

КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

Мы предлагаем вниманию читателей интервью, которое 12 февраля 2014 года дал нашему журналу **ГАТТАРОВ Руслан Усманович**, Председатель Временной комиссии по развитию информационного общества Совета Федерации Федерального Собрания Российской Федерации



Руслан Усманович, спасибо, что Вы согласились ответить на наши вопросы.

По Вашей инициативе Временная комиссия по развитию информационного общества представила для всеобщего обсуждения проект¹ Концепции стратегии кибербезопасности Российской Федерации.

Предусматривается ли разработка в нашей стране документов, в которых будут сформулированы понятия границ киберпространства?

Да, и такая разработка уже ведется. Концепцию, вернее, тогда еще Стратегию кибербезопасности мы начали разрабатывать два года назад на площадке Комиссии Совета Федерации по развитию информационного общества. Аудит нормативного регулирования и общей системности усилий, предпринимаемых в направлении обеспечения кибербезопасности, показал нам, что эти усилия фрагментированы, а в регулировании есть крупные пробелы. Проанализировав опыт зарубежных стран, мы пришли к выводу, что и России требуется свой доктринальный документ в этой области. После более чем пяти версий Стратегия стала Концепцией стратегии именно потому, что для прописывания всех уточнений, границ и шагов необходимо включенное участие большого количества государственных органов, прежде всего Совета Безопасности, правоохранительных органов и федеральных министерств. Разумеется, Концепция

писалась с участием их представителей, но речь идет о необходимости проработки документа в самих структурах. Мы свою задачу видели, главным образом, в том, чтобы привлечь к теме внимание (и если посмотреть на динамику роста количества принимаемых в России нормативных актов в сфере информационной безопасности, то, возможно, нам удалось в этой части добиться некоего успеха), а также сформулировать квинтэссенцию необходимых направлений деятельности для обеспечения кибербезопасности. Будет ли теперь на базе нашего документа разработана Концепция? Верю, что да, поскольку вопрос стоит остро. Возможно, речь даже может идти о коротком горизонте – примерно полутора годах. Но разработку вести будут уже другие ведомства, мы же готовы принимать участие и помочь консультациями. А если появится Концепция, при ней появятся и подзаконные акты, приказы и т.д. с самой что ни на есть подробной конкретикой.

Повлияли ли на работы по разработке Концепции кибербезопасности материалы, опубликованные Эдвардом Сноуденом?

Работы по разработке Стратегии кибербезопасности мы начали более чем за полгода до разоблачений Сноудена. Документы Сноудена, однако, наглядно доказали обоснованность наших опасений и, я думаю, привлекли к нашей работе больше внимания. Должен заметить, что именно поступок Сноудена побудил меня начать плотную работу с транснациональными интернет-корпорациями с тем, чтобы обеспечить соблюдение прав клиентов-россиян на защиту

1 Концепция стратегии кибербезопасности Российской Федерации. См. URL: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>

их персональных данных в соответствии с российским законодательством. И, конечно, поступок Сноудена облегчил нашу задачу в части обеспечения прав россиян - транснациональным интернет-корпорациям стало уже невозможно не откликаться на наши требования.

Как, на Ваш взгляд, Концепция будет гармонизирована с документами стран-участников Таможенного союза и других стран ближнего зарубежья?

Концепция выстроена с учетом международных стандартов, норм и опыта в части подготовки подобных документов. Получился качественный и сбалансированный документ. России стоит поторопиться с подготовкой и принятием Концепции, поскольку в мировом рассмотрении мы несколько запаздываем. Однако это относительно стран-лидеров. В целом же законодательное регулирование киберпространства пока находится в стадии активного становления, причем в большинстве стран процесс сейчас находится у начальной точки. Насколько мне известно, из стран Таможенного союза и ближнего зарубежья мы в первых рядах по срокам разработки такого доктринального документа, как Стратегия кибербезопасности. Думаю, мы можем предложить наш опыт соседям, и тогда вопрос гармонизации норм, возможно, и не появится – они будут гармонизированы с самого начала.

Как известно, в Китае политика государства направлена на жесткое регулирование киберпространства. В представленном на обсуждение проекте Концепции сказано, что «регулирование киберпространства исключительно на национальном уровне невозможно в силу его трансграничности». Как бы Вы могли это прокомментировать?

