ОБЩАЯ ПОВЕСТКА ДНЯ РОССИИ И АСЕАН В КИБЕРПРОСТРАНСТВЕ: ПРОТИВОДЕЙСТВИЕ ГЛОБАЛЬНЫМ УГРОЗАМ, УКРЕПЛЕНИЕ КИБЕРБЕЗОПАСНОСТИ И РАЗВИТИЕ СОТРУДНИЧЕСТВА

Год спустя после прошедшего в 2013 г. во Владивостоке саммита АТЭС регион Юго-Восточной Азии сохраняет и усиливает свою привлекательность для России в плане перспективной площадки для наращивания торговых и экономических связей. В то же время на фоне обострения противоречий с Западом и продолжающегося процесса становления новых мировых центров сил региональные форматы на юго-востоке азиатского континента и прежде всего АСЕАН становятся для Москвы все более значимыми партнерами по внешнеполитическому диалогу. Причем речь в рамках такого диалога идет о широком спектре вопросов, включая проблемы региональной и глобальной безопасности. Какие проблемы находятся на пересечении этих плоскостей сотрудничества, двух *широких корзин*?

Проработка этого вопроса привела сотрудников ПИР-Центра и приглашенных российских экспертов к выводу о том, что одним из наиболее востребованных и перспективных, но в то же время сложных и высококонкурентных направлений взаимодействия является сотрудничество России и стран АСЕАН в сфере информационно-коммуникационных технологий (ИКТ). По инициативе ПИР-Центра представители государства, бизнеса, научного и технического сообщества попытались ответить на вопрос о том, какие совместные интересы объединяют Россию и АСЕАН в укреплении глобальной безопасности в киберпространстве, а также оценить потенциал Юго-Восточной Азии как рынка сбыта российских средств защиты информации, производственной площадки программно-аппаратной продукции российских компаний[1]. Также в фокусе дискуссии оказался вопрос о целесообразности перенятия РФ опыта стран АСЕАН по созданию эффективно работающей системы Центров реагирования на киберинциденты (CERTs) и борьбы с киберпреступностью с использованием ресурсов частных компаний.

*В организованных ПИР-Центром дискуссиях и экспертных мероприятиях приняли участие ведущие российские специалисты в сфере информационной безопасности, в том числе третий секретарь Департамента по вопросам новых вызовов и угроз МИД РФ Борис **Васильев**, заместитель руководителя отдела реагирования на компьютерные инциденты GROUP-IB Александр **Калинин**, консультант по информационной безопасности Cisco Systems Алексей **Лукацкий**, председатель Совета Координационного центра национальных доменов .RU/.РФ Михаил **Медриш**, президент ПИР-Центра Владимир **Орлов**, исполнительный директор Делового совета Россия–АСЕАН при Торгово-промышленной палате РФ Виктор **Тарусин**, председатель Совета ПИР-Центра Михаил **Якушев**, руководитель стратегических проектов ЗАО Лаборатория Касперского Андрей **Ярных**.*

ОБЪЕДИНЕННЫЕ ОБЩЕЙ УГРОЗОЙ: КИБЕРАТАКИ И ТРАНСГРАНИЧНАЯ КИБЕРПРЕСТУПНОСТЬ В ПОВЕСТКЕ ДНЯ РОССИИ И АСЕАН

ЯРНЫХ: Хотел бы затронуть проблематику кибервойн и современных киберугроз, прежде всего применительно к региону АСЕАН.

Сначала небольшой исторический экскурс. В 1994 г. специалистами *Лаборатории Касперского* в среднем выявлялся один вирус в час, и в то время мы обходились без сложной машинной аналитики и обработки данных о вредоносных программах. В 2006 г. новые вирусы выявлялись уже каждую минуту — потребовалась автоматизация аналитики, начали бороться с вирусами с помощью программ-роботов. 2011 г. новые образцы вредоносного кода регистрировались нашими специалистами ежесекундно. При таких показателях даже автоматизированная аналитика не справляется, и анализ осуществляется за счет выведения определенных *поведенческих алгоритмов* — мы смотрим на то, как компьютер *ведет себя*. Статистика 2013 г. подтверждает, что тенденции к принципиальному улучшению нет.

Хотелось бы привести основанные на мониторинге данные *Лаборатории Касперского* по наибольшему риску заражения устройств в Интернете с учетом региональной специфики. У нас есть специальная сеть — *Касперский Security Net,* и каждому пользователю, использующему нашу антивирусную защиту, мы предлагаем защиту *из облака*, с предоставлением анонимной, неперсонифицированной информации о том, какие инциденты произошли на том или ином рабочем устройстве. Согласно полученным таким образом данным, Россия оказалась на первом месте по уязвимости в Интернете.

Порядка 49 установленных копий наших продуктов подавали информацию о случаях атак через Интернет. В выборке топ-20 стран по абсолютным цифрам, характеризующим Интернет-угрозы, представлены многие государств АСЕАН, включая Таиланд и Шри-Ланку. С ними по уровню и объему выявленных угроз соседствуют страны СНГ. Что касается рисков локального заражения, показано присутствие вредоносного кода на компьютере, а не в сети Интернет. Здесь ситуация немного другая. Высокий уровень рисков сохраняется во Вьетнаме, Непале, Бангладеш и Индии. Индия вообще находится на пике по числу и интенсивности крупномасштабных кибератак. Во Вьетнаме в 2013 г. около 61% всех персональных компьютеров содержали вредоносный код или же в течение года были заражены вирусами, распространяющимися не через Интернет, а через флешки и иные съемные носители.

В неофициальной классификации *Лаборатории Касперского* все угрозы, связанные с вредоносным кодом в Интернете, можно отобразить в виде пирамиды, или иерархии. В основании такой пирамиды находится традиционная киберпреступность, которая является основой криминала в Сети. Дальнейшее эволюционное развитие этого инструментария идет через целевые атаки, когда не преследуется цель заразить все подряд устройства, а вместо этого атакуются нужные компьютеры, содержащие банковские, финансовые и иные чувствительные виды данных. Вершиной эволюции вредоносного кода является кибероружие, и мы уже уверенно прибегаем к использованию этого термина для классификации некоторых программ, поскольку именно такое описание отражает их функционал. Ни для чего другого, кроме избирательного и изощренного поражения систем, они не предназначены. Их функции включают крайне продвинутый киберсаботаж и кибершпионаж, в последнем случае программа не просто похищает банковскую информацию, а целенаправленно ищет информацию, к примеру, составляющую коммерческую или государственную тайну. Также к классу кибероружия мы относим программы-разрушители, нацеленные на деструктивные действия против объектов критически важной инфраструктуры. Примерами таких программ в последние годы стали широко известные вирусы *Flame, DuQu, Gauss* и, конечно, *Stuxnet*, первый в истории образец вредоносного кода, классифицированный международным экспертным сообществом как кибероружие.

В частности, для региона АСЕАН актуален вирус *Net Traveller*, который в 2013 г. атаковал фактически весь мир. В первоочередную зону риска атаки данным вредоносным программным обеспечением попадают и дипломаты. В функционале этого вируса явственно прослеживается нацеленность на компрометацию дипломатических данных, служебной переписки и других видов конфиденциальной служебной информации. Присутствие продвинутого вредоносного кода имело место в Таиланде, Гонконге, Камбодже и в Малайзии — фактически во всех ключевых странах региона.

