. Больше того, я бы отметил повышенное стремление всех постоянных членов СБ ООН к своим единоличным, но и коллективным действиям, которые бы ужесточили санкции в отношении северокорейского режима. И, таким образом, в данном конкретном северокорейском случае, позволили бы начать решение задач по минимизации

угроз, исходящих из Северной Кореи, не нарушая при этом переговорного процесса, а, возможно, и где-то его подталкивая таким образом.

В частности, Российская Федерация не меньше других заинтересована в том, чтобы эффективно осуществлять действие резолюции 1718. Включая и набор финансовых, не предусмотренных этой резолюцией, воздействий на северокорейский режим, с которым у нас торговля небольшая, но с которым у нас идут обмены, в том числе и по чувствительным для руководства этого режима направлениям. Думаю, что здесь Россия, не меньше чем другие будет вносить свой вклад.

Отметил бы здесь и роль Китайской Народной Демократической Республики. Китай, не только полностью присоединился и начал аккуратно исполнять решение резолюции санкционного комитета Совета Безопасности, но проводит сейчас самостоятельные действия, которые, на мой взгляд, четко сигнализируют Пхеньяну о не просто разочаровании, а крайнем недовольстве Пекина тем, что произошло - а именно ядерными испытаниями и глухотой северокорейской верхушки. В этой связи я бы не исключал того сценария, что Китай...Пекин...уже начал или начинает подготовку смены в Пхеньяне. Причем, смены на китайских условиях, а не на американских, и не на японских, конечно, и даже не на Южнокорейских. В этой связи я думаю, что китайцы держат в уме возможность работы под нынешним северокорейским руководством, но активизируются на военном треке - на треке работы с некоторыми военными в КНДР, которые были бы более-менее идеологизированны, гораздо менее прагматичны и смогли бы со временем прийти к власти, осуществив в Северной Корее переход от нынешнего формата крайне идеологизированной диктатуры, к формату, который, скажем так, был когда-то излюбленным в Южной Корее - с крайне жестким управлением, но с привнесением туда совершенно иных экономических, управленческих методов, а также и с курсом на донуклеаризацию. Но это все в будущем. Это, понятно, потребует довольно тонких усилий от Пекина, если конечно, он на них пойдет.

И наконец, последнее по северной Корее. Хотел бы обратить ваше внимание на то, что и другие государства, в том числе и государства в регионах, сопредельных с Северной Кореей, чувствуют, так или иначе, в процессе, который был запущен резолюцией 1718. В частности, даже такая страна, как Мьянма, способствовала тому, что северокорейские грузы, как вы прекрасно знаете, были досмотрены, и сделано это было по просьбе к дискуссии Совета Безопасности, но реально по просьбе Японцев. Поэтому участие здесь даже таких государств как Мьянма в механизмах в отношении Северной Кореи, я думаю, помогают и способствуют тому, чтобы предотвратить потенциально самого опасного, а именно, расползания технологий двойного применения Северной Кореи, которые могут попасть как государственным игрокам, так и негосударственным субъектам - организованным преступным группам в том же золотом треугольнике, или международным террористическим организациям.

Иран. По Ирану, вы знаете, что сейчас идет сложный процесс в Нью-Йорке нахождения совместных подходов государств-постоянных членов Совета Безопасности и Германии. Эту группу можно называть 5+1, хотя реально она называется 3+3. Но, наверное, 5+1 не так уж плохо отражает ее реальную суть.

Думаю, что мы сейчас находимся еще пока далеко от взаимопонимания, но оно возможно. Так же как возможна и сама резолюция.

Пока мы по-разному видим, что находится в интересах международного сообщества больше. Россия, как вы знаете, выступила довольно резко против варианта, изначально предложенного европейцами, но я бы сказал, 3/5 текста было так аккуратно вычеркнуто, практически ничего не дописано. И, к разочарованию европейцев, были вычеркнуты все пункты, связанные с тем, что резолюция делала экзапшн - выводила вопросы Бушерской атомной станции, все вопросы мирной энергетики должны быть выведены из резолюции, поэтому делать какие-либо якобы приятные для России исключения для Бушера не стоит.

