С Т Е Н О Г Р А М М А

совещания Комитета Совета Федерации по науке, образованию, культуре и информационной политике на тему "О разработке стратегии национальной кибербезопасности Российской Федерации: состояние, предпосылки, механизмы и перспективы"

26 февраля 2013 года

Р.У. ГАТТАРОВ

Уважаемые коллеги, мы начинаем наше рабочее совещание по вопросу, который уже активно вошел в дискурс как в обществе, так и в госструктурах. У нас здесь присутствует большое количество журналистов, которым интересна эта тема. Я говорю о кибербезопасности, кибербезопасности нашей страны. И это действительно сейчас одна из тем, которая волнует как граждан, представителей средств массовой информации, так и экспертное сообщество.

Что хотелось бы отметить? Мы, наверное, полгода, как начали этим вопросом заниматься. Поначалу слово "кибербезопасность" считалось практически ругательным. И до сих пор мы еще спорим, что это кибербезопасность или информационная безопасность. Но, на мой взгляд, что все, что связано с кибербезопасностью, касается в первую очередь технических вещей, а все, что связано с информационной безопасностью, это уже включает в себя и кибербезопасность, и так называемую безопасность, связанную с контентом. Поэтому мне кажется, что эти два понятия абсолютно не коррелируются. Они, конечно, пересекаются, но мы говорим именно о кибербезопасности.

Вашему вниманию мы предложили некий набросок стратегии, которую сделала наша некая экспертная группа. Это уже второй набросок. Первый набросок мы здесь, собравшись, признали не очень отражающим те подходы, которые сами же обозначали. Я хочу отметить, что этот документ отличается от первого в первую очередь тем, что он не является слишком техническим. То есть там мы пытались задать некие стандарты. Там мы говорили о каких-то вещах, связанных именно с техническими вещами. То здесь мы в первую очередь говорим… этот документ получился более рекомендательным, политическим, если хотите.

И главная задача, во всяком случае, о которой я постоянно говорю, с которой согласна часть наших экспертов, цель стратегии – это обозначение приоритета государства к безопасности в киберсреде. Это политический документ, который должен быть понятен как любому гражданину, который увидит себя там, увидит, как он должен защищаться, что он должен делать при той или иной ситуации, куда он должен обратиться, также и увидит бизнес, как он сможет отражать те атаки на его бизнес, чем поможет ему государство, как координироваться будет эта работа, также и ведомства, которые получат четкие инструкции по тому, какой персонал они должны набирать, как их информационные системы должны соответствовать тем или иным стандарта безопасности.

Вот мы примерно, то, что сейчас у вас лежит на столе, в моем понимании уже очень похоже на то, что можно взять за основу. Еще раз повторю, очень похоже на то, что можно взять за основу.

Когда мы договоримся, что это можно взять за основу, тогда мы это будем вывешивать в свободный доступ, и уже совместно с более широким кругом экспертов, представителями граждан, любой человек, который считает, что он что-то понимает в кибер- или информационной безопасности, может поучаствовать потом в нашей работе.

Вот такое вступление я бы сделал для нашего мероприятия. А слово для основного доклада передаю Александру Шепилову. Он как раз более подробно расскажет о том, в чем же нововведения. Пожалуйста.

А.О. ШЕПИЛОВ

Да, коллеги, я представлю вам документ. Он рассылался заранее членам рабочей группы, есть в раздаточном материале. И тем не менее я хотел бы чуть более подробно остановиться на некоторых деталях. Хочу подчеркнуть, что мы, готовя данный документ, выступали в первую очередь интеграторами тех предложений, которые поступили от разных членов рабочей группы. Напомню, что эта рабочая группа при Временной комиссии Совета Федерации по развитию информационного общества, но мы после того, когда поняли, что там тема даже еще более актуальна, чем мы предполагали, мы приняли решение выделить именно такую рабочую группу, куда вошли те эксперты, кто посчитал необходимым.

Соответственно в этом документе, который вам представлен, там есть предложения от… скажем так, учтены предложения от научного сообщества. Мы работаем с Санкт-Петербургским университетом технологий, механики и оптики. Там есть предложения от компании "InfoWatch" – Наталья Ивановна Касперская, там есть предложения от Российской ассоциации электронных коммуникаций, от Ассоциации свободного программного обеспечения и ряда других субъектов.

Единственное, что мы сделали с этими предложениями, это мы постарались привести их к тому виду, о котором договорились на предыдущем совещании в декабре. То есть это вид, который максимально ориентирован на конкретику, на некие конкретные, но в то же время не технические, не технологические, а в первую очередь, условно скажем, политические позиции.

Можно второй слайд. И соответственно мы очень бы хотели, поскольку уже было достаточно много разговоров как на площадке Совета Федерации, так и на разных других площадках, мы хотели бы, если этот документ будет принят за основу именно, как сказал Руслан Усманович, чтобы дальше можно было уже начать обсуждение предметное.

Здесь вам представлена структура стратегии. Она содержит в себе некие стандартные разделы, такие как общие положения, ключевые понятия, цели, принципы и так далее, но отдельно, на что хотелось бы обратить ваше внимание, это фактически весь проект этой стратегии построен на принципе некого такого дерева задач, подзадач и действий. То есть задачи – это более такие глобальные вещи, глобальные ориентиры, которые мы ставим в этом документе. Далее они разбиваются на некие подзадачи и далее следует ряд конкретных действий.