Наибольшее количество продвинутых киберугроз навлекла на себя Индия, где спектр интересов злоумышленников вобрал фактически все критические сегменты, начиная от аэрокосмической и военной отраслей до дипломатических и управленческих структур. Россия и Китай находятся в сходной ситуации. На территории России и Китая специалисты *Лаборатории Касперского* находили вредоносный код под названием *Red October*, который был четко нацелен на шпионаж за дипломатическим корпусом — именно компьютеры работников внешнеполитических структур стали мишенями *Красного Октября*.

В процентном распределении существенная доля атак приходится на дипломатические ведомства и структуры; около 15% составляют правительственные органы. Значительная доля целей также относилась к сотрудникам и структурам военной отрасли. В деятельности этой сети четко идентифицируется мотив стратегического кибершпионажа, имеющий мало общего с мотивами криминального обогащения. Эпизод с *Red October* иллюстрирует тревожную и устойчивую тенденцию, с которой мы столкнулись в 2013 г. и которая актуальна по сей день — растущий размах кибератак и кибершпионажа в стратегических и политически мотивированных целях.

Хочу подчеркнуть, что подобные тенденции опасны и неприемлемы. Кибероружие должно быть запрещено для использования в сети Интернет, в противном случае все наши сети и устройства станут *питательной средой* для его дальнейшего развития и распространения. Хотелось бы закончить на оптимистической ноте и надеяться, что сегодняшнее обсуждения и другие встречи внесут вклад в эту борьбу с деструктивным потенциалом в Сети.

КАЛИНИН: Добавлю к выступлению Андрея Ярных видение того спектра киберугроз в регионе АСЕАН, с которым сталкивается *Group-IB* в рамках собственного сегмента деятельности — сегмента реагирования на киберинциденты. С 2011 г. *Group-IB* выпускает ежегодный отчет по ущербу мировой экономики от действий киберпреступников, и каждый год итоговая цифра растет. Если в 2010 г. она составляла 7 млрд долл. США, то в 2012 г. — уже 18 млрд долл. США. Значительная часть данной суммы генерируется за счет действий, так или иначе затрагивающих Россию и в не менее серьезной степени страны ЮВА.

Помимо физических лиц, в странах АСЕАН происходят атаки и на корпорации. Даже узкий список наиболее критичных и серьезных атак включает Малайзию, Таиланд, Филиппины — в общей сложности не менее половины стран АСЕАН. Такие инциденты, как исполнение вредоносного кода на серверах компании или сканирование корпоративной сети, происходят на постоянной, системной основе, и с целью их предотвращения мы взаимодействуем с десятками стран. Как правило, представители компаний и государственных органов, подвергающихся атакам, активно интересуются тем, что происходит, регулярно направляют отчеты о предпринятых ими мерах обеспечения безопасности, блокировке вредоносных ресурсов или применению санкций в отношении субъектов, которые осуществляли данные атаки.

Приведу пример из нашей практики. Одним из громких дел с участием *Group-IB* стало пресечение деятельности группировки киберпреступников, которая создавала и распространяла связки эксплойтов, использовавшие уязвимости в веббраузерах, в том числе *уязвимости нулевого дня*, не обнаруженные и не применяв-

шиеся ранее никем. Задержание группы, в которой состояло порядка 13 человек, было проведено в ноябре 2013 г. Решение суда по этому делу еще не вынесено, но членам группы грозит от 5 до 10 лет лишения свободы. Следует учесть, что за время своей деятельности они успели нанести ущерб на сумму около 70 млн рублей — и это с учетом только тех эпизодов, которые известны следствию и по которым собраны доказательства. Важно, что поимка киберпреступников была бы невозможна без помощи коллег из региона АСЕАН, в том числе профильных структур Малайзии. И это неслучайно: если взглянуть на панель управления эксплойтами, которые распространяла эта киберкриминальная группа, география их распространения охватывает многие страны АСЕАН. В связи с этим *Group-IB* была оказана большая поддержка: по нашему запросу были раскрыты данные о регистрации ресурсов для осуществления мошеннических действий, об источниках и целях атак и другие данные, которые смогли вывести нас непосредственно на создателей этих эксплойтов.

Я, как и Андрей Ярных, предпочту закончить на оптимистической ноте и подчеркнуть, что, несмотря на постоянное расширение предложения и рост объемов рынка компьютерной преступности на глобальном и региональном уровнях, параллельно расширяются возможности взаимодействия России и других форматов, включая АСЕАН, по эффективному противодействию этим угрозам. Но, конечно, очень многое еще только предстоит сделать.

ГЛОБАЛЬНЫЕ ЦЕЛИ СОТРУДНИЧЕСТВА РОССИИ И АСЕАН: ПРЕДОТВРАЩЕНИЕ КИБЕРВОЙН, ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

ОРЛОВ: Тема нашей дискуссии складывается из двух составляющих: общих для России и государств АСЕАН угроз в киберпространстве и совместных перспектив, позитива и негатива. Предыдущие докладчики достаточно подробно осветили спектр угроз, которые в равной степени затрагивают Россию и регион Юго-Восточной Азии. Однако, помимо киберпреступности, кибершпионажа и кибертерроризма нельзя не упомянуть и другие угрозы, например, военно-политические. Кроме того, страны региона не могут оставаться в стороне от вызовов в сфере глобального управления Интернетом, связанных с защитой права на тайну частной жизни в сети и программ глобального электронного слежения.

Нужно подчеркнуть, когда мы говорим о сотрудничестве России и государств АСЕАН в сфере информационной безопасности, мы ни в коем случае не говорим о его наработке с нуля. Сейчас есть все основания говорить об интенсивном и динамичном взаимодействии в рамках АСЕАН и региональных ассоциаций государств Юго-Восточной Азии по безопасности, в которых Россия играет заметную роль. В 2010 г. решением 17-й сессии *Регионального форума АСЕАН по вопросам безопасности* (*АРФ*) за Россией наряду с Австралией и Малайзией была закреплена курирующая роль в проработке проблематики кибербезопасности и борьбы с кибертерроризмом. С тех пор Россия в рамках формата *АРФ* является одним из ключевых участников работы по этим вопросам.

Важной вехой в сфере кибербезопасности как для АСЕАН, так и для России как участницы формата стала 19-я сессия *АРФ*, прошедшая в июне 2012 г. В ходе встречи по инициативе Российской Федерации был принят ключевой документ, определяющий политику форума в этой области — заявление министров иностранных дел *АРФ* по сотрудничеству и обеспечению международной кибербезопасности. В настоящее время в исполнение положений этого заявления Россией совместно с Малайзией и Австралией ведется подготовка ARF Work Plan on Cyber Security. Первый рабочий проект такого плана был представлен 9–10 декабря 2013 г. в рамках заседания межсессионной группы поддержки по мерам доверия превентивной дипломатии *АРФ*.

Таким образом, сотрудничество России и АСЕАН в сфере кибербезопасности не только успешно стартовало, но и приобрело устойчивую положительную динамику. Сегодня РФ участвует в проработке всех вопросов, обсуждаемых в рамках *АРФ* в сфере кибербезопасности, включая выработку общей терминологии, укрепление доверия, формулирование общих принципов и норм поведения в киберпространстве, обмен информацией и общими практиками, совместное противодействие трансграничной киберпреступности и кибертерроризму, а также формирование регионального центра компетенций и сети экспертов в сфере кибербезопасности.