Список тех, в отношении кого конкретно предлагается вводить жесткие механизмы недопущения поездок, включает в себя несколько юридических и физических лиц, причастных, как предполагается, не только к мирным, а скорее к двойным, и возможно к военным направлениям – ядерным, баллистическим и ядерно-баллистическим - в Иране. Но этот список, как, наверное, часть из вас представляет, небольшой, он уместается на одну страничку. И, в принципе, против нынешнего списка аппендикса или приложения к резолюции, Россия не имеет никаких возражений. Поэтому я думаю, что расхождения пока еще существенны, они носят не только тактический характер, но они могут быть сняты путем переговоров.

Как и у России, так и других государств-участников шестистороннего процесса, есть интерес и в том, чтобы вопрос решался дипломатическими средствами, но и в том, чтобы Иран не почувствовал себя безнаказанным, игнорируя резолюцию Совета Безопасности от 31 июля, под которой, как мы прекрасно понимаем, российская подпись, так же, как и другие. Таким образом, вопрос ограниченных санкций в отношении Ирана, видимо, будет еще долго занимать переговорщиков. Но Россия не собирается его «убивать», если так просто говорить. Китай пока прячется за нашу спину и как бы смотрит, как мы себя ведем. Я думаю, что у нас есть неплохой уровень диалога с Китайской Народной Демократической Республикой по этому поводу. И мы, конечно, информируем иранских коллег по траектории нашего движения и наших размышлений по этому поводу. Мы не играем втемную для иранцев. Больше того, они примерно представляют, какие люди и кампании скоро уже не получат возможность их экспорта, или поездок за пределы своей собственной страны.

Хотел бы также сказать, что, думая о том, что возможны какие-то небольшие ограниченные санкции, мы, в общем-то, не исключаем того, что будет двухступенчатый процесс или многоступенчатый. То есть, если Иран не поймет зачем предлагает эта, в общем, не слишком жесткая резолюция... А Россия даже предложила такую возможность, что эти санкции вводятся на трехмесячный срок - ситуация совершенно беспрецедентная для каких либо других санкционных предложений - они обычно вводятся на период до того, как страна показывает уже свой хороший рекорд... Так вот, если Иран поймет вот этого движения, то тогда, конечно, может быть введен механизм следующей ступени. В этой связи, как вы понимаете, мы уже завершаем подготовительные работы на Бушерской АЭС. Мы видим, проблем в ближайшем будущем для

запуска этой станции нет, но не видим необходимости спешить, с учетом того, что мы пока не очень чувствуем, поняли ли наш сигнал иранские коллеги или не поняли.

Но есть и другой набор предложений, который в частности мы обсуждаем с нашими американскими коллегами. Этот механизм, наверное, мог бы быть даже более конструктивным, чем какие-то слабые санкции. Это механизм, когда никаких санкций вообще нет, и происходит некий размен, в который очень активно включены США. С экономической точки зрения, возможно, это не так уж и интересно России. С политической точки зрения, с геостратегической точки зрения Россия в достаточной степени заинтересована в развитии сценария, когда Соединенные Штаты на определенный период заявили бы через свое исполнительное решение о приостановке действий собственных санкций в отношении Ирана. И то, что сейчас мы имеем на примере каких-то небольших поставок американских запчастей для самолетов, которые позитивно воспринимаются в Тегеране, было бы расширено на массу других параметров. Но именно на это же время Тегеран принял бы решение добровольно заморозить все свои действия по обогащению урана. Понятно, что в этот момент никаких коллективных санкционных действий Совета Безопасности, естественно, не предпринималось бы.

