С Т Е Н О Г Р А М М А

парламентских слушаний на тему "Законодательное обеспечение национальной кибербезопасности в Российской Федерации"

29 ноября 2013 года

Р.У. ГАТТАРОВ

Уважаемые коллеги, доброе утро! 10 часов утра. Мы начинаем наши парламентские слушания по кибербезопасности. Спасибо, что нашли возможность прийти сегодня на это мероприятие. Мы собрались здесь, чтобы обсудить плод годовых усилий экспертов в области информационной безопасности на площадке Временной комиссии Совета Федерации по развитию информационного общества. Специалисты из бизнеса, науки, из государственных органов подготовили этот документ. Он называется "Концепция стратегии кибербезопасности Российской Федерации".

Я предоставляю вступительное слово первому заместителю Председателя Совета Федерации Александру Порфирьевичу Торшину.

А.П. ТОРШИН

Спасибо большое, Руслан Усманович.

Уважаемый Руслан Усманович, уважаемый Александр Алексеевич, уважаемые участники наших слушаний! Прежде всего, позвольте мне приветствовать вас от имени Председателя Совета Федерации Валентины Ивановны Матвиенко. Вообще, эта тема у нее на контроле, она ею очень живо интересуется, но сегодня в Санкт-Петербурге проходит крупное международное мероприятие. И большое количество людей хотели бы принять участие в этих по-

своему уникальных слушаниях, потому что в таком объеме и с такой повесткой дня такие слушания за 20 лет существования Совета Федерации проводятся впервые. И надо отдать должное Руслану Усмановичу, который сумел эту тему сделать одной из ключевых в деятельности Совета Федерации.

Правда, надо сказать, что жизнь сама подтолкнула к этому, когда в особенно бурные последние два, может быть, два с половиной года вдруг ни с того ни с сего (как нашему старшему поколению показалось) появились очень серьезные проблемы и вызовы, угрозы кибербезопасности не только в Российской Федерации, но и в мире. Нас она пока, может быть, не так сильно коснулась, потому что есть еще поколение, которое не ушло, такие, как Герой России Александр Алексеевич Чекалин, как я. Мы всё больше полагаемся на старые испытанные средства: пишущая машинка, хороший замок, решетка на окнах. И попробуйте туда залезть!

Р.У. ГАТТАРОВ

Через провода.

А.П. ТОРШИН

Оказывается, можно уже и через провода залезть. На самом деле у нас здесь, в Совете Федерации сохранились помещения специальные, режимные...

Р.У. ГАТТАРОВ

Без проводов.

А.П. ТОРШИН

Практически без проводов. Только электрические.

Но это шутки, на самом деле шутки плохие, которые показывают, что преступления в области информационных

технологий имеют далеко идущие последствия, чему свидетельство – наш бурный век.

Надо сказать, что очень хороший охват аудитории. Приехали люди из регионов. Вот я смотрю – тут достаточно много представителей из разных регионов, в том числе Дальний Восток, потому что проблема эта общая. Очень сильные специалисты подошли – специалисты из ФСБ, специалисты из специальных исследовательских институтов. Очень радует то, что в зале в основном молодые. Еще раз апеллирую к Александру Алексеевичу. Он сказал мне: "Нам с тобой лет двадцать догонять". Я ответил, что они догонят быстрее. Я скромно сказал, что, наверное, вообще не догоню, не успею. Поэтому вся надежда на вас. И, я думаю, очень хорошо, что вовремя спохватились, вовремя стали готовить серьезные документы.

Во всяком случае, Валентина Ивановна Матвиенко просила передать вам всем, что Совет Федерации будет вам надежной площадкой и надежным защитником интересов нашего государства и каждого из нас в отдельности.

Я думаю, что документ, который у вас имеется, проект концепции стратегии кибербезопасности Российской Федерации, заслуживает самого пристального внимания. Над ним работали очень серьезные, квалифицированные люди. И я думаю, что рекомендации, которые тоже здесь сформулированы, пойдут на пользу. Ну а впереди еще непочатый край работы. Мы еще только, на мой взгляд, начинаем. Но то, что начинаем, и начинаем на нашей площадке, очень хорошо.

Тут я немножко краски сгустил про наше поколение. Вот у нас еще член-корреспондент Российской академии наук Тулохонов сидит скромненько среди вас, да? Тоже как-то вроде люди

достаточно грамотные. Мы со старшим поколением будем вам обязательно помогать.

А сейчас я бы хотел передать бразды правления нашими слушаниями Руслану Усмановичу Гаттарову. Я человек старой формации. И, знаете, Ленин хорошие слова сказал (немодно Ленина цитировать, а я процитирую): "Земля должна принадлежать тому, кто ее обрабатывает". А ведь верно сказано.

Пожалуйста, Руслан Усманович.

Р.У. ГАТТАРОВ

Спасибо, Александр Порфирьевич, за добрые слова. Спасибо, что нашли время присутствовать. Вы, кстати, я хочу сказать, посещали нашу комиссию не раз, и именно в тот день, когда мы договорились о разработке концепции стратегии кибербезопасности, Вы были с нами и поддержали нас.

А.П. ТОРШИН

Конечно. Спасибо.

Р.У. ГАТТАРОВ

Уважаемые коллеги! Есть острая необходимость сформулировать прозрачную систему государственной политики по минимизации рисков, которые возникают с развитием информационных технологий, и максимизации возникающих выгод. С одной стороны, ИКТ уже внедрились в уклад нашей жизни и в экономику так плотно, что стали определять развитие во многих отношениях, отраслях. Школьники учат английский через Skype прямо с мобильного телефона на переменах. Не видел, но говорят, что это есть. У самого не хватает на это воли, хотя очень хочется. Интернет-экономика составляет уже, по разным оценкам... кто-то говорит полтора, кто-то – пять процентов в российском ВВП с

прогнозом роста до 20 процентов. Государство движется к полной электронной коммуникации как с обществом, так и внутри себя.

С другой стороны, ИКТ вызывают изменения прямо сейчас, в реальном времени, и за этим сложно успеть не только с государственным регулированием, но и с осмыслением и реакцией. Как узнал весь мир, персональные данные в электронном виде стали ресурсом, за которым охотятся целые страны. Управляемые компьютером трубопроводы и ядерные лаборатории можно парализовать одним заказным вирусом, который тоже, кстати, разработан не хакерами, а, похоже, все-таки государствами. Шпионские программы и взломы стали идеальным инструментом для бесконечной холодной войны.

Мировые державы это понимают, и поэтому за последние годы у главных глобальных игроков появились стратегии кибербезопасности. У России своей пока нет, но действует ряд документов стратегического характера, такие как Доктрина информационной безопасности, например, и – более частного, например, указ Президента о создании системы обнаружения информационных угроз.

Эти документы относятся в первую очередь к государству. Но Интернет – это открытое пространство, и в нем присутствуют граждане и бизнес. Сейчас они недостаточно приняты в расчет, по нашему мнению. Кибербезопасность не обеспечить, если в своей части не позаботится кто-то один из триады "общество – бизнес – государство". Я абсолютно уверен, что нельзя минимизировать угрозы, если не будет мультистейкхолдерного подхода, того самого, о котором много говорится. Только государство не сможет обеспечить полноценной защиты. Здесь должна быть вот эта та самая триада "государство – бизнес – гражданин".

Поэтому мы подготовили концепцию стратегии, и она обосновывает, зачем России собственная стратегия, по каким направлениям нужно усиливать национальную кибербезопасность и кому какие роли в этом процессе отводятся.

Коротко пройду по критичным моментам. Это еще не стратегия, это концепция стратегии. Создание работающей стратегии, которую не пришлось бы постоянно латать, – это масштабный процесс и очень долгий, прежде всего в части согласований. Должен быть большой доктринальный документ, поэтому мы ставили задачу дать импульс разработке стратегии, привлечь к этой теме внимание.

Если посмотреть, как резко увеличилось количество государственных документов по информационной безопасности за этот год, то становится понятно, что тренд нарастает, возможно, благодаря нашим усилиям.

В написании документа мы шли не бюрократическим путем, мы не писали его за закрытыми дверями, не добивались, чтобы он во всём устроил профильные органы, и не спускали уже согласованный документ общественности.

На наш взгляд, бизнес и общество достаточно включены, поэтому мы пошли от них. Мы поставили в центр нашей стратегии именно гражданина и бизнес, потому что считаем, что вопросы безопасности критической инфраструктуры, информационной безопасности – это вопросы государства, компетентных органов, ФСБ. Концепция стратегии включила то, что они могли бы и, наверное, должны были сделать в части обеспечения национальной кибербезопасности.

На ранних этапах мы пытались активнее приглашать профильные органы. Они не были настроены критически, но и

большого интереса не проявляли. Теперь же ситуация, на мой взгляд, изменилась. Предвижу, что вопрос будет затрагиваться в каждом выступлении, поэтому скажу сам: давайте постараемся больше не концентрировать внимание на том термине, которым уже играют журналисты. Есть термин "информационная безопасность" и есть термин "кибербезопасность". Различие этих терминов сильно политизировано. Для России – это элемент ее в том числе внешней политики. Мы исходили из этого и знаем это. Но когда мы на наших встречах в самом начале начали спорить об этом (часть наших экспертов принципиально говорили: "Кибербезопасность", часть – говорили: "Нет, давайте пойдем все-таки по проторенному пути и будем называть это информационной безопасностью"), все-таки мы договорились, что в нашем документе, для того чтобы нам проще было понимать, о чем мы говорим, мы будем использовать слово "кибербезопасность". Дальше мы уже во взаимодействии с государственными органами (притом что стратегия будет дальше обсуждаться, писаться, развиваться) готовы будем обсуждать глоссарий, готовы будем обсуждать термин.

Информационная безопасность предполагает серьезный гуманитарный аспект. Наши специалисты, которых мы собирали, в этом аспекте не являются, как мне представляется, экспертами. Кибербезопасность, и от этого мы отталкиваемся, это именно технический аспект, и мы именно на нем были сконцентрированы – защита от взломов, безопасное поведение в сети... С МИДом и ФСБ мы эти вопросы обсуждали, теперь, на мой взгляд, мы друг друга понимаем.

Комиссия по развитию информационного общества была в первую очередь интегратором, а не автором документа. Мы предоставили площадку, организовали встречи, работали над текстом.

Но контент, я хочу это подчеркнуть, привнесли эксперты. Наверное, это очень важно, и это показательно, что этот документ мы писали по факту методом краудсорсинга. То есть Совет Федерации, я хочу это подчеркнуть, не довлел над экспертами, не ставил задачи. Если мне не изменяет память, то тот документ, который вы видите, – это версия 5.11, если говорить компьютерным языком, я думаю, вы поймете. То есть это пять принципиальных версий, и в пятой версии мы 11 или 12 раз меняли, я сбился со счета, сколько раз мы меняли. И это не финал.

Работа над концепцией не завершена. Мы будем размещать документ после наших слушаний с учетом замечаний, с учетом критики, которая будет, надеюсь, потому что мы все-таки хотим здесь предметно обсудить этот документ.

После этого он будет вывешен в свободный доступ, и любой гражданин, которому эта тема будет близка, сможет отозваться об этом документе, дать свои предложения. И мы считаем, что это тоже очень важно, потому что интернет-сообщество, пользователей Интернета в целом волнует эта тема, и, может быть, они нам подскажут какие-то интересные мысли.