Стоит ли оценивать ситуацию в части сотрудничества и достигнутых результатов позитивно? Безусловно. Означает ли это, что ключевые проблемы решены и можно остановится на достигнутом? Ни в коей мере. Есть задачи, которые нуждаются в более динамичной проработке, а главное, есть форматы и опции сотрудничества, востребованные и нужные, но пока не использованные в полной мере. Целесообразно, по оценкам ПИР-Центра, выглядит и более тесное встраивание проблематики борьбы с кибертерроризмом в общие подходы и механизмы деятельности *АРФ* в антитеррористической сфере. Речь идет о проработке практик борьбы с кибертерроризмом в тренинговом формате, который уже успешно практикуется странами форума в области борьбы с международным терроризмом.

Ряд вопросов, включая выработку правил поведения в киберпространстве, борьбу с киберпреступностью и укрепление мер доверия, может прорабатываться в рамках *полуторной дорожки*, где правительственные эксперты работали бы совместно с неправительственными. Это формат, как мы знаем, наши коллеги из стран АСАЕН любят и ценят. Учитывая обострение угрозы политически мотивированных кибератак в последние годы и рост напряжения вокруг главных проблемных точек АСЕАН, прежде всего островов в Южно-Китайском море, интересам России все больше отвечает выстраивание системы мер доверия с государствами АСЕАН в киберпространстве. Такая система могла бы препятствовать формированию и эскалации конфликтного потенциала в киберпространстве. Россия приобрела позитивный опыт такого взаимодействия с согласованием и подписанием пакета двусторонних соглашений с США о мерах по укреплению доверия в использовании ИКТ в июне 2013 г. В декабре 2013 г. был согласован перечень мер доверия в области использования ИКТ в рамках ОБСЕ, который также представляет ценный опыт для АСЕАН.

Кроме того, на перспективу можно задуматься и о реализации пакета мер доверия в киберпространстве в рамках формата АСЕАН–ШОС. Подобная композиция способствовала бы снижению рисков политически мотивированных кибератак и укреплению стабильности в этих регионах. Кроме того, возник бы стимул для подтягивания туда государств не только Юго-Восточной, но и Восточной Азии, которые территориально находятся вне границ АСЕАН, равно как и вне формата ШОС, однако через ШОС они могут быть более эффективно включены во взаимодействие. Буду рад комментариям коллег по высказанным мной соображениям.

ЛУКАЦКИЙ: Действительно, к возможным точкам соприкосновения между Россией и странами АСЕАН относятся прежде всего вопросы борьбы с киберпреступностью и кибертерроризмом. Также речь идет о проработке возможностей использования рынков стран АСЕАН для продвижения российских технологий и российских средств защиты информации (СЗИ), причем в этой части уже имеется положительный опыт. Кроме того, существует возможность, хотя и теоретическая, использования отечественного опыта в области разработки аппаратного обеспечения — *железа* — и создания сборочных площадок такой продукции, которая потом могла бы применяться в тех или иных критических областях.

В России есть свои нюансы, которые за последний год обозначились достаточно четко. Отчасти они связаны с *эффектом Сноудена*, отчасти просто отражают

специфику тех государственных органов, которые занимаются в России вопросами информационной безопасности. Но проблема сейчас стоит достаточно остро, и не так просто вынести за пределы территории России сборку элементов, используемых при создании критических информационных инфраструктур. Разумеется, очень важно взаимодействие, связанное с *Центрами реагирования на киберинциденты* (*CERTs*), тем более что страны АСЕАН имеют богатейший опыт создания и развития таких центров национального и регионального охвата, с участием государства и без него. Одно из направлений потенциального сотрудничества — это разработка доктринальных и стратегических документов, в том числе национальных стратегий кибербезопасности.

С 2000 г. существует и действует Доктрина информационной безопасности РФ, в отношении которой сегодня существуют разные точки зрения. Специалисты, непосредственно занимающиеся техническими аспектами безопасности при использовании ИКТ, склонны озвучивать большое количество претензий в связи с устареванием документа. Он не отражает реальных условий и действительной ситуации в этой области, которая развивается очень динамично, поэтому жить по документам 14-летней давности сегодня невозможно. Во многом с учетом этой проблемы в сентябре 2012 г. при Совете Федерации РФ была создана экспертная группа, которая приступила к созданию российской стратегии кибербезопасности. К концу 2013 г. проект документа был доведен до высокой степени готовности, но в ходе парламентских слушаний в Совете Федерации по проекту документа, состоявшихся 29 ноября 2013 г., мы столкнулись с достаточно серьезной критикой, которая концентрировалась прежде всего вокруг терминологических аспектов. Вновь встал вопрос о том, почему в проекте документа используется термин *кибербезопасность*, а не *информационная безопасность*. К тому же обозначилось недостаточно четкое понимание места концепции Стратегии среди иных доктринальных документов, связанных с внешней политикой России в области информационной безопасности, национальной безопасности, внешней политики и т. д. 10 декабря 2013 г. состоялась еще одна встреча, посвященная этому документу, где вновь были затронуты эти вопросы. Дальнейшая судьба концепции Стратегии кибербезопасности пока неясна; создается впечатление, что документ встречает противодействие со стороны ряда ведомств, хотя его положения выглядят достаточно здравыми и своевременными.

В этой связи для России может быть интересен опыт государств АСЕАН, в частности Сингапура, который уже в июле 2013 г. выпустил уже третью редакцию аналогичного документа — Five-Year National Cyber Security Masterplan 2018. Подобные документы в Сингапуре периодически выпускаются с 2005 г. на 5-летний период. Нынешняя редакция отражает практически все ключевые вопросы, которые упомянуты и в нашем проекте концепции Стратегии кибербезопасности. Сюда входят вопросы повышения осведомленности и обмена информацией, государственно-частное партнерство, международное взаимодействие, а также вопросы образования, повышение количества специалистов в этой области, создания государственных и развития сети частных центров реагирования на киберинциденты.

ЯКУШЕВ: В развитие прозвучавших выступлений хотелось бы уделить внимание терминологическим вопросам. 2013 г. продемонстрировал неожиданно положительную динамику в терминологической дискуссии в сфере ИКТ между Россией и США как одного из основных российских оппонентов в этой сфере. Известно, что 17 июня 2013 г. на полях саммита *Большой восьмерки* в Ирландии Барак Обама и Владимир Путин подписали ряд документов, предлагающих целый набор механизмов и решений для выстраивания двусторонних мер доверия для предотвращения угроз безопасности в сфере использования ИКТ. Возможно, указанный компромисс поможет предотвратить дальнейшие споры по терминологической проблематике в сфере информационной безопасности (ИБ).

Во-вторых, важно понять, насколько для нас и наших коллег из стран АСЕАН совпадает перечень тех объектов, которые мы должны защищать в киберпространстве

и других сферах, и здесь я прежде всего имею в виду критически важную инфраструктуру. В-третьих, вопрос касается различных способов противодействия киберугрозам, в том числе правовых, информационных и технологических инструментов и механизмов. У российских организаций и экспертов огромный опыт в разработке таких мер — целесообразно использовать его.