Насколько такой подход близок нынешней администрации США, это большой вопрос. Думаю, что до 7 ноября мы бы могли говорить об этом как о некоей интересной теоретической постановке вопроса, но сейчас ситуация несколько меняется, в частности, дело даже не столько в изменениях в Конгрессе как таковых, тем более, что они будут реализовываться реально тока с января следующего года - с началом работы нового состава Конгресса, но в смене Рамсфелда на Гейтса. Это, Михаил Владимирович, не Бил Гейтс, который 7 ноября, как вы знаете, был здесь и проводил встречу на высоком уровне. Наш докладчик, который через пару минут включится в наш разговор, как раз организовывал и готовил визит Била Гейтса в Россию, среди многочисленных своих прочих обязанностей. Но в США другой Гейтс в этот момент пришел. И смотря на то, какие работы проводил новый министр обороны США в последние месяцы в своем неформальном качестве...и как человек очень близкий к старшему Бушу, следует обратить внимание на то, что вот такие подходы в отношении Ирана ему могут быть симпатичными. И вот тандем с Кондолизой Райс может быть даст интересный результат.

И последнее, что касается демократов в Конгрессе, и как это влияет на российско-американский стратегический диалог. Легче всего было бы сказать: посмотрим как это повлияет. Вынужден сказать, что это никак не повлияет, потому что до окончания срока действия полномочий нынешней администрации США именно вот тот холодный мир, который установился...в основном он накладывает отпечаток на двусторонние российско-американские отношения, находящиеся сейчас на крайне низком уровне. Мы в России смотрим на эти стратегические отношения не только как на отношения по поводу Ирана, или по поводу Аль-Каиды - это американская повестка. Я думаю, нас они интересуют в комплексе, в том числе и в поведении США в таких точках как Каспий, Центральная Азия, Южный Кавказ. Мы смотрим комплексно и относительно ситуации с нашими проектами на Сахалине, на Штокмане, и готовы смотреть

комплексно и дальше, не разрывая уж так далеко вопросы нашего вступления во Всемирную Торговую Организацию с другими вопросами, которые принято называть вопросами стратегической стабильности, нераспространения и контроля над вооружениями.

Я сейчас уже должен сказать, что попытки реанимировать американо-индийский стратегический диалог сталкиваются с большими трудностями. Отчасти это отсутствие элементарного интереса в администрации США. Но в некоторых вопросах этот интерес присутствует.

Обращу внимание присутствующих - некоторые из вас являются экспертами в этом вопросе - на соглашение 123, на соглашение о сотрудничестве в области атомной энергетики между Россией и США, которое в теории может быть подготовлено и подписано до конца этого года. В общем-то, это могло быть серьезным политическим шагом, в настоящий момент, возможно, выгодным соединенным штатам больше, чем России, по крайней мере, с моей точки зрения. Но даже здесь мы видим, что уже не со стороны администрации США, выступающей сторонницей такого соглашения, а как раз со стороны будущего демократического Конгресса мы будем иметь очень жесткую оппозицию. То есть Россия оказалась не в ситуации «плохо и лучше», а «плохо и хуже», или, по крайней мере, есть риск такой ситуации. В то время, как человек, который станет локомотивом обсуждения российско-американских совместных соглашений...инициатив, если таковые будут, сенатор Джо Байден, который относится позитивно к этому движению, хотя и встретит серьезную оппозицию среди своих же коллег демократов. Лантос в Палате Представителей, конечно, будет очень серьезно «топить» эти усилия. И у него на это есть целый ряд аргументов – от Iran Freedom Support Act, на который будут ссылаться, и не только он, до ситуации с правами человека в России, которые, таким образом, окажутся тесно увязаны с вопросами и перспективами нашего сотрудничества, как в атомной энергетике, так по Ирану и другим.