В заключение интересный факт. Microsoft месяц назад опубликовала рекомендации по разработке стратегии кибербезопасности. В нескольких мероприятиях принимали участие их специалисты. Мы приятно удивились, когда увидели совпадение по очень многим вопросам: то ли их специалисты дали нам эти предложения, то ли их специалисты услышали эти предложения у нас на обсуждениях. И сейчас эти предложения Microsoft продвигает как некие предложения именно для стратегий разных стран, которые сейчас пишут эти вещи. Так что, может быть, другие страны сейчас

будут пользоваться в том числе уже нашими рекомендациями. Но это такая шутка.

Для более полного доклада, для представления стратегии я передаю слово Александру Шепилову. Большинство присутствующих его знают. Именно он вёл основную работу, основные встречи, сводил документ. Он у нас является нашим секретарем комиссии по развитию информационного общества.

Александр Олегович, Вам слово.

А.О. ШЕПИЛОВ

Руслан Усманович, спасибо.

Уважаемый Александр Порфирьевич, уважаемые коллеги, добрый день! (Презентацию можно включить?) Предлагаю обратиться к собственно содержанию документа. Он у вас есть в "раздатке", он рассылался заранее членам рабочей группы и всем участникам слушаний, которые приглашались. Но тем не менее мы посчитали необходимым акцентировать здесь внимание на некоторых ключевых деталях.

Первое. Еще раз, почему, собственно говоря, именно концепция стратегии, а не стратегия? То есть в концепции обосновывается прежде всего необходимость разработки стратегии кибербезопасности, устанавливаются ее ключевые принципы, основные направления, определяется место документов в системе других аналогичных документов Российской Федерации. Но так как мы посчитали и наши эксперты посчитали неправильным не наполнить эту концепцию хотя бы какой-то конкретикой, то помимо обоснования актуальности необходимости в ней есть все-таки указание на ряд направлений и на ряд мероприятий, которые, по мнению экспертной группы, должны в обязательном порядке войти в последующем в текст стратегии.

Почему, еще раз коротко, мы говорим всё же о кибербезопасности? Потому что мы полагаем, что она имеет более четко очерченную предметную область, она касается в первую очередь физики, то есть это каналы Интернета, другие каналы, инфраструктура, это аппаратное обеспечение, программное обеспечение и деятельность. То есть, таким образом, она у́же информационной безопасности и затрагивает в основном технические аспекты. И хотелось бы подчеркнуть, что она дополняет существующую систему регулирования без противоречий.

Сейчас ряд документов именно по информационной безопасности действует, но, как уже было сказано выше, на наш взгляд, в них недостаточно отражены какие-то действия бизнеса и граждан, в них не всё указано, что должно быть указано в части кибербезопасности как технологической защищенности. И это не потому, что это какая-то недоработка тех органов власти, которые эти документы разрабатывали и принимали, а потому, что настолько быстро меняется всё в этой области, что нужно постоянно принимать новые документы и дорабатывать, для того чтобы быть в тренде.

И, наконец, как мы считаем, все-таки не хватает на национальном уровне некой понятной прозрачной единой системы действий, которая включала бы всех стейкхолдеров и которая была бы разработана хотя бы на среднесрочную перспективу.

И здесь мы терминологически совпадаем с международными подходами и полагаем, что это даст дополнительные возможности в международной коммуникации, потому что киберпространство исключительно на национальном уровне регулировать невозможно, в нем нет границ. Огромное количество атак, воздействий на нашу инфраструктуру, на наших граждан, на наш бизнес происходит из-за

рубежа. И если не будет эффективная коммуникация выстроена, то мы не сумеем наших граждан защитить.

Собственно говоря, цель стратегии – это обеспечение кибербезопасности личности, бизнеса и государства в Российской Федерации путем определения системы приоритетов, принципов и мер в области внутренней и внешней политики. И основные задачи – это систематизация действий всех заинтересованных сторон, это включение в этот процесс помимо государства бизнеса и гражданского общества и это устранение существующих пробелов в регулировании.

По нашему мнению, приоритетами в обеспечении кибербезопасности являются: первое – это развитие национальной системы защиты от кибератак и предупреждения киберугроз и поощрение создания частных систем, аналогичных национальной (я здесь хочу отметить, что нормативные акты о создании такой системы уже существуют, но это, безусловно, не статическая вещь, она должна постоянно развиваться, совершенствоваться, находиться в духе требований времени), второй принцип – это совершенствование и обновление механизмов защиты критической информационной инфраструктуры; это разработка механизмов партнерства государства, бизнеса и гражданского общества; это усиление безопасности государственных информационных ресурсов, потому что здесь есть над чем работать, и, наконец, очень важная вещь, где точно есть над чем работать (мы уже подступались к обсуждению этого отдельного такого, частного элемента), – это развитие цифровой грамотности граждан и культура безопасного поведения в киберпространстве.

И далее я коротко акцентирую ваше внимание на некоторых направлениях обеспечения кибербезопасности, которые включены в

текст концепции стратегии, и экспертная группа полагает, что в тексте самой стратегии они в обязательном порядке должны найти отражение и развитие.

Первое – это то, что мы называем общесистемными мерами. Сюда входит, во-первых, регулярный аудит защищенности информационных систем и критической инфраструктуры. Причем я подчеркну, естественно, критическая инфраструктура не только государственная, то есть она является в том числе и частной. Самый такой яркий пример – это банки.

Во-вторых, это принятие стандартов, национальных стандартов кибербезопасности и выработка механизма проверки их соблюдения, развитие национальной системы защиты от кибератак. И тоже важная вещь – это разработка антикризисного плана национального масштаба, в том числе с учетом возможностей для международного взаимодействия. Больше того, мы на заседаниях группы даже обсуждали возможность (это не нашло отражения в итоговом тексте документа, но в одной версии это было) проведения учений в соответствии с этим планом. Точно так же, как у нас сейчас Министерство обороны проводит регулярно учения, которые касаются оффлайновых структур, мы точно также считаем актуальным проведение учений в онлайне.

Второе направление – это совершенствование нормативно-правовой базы. Сюда входят и регулярный аудит, и включение механизма обновления требований и рекомендаций, и системное совершенствование законодательства, в том числе анализ того, что происходит за рубежом. Почему нет? Если мы найдем там что-то приемлемое для нас, что может быть эффективно реализовано, почему не взять это на вооружение?

Далее – это широкое включение экспертов из бизнеса, некоммерческих организаций, академических кругов в подготовку проектов документов, чтобы это не происходило кулуарно, за закрытыми дверями. Это ужесточение административной и уголовной ответственности за киберпреступления, в том числе, возможно, введение новых составов. Понятно, что это очень тонкая и больная тема, но тем не менее целый ряд экспертов, с которыми мы обсуждали этот вопрос, постоянно говорят нам о том, что, к сожалению, существующее законодательство (Кодекс об административных правонарушениях, Уголовный кодекс) не всегда позволяет эффективно вести расследование, не всегда позволяет эффективно давать преступникам, скажем так, то наказание, которого они заслуживают, которое соответствует масштабу ущерба от их действий. И упрощение взаимодействия правоохранителей с зарубежными коллегами, поскольку киберпреступность транснациональна.

И, наконец, в качестве такого, может быть, более частного, но тем не менее важного примера, потому что сейчас это очень активно развивается, – это регулирование сферы "облачных вычислений", потому что сейчас всё больше и больше все переходят в "облака" и, наверное, этот процесс нельзя остановить уже, но вопросы безопасности и транснациональной безопасности очень остро здесь встают.

Следующее направление очень важное, оно достаточно скупо обозначено в документе, но оно принципиальное – это проведение научных исследований. То есть это создание центров разработок, R&D-центров, их адресная поддержка, потому что без этого мы не сможем создавать национальные продукты здесь.

И, собственно, четвертое направление – это создание и производство собственных средств обеспечения кибербезопасности. Это принципиальный вопрос. Без этого мы не сможем утверждать, что обладаем цифровым суверенитетом в полной мере. И здесь, естественно, необходимо говорить о поддержке российских производителей разными способами, в том числе, может быть, финансовым стимулированием. Это содействие новым разработкам, это приоритетное внедрение российских средств кибербезопасности в критических информационных системах.

Следующая вещь (тоже принципиально важная, может быть, даже номер один, ее последствия не всегда представляются такими очевидными, но на самом деле они имеют системное воздействие, и мы пригласили специально коллег из Министерства образования и науки и рассчитываем, что они это прокомментируют) – это совершенствование кадрового обеспечения, это обновление стандартов подготовки специалистов именно в области информационной безопасности и кибербезопасности. Это с одной стороны. С другой стороны – это введение модулей по кибербезопасности в образовательных учреждениях, то есть так, чтобы специалисты всех профилей обладали какими-то базовыми знаниями по этому поводу. Это подготовка требований для аттестации госслужащих в этой сфере. Причем, очевидно, это должны быть разные требования. С одной стороны, понятно, более жесткие и более детальные для тех госслужащих, которые этим профессионально занимаются, и более мягкие, но тем не менее какой-то базовый уровень должен быть, для всех госслужащих, потому что сейчас эти технологии, информационные технологии, они очень активно внедряются в государственном управлении.

И, наконец, стимулирование частно-государственного партнерства и инвестирование в дополнительное узкоспециализированное образование.

Далее. Внутреннее и международное взаимодействие. По международному взаимодействию, понятно, это в основном компетенция Министерства иностранных дел. Но мы посчитали правильным хотя бы рамочно в нашем документе обозначить это, потому что это важно. Это расширение сотрудничества как внутреннего, так и внешнего для обмена информацией. Это подготовка государством и организация отчетности по вопросам кибербезопасности для последующего анализа и коррекции действий. Очень важно, чтобы здесь начало появляться больше открытых данных, но до той степени, до которой это не будет противоречить национальным интересам, потому что открытые данные, они всегда стимулируют действия разных стейкхолдеров в этом направлении, они позволяют вскрыть проблемы, которые, может быть, были не так очевидны до этого. Это облегчение регистрации и начало расследований киберпреступлений, разработка механизмов оказания помощи государству в этом расследовании. Это консультирование владельцев критической информационной инфраструктуры. И поощрение граждан в борьбе с киберугрозами, в том числе в части поиска уязвимостей и формирования предложений по ликвидации этих уязвимостей. Это люди, которые называются на жаргоне "белыми хакерами", перешедшими на сторону добра.

Далее, очень важная вещь – это развитие культуры безопасного поведения в киберпространстве, организация комплексных информационных кампаний о рисках, уязвимостях, способах защиты, рекомендациях по использованию тех или иных сервисов. Это, возможно, создание и популяризация некоего единого

государственного портала по кибербезопасности. Это обеспечение информационной поддержки большому количеству тематических мероприятий. И могу сказать, что в этом направлении мы уже двинулись. В Государственную Думу был внесен законопроект о родительском контроле, который, скажем так, определяет обязанность операторов, предоставляющих услуги доступа в Интернет, информировать пользователей о доступности сервисов родительского контроля.

Коллеги, и завершая представление документа... Как уже было сказано, документ не завершен, его ждет еще как минимум два этапа доработки: первый – это по итогам этих слушаний учет всех тех рекомендаций, которые будут здесь высказаны, и второй – это обсуждение в режиме онлайн. Поэтому по факту сегодня мы завершим и сразу же после этого продолжим работать с документами.

И наше видение дальнейшей судьбы этого документа следующее. После того, как документ пройдет все эти этапы обсуждения, будет доработан, мы будем просить Валентину Ивановну Матвиенко, как члена Совета Безопасности, вынести доработанный документ на обсуждение уже Совета Безопасности, прямым полномочием которого в соответствии с нашей Конституцией является обеспечение безопасности государства, и граждан, и общества, в том числе, в частности, естественно, и кибербезопасности. И дальше мы рассчитываем, что, если Валентина Ивановна поддержит наше предложение, документ будет внесен и пройдет согласование в соответствии с внутренними процедурами уже Совета Безопасности... это как некая такая сверхзадача – чтобы он попал на рассмотрение Президента Российской Федерации.