С вопросами ИБ тесно связан вопрос глобального управления Интернетом и управление критическими ресурсами Сети. Все мы понимаем, что указанная проблематика приобрела особую остроту после так называемых событий лета 2013 г., связанных с разоблачениями правительственных программ глобальной электронной слежки в Интернете, раскрытых Эдвардом Сноуденом. Было бы интересно выслушать точку зрения экспертов о том, как эти проблемы воспринимаются сейчас, по прошествии года.

ВАСИЛЬЕВ: Для пояснения приоритетов российского подхода к обеспечению ИБ, в том числе по вопросам сотрудничества со странами АСЕАН, упомяну некоторые ключевые российские документы в этой области. В августе 2013 г. Президент России Владимир Путин подписал *Основы государственной политики Российской Федерации в области международной информационной безопасности (МИБ) до 2020 г.* Именно этот координирующий документ задает вектор нашей работе, перечисляет все угрозы в этой сфере и способы борьбы с ними, которые мы должны использовать именно на международных площадках, а также сами международные площадки, приоритетные для нас. В документе выделяется несколько ключевых типов угроз в области МИБ, в том числе основополагающая триада угроз: использование ИКТ в военно-политических, террористических и преступных целях.

Однако помимо этой базовой классификации в документе вводится новый, четвертый тип угрозы — «вмешательство во внутренние дела суверенных государств, нарушение общественного порядка, разжигание межнациональной розни, расовой и межконфессиональной вражды, пропаганда расистских и ксенофобских идей или теорий, порождающих ненависть, дискриминацию или подстрекающих к насилию». Это интересный и важный момент, потому что эта угроза новая, ранее в доктринальных документах она не фигурировала, теперь же мы должны принимать ее во внимание. Для сегодняшней дискуссии также важно, что большое внимание в *Основах государственной политики...* уделяется сотрудничеству России с региональными объединениями и организациями, в частности в рамках формата *Регионального форума АСЕАН–АРФ*.

Теперь я хотел бы прокомментировать выступление Владимира Орлова, в рамках которого был практически полностью освещен ход работы, которая ведется в рамках *АРФ* по вопросам ИБ. Одно из немногих уточнений можно сделать в отношении Плана действий АРФ в области использования ИКТ. Начиная с 2012 г. австралийская сторона взяла на себя разработку этого плана как один из лидеров процесса наряду с Россией и Малайзией. В 2013 г. проект такого документа был австралийцами разработан и представлен, дальнейшая работа над ним велась с учетом критических замечаний сопредседателей — России и Малайзии. В ноябре 2013 г. соображения Австралии и заинтересованных стран были сведены в предварительный проект плана, который по инициативе австралийской стороны был представлен на рассмотрение 9–10 декабря 2013 г. в Мьянме на заседании межсессионной группы *АРФ*. В 2014 г. продолжилось согласование проекта документа с российской стороной. Этот процесс должен завершиться до конца 2014 г., если пожелания представителей России будут учтены австралийской стороной. В этой работе нас полностью поддерживает Малайзия как третий сопредседатель процесса работы над Планом действий.

Также на площадке *АРФ* ведутся активные дискуссии по международной ИБ. В частности 11–12 сентября 2013 г. в Пекине состоялся семинар *АРФ* по кибербезопасности и ее правовым и культурным аспектам. Организаторами семинара выступили Китай и Малайзия, участие в нем приняли эксперты из 19 стран — участ-

ников *АРФ*, а также представители Евросоюза и секретариата АСЕАН. В рамках мероприятия возможность выступить и высказаться по повестке дня была предоставлена всем присутствовавшим представителям. По сумме выступлений были подробно освещены два существующих подхода к обеспечению международной ИБ. Первый из них, который продвигается прежде всего нашими партнерами из США, состоит в том, чтобы не отказываться от использования ИКТ в военно-политических целях, а лишь регулировать эти действия надлежащим образом. При этом предлагается опираться на действующие нормы международного права, а не заниматься выработкой новых норм и международно-правовых механизмов. Мы выступили с критикой этого подхода и продвигаем свою альтернативу, которая заключается в попытке создать международно-правовой режим неиспользования ИКТ в военно-политических целях.

В принципе, эти два подхода в совокупности заключают в себе тот спектр позиций, на который ориентируется та или иная страна. Россия выступает заодно с Китаем, который в целом поддерживает наш подход, нацеленный на обеспечение безопасности нашего общества и государства. Что касается наших западных партнеров, они хотят обеспечить свою безопасность при использовании ИКТ в военно-политических целях против третьих стран — такая постановка вопроса, на наш згляд, четко прослеживается. Фактически сейчас любое государство может дать адекватный ответ на кибератаку страны другого государства, и поэтому сильные государства, атакуя слабые, рискуют получить адекватный ответ. Причина в том, что не нужно вкладывать серьезные ресурсы или какие-то особо продвинутые технологии, чтобы нанести серьезный ущерб критически важной информационной инфраструктуре и репутации государства. Отсюда понятно, что хотят сделать страны Запада: оставить за собой возможность использовать ИКТ в военно-политических целях в виде своего рода сдерживающего механизма, который бы не позволял слабым государствам симметрично отвечать на подобные действия.

ЯКУШЕВ: У меня вопрос к Борису Васильеву и Андрею Ярных: в своем выступлении представитель *Лаборатории Касперского* употреблял термины *кибероружие*, *кибервойна*, *кибервооружение*. Я хотел бы уточнить, оправданно ли, по вашему мнению, использование слово *кибервойна,* в том числе применительно к тем проблемам, которые мы обсуждаем в части взаимодействия России со странами АСЕАН, или у МИД РФ и российского бизнеса есть какие-то альтернативы? Что такое кибервойна, должны ли мы говорить об этом явлении и как его предотвращать в международных реалиях?

ВАСИЛЬЕВ: Я бы предпочел говорить об использовании ИКТ в военно-политических целях, в принципе, это одно и то же. Действительно, угрозы есть, и если посмотреть на то, что сейчас происходит в рамках формата *АРФ*, следует отметить, что все действия, которые будут использоваться при исполнении разрабатываемого Плана действий, будут направлены на обеспечение безопасности государств от военно-политического использования ИКТ. Иначе говоря, преступность и терроризм в информационном пространстве в данном случае рассматриваются исключительно как сопутствующие угрозы, а не основные. Основные угрозы в соответствии с будущим планом увязываются с использованием ИКТ государствами в военно-политических целях, и им планируется уделить самое серьезное внимание в рамках формата *АРФ*.

ЯРНЫХ: Фактически в моем выступлении была представлена информация о кибероружии, т. е. вредоносном коде, который используется для ведения боевых действий в киберпространстве, например, для организации серьезных масштабных акций в Интернете против тех или иных стран. Мы однозначно и категорично стоим на том, что для подобного инструментария не существует вариантов положительного, конструктивного применения. Сам по себе вредоносный код незаконен и не должен использоваться государствами даже с благими намерениями, поскольку это всегда ведет к противоправным действиям для всех сторон и может спровоцировать хаос в сети Интернет.