И в этой связи для России есть один понятный вопрос. А нужно ли нам выступать инициаторами каких-либо соглашений, или, по крайней мере, активно их продвигать, в то время как мы все равно максимум, что получим – это долгое и мутное обсуждение с администрацией? Возможен и позитивный результат, но потом мы получим документ из Конгресса, который как бы будет тем же соглашением, но с какими-то пятью или десятью различными условиями. То есть по сути это будет уже другой документ.

Когда-то в начале 90-х годов мы это уже проходили – то, что было связано с Соглашением по совместному уменьшению угрозы. Тогда была другая внутренняя ситуация в России, мы это «съели». Нужно ли нам это сейчас? Думаю, что завтрашняя встреча Путина и Буша, а точнее, я бы сказал, тональность этой встречи, во многом даст понять и настроение Кремля – насколько мы хотим поддерживать диалог просто, чтобы его поддерживать, или же мы должны услышать четкие инициативные шаги из Вашингтона, иначе инициаторами мы здесь выступить не будем.

На этом я закончу свою вступительную часть.

Хотел бы обратить внимание членов Клуба на то, что наше с Вами следующее большое событие пройдет либо в самом конце января, либо в начале февраля. Примерно Вы можете пометить карандашом либо 31 января, либо 1 февраля.

Проведение презентации нашего нового журнала «Индекс Безопасности», информация о котором Вам роздана, и Вы увидите там, какие статьи, проблемы и темы мы обсуждаем. Так как я рассказывал об этом на предыдущем заседании, не буду останавливаться на этом подробно.

Также хотел обратить внимание членов Клуба, у которых истекает членство, что продлить его следует уже сейчас. И здесь следует контактировать с Ириной Котовой.

Теперь разрешите мне с большим удовольствием передать слово нашему сегодняшнему основному докладчику, которого я очень рад видеть за нашим клубным столом, за нашим клубным завтраком. Михаил Владимирович Якушев не просто эксперт в области Интернета, Интернет-технологий, вопросов информации, информационной безопасности. И он не просто работает в компании Майкрософт, которую он так ненавязчиво сейчас будет рекламировать своими софтами, которые у него наверняка там загружены на его технику. Но Михаил Владимирович очень разносторонний человек. Он имеет образование МГИМО, правовое образование. Он работал на дипломатических постах в Латинской Америке, говорит по-испански, работал в бизнесе. И кроме того, работал в телекоммуникационных компаниях, и затем, работал в Министерстве по делам Информационных технологий и связи, где Михаил Владимирович отвечал за целый блок наших законодательных инициатив в этой области, и работал с другими государственными структурами - и с Федеральным Собранием по продвижению законодательного обеспечения в области информатизации и связи. Сейчас вернулся в Майкрософт.

Должен сразу сказать, что Майкрософт не оплачивает заседание нашего Клуба. Рекламы Майкрософт мы здесь не проводим. Михаил Владимирович выступает в своих многочисленных личных качествах. Хотел бы обратить внимание на его работу в группе ООН. Это была межгосударственная группа, которая занималась вопросами роли Интернета в XXI веке, его действительного глобального характера. Я думаю, что так или иначе, вопросы сегодня с этим могут быть связаны, кот мы будем обсуждать.

Михаил Владимирович является автором нашего выходящего журнала «*Индекс Безопасности*», где, в частности, он анализируют книгу Фридмана, которая большинству из вас известна – «*World is Flat*» – «Плоский мир», и анализирует шероховатости самого этого плоского мира и теории плоского мира. Там он, в частности, задается среди прочего таким вопросом, устраняет ли движение по, так называемому по Фридману, плоскому миру информационный разрыв, который все более острым становится не только между различными странами, но и между различными социальными группами, различными поколениями, и территориальными единицами внутри одних и тем же стран. В данном случае, это вполне применимо и к России. Михаил Владимирович, не отрываю время от вашего выступления. Пожалуйста.

М. В. Якушев

Большое спасибо!