Коллеги, собственно, на этом всё. Таков был подход, такие результаты получили по итогам.

Р.У. ГАТТАРОВ

Спасибо, Александр Олегович. Мы ставим себе только сверхзадачи.

Я хочу предоставить слово советнику Министра связи и массовых коммуникаций Игорю Анатольевичу Милашевскому. Он как раз ведет этот блок в Министерстве связи и массовых коммуникаций, полностью отвечает за международные контакты, является серьезным специалистом в этой области.

Пожалуйста.

А.П. ТОРШИН

У нас протокол. Игорь Анатольевич, пожалуйста.

Р.У. ГАТТАРОВ

Вам не смог отказать.

И.А. МИЛАШЕВСКИЙ

Добрый день! Во-первых, хочу выразить большую благодарность руководству Совета Федерации, Руслану Усмановичу и Александру Олеговичу за очень большую работу, которая проделана по такому актуальному вопросу. Министерство принимает участие, я полагаю, достаточно активно. Мы с уважением относимся к этой работе, идет дискуссия. Может быть, мы делаем какие-то замечания, может быть, даже сейчас я их произнесу, но в целом, безусловно, работу поддерживаем, и все эти дискуссии носят рабочий характер, направленный на улучшение документа.

В настоящее время весь мир в целом, каждая страна создают руководящие документы, способные сформировать целостный, интегрированный, комплексный подход к регулированию вопросов защиты от киберугроз. При этом комплексность определяется необходимостью выработки механизмов информационной безопасности во всех сферах жизнедеятельности государства и

общества: экономической, социальной, образовательной, правоохранительной. Целостность подразумевает четкую взаимосвязь всех руководящих документов в указанной сфере и методов их реализации. Интегрированность обозначает необходимость привлечения к управлению информационной инфраструктурой в целом и к обеспечению информационной безопасности в частности и государства, и бизнеса, и общества. Разграничение ролей каждого из участников в процессе управления информационной инфраструктурой, определение их прав и обязанностей и ответственности, развитие механизмов частно-государственного партнерства для реализации мер по обеспечению информационной безопасности является основой успешной государственной политики в информационной сфере.

Кроме того, интегрированность подразумевает взаимодействие вышеперечисленных участников не только в рамках отдельно взятой страны, но и на международном уровне. Необходимо признать, что информационно-телекоммуникационные технологии – важнейшая инфраструктурная составляющая жизни людей, функционирования государственных структур, развития экономики.

На сегодняшний день киберугрозы трансграничны, а целью кибератак становится причинение вреда большому количеству субъектов, независимо от гражданства и социального статуса.

Характер угроз в информационной среде различен: это привычные нам кражи личных данных, финансовых активов, сведений, составляющих коммерческую или государственную тайну, искажение, ограничение или отказ в доступе к необходимой информации, предоставление заведомо недостоверной или опасной (для здоровья детей, например) информации, нарушение прав на результаты интеллектуальной деятельности.

Защититься от киберугроз точечно на уровне отдельных групп пользователей на сегодняшний день невозможно, поэтому государство обязано взять на себя координирующую роль в этом процессе.

Наиболее важным и сложным в данной ситуации является соблюдение баланса между укреплением информационной безопасности при координирующей роли государства и соблюдением и обеспечением информационных прав и свобод граждан Российской Федерации, а также открытости сети Интернет.

Если говорить об уровне федеральных законов, относящихся к сфере ведения Минкомсвязи, то базовыми документами в части защиты информации, в частности, являются Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации", устанавливающий основные положения, касающиеся защиты информации, Федеральный закон № 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления", обеспечивающий гарантированное Конституцией Российской Федерации право каждого на доступ к информации, в том числе затрагивающей его права и обязанности, Федеральный закон № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", Федеральный закон № 63-ФЗ "Об электронной подписи", Федеральный закон № 152-ФЗ "О персональных данных", устанавливающий особенности обработки так называемых личных данных, то есть информации, прямо или косвенно относящейся к идентифицируемому человеку, а также механизмы защиты такой информации.

Важно отметить, что указанным федеральным законом Минкомсвязь России планирует явно реализовать принцип

сотрудничества между государством, бизнесом и обществом. Так, в Плане законопроектной деятельности Правительства Российской Федерации на 2014 год Минкомсвязью России предложен законопроект "О внесении изменений в Федеральный закон "О персональных данных" в части установления обязанностей оператора персональных данных (в дополнение к имеющимся) уведомлять субъекта персональных данных о том, что без его согласия и без поручения оператора персональные данные стали доступны третьим лицам или общедоступны, а также предоставить информацию о мерах, которые могут быть приняты субъектом персональных данных самостоятельно или совместно с оператором для снижения негативных последствий такой доступности данных.

Кроме того, в случаях, когда утечки данных приобретают массовый характер, негативные последствия могут быть значительными, оператор должен уведомить уполномоченный орган по защите прав субъектов персональных данных, который вправе подключить иные федеральные органы исполнительной власти для решения проблемы, а также обязан оказать содействие оператору и субъекту в минимизации негативных последствий таких утечек.

Отдельно отмечу один из важнейших законопроектов в сфере информационной безопасности Российской Федерации – это проект федерального закона о безопасности критической информационной инфраструктуры Российской Федерации, в котором, в частности, предусматривается создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, закрепление практики систематической оценки и контроля защищенности объектов инфраструктуры, а также создание структур различного уровня и принадлежности, обеспечивающих

реагирование на компьютерные инциденты. В данном случае мы являемся соисполнителем ФСБ по подготовке законопроекта.

Николай Николаевич, ничего, что я анонсировал ваш законопроект?

Н.Н. МУРАШЁВ

Он общий.

И.А. МИЛАШЕВСКИЙ

Он реально базовый, да, и нам предстоит его...

Также хотелось бы отметить деятельность Минкомсвязи по направлению обеспечения и контроля целостности и повышения устойчивости функционирования и безопасности российского сегмента сети Интернет. Так, нами подготовлен комплекс предложений в данной сфере, рассмотренный в мае 2013 года и одобренный межведомственной комиссией по информационной безопасности и научно-техническим советом Совбеза России. Основные предложения и положения нашли отражение в ряде последующих поручений Президента Российской Федерации, в решениях Совета Безопасности России и его координационных органов.

В частности, поручена подготовка представления Президенту Российской Федерации предложений о документах стратегического планирования в сфере обеспечения целостности и устойчивости функционирования и безопасности российского сегмента сети Интернет.

Другой порученной задачей является образование с участием отраслевых саморегулируемых организаций центра мониторинга национального сегмента, который обеспечит мониторинг целостности, устойчивости функционирования и критических

ресурсов сегмента сети, а также координацию взаимодействия операторов и других заинтересованных сторон.

В целом, учитывая надсетевой характер сети Интернет и, как следствие, неэффективность ее регулирования на уровне операторов связи, а также принцип саморегулирования управления критическими ресурсами сети Интернет, закрепленный российским законодательством в области связи, Минкомсвязь России планирует реализацию мер по обеспечению целостности, устойчивости функционирования и безопасности национального сегмента сети Интернет с привлечением отраслевых саморегулируемых организаций, в том числе инициируя и участвуя в подготовке ими стандартов и правил ответственного ведения деятельности субъектами интернет-отношений, а также побуждая к принятию широким кругом субъектов таких стандартов и правил.

Также к разрабатываемым документам относится концепция, которую коротко назову "Гособлако". Наверное, многие ее видели на сайте, она была представлена для обсуждения, сейчас она находится на доработке, в декабре продолжим ее обсуждение. В основном всё. Спасибо.

Р.У. ГАТТАРОВ

Спасибо, Игорь Анатольевич.

Уважаемые коллеги, здесь все-таки собрались люди, которые так или иначе представляют, что происходит.

Вам спасибо за доклад о том, что делает министерство, действительно, он достаточно полный.

Но хотелось бы все-таки, чтобы мы обсуждали предметно документ, именно для этого мы здесь собрались. Это я к коллегам, которые будут выступать, хотел бы обратиться.

У нас от Министерства образования и науки Российской Федерации присутствует Мосичева Ирина Аркадьевна, заместитель директора Департамента государственной политики в сфере высшего образования.

Пожалуйста.

И.А. МОСИЧЕВА

Добрый день, уважаемые коллеги! Следуя призыву руководителя, я хочу совершенно конкретно остановиться на ряде моментов.

Когда мы анализировали текст концепции стратегии кибербезопасности Российской Федерации, то свое место Министерство образования и науки видит как минимум в двух ее разделах. Это раздел, связанный с обеспечением научных исследований, и, естественно, раздел, связанный с обеспечением данной сферы деятельности Российской Федерации кадровым потенциалом. И скажу совершенно конкретно: цели поставлены, задачи определены, и работа у нас в этом направлении идет достаточно давно.

Если говорить о составляющей научной деятельности по обеспечению информационной безопасности страны, то начиная с 2007 года и по настоящее время (а также в планах научных разработок Министерства образования и науки в рамках федеральной целевой программы "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России" с 2007 по 2020 год) регулярно проводится цикл научно-исследовательских работ, направленных на реализацию основных моментов в части научного обеспечения, материально-технического обеспечения, исследований в области фундаментальных проблем данной сферы деятельности. За

последние годы как минимум восемь крупнейших разработок уже было завершено. В планах новой программы на 2014–2020 годы также будут поддержаны научные исследования.

Если мы говорим о подготовке кадров, то здесь, наверное, надо задаться следующими вопросами: кого мы учим, кто это будет делать, чему мы будем учить нынешних студентов и будущих абитуриентов, на какой материально-технической базе?

Я не буду говорить о том, наверное, вы все прекрасно знаете, что с 1 сентября 2013 года вступил в силу новый Федеральный закон "Об образовании в Российской Федерации". Его введение в действие тоже привело к тому, что придется, наверное, скорректировать в некой части и основные моменты концепции стратегии кибербезопасности Российской Федерации, потому что он внес не только структурные изменения, но и принципиальные. Вот на них я бы и хотела остановиться.

Итак, на протяжении последних 15 лет Министерство образования и науки (как бы оно ни называлось до этого и сейчас) осуществляет подготовку кадров для сферы информационной безопасности страны. В настоящее время более 150 высших учебных заведений и более 35 образовательных учреждений среднего профессионального образования осуществляют подготовку по трем направлениям и специальностям в сфере среднего профессионального образования и более чем девяти направлениям и специальностям в сфере высшего профессионального образования, как это называлось раньше.

В системе бывшего послевузовского, а теперь уже нового уровня высшего образования – подготовки кадров высшей квалификации – открыта научная специальность, специальность

научных работников "информационная безопасность" (050319). Работало более 20 диссертационных советов.

Можно сказать, что материально-техническая база для подготовки специалистов тоже соответствует среднему уровню. Но, наверное, всё не так хорошо, и всё не так гладко, как хотелось бы. На сегодняшний день перед Министерством образования и науки совершенно конкретно стоит задача более четкой "заточки" специалистов, которые выходят в эту сферу деятельности. А более точная "заточка" невозможна без определения: а) потребности в выпускниках; б) квалификации выпускников. Вы знаете о том, что мы выпускаем специалистов со средним профессиональным образованием, мы выпускаем в соответствии с новым законом специалистов с дипломом бакалавра, специалистов с дипломом специалиста, магистра и, естественно, кандидатов, в данном случае в большей мере это специальность "кандидат технических наук". Вот реальная потребность нашей страны в специалистах должна быть более четко спрогнозирована для того, чтобы Министерство образования и науки могло сконцентрировать свои усилия. На сегодняшний день потребность оценивалась в 5 тысяч человек. Реально мы выпускаем 12 тысяч человек в год. Но вопрос, насколько они востребованы, их компетенция востребована сегодня.