КАПИТАЛИЗАЦИЯ СОТРУДНИЧЕСТВА: ИНТЕРЕСЫ И ПЕРСПЕКТИВЫ РОССИЙСКОГО ИТ-СЕКТОРА НА РЫНКАХ АСЕАН

ТАРУСИН: Сегодня на рынке АСЕАН сложилась ситуация, достаточно выгодная для игроков отечественного ИТ-сектора. На фоне прошлогодних событий, связанных с разоблачениями Эдварда Сноудена, основные конкуренты российского ИБ-бизнеса — компании из США — серьезно потеряли доверие у своих покупателей, и традиционных, и потенциальных. По независимым оценкам, ущерб от данных событий для ИТ-сектора США до 2020 г. может составить до 35 млрд долл. США. Таким образом, открывается определенная ниша, которую российские производители программных продуктов по обеспечению ИБ могут частично занять или заместить. В общемировом рынке ИТ-продукции страны АСЕАН составляют уже существенную часть, и, конечно, сегодня необходимо воспользоваться моментом и активизировать работу российских компаний по продвижению на эти рынки.

Российские компании ИТ-сектора во второй половине 2013 г. отмечали нехарактерный всплеск спроса на свои услуги в необычных и не типичных для себя региональных рынках. Например, портал Mail.Ru, ежедневно регистрирующий 30–40 тысяч новых адресов электронной почты, во втором полугодии 2013 г. 70% заявок получал из стран Ближнего Востока. Эта тенденция весьма показательна, и думается, что и страны АСЕАН при правильном продвижении и подаче российских интересов и возможностей также могут обратиться к отечественному ИТ-рынку в массовом порядке. В этой связи еще раз хочу обратить ваше внимание на возможности деловых контактов со странами АСЕАН, с представителями как государственных, так и частных структур, которые занимаются разработкой и замещением программной и аппаратной ИТ-продукции, активно продвигаемой на региональных рынках. Нельзя утверждать, что российские ИБ-компании являются единственной альтернативой западным игрокам на рынках стран АСЕАН.

Весьма серьезную конкуренцию составляют китайские производители, прежде всего собственно в сегменте ИБ. Но тем не менее возможность и необходимость форсированной работы на региональном рынке с российской стороны в данный момент не вызывает сомнений. Еще раз, пользуясь моментом, обращаю внимание всех заинтересованных участников ИТ-индустрии на положительный опыт бизнес-миссии российских предпринимателей в Юго-Восточную Азию, которая состоялась 22–30 марта 2014 г. с Минэкономразвития РФ и МИД РФ и охватила три страны: Индонезию, Малайзию и Сингапур. В мероприятиях в рамках миссии приняли участие высокопоставленные представители государственных структур и лидеры бизнес-сообщества трех стран региона. Думаю, что подобными действиями, подобными миссиями мы можем реально показать заинтересованность, а самое главное — высветить возможности российских компаний в предоставлении адекватных конкурентных услуг и продуктов.

ЛУКАЦКИЙ: Что касается российских бизнес-перспектив на рынках ИБ АСЕАН, здесь специфический аспект во взаимодействии России и АСЕАН — сбыт СЗИ, основанных на российских решениях, которые можно предлагать на рынке стран Юго-Восточной Азии. На данный момент мы имеем здесь достаточно позитивный опыт: это и компания *Лаборатория Касперского*, и *Doctor Web*, и *Positive Technologies*, которые либо имеют представительства в странах Юго-Восточной Азии, либо из ближайших, соседних стран осуществляют продажи тем или иным заказчикам в регионе. Но при этом в 2013 г. эти компании часто сталкивались с агрессивной политикой со стороны китайских производителей, которые территориально ближе, а также они обладают более тесными культурными и деловыми связями с участниками регионального рынка. В силу этих специфических факторов они могут более тонко, точно и сфокусированно работать с заказчиками в странах АСЕАН, поэтому у российских компаний возникают очевидные сложности, которые, как показывает опыт, все же преодолимы.

Также интересен тот факт, что в отношении производителей СЗИ не прослеживается четкой национальной специфики. Несмотря на уже упомянутый сегодня

эффект Сноудена, я как представитель американской компании *Cisco Systems*, не могу сказать, что в 2013 г. заметил сильное *проседание* продаж нашей продукции на тех или иных региональных рынках. Многое зависит не от *национальности* той или иной компании, а от отношения, которое транснациональная компания проявляет к национальному рынку. Здесь я имею в виду возможности работы с национальными регулирующими органами, возможность обеспечения соответствия продвигаемой ИТ-продукции национальным требованиям. В этом плане как российские продукты в области ИБ сегодня имеют все шансы выйти на рынок АСЕАН, так и продукция компаний Юго-Восточной Азии может достаточно эффективно продвигаться на российский рынок.

Однако российский рынок ИБ-регулирования очень специфичен, он отличается от тех моделей, которые работают за рубежом. Так, в России имеются специфичные требования по оценке соответствия, нередко включающие предоставление исходных кодов продукта, на что многие зарубежные компании зачастую не идут. При этом одна из причин отказа — нежелание терять права на свою интеллектуальную собственность. За прошлый, 2013-й, год разоблачения Эдварда Сноудена показали, как на этом могут сыграть российские участники рынка. Не берусь утверждать в отношении стран ЮВА, но арабские страны в конце 2013 г. начали отворачиваться от американской продукции как минимум в области криптографии и ориентироваться на продукцию российских производителей. В результате в странах арабского мира прослеживается определенный всплеск интереса к российским криптографическим алгоритмам и средствам шифрования. Это достаточно интересная тенденция, которую можно использовать, не теряя тот запас инициативы, который появился за последний год.

Еще один вопрос — производство аппаратного обеспечения, *железа*, в странах Юго-Восточной Азии. Если говорить о массовом рынке конечной пользовательской ИТ-продукции, здесь особых вопросов и сложностей не возникает. Но если мы говорим о сегментах, связанных с ИБ, то, к сожалению, последний опыт и инциденты, которые происходят и фиксируются, а это лишь вершина айсберга, которая попадает в СМИ, обусловливают ситуацию, когда ни одна строна не хочет выносить разработку элементов критичных систем за пределы своей национальной территории, несмотря на гарантии 100-процентного контроля технологических процессов на зарубежном предприятии.

Эта тенденция отчетливо проявлется в США, которые часть своего производства аппаратного обеспечения в сегменте ИБ переносят из стран ЮВА и Китая обратно, в США. Сходный мотив существует и в России: нежелание государственных регуляторов отдавать критичные для национальной безопасности компоненты и узлы аппаратного обеспечения информационных систем на сборку в страны Юго-Восточной Азии. Разумеется, подобная логичная мотивация имеет место и в других регионах, в том числе в Европе, — любая страна хочет производить и собирать ключевые аппаратные элементы ИТ-продукции у себя дома. И, наверное, больших перспектив в этом вопросе у России применительно к региону АСЕАН нет. С точки зрения массового рынка, повторюсь, таких сложностей не должно возникнуть, потому что массовому потребителю вопросы закладок на аппаратном и программном уровнях не столь интересны.

ТАРУСИН: Развивая тезисы, освещенные Алексеем Лукацким, хотелось бы пояснить, почему именно формат и регион АСЕАН представляются сегодня одной из наиболее перспективных площадок для продвижения российской ИТ-продукции. Во-первых, АСЕАН наиболее стабильный рынок на сегодняшний момент. Во-первых, на фоне глобальных экономических катаклизмов, которые мы наблюдаем и в США, и в Европе, сообщество АСЕАН представляется наиболее развивающимся и динамичным, составляя практически единый экономический механизм. Во-вторых, ухудшающаяся политическая конъюнктура со странами Запада стимулирует нас к поиску возможностей на тех рынках, где отсутствует риск санкций и иных ограничивающих механизмов в отношении продукции российкого ИТ-сектора.