Мне доставляет большое удовольствие выступать перед Вами. Я понимаю, что та тема, которой профессионально занимаюсь я, может быть, не совсем соответствует основам профиля Вашей деятельности. Но я постараюсь, во-первых, рассказать о ней интересно, чтобы Вы заинтересовались этими вопросами. А в случае, если у вас есть уже какие-то темы, которые было бы необходимо детально прояснить, я с удовольствием постараюсь это сделать.

Можно следующий слайд, пожалуйста.

Темой моего выступления является Интернет, телекоммуникации и глобальная безопасность. Соответственно, в первую очередь пойдет речь о тех вопросах, которые обычно называют достаточно новыми словами: киберпреступность, кибертерроризм. И я сразу же хочу сказать, что я, скорее всего, не буду в своем выступлении говорить о том, что нужно менять в самом Интернете, в самих телекоммуникациях, чтобы уменьшить угрозу глобальной безопасности. А буду говорить о том, как существовать в тех условиях, которые нам предоставляет Интернет и телекоммуникационные технологии, поскольку развитие и Интернета, и телекоммуникационных технологий в целом всегда будет обгонять наши попытки что либо изменить в его развитии путем нормативно-регулятивным воздействия. То есть Интернет развивается, телекоммуникации развиваются, в них происходят различные события, в том числе противоправного характера. Необходимо знать, в чем заключается это противоправное поведение, криминальное поведение. Является ли оно на самом деле проблемой. Для кого именно оно является проблемой. И какие меры предпринимаются для того, чтобы бороться как с киберпреступностью, так и с кибертерроризмом.

Следующий слайд, пожалуйста.

Я хотел бы начать с нескольких определений, с тем, чтоб более точно опередить сферу того, о чем я буду рассказывать. И в принципе, я был бы признателен... если у кого-то появится вопрос уточняющего характера, я бы просил их задавать с тем, чтобы я мог в процессе изложения материала сразу же на них ответить, с тем, чтобы не возникало недопонимания и двусмысленности.

Итак, по поводу определения. Что же такое киберпреступность, то, что по-английски называется *cybercrime*? В двух словах самое короткое определение может быть следующим – это любой вид криминальной уголовно преследуемой деятельности, в которых компьютеры и сети связи выступает в качестве инструмента с целью воздействия или местом совершения преступления. Мы чуть попозже поговорим о различных видах киберпреступлений.

Что касается понятия кибертерроризма, представляющего наибольшую угрозу для глобальной безопасности, то здесь необходимо иметь в виду, что до сих пор нет общепризнанного, общеупотребительного понятия терроризма, которое существенно отличается от одной до другой страны. Поэтому исходя из некого

обобщенного понимания понятия «терроризм», «кибертерроризм» можно определить как политически мотивированное использование компьютеров, компьютерных средств и сетей связи в качестве либо средства совершения правонарушения, инструмента, либо цели воздействия для того, чтобы оказывать воздействие на общественное мнение, в том числе создавать панику для населения определенных стран или территорий, либо таким образом воздействовать на принятие решений правительствами, государственными органами тех или иных стран. То есть кибертерроризм - это использование технических компьютерных средств в террористических целях. И, наконец, видимо, самое сложное для юриста определение - что такое Интернет, поскольку оно в Российском законодательстве отсутствует, в большинстве других стран мира точно также с юридической точки зрения не определено, предлагается считать как совокупность сетей связи, в которых обмен информацией производится на основании так называемого межсетевого IP-протокола. Тем самым мы отграничиваем Интернет от других сетей связи, например, мобильных сетей, в которых обмен информацией происходит по другим принципам и по другим стандартам обмена.

Следующий слайд, пожалуйста.