Второй вопрос – не столько численность, сколько качество выпускников определяет, наверное, обе стороны той проблемы, которую мы сегодня рассматриваем. Проблема – кто защищает и от кого защищает – рождается в стенах одного и того же образовательного учреждения. Поэтому компетенцию и квалификацию должен определить профессиональный стандарт в этой сфере деятельности. Тогда Министерство образования и науки, опираясь на профессиональный стандарт, более четко сможет

организовать подготовку специалистов, поскольку нынешние федеральные государственные образовательные стандарты по своей структуре совершенно спокойно могут это обеспечивать.

Я приведу пример. Допустим, на сегодняшний день федеральный государственный образовательный стандарт в области подготовки бакалавра позволяет содержать вариативную часть, это часть, которая может определяться работодателем, в первую очередь работодателем, то есть потребителем наших образовательных услуг, на 50 процентов. То, что касается магистранта, то у него в рамках его подготовки вариативная часть составляет 70 процентов. Это означает, что при более точной и четкой постановке задачи Министерство образования и науки может готовить точечных специалистов для определенной сферы деятельности.

В аспирантуре такой вариативной частью являются научные исследования, которые в общей сетке федерального стандарта, который сейчас разрабатывается впервые для института аспирантуры и адъюнктуры в том числе, составляют почти 80 процентов. Ну, это научное исследование, оно всегда индивидуально, хотя, в общем, стандарт предполагает более серьезную подготовку общую, общекультурную, общепредметную. Но она всё равно определяется сферой деятельности соискателя степени.

Что касается подбора наших абитуриентов, то Министерство образования и науки на протяжении многих лет проводит различные олимпиады. И надо сказать, что на сегодняшний день, начиная с 2010 года мы ведем статистику (вы знаете, что прием в высшие учебные заведения осуществляется по результатам единого государственного экзамена), − так вот, у поступающих ребят на специальность "информационная безопасность" в бакалавриат средний балл ЕГЭ на третьем месте, а у магистрантов это самый

высокий балл – более 72 при поступлении (средний балл). Поэтому... мы имеем хороших абитуриентов.

Когда мы говорим, что мы имеем хороших абитуриентов, мы должны иметь хорошие программы и хороший педагогический состав. И говоря о педагогическом составе, мы должны в первую очередь говорить о системе повышения квалификации тех специалистов, которые осуществляют подготовку будущих специалистов.

На сегодняшний день такую подготовку осуществляют более 20, почти, можно сказать, 30 научно-методических центров. Головной организацией в Минобрнауки является созданный центр на базе Московского инженерно-физического института. Эта работа будет продолжаться. Но я еще раз говорю: работу сдерживают, конечно, реальные требования работодателя к содержанию образования, которых мы пока не знаем.

Но в связи с введением в действие нового закона возникает одна проблема. В соответствии с нормой закона мы обязаны формировать реестр примерных образовательных программ. Эта вещь публичная, открытая, проходит открытую экспертизу. Ясно со всей очевидностью, что часть тех модулей (вот задача перед нами поставлена – разработать программы, модули), они не могут быть достоянием открытой экспертизы и размещены в открытый реестр примерных образовательных программ. Поэтому я думаю, что в процессе работы над концепцией необходимо будет решать и ряд таких достаточно специфических вопросов, которые так или иначе с введением в действие нового закона перед нами встанут.

И еще один момент, на котором надо остановиться. В соответствии с законом образовательную программу разрабатывает образовательное учреждение. И поэтому связь потребителя

(выпускника) с образовательным учреждением должна быть более тесной, что ли, для того чтобы то, что у нас "на выходе", удовлетворяло вас "на входе", минуя Институт повышения квалификации сразу по окончании вуза, как иногда это бывает: выпускник приходит и идет до полугода стажироваться куда-то, а потом его, может быть, до чего-нибудь допустят. Не очень бы хотелось, чтобы эта тенденция продолжалась. Нам нужен отклик работодателя.

Я могу много говорить на эту тему, но говорить я, наверное, не буду, для одного раза, первого, хватит. Если будут какие-то вопросы, я готова ответить на них. Спасибо.

Р.У. ГАТТАРОВ

Спасибо большое.

Хотелось бы, чтобы Вы также заметили, что у нас в целях, вернее, в принципах стратегии есть повышение уровня цифровой грамотности общества. Мы считаем, что здесь это не только задача бизнеса, но в первую очередь задача образования, и начинать выполнять ее надо сейчас, как минимум со школы. И мы, в общем-то, в этом смысле с министерством работаем и надеемся, что мы эту работу будем продолжать более эффективно в дальнейшем.

И.А. МОСИЧЕВА

Вы абсолютно правы, да. И можно, я как раз в контексте этого скажу, что сегодня по плану работы министерства в 15 часов 30 минут состоится заседание коллегии министерства, посвященное математическому образованию в Российской Федерации, что неразрывно связано с тем, что Вы только что сказали. Поэтому то, чем закончится сегодня заседание коллегии по математическому образованию в России, – это новая концепция, она является вот тем самым вкладом в ту проблему, которую мы сегодня обсуждаем.

Р.У. ГАТТАРОВ

Спасибо.

Большая заслуга в написании концепции стратегии принадлежит Российской ассоциации электронных коммуникаций. Начальник этой ассоциации, если так вообще можно говорить про ассоциацию, он первый среди равных – Сергей Александрович Плуготаренко.

Пожалуйста.

С.А. ПЛУГОТАРЕНКО

Спасибо большое. Так меня еще не называли, приятно.

Директор РАЭК Сергей Плуготаренко.

Во-первых, естественно, большое спасибо как инициаторам этого продукта и президиуму, так и залу, потому что в зале есть большое количество экспертов, которые принимали участие, в том числе под каким-то нашим руководством, в проработке основных положений концепции.

Что хочу отметить? Во-первых, некий достаточно спокойный тон, что странно для реалий последних нескольких месяцев. Отрасль спокойно обсуждала этот закон, эту концепцию, и не видела за ним пока каких-то моментов, которые могли бы нанести особый урон бизнесу, инфраструктуре, развитию Интернета, что в принципе в последнее время является, как я уже сказал, общим местом. Мне кажется, что эту позитивную повестку, этот позитивный, ровный, спокойный тон нужно сохранить и на выходе этого продукта.

Те положительные моменты, которые наши эксперты отметили для себя при изучении финального варианта документа.

Во-первых, наши отраслевые замечания учтены, что очень приятно. Обычно нам тяжело координировать работу по таким судьбоносным документам. В данном случае это было проще, потому

что в РАЭК есть профильная комиссия – комиссия по борьбе с киберугрозами и по повышению информационной безопасности. Вот ровно она и занималась анализом и доработкой этого продукта.

Мы считаем, что также позитивным моментом является то, мы на этом настаивали, что излишнее бремя, в том числе экономическое, на бизнес по обеспечению информационной безопасности было устранено и не проходило такой красной нитью через итоговую версию документа. Нам понравилось, как осуществлялась работа с терминологией, и тот компромисс между информационной безопасностью и кибербезопасностью, который был достигнут на уровне терминологии, нас абсолютно устраивает, мы считаем правильным, некая такая интеграция понятий, привычных на западном уровне, на российском уровне. Это некое напряжение первоначальных дискуссий было снято.

Мы считаем, что мы можем легко консолидироваться со всеми подходами, которые изложены в концепции, и это в принципе достаточно большая заслуга бизнеса и государства в данном случае, потому что мы шли бок о бок.

Важно, что положения стратегии не противоречат уже имеющимся документам (этот этап был пройден, все-таки почти год над стратегией велась работа): то есть это и Доктрина информационной безопасности Российской Федерации, и Стратегия развития информационного общества в Российской Федерации, и другие документы.

Документ, на наш взгляд, является целостным, непротиворечивым и носит сейчас какой-то уже финальный характер. При этом очень важно, что в какой-то момент на этапе разработки было добавлено слово "концепция", что предполагает, что дальнейшая проработка стратегии может еще занять некоторое время,

и там будут учтены дополнительные аспекты, не будет какой-то гонки в принятии финальной версии, будет возможность экспертам еще работать.

Что вызывает однозначное одобрение отрасли?

Во-первых, закрепление конституционных прав на доступ к информации, получение информации гражданами. Это важно было отметить, и это открытым текстом сказано в документе.

Особый акцент сделан на критически важные инфраструктурные вопросы и особую защиту государственных информационных систем. Бизнес готов консультировать, помогать, снабжать решениями.

Принцип мультистейкхолдеризма, который также прописан красной нитью в этом документе, является очень важным. Мы считаем, что очень правильно, что в концепции закрепляется большой пласт работы за научно-исследовательскими разработками, которым отрасль отводит (и надеется, что все будут отводить) определенное место. Экспертная сила Рунета такова, что мы можем, умеем, хотим консультировать, в том числе госструктуры.

Важно отметить, что поддержка отечественных производителей, закрепленная также в концепции, тоже вызвала положительную оценку со стороны отрасли.

Кадровый вопрос и вопрос медиаграмотности, об этом очень много говорилось, вызывают однозначное одобрение. Более того, у нас в ассоциации есть целый продукт, которым мы готовы будем поделиться, – это некие подходы к обеспечению ссузов и вузов определенными концепциями и курсами по инфобезопасности. Я думаю, что эти разработки пригодятся и при реализации стратегии, еще раз говорю, что готовы ими поделиться.

Вызывает одобрение заложенная, отрытым текстом прописанная поддержка профильных мероприятий, нам это достаточно важно, потому что, если государство будет принимать более активное участие в отраслевых конференциях, семинарах, "круглых столах", это будет на пользу всем.

Я считаю, что главным аспектом положительным, который стратегия привнесла, является обсуждение вопросов информационной безопасности в СМИ и в обществе, потому что в последнее время очень часто обсуждаются всевозможные тенденции к "закручиванию гаек", "охоте на ведьм", а в данном случае мы предложили некий позитивный посыл и некий конструктивный подход к тому, как можно заниматься (не спеша, с участием экспертов) разработкой вопросов информационной безопасности.

Теперь о том, что вызывает вопросы и, может быть, некую настороженность в отрасли. Хочу об этом тоже сказать, потому что это важно.

Во-первых, мы хотели бы, чтобы сохранился тот формат открытого обсуждения документа, когда из этапа концепции он перейдет к этапу становления стратегией. На этом этапе не должно быть каких-то скрытых обсуждений, переговоров за закрытыми дверями. Мы очень надеемся, что нас также будут приглашать и что режим максимальной открытости обсуждения документа сохранится.

Вызывает опасение потенциальная возможность создания неких запретительных регуляторных механизмов на основе этой стратегии. Мы знаем, что в последнее время (мы даже провозгласили 2012–2013 годы годами беспрецедентного внимания государства к интернет-отрасли) очень большое количество новых законов, законопроектов, поправок. Бóльшая часть из них носит запретительный характер, не стимулирующий. Мы очень надеемся,

что в данном случае удастся избежать такого тренда, и стратегия будет предназначена для того, чтобы все-таки стимулировать определенные сегменты, связанные с информационной безопасностью, развитием Рунета, ну и вообще весь Рунет.

Еще вызывает опасение возможность сегментации Интернета по географическим признакам. Но мы надеемся, что этого не случится, потому что предпринята большая попытка в этой стратегии консолидироваться с международным сообществом и признать то, что Интернет имеет трансграничную природу.