В 2015 г. планируется реализация единого экономического пространства в странах АСЕАН, что создаст реальную зону свободной торговли, поддержанную и другими административными мерами, такими как единая виза в АСЕАН, а также позволит снять многочисленные барьеры для дальнейшего развития торговли. АСЕАН — это 600 млн человек и потребительский рынок, открывающий реальный доступ как минимум в 10 стран для технических продуктов из России. К сожалению, на сегодняшний момент общий объем товарооборота между Россией и странами АСЕАН составляет чуть более 15 млрд долларов США, а его состав тяготеет к энергоносителям и другим сырьевым продуктам, таким как пальмовое масло и каучук.

Но при этом есть и прорывные сюжеты, зачастую связанные с сегментом ИТ. Когда в 2012 г. заместитель генерального секретаря АСЕАН Лим Хонг Хин попросил меня назвать хотя бы одно харизматичное, узнаваемое лицо российского бизнеса в странах АСЕАН, я, недолго думая, назвал Евгения Касперского и его компанию — ведь это действительно *лицо России* в регионе. Остается только грамотно использовать этот плацдарм, чтобы продвинуться в смежные отрасли и сегменты, закрепить и нарастить свое присутствие. Необходимо продвигать не только *коробочный* продукт, который сейчас легко узнаваем на полках магазинов Джакарты, Коломбо, Куалу-Лумпур, Ханоя, но и корпоративные продукты, по которым мы можем серьезно конкурировать с производителями из других стран. Поэтому Деловой совет Россия–АСЕАН предпринимает все усилия для продвижения высокотехнологичных продуктов на рынок АСЕАН. На сегодняшний момент мы объединяем более 20 компаний, как минимум четверть из них специализируются в сфере ИБ.

Мы стараемся использовать наши площадки, чтобы представители и руководители этих компаний могли обращаться непосредственно к бизнесу в странах АСЕАН. Так, в июне 2013 г. в Санкт-Петербурге мы провели 1-й Деловой форум Россия–АСЕАН, на котором выступали такие известные вам лица, как генеральный директор *InfoWatch* Наталья Касперская и один из ведущих мировых экспертов по ИБ Анатолий Клепов. Доклады делались по теме обеспечения ИБ, мобильных и корпоративных сетей бизнеса и банковского сектора. Кроме того, сейчас через механизм финансовой поддержки диалогового партнерства Россия–АСЕАН мы запустили две программы, которые позволят представить секретариату АСЕАН и бизнесу в странах АСЕАН продукты, реализуемые нашими участниками. В перечень таких продуктов входят единые электронные торговые площадки, интерактивный инвестиционный портфель, который можно увидеть в Google Store в открытом доступе.

Я думаю, что сегодня мы сможем обменяться знаниями и мнениями о тех продуктах и возможностях по продвижению наших высокотехнологичных продуктов и программ, которые до сих пор не полностью использованы в странах АСЕАН. Хочу обратить особое внимание на то, что АСЕАН — это достаточно специфический рынок для нас. С присущим российским представителям европейским менталитетом весьма трудно понять некоторые особенности. Когда вы приходите на рынки стран АСЕАН с чем-то новым, как вы считаете, наиболее важным и необходимым для этого региона, первое, о чем вас спросят: кто будет инвестировать в проект? Именно эту проблему мы начали решать совместно с Министерством экономического развития РФ в 2013 г. С Алексеем Улюкаевым, главой министерства, у нас есть договоренность, которая получила поддержку и министерства, и российского *Фонда прямых инвестиций*.

Сейчас работа идет над созданием *Фонда поддержки инвестиций Россия–АСЕАН*, который, в частности, будет нацелен на продвижение в регион российской продукции, в том числе высокотехнологичных продуктов из России в эти 10 стран региона. С таким механизмом мы сможем сделать существенный прорыв на региональном рынке ИТ и рассчитываем на то, что участвующие в дискуссии представители частного сектора, смогут, с одной стороны, получить выгоду от совместной деятельности с Фондом по продвижению этих продуктов, а с другой стороны, помогут нам наполнить этот Фонд реальными, конкретными продуктам, которые находятся

не на стадии стартапа, а уже готовы к запуску в полномасштабное промышленное и коммерчески жизнеспособное производство. Будем надеяться, что наши амбициозные планы в полной мере воплотятся в жизнь.

ОБМЕН ИНФОРМАЦИЕЙ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ: РОЛЬ *CERT* В СОТРУДНИЧЕСТВЕ РОССИЯ–АСЕАН В КИБЕРПРОСТРАНСТВЕ

ЛУКАЦКИЙ: Среди всего спектра потенциального взаимодействия России и АСЕАН в области ИКТ есть важная ниша, где мы действительно можем очень активно сотрудничать, в том числе с точки зрения перенимания опыта АСЕАН. Речь идет о развитиии механизма *CERTs и CSIRTs* — специальных групп или команд реагирования на инциденты и различные угрозы кибербезопасности, которые могут исходить из любой страны и точки мира. И если в России на сегодняшний день формально существуют четыре *CERT*s, то в странах АСЕАН, которые по территории и населению значительно уступают нашей стране, — порядка 30 таких команд. Один из таких примеров — это региональный механизм *Asia-Pacific CERT* (*AP-CERT*), объединяющий 30 команд из 20 различных стран, которые находятся в этом регионе. *AP-CERT* не только предлагает различные сервисы для коммерческих организаций или государственных органов, но и публикует полезную информацию по вопросам кибербезопасности, об уязвимостях в информационных системах, чтобы заинтересованные лица могли своевременно устранять проблемы и не допускать серьезных киберинцидентов.

Еще одна интересная практика, которая в России пока не нашла применения, — это *киберучения* (учения в области ИБ), формат, который изначально был опробован еще в Австралии в начале 2000-х гг. Потом опыт Австралии взяли на вооружение США, страны Европы и государства АСЕАН. Этот формат позволяет в приближенных к реальным условиях разработать способы взаимодействия и методы отражения и нейтрализации различных угроз, будь то киберпреступность, кибертерроризм или же кибервойны, о которых сегодня уже рассказывал представитель *Лаборатории Касперского*. Это действительно хороший опыт, и России есть, чему поучиться в этой сфере.

Из числа существующих сегодня в России CERTs, пожалуй, наиболее активный — *CERT-GIB компании Group-IB*. Остальные *CERTs* по своей сути либо находятся в частично нерабочем состоянии, либо очень узко специализированы и работают на решение какой-то конкретной задачи, например, обнаружение и реагирование на атаки против исследовательских и научных организаций. В частности можно назвать государственный *RU-CERT* и *CERT* крупнейшего петербуржского Интернет-провайдера *Web Plus* (в задачи последнего входит обслуживание собственных заказчиков и клиентов провайдера). Нужно упомянуть Центр реагирования на компьютерные инциденты в информационно-телекоммуникационных сетях (ИТС) органов государственной власти РФ (GOV–CERT) — проект ФСБ РФ, который стартовал в 2012 г., но пока не заработал в полном объеме и функционале, на которые обычно ориентированы *CERT*s. Но возможно, что со временем этот центр выйдет на уровень ведущих мировых аналогов, которые реагируют на угрозы в режиме 24/7, направлены на обеспечение потребностей государственных органов и других подобных структур, в том числе критически важных объектов.