Как я уже говорил, под киберпреступностью понимается деятельность, в которой Интернет, телекоммуникации являются либо инструментом, либо целью, либо средой совершения преступления. Существуют различные виды классификации противоправных действий, угрожающие безопасности как на национальном, так и на глобальном уровнях. Я хотел бы сразу же сделать одно важное замечание, которое часто задается, когда говорят про киберпространство. По традиции, все, что связано со словом «кибер», относят только к Интернету - именно к этой сети в IP-протоколе. Однако, развитие технических средств подтверждает, что те же самые проблемы, которые мы уже увидели и почувствовали, используя Интернет-технологии, мы видим и в огромном большинстве других видов телекоммуникаций, других видов сетей. И очень многие правонарушения, которые традиционно относились к Интернету, мы видим сейчас в мобильных сетях, сетях сотовой связи. Мы видим даже их распространение на такие уже ставшие традиционными средствами связи как факсимильная связь. Все больше и больше проникают нарушения правопорядка в такую сферу, как телевидение, непосредственное телевизионное вещание и интерактивное телевидение. Поэтому, говоря об уголовно наказуемых действиях в киберпространстве, мы должны понимать, что это относится не только к Интернету как таковому, но и к большому количеству других видов сетей связи, активными пользователями которых является каждый из нас.

В качестве примера по каждой из групп криминальных активностей в Интернете можно привести следующее. Когда киберпространство используется в качестве инструмента противоправной деятельности, самый простой и известный пример это СПАМ - рассылка не запрошенной информации, как агитационного, так и коммерческого характера - которые напрямую запрещаются и караются уголовным законом во все большем количестве стран мира. Также традиционным для киберсетей является нарушение прав интеллектуальной собственности, которые, наверное, в настоящий момент имеет наибольший экономический эффект. Причем, речь идет не просто о плагиате, не просто

торговли какими-то музыкальными файлами и произведениями литературы и искусства по Интернету, но также вроде бы такой необычный объект, как рингтон - когда продаются мелодии для того, чтобы они исполнялись на мобильных телефонах. Мы как-то очень часто забываем, что в абсолютном большинстве случаев, те операторы, которые продают картинки или музыку, не осуществляют выплаты авторских вознаграждений, отчислений, тем кто, собственно говоря, является правообладателем этих объектов. То есть это пример нарушения прав интеллектуальной собственности в мобильных сетях.

Примерами того, когда телекоммуникационная инфраструктура или Интернет становятся целями неправомерного воздействия – это несанкционированный доступ к информации, к компьютерным устройствам, преодоление средств защиты, средств ограничения доступа - то что называется обобщающим понятием как «хакинг». Это незаконный перехват информации, которая передается по сетям электросвязи, а также оказание неправомерного воздействия, интерференции, на то, что передается по сетям связи.

Все большей проблемой становится распространение так называемых вредоносных программ. В отличие от СПАМа, вредоносные программы, как правило, распространяются скрытно - мы не видим, как это происходит, и мы не видим, что именно происходит с нашими компьютерными системами, по которым происходит распространение так называемого *malware*.

К вредоносным программам, к сожалению, относится все больше и большее количество видов программного обеспечения, которое нарушает либо функционирование компьютерных систем, либо просто нарушает наши права как потребителей, как пользователей компьютерных устройств. Началось все достаточно давно с распространением так называемых вирусных программ, которые препятствуют нормальной работе компьютерных устройств. Но все больше и больше говорится о так называемом «шпионском» программном обеспечении, которое отслеживает исходящие процессы на компьютерах и сетях связи. Все больше и больше мы видим, что проникают на компьютеры вредоносные программы, обеспечивающие незаконную рекламу тех или иных продуктов, товаров услуг. Проникают такие вредоносные компьютерные программы, как компьютерные черви, которые может быть и не оказывают непосредственного негативного воздействия, но затрудняют, замедляют работу компьютерного устройства. Так называемые троянские программы, путешествующие от одного компьютера к другому. Логические бомбы, которые затрудняют работу компьютерных процессов, и так далее.