Очень внимательно нужно будет отнестись (о чем уже говорили) к вопросам "облачных вычислений" как к новым технологиям, новым трендам, которыми достаточно много в последнее время приходится заниматься на экспертном и законодательном уровнях. Но при этом общий фон пока, конечно же, ровный. И я считаю, что его нужно сохранить. А у России есть все предпосылки для того, чтобы сказать, что мы в принципе можем и уже сейчас занимаем лидирующие позиции в области информационной безопасности. Ряд игроков коммерческого сегмента у нас достаточно сильные, они известны и на международном рынке, что вообще для российских компаний не является общим местом. Это большое достижение, большая наша гордость. Все экономические, аудиторные показатели Рунета растут, растут темпами порядка 30–40 процентов в год. И никакие дополнительные, скажем так, регуляторные воздействия на Рунет, конечно, не должны привести к снижению этих показателей и динамики их роста.

Привлекайте. Будем консультировать. Будем делиться наработками. Будем активно продолжать участвовать в разработке

документа с того момента, как из концепции он превратится в стратегию. Спасибо.

Р.У. ГАТТАРОВ

Спасибо, Сергей Александрович.

Я вот, единственное, всё время спрашиваю: а какое большое количество законов мы приняли в отношении Интернета? Законопроектов – большое количество. Законов...

С.А. ПЛУГОТАРЕНКО

У нас была аналитика в 2012 году. Мы насчитали порядка 60 законодательных инициатив, поправок к законам, из них 42 процента, по мнению экспертов опять же (то есть дают сухие цифры, которые мы...), являются негативными.

Р.У. ГАТТАРОВ

Их могло бы быть 600, но это всё законодательные инициативы, которые в законы-то не превращаются.

С.А. ПЛУГОТАРЕНКО

Полностью согласен, но беспрецедентное внимание государства. Все-таки некий момент, некий рубеж был пройден. Я считаю, что это случилось. Может быть, это и правильно, потому что более 50 процентов граждан России – это уже пользователи.

Р.У. ГАТТАРОВ

Да. Еще короткая реплика. Я считаю, что с каждым годом внимание к Интернету политиков – оппозиционных, властных – будет всё больше и больше. Количество экспертов, которые занимаются регулированием Интернета, будет увеличиваться. Но это нормальная реакция, потому что чем больше Интернет влияет на жизнь, тем больше политиков будет там появляться. Это мировая тенденция, которая идет.

Ну а насчет государства... Государство не обращает внимания – плохо, государство обращает внимание – всё равно плохо.

Андрей Вячеславович Колесников, один из идеологов этой стратегии и вообще создания стратегии кибербезопасности Российской Федерации.

Пожалуйста.

А.В. КОЛЕСНИКОВ

Спасибо, Руслан Усманович.

Я буду краток. Когда мы начинали эту работу, это было больше года тому назад, я точную дату не помню...

Р.У. ГАТТАРОВ

Конец сентября.

А.В. КОЛЕСНИКОВ

Конец сентября, да.

Р.У. ГАТТАРОВ

Журналисты нам напомнят.

А.В. КОЛЕСНИКОВ

Да. Собственно, работа с чего началась? Стало интересно провести анализ стратегий ведущих интернет-держав в отношении кибербезопасности.

В рамках координационного центра, организации, которую я возглавляю, мы сделали некий достаточно широкий анализ, в котором мы не давали никаких оценок, а просто собрали вместе практику держав. При этом, естественно, мы отдавали себе отчет в том, что Россия является одной из этих ведущих держав, то есть мы в Интернете далеко не развивающаяся страна, а вполне развитая. Например, с точки зрения бизнес-потенциала и реального бизнес-оборота в Интернете мы в Европе (я не знаю, Сергей Александрович,

может быть, меня поправит), наверное, занимаем лидирующие позиции, и наш потенциал весьма велик.

Также в свое время было очень интересное исследование на предмет того, как страны (в том числе ведущие страны, интернет-державы) связаны с окружающим миром, насколько надежна их инфраструктура, насколько хорошо она развита. Мы поняли, что Россия входит буквально в "пятерку" ведущих держав вместе с США, Гонконгом, Тайванем, Великобританией. То есть с точки зрения надежности инфраструктуры (именно взаимосвязанность с окружающим миром, количество каналов – привязанных, увязанных – с другими странами, с другими операторами) у нас всё хорошо.

Когда мы с Русланом Усмановичем встретились и стали обсуждать этот вопрос, родилась мысль, что неплохо было бы немного формализовать те проблемы, те вещи, которые во всем мире называются проблемами кибербезопасности. Например, мы прекрасно оценивали масштаб этой задачи и базовые проблемы, начиная с терминологии буквально, когда понятно, что даже тот самый термин "кибербезопасность", в общем, многие эксперты воспринимают не очень хорошо, все привыкли оперировать понятием "информационная безопасность". И вот, например, одно из достижений, я считаю, рабочей группы – это как раз правильное позиционирование этого самого документа среди соседствующих, схожих по теме. К этому я еще вернусь.

Также было понятно, что единственный способ работать над этим документом, над этой стратегией – это привлечение всех заинтересованных сторон, исходя из простой человеческой логики. Дело в том, что сама по себе проблема кибербезопасности затрагивает все области. То есть не может быть такого, что она всех

затрагивает, а реагирует на это только государство. Ну, просто она работать не будет, это из простой человеческой логики вытекает.

Руслан Усманович проделал большую работу, он привлек к работе над документом большое количество экспертов. Я с большим удовлетворением хочу сказать, что, конечно, цель важна, но еще важно, с кем ты идешь по этой дороге к этой цели, и, конечно, очень приятно работать в таком коллективе: великолепные эксперты, абсолютно трезвые и разумные люди. Никакой политики у нас не было в этой рабочей группе, что очень приятно. И на удивление, где-то я повторю Сергея, мы действительно как-то вот так работали... и даже об этом никто особо и не писал.

Р.У. ГАТТАРОВ

Это заслуга Натальи Ивановны.

А.В. КОЛЕСНИКОВ

Наталья Ивановна еще скажет по поводу этого документа.

Что еще хотел отметить? Я буду заканчивать, потому что, с моей точки зрения, документ хорош. Что, я считаю, будет действительно проблематично и сложно сделать – это вставить этот документ (вот эту концепцию, вот эту стратегию) в действующий блок законодательных и регуляторных актов, потому что... К примеру, есть документ, наверное, все знают (как же он назывался?), – культура информационной безопасности, который в рамках Совета Безопасности разрабатывается.

Р.У. ГАТТАРОВ

Это проект еще.

А.В. КОЛЕСНИКОВ

Проект, да. Я уверен, что существует множество подведомственных документов схожего плана. И здесь надежда на Руслана Усмановича, что он как-то своим спортивным зарядом,

своей энергией постарается этот документ, эту стратегию, соответственно, как-то внедрить, потому что она затрагивает абсолютно конкретные вещи, к конкретным проблемам адресует, и она пойдет на пользу всем – и государству, и пользователям, и бизнесу. Так что, я думаю, надо всё это дело довести как-то до логического завершения. И всем спасибо, конечно, кто работал над этим. Просто молодцы, хороший пример очень.

Р.У. ГАТТАРОВ

Спасибо, Андрей Вячеславович. Но мы легких путей не ищем, стандартных.

Я хочу предоставить слово члену Совета Федерации, члену Комитета по образованию, науке, культуре и информационной политике, академику Арнольду Кирилловичу Тулохонову.

Пожалуйста.

А.К. ТУЛОХОНОВ

Уважаемые коллеги! Передо мной молодые люди выразили, так скажем, солидарное мнение, что стратегия хороша, что мы все ее поддерживаем. Когда все шагают в ногу, у меня всегда возникает подозрение: а все ли так просто? Это первое.

Второе. В любой компании или при обсуждении, наверное, должен быть дилетант, который должен задавать дурацкие вопросы. Я хочу выступить в роли этого дилетанта и выразить несколько мыслей вслух.

Первое. Вот сидит Сергей Евгеньевич, доктор философских наук, наверное, он может сказать несколько шире о том, что здесь написано. Стратегия должна базироваться на следующей системе понятий. Первое – информационное пространство. Это совокупность всей информационной деятельности человека. Если мы читаем учебники философии или вообще по информационным

технологиям, то мы знаем, что информация бывает как минимум четырех видов: компьютерная, о чем мы сегодня, вероятно, говорим, письменная, картографическая, визуализированная и так далее и тому подобное. Поэтому я хотел бы для себя уяснить, о чем мы говорим в нашей сегодняшней стратегии. Скорее всего, все-таки о компьютерной, потому что ни слова о письменной, о картографической здесь не было. Для каждой информации должна быть своя защита и своя система операций.

Когда мы говорим о технологии информации, мы всегда должны ее разделить: есть получение информации, есть передача информации, есть обработка информации, архивирование информации и применение информации. На каждой из этих ступеней должна быть своя система, если мы говорим только о безопасности, то, естественно, безопасности. Об этом я, может быть, не слышал, может быть, не всё понял. Я хотел бы все-таки этот вопрос уточнить.

Дальше – с точки зрения логики и, вообще, так скажем, человеческой деятельности, нашей деятельности на примере банковской. Вот Мастер-Банк распространял информацию, которая как минимум бывает легальная, которая реальная, или действительная, нелегальная, которую он не распространял, и лжеинформация, которую он распространял. Поэтому для каждой системы информации нужна опять же своя система обработки и своя система подходов. Поэтому когда мы говорим о той информации, которую мы сегодня обсуждаем, мы должны все-таки разделить на много-много ступеней, то есть подвести философскую или методологическую основу. И не говорить огульно об информации, это тогда всё равно, что средняя температура у больного: не понятно, о чем мы ведем речь.

Дальше. Мы должны все-таки понимать, что подходы бывают разные. Мы сегодня ведем речь о технократическом подходе. Есть экономический подход, есть социальный подход и многие другие подходы, которые имеют своей целью достижение совершенно разных результатов. Об этом мы должны были, наверное, изначально договориться и отразить это в стратегии.

Я, как географ, хотел бы, прежде всего, обратить внимание на картографическую информацию, о которой сегодня речи не было, нет и, вероятно, не будет. Сегодня наша ФСБ и другие структуры засекречивают информацию крупнее масштаба 1:25. Поэтому мы вынуждены пользоваться Google, Yandex и другими структурами, брать у "буржуев", которые дают нам ее, во-первых, бесплатно, во-вторых, точнее. И когда мы пользуемся этой информацией, у меня всё время возникает вопрос: а вдруг зайдет эфэсбэшник и арестует мою информацию? Как тут быть, я, вообще, не представляю. И, наверное, в этой ситуации люди, которые занимаются географическим пространством (это геологи, географы, биологи, лесники), с этой проблемой сталкиваются. Я хотел бы, вот сегодня я пришел, узнать, а что же делать простым этим людям, которые не имеют иммунитета депутата или члена Совета Федерации? А вдруг их арестуют за то, что они используют высокоточную буржуйскую информацию, секретную для нас, но несекретную во всем мире? И вот таких вопросов в жизни возникает много.

Поэтому я благодарю вас за то, что имел возможность послушать некоторые рассуждения на эту тему, но все-таки много у меня вопросов осталось открытыми. Спасибо за внимание.

Р.У. ГАТТАРОВ

Спасибо, Арнольд Кириллович. Наталья Ивановна Касперская хочет Вам ответить. А, вообще, у нас здесь Мурашёв Николай

Николаевич, заместитель начальника 8-го Центра ФСБ. Вот он ответит на вторую часть Вашего вопроса.