Следующий возможный сюжет для взаимодействия — обмен информацией об угрозах в киберпространстве. Этой теме в странах АСЕАН посвящено достаточно много различных ресурсов, платформ и онлайн-проектов. Одним из примеров является филиппинская *HoneyNet*, которая собирает информацию о киберугрозах и сетевых атаках, анализирует ее и на выходе предоставляет обработанную статистику. С помощью этих данных специалисты могут понять существующие тенденции, распознать методы, используемые злоумышленниками, и, возможно, собрать доказательства противоправной деятельности, чтобы использовать их затем при разработке методов нейтрализации актуальных киберугроз. Основные угрозы

и атаки на Филиппины, как правило, исходят со стороны США и Китая — ближайшие партнеры являются и крупнейшими источниками угроз в киберпространстве.

Однако здесь возникает одна из ключевых проблем, которая пока не имеет решения, — некорректные попытки переложить на страну, с территории которой осуществляется атака, ответственность за нее. Владеть тем или иным устройством или узлом, с которого ведется атака, независимо от его физического расположения может абсолютно любое государство либо лицо, являющееся гражданином другого государства. И если атака идет с территории Китая или США, это не означает, что именно эти государства стоят за ней. В отличие от угроз в реальном мире в киберпространстве отследить источник крайне затруднительно, и в этом заключается проблема атрибуции — одна из ключевых проблем, которая до сих не решена и требует международного сотрудничества и совместной разработки инициатив по ее преодолению.

С точки зрения обмена информацией в различных странах АСЕАН эта задача решается по-разному, но можно отследить несколько общих моментов. Первый из них — это наличие единого координирующего органа, его, к сожалению, в России пока нет, поскольку за различные аспекты, связанные с информационной безопасностью, у нас отвечают разные регуляторы: ФСТЭК, ФСБ (различные управления которой отвечают за разные вопросы), Генштаб ВС РФ, МВД, Центробанк РФ, МЧС, Мининстерство энергетики, а также ряд других федеральных ведомств. Конкретный пример: в декабре 2013 г. обсуждался вопрос о том, кто из государственных ведомств отвечает за противодействие киберугрозам в Сочи во время зимней Олимпиады 2014 г. В итоге не нашлось ни одного ведомства и представителя, которые бы заявили о своих координирующих функциях и полномочиях. Подобное отсутствие эффективной координации в условиях крайне динамичной среды, в которой осуществляются кибератаки, накладывает негативный отпечаток на процесс их предотвращения, противодействия и минимизации их последствий. Цена несвоевременного реагирования — задержки в несколько минут и даже десятков минут — может быть не столь критична в условиях военного конфликта (если мы, конечно, не говорим о ядерном оружии). Но в сфере кибербезопасности выведение из строя той или иной системы на несколько минут может привести к катастрофическим последствиям, и об этом нельзя забывать.

Для сравнения, в 2012 г. на форуме, посвященном вопросам кибербезопасности в Малайзии, обсуждалась схема взаимодействия различных заинтересованных сторон по данному вопросу. Предложенный формат был рассчитан на применение как внутри государства, так и на уровне международного взаимодействия внутри региона АСЕАН, а также за его пределами. И в случае с Малайзией, и в случае с Филиппинами, и в случае с другими странами АСЕАН в решение этих вопросов очень активно вовлекается частный бизнес. В России пока контакт частного бизнеса и государства в сфере кибербезопасности и обмена информацией налажен не так хорошо, как того хотелось бы. Отдельные частные инициативы имеют место, но признать, что сегодня в России осуществляется отлаженный и выстроенный процесс, понятный и открытый для всех потенциальных участников, к сожалению, не получается.

В настоящее время в рамках Указа Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» активно идет создание единой системы обмена информацией об угрозах и атаках. Одна из задач, которая остро стоит на повестке дня, — эффективная автоматизация такого обмена данными. К этой задаче мало кто подступился в каком-то финальном приближении. Есть первые шаги, попытки разработать стандарты для такой системы, которые позволяли бы ее участникам из различных стран обмениваться информацией о киберугрозах, но до финальной стадии дело пока не дошло, и дальнейшая работа в этом направлении может представлять еще одну возможность для активизации международного сотрудничества для более оперативного обмена информацией о киберугрозах и эффективного реагирования на них.

Еще одним полезным направлением деятельности является обмен образовательными программами, и здесь Россия может поделиться со странами АСЕАН некоторыми наработками, а государства АСЕАН также могут обогатить российские практики своим опытом. Например, *AP-CERT* практикует 5-дневные тренинговые программы, сконцентрированные по уровню и наполнению, дающие одновременно теоретические и практические знания по реагированию на кибератаки и угрозы в киберпространстве. За последние годы такие тренинги прошло достаточно большое число специалистов из различных стран Юго-Восточной Азии и других регионов. Иными словами, с обеих сторон нарабатывается опыт, которым стоит активно делиться и который стоит воспринимать, чтобы не пытаться выстраивать некие подходы с нуля, игнорируя уже имеющиеся практики и решения.

КАЛИНИН: Хочу поддержать высказанный Алексеем тезис о важности *CERT* во взаимодействии России и стран Юго-Восточной Азии. В *Group-IB* я отвечаю за собственную команду реагирования на киберинциденты — *CERT-GIB*, — и это фактически первый частный *CERT* в России. В настоящий момент Group-IB имеет три офиса по всему миру: помимо основного офиса в Москве наши сотрудники еще работают в Нью-Йорке и Сингапуре, — это необходимо прежде всего для того, чтобы обеспечить круглосуточный рабочий цикл — 24/7. С 2012 г. мы начали активно вступать в профильные региональные и глобальные организации и форматы сотрудничества, такие как сообщество *Trusted Introducer*, объединяющее европейские команды реагирования на инциденты, и глобальный Форум групп по реагированию на инциденты и обеспечению безопасности (FIRST).

Оба этих формата объединяют *CERT*ы по всему миру, при каждом из них аккредитованы многие десятки таких центров. У нас тоже развивается диалог о сотрудничестве с *AP-CERT*: мы подали заявку на членство в 2013 г., которая должна быть удовлетворена до конца 2014 г., как только *AP-CERT* перейдет на новый стандарт документооборота. Принятие CERT-GIB в AR-CERT станет прецедентом для российских организаций. Учитывая навыки и багаж AP-CERT в части учебных программ, а также их влияние в регионе АСЕАН, мы сильно ждем этого и планируем максимально активно обмениваться опытом с нашими партнерами в Юго-Восточной Азии.