И наконец, к сожалению мы были частыми свидетелями того, что в киберпространстве оказываются так называемые атаки отказа от обслуживания (*denial of service*), при которых с большого числа компьютеров на определенные сайты проходят запросы, которые просто выводят из строя соответствующий сайт. Причем, указанные атаки *denial of service* становятся характерными, к сожалению, не только для Интернета, но и для телефонных номеров, для обычной телефонной связи, что особенно опасно, если такого рода атаки оказываются против служб экстренной помощи. Например, 911, или планируемую в нашей стране службу 112. И, наконец, говоря об Интернете и телекоммуникационных сетях, как незаконной среды оказания противоправных

действий, то здесь необходимо обратить внимания на самые разнообразные способы кражи идентичности, то есть тех правонарушений, при которых подставляются вместо реальных лиц сайты, электронные адреса злоумышленников, которые тем самым либо получают доступ к определенным ресурсам, в том числе телекоммуникационным – то есть фактически речь идет об использовании чужого оплаченного времени использования мобильных телефонов - либо другие способы электронного мошенничества. Кроме того, появляются, становятся все более актуальными так называемые бут-неты (bot-net), которые по-русски все больше переводятся как «зомбированные сети», когда сети корпоративные, локальные заражаются всем тем вредоносным программным обеспечением, о котором говорилось выше, и без контроля со стороны владельца этих сетей, становятся источниками опасности для других сетей, с которыми у них есть связь.

Следующий слайд, пожалуйста.

Однако, необходимо отметить, что помимо специфических для Интернета и телекоммуникационных сетей преступлений, сама инфраструктура телекоммуникаций и Интернета представляет собой удобную площадку для совершения так преступлений, в которых Интернет является лишь одним из дополнительных способов осуществления подобного рода противоправных действий. Ну, например, большинству из нас известно такие печально известные письма, сообщения, как «нигерийские» письма, являющие собой разновидность мошенничества, связанного с просьбами о различных предоплатах. В условиях Интернета, электронной почты несколько лет назад такого рода правонарушения распространилось чрезвычайно. Мы видим, что Интернет становится удобным средством применения различных психосоциальных технологий, позволяющих, например, осуществлять доступ к персональным данным, к различного рода видам конфиденциальной информации, то что по-английски называется *password fishing*, то есть иначе говоря, ловля паролей, которую осуществляют самыми различными средствами, когда человек даже не задумывается и не замечает, что его персональные данные уходят к злоумышленникам.

Проблемой на современном этапе развития Интернета является развитие детской порнографии, которая является уголовным преступлением в абсолютном большинстве стран мира. В то числе, соответствующее законодательство появилось и в Российской Федерации.

Необходимо отметить, что криминализируется, признается незаконным и такой вид активности, как онлайн-игорный бизнес, который уже запрещен в Соединенных Штатах. В настоящее время Государственная Дума рассматривает президентский проект российского закона об игорном бизнесе, в котором также запрещается игорный бизнес с использованием Интернет-технологий. Соответственно, в определенных юрисдикциях это также является уголовным преступлением.

Существует и кибернетическая разновидность сексуального харасмента, то есть действий сексуального характера, которые точно так же, как и в некомпьютерном виде, подлежат расследованию, наказанию и пресечению.

К сожалению, полный перечень подобного рода правонарушений привести не представляется возможным, поскольку этот список постоянно пополняется. Здесь можно только выразить сожаление, но это, к сожалению, характерно для любого развития технических средств. Кроме того, Интернет является удобным способом, инструментом совершения так называемых информационных преступлений, например, экономический шпионаж, когда информация, представляющая собой коммерческую тайну, становится доступной как раз через Интернет, через Интернет-сайты; кража коммерческих секретов, и так далее.

И, наконец, есть целый ряд действий, характерных для Интернета и телекоммуникационных сетей, которые представляют собой противоправную деятельность, представляющую угрозу национальной безопасности. Это так называемые разновидности «хактивизма» иначе говоря, общественных неформальных движений, которые призывают к противоправным действиям в Интернете и являются примером такого рода действий. Хактивизм – это объединение слов «хакерство» и «активизм» - то есть активность в пользу совершения противоправных действий с использованием компьютерных устройств.