А.К. ТУЛОХОНОВ

Я просто задал всуе. Я ответов не требую, их не может быть! *(Смех в зале.)*

Р.У. ГАТТАРОВ

Извините, всё уже, всё записано.

Н.И. КАСПЕРСКАЯ

Давайте я все-таки, пользуясь случаем, скажу, что, на мой взгляд, концепция стратегии оказалась чрезвычайно своевременна, потому что когда мы задумались о ее разработке, тут самые сильные пиарщики мира начали работать как раз на нас, я имею в виду Эдварда Сноудена и Агентство национальной безопасности США, которые объяснили всем, что, оказывается, Интернет – это не трансграничное некое пространство добра, а вотчина Соединенных Штатов, что, конечно, Россию, как суверенную страну, устроить не может.

Таким образом, задача защиты границ Российской Федерации в киберпространстве, в информационном пространстве является чрезвычайно важной, поэтому... Существующая Доктрина информационной безопасности очень хорошая, но она была написана все-таки в 2000 году, и, конечно, современных угроз она, во-первых, не отражает, а, во-вторых, изменение мира, которое произошло за 13 лет, требует просто новых подходов. И мне кажется, что вот эта концепция как раз и послужила такой базой, началом для этих подходов и создания.

И вот адресуя к вопросу уважаемого академика: когда мы разрабатывали этот документ, мы не ставили себе задачу охватить все сферы, потому что на самом деле информационная безопасность

и даже кибербезопасность как ее подмножество – это чрезвычайно большая сфера. Если бы мы занялись обработкой информации или рассмотрением информации на всех ее этапах, что в принципе является правильным действием абсолютно, то мы бы не закончили никогда.

У нас эта работа заняла год, и, в общем, она в самом начале, мы сделали первый шаг. Если ставить себе неохватную задачу, то она просто не решается, и всё. Я думаю, что результатом, дальнейшим действием должен стать целый веер различных документов, которые будут адресовать различные аспекты, в том числе аспекты безопасности, в том числе аспекты картографические какие-то, аспекты информации на ее различных стадиях и так далее, много других аспектов, которые здесь не адресованы.

Кстати, хочу поблагодарить за то, что Вы обратили внимание на определение информационного пространства. Действительно, слово "компьютерный" здесь отсутствует. Явно методологическая ошибка. Я, кстати, тоже, когда смотрела определение, заметила, что в определении кибербезопасности заявлена совокупность условий, при которой составляющие киберпространства защищены от любой угрозы. И мне это, как специалисту по информационной безопасности, просто режет глаз, потому что защиты от любой угрозы не существует. То есть мы никогда не сможем достичь вот этого состояния в принципе, поэтому я бы здесь все-таки предложила: "от максимально возможного в данном контексте числа угроз" или как-то так. То есть защиты от любой угрозы... просто как горизонт, к которому мы будем вечно приближаться и никогда не приблизимся.

Еще, если позволите, я бы хотела одно слово, может быть, или пару слов сказать Ирине Аркадьевне по поводу уровня выпускников

и качества стандартов. Просто нас эта тема очень волнует. Мы являемся непосредственно работодателями, которые нанимают тех самых выпускников, которых вы готовите. Я бы хотела очень попросить Министерство образования и науки, Вас в его лице как-то стараться не стремиться к тому, чтобы затачивать выпускников под узкую задачу. Нас вполне устраивает необходимость учить выпускников по полгода, мы к этому готовы. Мы знаем, что их всё равно придется переучивать. И почему я об этом прошу? Гораздо важнее дать людям некие базовые знания. То есть советское образование было хорошо чем? Оно давало человеку широкие, хорошие базовые знания, с которыми он выходил и мог работать хоть в области ядерной энергетики, хоть в области, не знаю, построения самолетов, хоть чего-то еще. И всё равно год уходил на то, чтобы этого специалиста как-то "докрутить" или довести до кондиции в той области, в которой он работал. Это неизбежная часть.

Если мы будем выпускать узких специалистов, то в условиях чрезвычайно быстрого изменения технологий и развития мы будем получать людей вчерашнего дня. И это самый большой риск, потому что система образования чрезвычайно медленная: пока она адаптируется, пока мы создадим стандарты, пока эти стандарты внедрятся, пока они разработаются... Если этот стандарт будет очень точно заточен под конкретную задачу, то эта задача будет устаревать до того, как стандарт будет принят.

Поэтому если у нас будут специалисты просто хорошие широкого профиля, которые будут получать хорошее базовое математическое образование, этого будет вполне достаточно для того, чтобы потом из этих специалистов сделать нормальных уже, заточенных под задачи специалистов или их переквалифицировать,

например. Это такое пожелание, я очень надеюсь, что мой голос будет услышан. Спасибо большое.

С МЕСТА

Я правильно понимаю, что вам нужны бакалавры? Хорошая базовая подготовка...

Н.И. КАСПЕРСКАЯ

Нам нужны специалисты. Я очень большой противник этого распределения на бакалавров, магистров. Была хорошая система образования в Советском Союзе, у нас лучшие выпускники, мы имеем то преимущество перед западными странами, что у нас очень качественные выпускники. И вместо того, чтобы сохранять эту систему образования, мы пытаемся ее сломать на западный манер, где вообще нет специалистов.

Например, в Германии (мы работаем в Германии) найти IT-специалиста – просто днем с огнем. Они стоят бешеных денег, и они редки, их просто нет. А тот уровень, который нам удается получить, это уровень, я не знаю, хуже среднего студента нашего четвертого курса. Понимаете? Хотелось бы все-таки получать хороших специалистов, которые понимают базовые принципы, имеют базовую основу. Спасибо.

Р.У. ГАТТАРОВ

Спасибо, Наталья Ивановна.

Мурашёв Николай Николаевич. Про стратегию и про карты.

Н.Н. МУРАШЁВ

И навеяли... Если можно, философское.

Р.У. ГАТТАРОВ

Это как всегда.

Н.Н. МУРАШЁВ

Во-первых, хотелось бы отметить следующее, что мы в стенах законодательного органа находимся и, наверное, должны внимательно читать соответствующие законодательные и иные нормативные правовые акты. Поэтому мне хотелось бы сказать, что отнесение сведений, относящихся к картографии, к сведениям, составляющим государственную тайну, в компетенцию ФСБ России не входит. *(Смех в зале.)* Извините.

Уважаемый председатель, уважаемые члены Совета Федерации! В начале своего выступления хотелось бы поблагодарить Совет Федерации за постоянное внимание к вопросам законодательного обеспечения безопасности Российской Федерации.

Информационное право, которое стоит у нас сегодня в повестке дня, является одной из наиболее быстро развивающихся отраслей права. Вместе с тем сам объект права – информация – в большинстве отраслей знания носит так называемый аксиоматический характер, то есть не определяется. В этом отношении это создает достаточно большие сложности для законодателя, эти сложности видны. И конечно, хотелось бы приветствовать наличие такого большого количества специалистов на этой площадке, что поможет, видимо, решить те сложности, которые будут возникать в этой области.

Информация в качестве объекта права обладает фактически уникальными свойствами, принципиально выделяющими ее среди других объектов права и в первую очередь обособляющими ее от объектов вещных прав. Она не является вещью, она не овеществлена фактически. У нее есть такие свойства, как возможность произвольного распространения, нахождения в любом объеме в нескольких местах, одновременного использования любым количеством объектов; самостоятельность информации как объекта

(то есть отсутствие зависимости ее характеристик, объема, семантической полноты, ценности от среды, в которой информация находится, и от носителя, на котором она зафиксирована); отсутствие зависимости между объемом информации и процессами, которые начинают проистекать благодаря ее воздействию (это особенно относится к небезызвестным компьютерным вирусам, где модуль совершенно маленького объема может вызвать катастрофические последствия). Данные свойства информации предопределяют конструирование в праве систем ограничения на доступ и распространение сведений, это институт тайн, установление особых механизмов признания авторства по отношению к информации, получение вознаграждения за ее использование иными субъектами – институт авторского и патентного права и ряд других институтов права.

Поэтому, как я еще раз сказал, очень интересно бывает на площадке, где большое количество специалистов (специалистов технических, специалистов в области права, специалистов в других областях знания) объединяются в единое целое, что, на мой взгляд, должно помочь нам успешно реализовать те проблемы, которые перед нами ставят всё более и более ускоряющиеся темпы развития информационно-коммуникационных технологий.

Что касается обсуждаемого документа, во-первых, хотелось бы понять его характер и как бы определить его место среди других документов. К сожалению, в процессе обсуждения не упоминался один из основных документов – это Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 года.

Если мы обратимся к этому документу, то по идее концепция документа, которая сейчас представлена, должна быть отнесена к так

называемым документам стратегического планирования. Я напомню, что к числу таких документов относится Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, там в статье 101 приведен полный перечень этих документов, и дальше я просто читаю выдержку из него: "Концепции, доктрины и основы (основные направления) государственной политики в сферах обеспечения национальной безопасности и по отдельным направлениям внутренней и внешней политики".

Если мы признаем тот факт, что по идее предполагаемый документ относится именно к документам стратегического планирования, то в разделе пятом Стратегии национальной безопасности определен фактически порядок их подготовки, а также то, что они должны включать. Но если мы это признаем, мы должны третий раздел из стратегии – место стратегии в системе действующего законодательства – просто-напросто исключить, потому что документы стратегического планирования, как известно, не являются ни нормативными документами, ни правовыми, ни законодательными актами.

Поэтому если мы говорим, что это этот документ, но по целям и задачам он больше всего именно напоминает документ стратегического планирования, ну, наверное, его таковым и надо рассматривать, но приведя, как я уже сказал, его положения в соответствие с имеющейся Стратегией национальной безопасности.

Второй существенный момент, который здесь был поднят, – это терминология и как бы область, рассматриваемая в данном документе. Дело в том, что действительно термины, которые в нем введены, они являются новыми. Ранее, в действующих документах стратегического планирования, они как бы не употреблялись. Они

не употребляются в Стратегии национальной безопасности. Ну и, кстати, тогда название: скорее всего, всё же не стратегия, потому что стратегии там соответствующие определены, может быть, основные направления государственной политики, может быть, концепция, ну, там много названий. Но при этом сам документ надо соотнести с уже принятыми, видимо, документами и с теми документами, которые готовятся к принятию.

В первую очередь я бы к этим документам отнес Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. В этом документе введено понятие "критическая информационная инфраструктура", и фактически он представляет собой основные направления обеспечения безопасности критической информационной инфраструктуры. Документ 3 февраля 2012 года Президентом Российской Федерации утвержден, действует. Есть соответствующие планы его реализации, они успешно реализуются. Поэтому если мы будем в дальнейшем продолжать работу над рассматриваемым документом, наверное, всё же критическую информационную инфраструктуру из него как бы надо извлечь, либо инкапсулировать его в существующий документ, либо в основные направления... но это уже как бы авторам.

Второе – вернуться всё же к определениям. Авторы используют термин "кибербезопасность". Я согласен с тем, что он крайне неудачно определен, потому что действительно от всех угроз защититься никогда нельзя, и тут, видимо, надо говорить о каких-то минимизациях ущерба, ну, и действительно почитать существующие документы.

Что касается международной жизни, то у нас есть основные направления государственной политики в области обеспечения международной информационной безопасности, утвержденные Президентом Российской Федерации 3 июля этого года, которые определяют внешнеполитическую деятельность государства, общества в этой области. И, видимо, действительно будущий документ (как-то он будет называться, наверное) должен соотнести то, что в нем написано, с этими основными направлениями, а, может быть, иметь отсылочную норму о том, что они таким образом определены.