Этот тезис отражает нашу позицию, она заключается в том, что развитие электронных коммуникаций вместе с неизбежными рисками предоставляет и уникальные, широчайшие возможности, и мы считаем неверным их игнорировать, обрывая контакты с другими сегментами интернета, чтобы повысить свою кибербезопасность. Заметьте, я говорю повысить, а не обеспечить. Изоляционистская политика Китая в сфере киберпространства, безусловно, упрощает задачу поддержания кибербезопасности страны в силу его подконтрольности, однако в первую очередь это отно-

сится к возможности контролировать действия китайских граждан, а не к неуязвимости против кибератак из-за рубежа. Абсолютной защиты не существует, и все мы имеем дело с рисками.

На Ваш взгляд, насколько возможно международное сотрудничество в области кибербезопасности без взаимного ущемления национальных интересов?

Международное сотрудничество всю свою историю существует поверх ущемления взаимных интересов, но это не мешает ему снимать часть действительно серьезных проблем. Например, сейчас очень остро строит вопрос выработки единых правил игры в части защиты персональных данных граждан при их обработке транснациональными корпорациями. Согласно конструкции международного права такие корпорации, если они не имеют в определенной стране официального представительства, не обязаны соблюдать ее законодательство в сфере защиты персональных данных, что, разумеется, вызывает конфликты. Но для их разрешения на международном уровне нет ни единой площадки, ни уполномоченных органов, ни инструментов арбитража. Между тем в скором времени, я считаю, проблема будет решена именно переговорным путем и недостающие институты будут созданы.

В чем суть деятельности российских «киберотрядов»?

«Наблюдать, ликвидировать, защищать», я считаю. Смысл их создания в том, чтобы появился инструмент постоянной готовности для реагирования на кибератаки против информационных ресурсов России. Это требует постоянного мониторинга, протоколов действия, жесткой дисциплины. Параллельно, думаю, будет организовано «патрулирование периметра», т.е. проверки защищенности наших киберобъектов.

Какие меры будут применяться для стимулирования российских производителей продукции в области кибербезопасности?

Рассматривается широкий перечень мер поддержки – от создания национальной программной платформы с доверяемой средой разработки и контрактами на госзакупки программного обеспечения (ПО) для государственных органов до введения налоговых льгот. Однако о том, какие

Наши интервью

меры будут введены, говорить пока рано. Могут лишь сказать, что понимание проблемы в государственных органах есть.

Вы много усилий приложили в области создания российского электронного правительства. Какие там последние новости?

Процесс движется вперед, но не так быстро, как мог бы. Разумеется, успехи есть. Постепенно выполняются прописанные программы и нормативы. Однако остаются проблемы с едиными стандартами, налаженностью межведомственного взаимодействия, корректной статистикой и публичным мониторингом. На мой взгляд, необходимо создание службы профессионального государственного заказчика, стимулирование спроса на электронные госуслуги со стороны населения – соответствующий законопроект я внес в Государственную Думу еще в 2011 году. Концентрироваться, полагаю, следует на образовании, здравоохранении, ЖКХ и транспорте.

Учитывается ли зарубежный опыт организации защиты информации при разработке российского электронного правительства, в частности, по вопросам защиты персональных данных?

Разумеется. Что касается, например, защиты персональных данных, то разработанный нами при широком привлечении экспертов и представителей ведомств законопроект «О персональных данных» не только полностью соответствует требованиям Конвенции ЕС о защите прав субъектов персональных данных с последними поправками, но и где-то даже опережает

мировые нормы – например, в части поддержки развития «облачных сервисов» путем либерализации условий трансграничной передачи данных без падения их защищенности.

Вы в прошлом профессионально занимались спортом. Чем это сейчас помогает Вам в работе? Какие качества и навыки, полученные в те годы, Вы используете?

Да, занимался тяжелой атлетикой, даже выступал за Челябинскую область. Там научился сжимать зубы и делать дело несмотря ни на что. Сейчас, когда выдается время, катаюсь на горных лыжах, иногда играю в хоккей, иногда – в гольф. Спорт помогает вести гармоничную жизнь, отвлекаться от ментальной работы. Помогает поддерживать форму и сбрасывать накопившееся напряжение. Поэтому заниматься им никогда не прекращал.

Какие пожелания Вы хотели бы высказать нашим читателям?

Повышайте свои компетенции в обеспечении кибербезопасности хотя бы на бытовом уровне – обновляйте программное обеспечение, базы антивирусов, не пользуйтесь одной и той же флешкой дома и на работе. Будьте аккуратны со своей личной информацией, не выкладывайте ее в сеть без необходимости – Интернет помнит все. И, разумеется, приглядывайте за детьми. Инструменты родительского контроля сейчас распространены, но используются очень мало. Между тем обеспечение безопасности детской активности в Интернете одними законами не решить, необходимо и участие семьи.