Кроме того, и Интернет, и современные телекоммуникации, безусловно, являются огромным подспорьем в совершении так называемой традиционной разведывательной деятельности. В первую очередь как способ передачи информации, которую практически невозможно или затруднительно перехватить органами правопорядка той страны, на территории которой она осуществляется.

И последнее – это использование так называемого информационного оружия, использования интернета, телекоммуникаций как средств воздействия для достижения барьерных целей в вооруженных конфликтах, подготовительных этапах таких конфликтов и в их процессе. Следующий слайд, пожалуйста.

Если мы обратимся к понятию кибертерроризм, то мы должны помнить, что, во-первых, как мы видим терроризм сам по себе активно использует Интернет, в первую очередь как средство коммуникации между различными террористическими группами, опять таки, чтобы предпринять перехват соответствующих сообщений, и особенно что связано с активным использованием средств криптозащиты, шифрования информации так, что становится даже в случае перехвата непонятно о чем идет речь, о чем договариваются участники террористических групп. Интернет используется террористическими группами для получения так называемой чувствительной информации, например, для выбора объектов для атак.

Интернет активно используется для вербовки новых членов террористических групп, в том числе в других странах, а также для получения средств финансирования такого рода террористических групп. И соответственно, кибертерроризм представляет собой угрозу так называемым политическим инфраструктурам, причем, это вопрос как к Интернету в традиционном его

понимании, так и к таким частям инфраструктуры, как спутниковые и наземные сегменты. Об этом мы будем говорить поподробнее чуть ниже.

И наибольшую опасность представляет собой то, что Интернет, благодаря своим таким особенностям, как глобальный характер, как дешевизна доступа, и как, в общем-то, уже всеобщая доступность соответствующих средств, опасен тем, что затраты на производство террористической атаки, террористического воздействия, несопоставимо малы по сравнению с теми убытками, с тем ущербом, который может быть причинен в результате их совершения.

Следующий слайд, пожалуйста.

Безусловно, все, что я сказал выше, является предметом серьезного рассмотрения как на локальном, национальном, так и на международном уровнях. Здесь есть целый ряд проблем, которые предстоит решить и экспертами, государственными экспертами.

Отмечается следующий набор проблем, которые препятствуют эффективной борьбе со всем тем, что было сказано выше.

Во-первых, это отсутствие надлежащего контакта и коммуникации, общения между государственными органами и бизнесом по поводу возможных террористических угроз. Здесь же необходимо отметить отсутствие нормальной системы взаимодействия, совместимости информационных систем правоохранительных органов различных стран в процессе расследования и предотвращения кибернетических атак и актов терроризма. Иначе говоря, внутри каждой страны, где больше, где меньше, уже существует целый набор средств, позволяющих эффективно, опять таки, с большей или меньшей эффективностью защищать национальную инфраструктуру. Однако, отсутствуют механизмы, которые бы позволяли оперативно обмениваться информацией, оперативно препятствовать глобальным, транснациональным атакам террористов. Это еще предстоит решить, тем более, что требуется дополнительный выход к технологическим средствам - проблемность вопроса гармонизации законодательств, как материального законодательства, с тем, чтобы одно и то же правонарушение преследовалось в разных странах по одним и тем же принципам и законодательным подходам; так и процессуальное законодательство, когда доказательство вины того или иного террориста или преступника признавались бы таковыми не только в странах, где они были собраны, но и в тех странах, где осуществляется преследование злоумышленников. Необходимо также понимать, что расходы на поддержание кибербезопасности постоянно растут, как в глобальном, так и в национальном масштабе, и если эту проблему достаточно хорошо понимают в бизнесе владельцы корпоративных сетей, то на уровне государства это требует дополнительных разъяснений. Я, например, на протяжении долгих лет пытался проявлять активность, скажем, у здания напротив...