С моей точки зрения, очень важным документом являются готовящиеся в настоящий момент третьи основные направления. Это основные направления в области обеспечения культуры информационной безопасности, которые находятся сейчас на стадии, так сказать, уже обсуждения и выхода. Я думаю, что этот документ в ближайшее время будет принят в установленном порядке. Поэтому, конечно, нужно соразмериться и с ним, наверное, и соответствующие формулировки, которые есть в проекте концепции, документе, который мы рассматриваем, наверное, должны быть, видимо, подкорректированы.

Ну и теперь перейдем к терминам всё же. Вот я внимательно прочитал документ, и я не понял, зачем вводить новые термины. У нас, в первую очередь, в ШОСовских документах, в международных договорах Российской Федерации зафиксированы термины "информационная инфраструктура", "информационный ресурс". Они вполне подходят, на мой взгляд, к тому объекту применимости, который рассматривается в концепции документа, который мы сегодня рассматриваем. Поэтому я думаю, что... Более того, внесение каких-то дополнительных терминов, оно будет затуманивать процесс.

А те термины, как я уже сказал, даже в международных договорах Российской Федерации используются. Они уже обкатаны, включая международную арену. Поэтому я думаю, что если авторы концепции еще раз посмотрят на существующую терминологическую базу, то они смогут найти для себя там достаточно большое количество уже введенных и апробированных терминов, которые позволили бы достаточно точно описать ту предметную базу, в рамках которой они собираются строить свои планы и стратегии. Это еще один вопрос.

И я бы привлек внимание еще к одному моменту. На мой взгляд, это вопрос действительно такой дискуссионный, и, возможно, дискуссионный на этой площадке, но в совместном заявлении президентов Соединенных Штатов Америки и Российской Федерации в Лох-Эрне употребляется термин, который устраивает в настоящий момент, на мой взгляд, всех, – это безопасность использования информационно-коммуникационных технологий и безопасность самих технологий.

Поэтому, может быть, с точки зрения этих последних документов, носящих такой принципиальный характер, имеет смысл еще раз взглянуть на концепцию стратегии. Я думаю, что она может и поменять свое название. Как сказали, документ этот рабочий. И тогда, я думаю, те сложности, о которых в выступлении господина Колесникова говорилось, его встраивание в существующую систему документов стратегического планирования и других документов, уже нормативно-правового и законодательного регулирования, будет значительно более упрощенным, он будет как бы гармонизирован со всем тем, что есть.

Я хотел бы еще последнюю справку дать по поводу международных стандартов. 90 процентов международных стандартов,

касающихся информационной безопасности, действуют в Российской Федерации в качестве национальных. И сейчас не понятно: 95 – о каких стандартах идет речь, которые необходимо развивать? Практически основная масса стандартов ISO нами принята, гармонизирована с российским законодательством. Я бы тоже обратил ваше внимание на это.

Р.У. ГАТТАРОВ

Спасибо большое, Николай Николаевич, за очень хорошую проработку документа, за абсолютно разумные замечания. И вообще с 8-м Центром у нас в последнее время очень активное взаимодействие по части изменений в закон № 152. Еще раз руководителю наш привет и спасибо.

Раевский Алексей Викторович, председатель отраслевого отделения по информационной безопасности ООО "Деловая Россия".

А.В. РАЕВСКИЙ

Добрый день, уважаемые коллеги! Во-первых, я от лица экспертного сообщества хотел бы поприветствовать создание этой концепции и выразить благодарность всем создателям и участникам, поскольку киберпространство сейчас уже вторгается в нашу жизнь всё сильнее и сильнее. Для некоторых оно даже полностью заменило реальное пространство. Поэтому безопасность киберпространства – это сегодня очень важный вопрос.

Но что касается самой концепции, на наш взгляд, в ней упущена, не знаю, сознательно или нет, одна тема – это кибербезопасность компаний (здесь речь не идет о тех компаниях, которые поддерживают критическую инфраструктуру, жизненно важную для функционирования государства и общества), обычных частных компаний.

Почему важно говорить об их кибербезопасности? Дело в том, что их убытки – это убытки, связанные с киберинцидентами, это снижение налоговых поступлений в бюджет, это уменьшение их капитализации, в конечном счете это ухудшение экономической ситуации в стране.

Во-вторых, нельзя забывать про промышленный шпионаж. Дело в том, что есть компании, даже частные, которые занимаются разработкой различных высокотехнологичных решений, и другие компании из других стран, которые могут каким-то образом украсть или получить доступ к их разработкам. Таким образом, ухудшается конкурентоспособность компаний на международном рынке. И тоже этот вопрос, на наш взгляд, достоин включения в концепцию.

В поддержку этого я хотел бы сказать, привести пример других стран. Например, в США в 1977 году была принята директива президента Рейгана, которая вводит концепцию национальной безопасности, и в ней говорится о важности защиты несекретной важной информации как части национальной безопасности. И сюда же относится, на наш взгляд, внутренняя безопасность компаний. Естественно, здесь не идет речь о том, что надо кого-то заставлять что-то делать, но обратить на это внимание, включить это в концепцию, на наш взгляд, было бы нелишним.

И еще хотелось бы сказать, что в рамках данной стратегии будет очень логичным смотреться создание некоего ситуационного центра по кибербезопасности, который аккумулировал бы информацию о текущем состоянии угроз, рассылал бы какие-то "алерты" подписчикам любым – и частным лицам, и компаниям, и государственным организациям, тем, кто за это отвечает, выступал бы неким центром по координации в данной области и с правоохранительными органами, и участвовал бы в

информационном обеспечении, и занимался бы образовательными вопросами. Вот это, на наш взгляд, было бы крайне нелишним.

Р.У. ГАТТАРОВ

Спасибо, Алексей Викторович. Начну с окончания Вашего выступления. Мне кажется, центральное место в стратегии уделено последнему вопросу. Что касается начала, того, что недостаточно внимания уделено обычному бизнесу, а не информационному бизнесу и бизнесу безопасности, я думаю, что теперь Вы знаете дорогу к нам, и мы с удовольствием Вас включили в рабочую группу, чтобы те мысли, которые у Вас есть, помогли нам. Спасибо большое.

У нас еще одно выступление. Сергей Евгеньевич Рыбаков, член Совета Федерации.

Пожалуйста.

С.Е. РЫБАКОВ

Спасибо большое за предоставленное слово, Руслан Усманович.

Я бы хотел сказать несколько слов, поскольку, как говорится, помянешь черта, он и появится: я и есть тот самый доктор философских наук, к которому Арнольд Кириллович апеллировал. Но помимо того, что я доктор философских наук, занимался еще кое-чем в жизни. Поэтому хотел бы начать не с философии все-таки.

Понимаете, я на самом деле кое в чем не соглашусь с предыдущими выступающими – в том, что, на мой взгляд, актуальность этого документа, она очень велика. Можно долго спорить о самом термине. Кстати, я тоже на нем спотыкаюсь, если честно, вот я сам лично. Но я очень часто, работая в различных местах, выполняя различные задачи, всё время сталкивался с проблемой смешения технических аспектов информационной безопасности и вот того, что здесь было вскользь названо, –

гуманитарными аспектами. Но я бы, скорее, назвал – о проблемах контента (да?) в плане безопасности. Потому что на самом деле это совершенно разная, вообще, работа и совершенно разная деятельность. Абсолютно. А нормативные акты не всегда это учитывают, и очень часто даже органы определенные или какие-то структуры занимаются параллельно и тем, и тем.

Вспомнить даже проблемы Роскомнадзора сейчас. Это просто очевидная тема. Даже в практической работе с этим органом очевидно, что те люди, которые, грубо говоря, технари по образованию и по своему менталитету, не очень понимают, что делать с контентом.

Поэтому, наверное, задача выделения в отдельную сферу именно технических аспектов безопасности или, наоборот, выделения контентных аспектов безопасности в отдельную сферу и отделения от технических аспектов безопасности, на мой взгляд, очень важна. Разработчики этого документа взялись за очень благое, нужное дело, как мне кажется.

Если же говорить, скажем, о конкретном документе, то действительно справедлив целый ряд замечаний. На мой взгляд, это касается и встраиваемости этого документа в общую систему существующих уже документов. Тут есть некоторые проблемы, это справедливо было отмечено. Можно спорить по терминологии, по отдельным каким-то частностям, просто не хотелось бы сейчас заниматься критиканством отдельных статей, потому что это концепция документа, и, наверное, она претерпит еще версию, не только 5.12, но и 6, как мне кажется, потому что кое-что, конечно, стоило бы еще отрегулировать.

Кстати говоря, один из выступающих сказал, что здесь не отмечена проблема безопасности компаний. Я бы с этим

не согласился, потому что здесь в одном месте (уж не знаю, это оговорочка по Фрейду или как это понимать?) написано, что целью стратегии является обеспечение кибербезопасности личности, организаций и государства. Я просто такого сочетания еще никогда не встречал, потому что обычно: личность, общество и государство.

И, например, есть тут такие маленькие нюансы типа того, что "принцип баланса между установлением ответственности за несоблюдение требований кибербезопасности и введением избыточных ограничений". Наверное, тут избыточных ограничений просто быть не должно, поэтому принцип не может быть установлен. Я просто к тому говорю, что, конечно, документ еще должен дорабатываться, и сейчас цепляться за отдельные частности не стоит.

Я бы все-таки еще немного сказал по поводу более принципиальных, идеологических вещей, которые у меня лично вызвали вопросы. Все-таки, если вернуться к философии, наверное, сначала нужно определить предмет разговора. Мне не до конца понятен предмет, вот лично мне, потому что мы всё время... Понимаете, даже, например, формулировка киберпространства написана так: "среда, образованная совокупностью коммуникационных каналов Интернета и других сетей". То есть получается, что во главу угла всё равно как бы подспудно ставится Интернет. Видимо, на это повлиял состав разработчиков.

Я не очень понимаю, как в наше время технически отделить проблему Интернета от, например, телевидения, телефона, радио и так далее. То есть встает вопрос: наш документ затрагивает эти сферы или мы концентрируемся только на том (кстати, есть такой термин, он, может быть, не очень распространен – "компьютерная безопасность"), что занимаемся собственно компьютерной безопасностью и на этом ставим точку? Это важно понять на самом

деле нам всем. Потому что любой пользователь мобильного телефона одновременно является пользователем Интернета. То есть как это разделить, вообще? А как разделить цифровое телевидение, которое сейчас поставляется именно по каналам Интернета?

Я понимаю, может быть, это такие тоже дилетантские вопросы, но когда мы говорим не о какой-то технической инструкции, а говорим о законодательном акте, это очень важно.

Опять же есть некоторое непонимание у меня лично, после прочтения документа, какое место в нем уделяется, например, собственно программным методам защиты, а какое техническим, грубо говоря, железу. Это ведь тоже важно, чтобы не было определенного перекоса.

Поэтому ряд этих вопросов остается, и, может быть, из-за этого постоянно продуцируется вопрос: что же такое кибербезопасность и правомерен ли этот термин? Может быть, я ошибаюсь, Руслан Усманович, мне просто хотелось бы озвучить этот тезис как вопрос: может быть, стоит как-то расширить круг разработчиков и участников этого процесса, в том числе все-таки, может быть, более по-доброму привлекать в этот круг в том числе оппонентов, которые совершенно не приемлют каких-то отдельных положений, я так понимаю, в том числе из некоторых государственных органов, чтобы понять их позицию, понять, на чем она основана?

На мой взгляд, еще раз повторю этот тезис, сам подход к созданию этого документа требует какого-то содержательного расширения. На мой взгляд, вот так. Я еще раз повторяю, что я выражаюсь несколько абстрактно и, может быть, не совсем четко, но я понимаю, что это концепция, и мы ее всего лишь обсуждаем.