В чем же состоят ключевые преимущества и сильные стороны собственного CERT в России? У нас есть особые полномочия в зонах таких доменов, как .RU и .РФ, по блокировке доменных имен. Блокировать их мы имеем право за распространение вредоносного программного обеспечения, а также создание и эксплуатацию ботнет-контроллеров и фишинговых ресурсов. Подобная практика делегирования полномочий в этой сфере частным структурам в мире встречается достаточно редко. *Таиландский центр реагирования на инциденты* (*ThaiCERT*) очень интересовался нашей моделью работы на конферернции FIRST в Бангкоке летом 2013 г., и подобный интерес мы встречаем со стороны множества различных структур. Мы располагаем довольно серьезными полномочиями, но при этом наша деятельность в части доменов тщательно перепроверяется самим регистратором, поэтому за два года, в течение которых мы практикуем такой формат работы, не было ни единого конфликтов с точки зрения ее правомерности. Полномочия, которые я упомянул, были предоставлены *Group-IB Координационным центром национальных доменов .RU* и *.РФ*.

В марте 2013 г. *Group-IB* вошла в число участников международного государственно-частного партнерства *Международный многосторонний альянс против киберугроз* (*IMPACT*), действующего при *Международном союзе электросвязи*. Участие в этом механизме оказалось для нас очень полезно в плане взаимодействия с регионом АСЕАН. Раньше, когда мы наблюдали и фиксировали попытки атак, нацеленных на российских граждан и организации, с территории государств АСЕАН на жертвы в России, было нелегко найти общий контакт с профильными государственными органами в этом регионе. Источником проблемы был не только языковой барьер, но и отсутствие мотивации к взаимодействию либо игнорирование запросов с нашей стороны по иной причине. Сейчас, когда появились инсти-

туциональные партнеры или присутствующие в регионе компании, в частности партнеры по альянсу *IMPACT*, взаимодействие сразу приобрело намного более динамичный характер. После вступления в *IMPACT* и *AP-CERT* последовал существенный рост случаев конструктивного реагирования со стороны зарубежных партнеров и прежде всего государтв АСЕАН.

Взаимодействие и обмен информацией носят взаимный характер. Помимо того что нам передают необходимые данные от профильных структур в странах АСЕАН, после вступления в *IMPACT* мы также начали получать много данных о тех российских ресурсах, которые государства АСЕАН со своей стороны хотели бы заблокировать. К тому же мы обмениваемся информацией с российскими государственными органами, со многими компаниями и центрами реагирования, *Лабораторией Касперского*, различными организациями других стран, а также еще одним международным форматом, объединяющим различные CERT–FIRST. В течение 2014 г. намечен обмен опытом с испанским *CERT*, параллельно идут переговоры о взаимодействии с *CERT* Германии. А как только *Group-IB* вступит в *AP-CERT*, мы сразу начнем переговоры с китайским *CERT*. Китайское направление взаимодействия нам крайне интересно, так как через китайскую территорию идет множество атак, в том числе на российские ресурсы. Мы всегда готовы сотрудничать в части нормативной документации, что периодически и происходит в дополнение к обмену готовыми данными об атаках и инцидентах.

ВАСИЛЬЕВ: Немного о деятельности CERT-GIB. У нас безопасностью государства и личности занимается государство, и при массированных компьютерных атаках ничто не мешает юридическим лицам обратиться за помощью в правоохранительные органы. Непонятно, почему этого в ряде случаев не делается, почему прослеживается такое стремление уйти в плоскость негосударственного взаимодействия в плане получения помощи и услуг по расследованию инцидентов. В России существует сеть национальных контактных пунктов, функционирующих в формате 24/7 в рамках *Римско-Лионской группы большой восьмерки*. Российский национальный контактный пункт — это управление «К» МВД РФ, сотрудники которого активно участвуют в информационном обмене и реагируют на поступающие запросы по поводу компьютерных инцидентов и атак. После получения запросов они обрабатываются, и направляется оперативный ответ. В работе сети участвуют более 60 государств, сотрудничество в 2013 г. находилось в активной фазе.

Однако одна из проблем, на мой взгляд, состоит в том, что в рамках установленных форматов взаимодействия мы не всегда получаем достаточную информацию. В 2013 г. МВД России проводило очередную операцию *Сорняк* по поиску источников детской порнографии в Интернете и, по результатам операции определив такие источники, направило большое количество запросов в те государства, в чьей юрисдикции были зарегистрированы соответствующие ресурсы, нарушающие законодательство. Подавляющая часть запросов — больше 800 — было направлено в США. Но, к сожалению, на все эти запросы были получены лишь 4 ответа, т. е. эффективность трансграничного взаимодействия в некоторых случаях крайне низкая, и мы считаем, что в этом направлении есть над чем работать и что улучшать.

МЕДРИШ: *CERTs* — это ключевая точка для многих вопросов, именно поэтому про них стоит говорить. Некоторые российские структуры, например, RU-CERT, вообще не являются CERT по своей сути, поскольку они не реагируют на инциденты в компьютерных сетях. Полноценный *CERT* работает как пожарная команда: это группа людей, которая в обычной ситуации могут работать в разных местах. Но когда происходит киберинцидент, они максимально оперативно собираются в одном месте и приступают к оперативному решению проблемы. Для этого члены *CERT* должны регулярно и интенсивно тренироваться, что уже было очень правильно отмечено в выступлении Алексея Лукацкого. Кроме того, им нужно обладать рабочим инструментарием для решения проблем и устранения инцидентов. С учетом этих требований и критериев лишь *Web Plus*, который назвал свою команду *CERT*ом, с натяжкой может действительно считаться таковым. Я не знаю,

как обстоит ситуация в российских спецслужбах, там действительно может быть *CERT*, соответствующий мировым практикам и характеристикам и действующий определенным образом.

К сожалению, Россия существенно отстает от мирового опыта в части развития системы CERTs. У нас на законодательном уровне отсутствует описанная структура *CERT*ов, во главе которой стоял бы Координационный центр *CERT*ов, выступающий связующим звеном для деятельности остальных центров. При этом в мировой практике другие *CERT*ы могут работать как в составе государственных структур, так и при частных компаниях. В качестве примера можно упомянуть США, где есть *Координационный центр CERT при Университете Карнеги–Меллон*, который в той или иной мере координирует деятельность гражданских *CERT*ов; отдельные *CERT*ы есть только у военных. В общей сложности в США насчитывается до 50–60 CERTs, при этом в некоторых частных компаниях их бывает два, как в *Adobe Systems* и других крупных транснациональных корпорациях, где протекают абсолютно разные виды деятельности, сопровождаемые различными ИТ-процессами.

Таким образом, тематика взаимодействия Центров реагирование на компьютерные инциденты в рамках Координационного центра *CERT*, в том числе с *CERT*ами других стран несет потенциал для обмена опытом и лучшими практиками между Россией и странами Юго-Восточной Азии. Нужно брать на вооружение пример AP-CERT, который совместно с другими государствами решает вопросы, касающиеся всего региона, поскольку Интернет не замыкается в границах одной страны. И страны АСЕАН успешно научились это делать. Поэтому я хотел бы призвать людей, причастных к процессу выработки и принятия решений в России: необходимо продвигаться по этому пути, который может привести к созданию гибкой и эффективной системы CERT, отражающей киберугрозы на уровне лучших мировых практик. Именно этим призывом я хотел бы сформулировать некий итог дискуссии и подвести под ней черту. Большое спасибо.

Примечание

[1] При подготовке данной публикации использованы материалы совместного круглого стола ПИР-Центра и Центра АСЕАН при МГИМО «Общая повестка России и АСЕАН в киберпространстве: противодействие глобальным угрозам, укрепление кибербезопасности и развитие сотрудничества», который состоялся в Москве 10 декабря 2013 г.