Р.У. ГАТТАРОВ

Спасибо большое, Сергей Евгеньевич. Очень интересные мысли.

Что касается Интернета, то нельзя сейчас Интернет и другие сети отделять от телефона, от радио, от телевидения, так или иначе всё будет там. То есть это будет единая цепь, это из концептуального, то есть это всё – одно. Так или иначе если взломают сеть, если взломают систему, то и по телевизору покажут то, что захотят.

С.Е. РЫБАКОВ

Руслан Усманович, извините, так я именно об этом и говорю. Но дело в том, что при чтении документа и проникновении в его смысл это не просматривается, не до конца.

Р.У. ГАТТАРОВ

Хорошо.

Что касается... Мы ни от кого не закрывались. Для государственных органов двери всегда открыты, они всегда могли прийти, правда, не всегда это делали. Кстати, ФСБ приходила на каждое совещание, их представители были на каждом совещании. Они не всегда участвуют, точнее, никогда не участвуют в дискуссии, мы потом с ними отдельно проводим...

Н.Н. МУРАШЁВ

Нет, но я-то участвовал.

Р.У. ГАТТАРОВ

Да, кроме сегодняшнего... Но они всегда рядом с нами. *(Оживление в зале.)* Мы общаемся и обсуждаем обсуждаемое.

Безусловно, считаем, что на данном этапе важно перейти к более четкому определению терминов. Мы принципиально уходили от этого, потому что мы бы этот год потратили только на то, чтобы обсудить термины. Наверное, отчасти это неправильно, с научной точки зрения особенно. Сначала надо с терминологией определиться,

а потом идти дальше. Мы немного, в общем определились с терминологией и пошли дальше. Но сейчас пришло время (и я с вами согласен) более четко определить круг тех терминов, которыми мы пользуемся, и очень четко.

У меня просьба к коллегам... Мы уже работаем 1 час 50 минут. У нас есть еще один записавшийся, который подытожит...

Пожалуйста, в очень коротком формате, одна минута.

И.А. БУХШТАБ

Добрый день! Игорь Бухштаб, директор компании "Линукс-Союз". Я просто хотел товарищу Рыбакову дать краткое пояснение, чтобы стало понятнее, почему использовался именно термин "кибербезопасность".

Понимаете, в чем дело? На сегодняшний день, когда мы говорим про киберугрозы, это не только зона Интернета, телевидения, связи и так далее. Проникновение этих киборгов в нашу жизнь практически повсеместно. Они присутствуют в бытовой технике, в автомобилях и так далее. И, собственно говоря, когда мы говорим о кибербезопасности, мы говорим о том, что сегодня человечество, во всяком случае цивилизованная часть человечества, уже не может существовать без этих вспомогательных средств и средств коммуникации, и вещи начинают общаться с вещами в отсутствие человека и даже в отсутствие того же самого Интернета, потому что есть другие, альтернативные каналы передачи информации, и, соответственно, возникают какие-то дополнительные угрозы – остановка какого-то технологического процесса и так далее.

Поэтому в этом смысле, может быть, мы с точки зрения философской или лингвистической не очень правы, но с точки зрения понимания общечеловеческого смысла этого... мы именно к

этому и шли. Поэтому мы ушли от терминологии "информационная безопасность", "государственная безопасность". Мы расширили зону обсуждения: не только бизнес, не только государство, мы перешли к личности. Это и есть та основа, от которой мы хотели оттолкнуться. Да, базовых, фундаментальных знаний, там, специализированных у нас, наверное, нет, но для этого и есть эта рабочая группа, на заседаниях которой мы можем всё это обсуждать. Спасибо.

Р.У. ГАТТАРОВ

Спасибо.

У нас слушания, а не дебаты. Дебаты, кстати, можно будет как-нибудь провести. Пригласить научное сообщество, географов, академию наук, а с другой стороны – мы с вами про "железки" поговорим.

С.Е. РЫБАКОВ

Руслан Усманович, кстати, про географов что-то уж как-то слишком иронично всё это получилось, а проблема ведь архиважная. Это просто чудовищная проблема, если честно. Арнольд Кириллович абсолютно правильно ее поднял.

А я уж в качестве реплики в ответ просто... Вы поймите меня правильно.

Во-первых, я начал с того, что потребность в документе очевидна. Это раз. Точка. То есть сама потребность в нем видна, и, наверное, за ту работу, которая проведена, можно просто низкий поклон сделать, потому что действительно это то, что сейчас нужно, о чем я и сказал вначале.

Во-вторых, на чем бы я хотел сакцентироваться? Извините, пожалуйста, но не надо мне рассказывать про суть вопроса, я ее понимаю. Мы сейчас обсуждаем бумагу. Вот я высказался по тому, что, глядя на бумагу, я вижу, что многие вопросы не отражены,

которые наверняка разработчики имели в голове, но там их нет. И я подспудно всё время вижу, что авторы, писавшие этот документ, скорее всего, работали именно в области, где работает бóльшая часть (уважаемая Наталья Ивановна, да?..), и свои профессиональные навыки, свои профессиональные подходы большей частью они отразили, а надо бы туда добавить еще нечто.

Извините, пожалуйста, Руслан Усманович.

Р.У. ГАТТАРОВ

Сергей Евгеньевич, так как Вы имеете большой опыт в этой работе, теперь Вы здесь у нас, в Совете Федерации, мы Вас приглашаем принять активное участие в этой работе. Я думаю, что Вы нам как раз поможете с Вашим опытом сделать то, о чем говорили несколько раз Николай Николаевич, Андрей Вячеславович, – найти нашему труду место в системе государственных документов. Мне кажется, это очень важно.

Коллеги, у кого-то еще есть принципиальные?..

Да, пожалуйста.

Александр Алексеевич Чекалин. Его все знают.

А.А. ЧЕКАЛИН

Коллеги, в российском уголовном и административном законодательстве ряд составов правонарушений признаются таковыми и имеют квалифицирующий признак, если сведения, информация, причинившая вред физическим и юридическим лицам, была размещена, обращаю внимание, в средствах массовой информации. Это клевета, оскорбление, разглашение гостайны, инсайдерская информация, отдельные виды мошенничества, пропаганда экстремизма, терроризма и так далее.

Однако при юридической квалификации этих составов возникает проблема. По российскому законодательству газеты, радио,

телевидение – это средства массовой информации, а Интернет – на усмотрение правоприменителя, чаще – нет. Это проблема международная. Единичные государства предпринимают попытки признать Интернет средством массовой информации для последующей правовой квалификации вреда, причиненного с помощью Интернета, поэтому предложение такое: может быть, предусмотреть в концепции начало работы по международному правовому признанию Интернета средством массовой информации с соответствующими правовыми последствиями. Спасибо.

Р.У. ГАТТАРОВ

Спасибо большое.

Александр Анатольевич, Вы как раз от граждан.

А.А. АЙГИСТОВ

Уважаемые коллеги, общие слова не приветствуются за пять минут до конца совещания. Я сейчас выступлю не от Российского Агентства развития информационного общества, а больше, наверное, от Общероссийского совета некоммерческих организаций, который я возглавляю, и от делегатов IV Съезда некоммерческих организаций, который в октябре – ноябре прошел в Москве при поддержке Временной комиссии Совета Федерации по развитию информационного общества.

Во-первых, я хочу сказать буквально два слова про то, как обсуждали эту концепцию, и наши представители тоже в этом участвовали. Хочу искренне поблагодарить и еще раз удивиться мастерству ведения наших экспертных совещаний, потому что это была довольно сложная полемика, и у нее был такой поступательный прогрессивный характер при обсуждении документов. Это довольно сложно сделать. Почему? Потому что каждый раз приходили новые эксперты, и они, пропуская пять различных этапов, начинали всё

заново. И нужно было иметь особое мастерство – людей успокоить, объяснить за короткий промежуток времени, допустим, к чему мы уже пришли. Я считаю, что это нужно особенно отметить.

И теперь о съезде. Съезд шел четыре дня, и мы на третий день съезда, который был посвящен как раз информационным технологиям (он так и назывался "Инфо = общество 2013"), применению информационных технологий и развитию электронной демократии, некоммерческому сектору страны, – мы в этот день обсуждали вот эти вопросы концепции стратегии кибербезопасности Российской Федерации.

И наши делегаты очень активно восприняли эту тематику, инициировали на следующий год мастер-класс по информационной безопасности, по кибербезопасности обязательно. И в проект резолюции съезда (она еще не готова) сочли нужным записать следующие вещи. Я очень кратко о них скажу, не буду полностью.

Было отмечено делегатами, что существующее сегодня государственное регулирование сферы кибербезопасности написано в основном государством и для государства, а вот бизнес и гражданское общество на программном уровне в процесс обеспечения кибербезопасности сегодня не включены. Хорошо, что эта ситуация исправляется.

Следующий пункт. Мы понимаем, что Россия сейчас уже лидирует, занимает первое место в Европе по количеству интернет-пользователей, и эта цифра еще растет. Нам говорят, что к 2014 году, возможно, эта цифра будет 80 миллионов (даже западные эксперты). И соблюдение прав этих пользователей в информационном обществе должно гарантироваться, тем более мы знаем, что сейчас всё большее количество коммуникаций осуществляется именно в

цифровом виде. Эта задача достаточно масштабная и требует таких масштабных мер, которые мы описали в этой концепции.

И последнее, что хотелось бы сказать, – что здесь, конечно же, решая эти вопросы, не всё может сделать государство. Сеть у нас (и российский ее сегмент) – это сеть общественная. Поэтому обязательно нужно включать гражданское общество в обеспечение кибербезопасности. И нужно вооружить наше гражданское общество знаниями в этой области, рассказать о способах защиты, дать определенные механизмы обращения за помощью в случае каких-то инцидентов.

И самое последнее. На заседании бюро президиума было решено создать комиссию по вопросам национальной безопасности при Общероссийском совете некоммерческих организаций. И члены комиссии с удовольствием бы работали дальше по созданию стратегии.

В связи с этим предложение последнее. В пункт 8 концепции, где как раз идет речь о рабочей группе, о ее составе, включить представителей общественных организаций и этих структур. Это там, к сожалению, упустили, просто выпало.

И последнее скажу, что у нас 17 декабря в Центральном Доме журналиста в 14 часов будет большая пресс-конференция "Информационное общество в России. Итоги года", и один из вопросов, а всего шесть будет обсуждаться на этой конференции, посвящен как раз концепции стратегии кибербезопасности. Пресс-конференция будет проходить, естественно, при поддержке Временной комиссии, вы там в списке. Спасибо большое.

Р.У. ГАТТАРОВ

Спасибо, Александр Анатольевич.

Уважаемые коллеги, завершаем прямо минута в минуту. Спасибо всем огромное за конструктивную работу. Я считаю, что прозвучало достаточно аргументов к тому, что мы все-таки продолжаем работу. Мы делаем нужное, необходимое дело. Понятно, что не ошибается тот, кто ничего не делает, и это мы тоже отмечаем. И будем работать над ошибками все вместе. Появился еще один двигатель у этого процесса: Сергей Евгеньевич дал согласие включиться. Николай Николаевич, я думаю, тоже сейчас будет более активное принимать участие в нашей работе. И я думаю, что мы сможем в ближайшее время сделать этот документ абсолютно готовым для того, чтобы он нашел достойное место в том пакете государственных документов, которые регулируют безопасность в той среде, которую мы хотим отрегулировать.

Еще раз, всем спасибо большое. Я думаю, что это не последние слушания по этому вопросу.

_____