Я бы, наверно, вас просил в большей степени на сегодня при обсуждении сконцентрироваться именно на задачах, потому что то, как мы выберем задачи, а это основные ориентиры, в значительной степени определит содержание документа в целом, потому что в том проекте, который здесь представлен, здесь, безусловно, далеко не полная разбивка задач на подзадачи. И мы, понимая это, намерено не стали добавлять от себя ничего, поскольку хотели бы в большей степени ориентироваться на экспертное мнение.

Действия, которые здесь предложены, они, скажем так, также предложены в большей степени для того, чтобы стать отправной точкой для дискуссий.

С одной стороны, отправной точкой для дискуссии, с другой стороны, неким примером того, как мы считаем правильным, скажем, до какой степени детализации формулировку действий в тексте документа. (Следующий слайд.)

Коллеги, вот я коротко обозначу, хотя они у вас есть в документе, задачи стратегии. Это создание механизмов мониторинга, потенциальных киберугроз и выработки ответов на них. Это содействие формированию культуры информационной безопасности. Это реализация механизмов партнерства государства, бизнеса и гражданского общества в сфере кибербезопаности. Это обеспечение консолидации ведомственных информационных ресурсов. Это повышение надежности критической инфраструктуры кибербезопасности. (Дальше, пожалуйста.)

Это совершенствование нормативной правой базы. Это поддержка отечественных производителей программного обеспечения, ну и, конечно же, в первую очередь, программного обеспечения, связанного с решением вопросов безопасности.

Это повышение компетентности специалистов различных сфер в вопросах кибербезопасности. Здесь речь идет как об узкопрофильных специалистах технических, которых, мы считаем, недостает, так и о специалистах, которые просто в процессе своей каждодневной деятельности тем не менее сталкиваются с киберугрозами. И это, безусловно, международное сотрудничество в сфере кибербезопасности. (Следующий слайд.)

Вот здесь просто в качестве неких выдержек (в тексте документов их больше) – это примеры действий, которые, как мы предполагаем, могли бы войти в этот документ. Это, например, создание ситуационного центра, который функционирует в режиме 24 на 7, и обеспечивает, как мониторинг киберугроз, так и реагирование на них. Это создание портала, содержащего статистическую информацию обо всех инцидентах, о потенциальных уязвимостях в компьютерных системах, о способах нейтрализации этих уязвимостей и параллельно реализующих функционал обратной связи от граждан и организаций, которые столкнулись с какими-то инцидентами.

Это вот такой, может быть, экзотический пункт, но, мне кажется, заслуживающий обсуждения, – это организация национальных учений в области кибербезопасности с участием правоохранительных органов, военных подразделений, государственных органов руководства критически важных объектов.

Это полноценный запуск и широкое использование инфраструктуры электронной цифровой подписи. (Следующий слайд.)

Безусловно, мы считаем важным разработку и принятие государственных стандартов кибербезопасности и реализацию механизмов их регулярного пересмотра и обновления. Это предоставление правоохранительным органам полномочий, которые, возможно, расширят их оперативные возможности по борьбе с киберугрозами.

Это принятие программ развития отечественных программных средств обеспечения кибербезопасности. Это пересмотр квалификационных требований к государственным служащим в области IT. (И следующий слайд.)

Вот, коллеги, и здесь представлено на этом слайде некий альтернативный список задач. Просто мы, когда анализировали различные информационные материалы, которые выходили по поводу кибербезопасности, то вот эти материалы очень часто были вот в такой логике. Мы посчитали необходимым, вам в качестве некого альтернативного списка задач эту логику показать.

То есть здесь, вы видите, что немного другой принцип классификации. Здесь мы говорим о безопасности online-бизнеса, о гарантиях прав граждан в Интернете, о национальной кате-инфраструктуре, о современных системах управления, об эффективных механизмах борьбы с киберпреступлениями и о системе противодействия массированным кибератакам.

Это в каком-то смысле такая более общая постановка задач. И она, наверное, в большеq степени идет от проблем, потому что вот тот вариант, разбивка которого представлена в тексте, он, в каком-то смысле, идет уже о возможных путях решения. Коллеги, у меня все.

Р.У. ГАТТАРОВ

Коллеги, примерно вот так мы видим эту ситуацию, то есть это опять же Александр четко сказал, что по факту нашего творчества в этом нет. Наше творчество было в том, что мы подошли и обработали ваши предложения и положили их в эту структуру.

Вот я уже сказал, что эта структура, это изложение, это понимание вопроса мне лично больше по душе, оно в большей степени понятно. Оно не является там технически очень

сложным, и по которым есть три тысячи одно мнение, по которым нам очень трудно будет договориться.

И вот на данный момент я предлагаю высказаться, высказать свое мнение, как-то отнестись к предложенному документу. И, единственно, у меня просьба – не забывать, и стараться представлять на более-менее понятных, в том числе для журналистов, словах.

Я ни в коем случае не хочу обидеть представителей "четвертой власти", но очень часто, когда мы мероприятия здесь проводим, то я читаю то, что потом выходит, не с точки зрения, цензуры, не с точки зрения всего, но просто очень много вещей напутано. Наверное, это мы так говорим, а не вы так слышите.

Поэтому я, в первую очередь, обращаюсь к нашим экспертам, говорить чуть проще, для того чтобы сегодня уже, там через несколько часов мы прочитали абсолютно понятные, нормальные вещи о нашем мероприятии.

Пожалуйста, кто начнет.

Наталья Ивановна Касперская, пожалуйста.

Н.И. КАСПЕРСКАЯ

Я хочу, во-первых, поблагодарить за документ, который представлен. На мой взгляд, очень неплохой получился документ. Вот я, когда готовилась к сегодняшнему заседанию, прочла. У меня, из всех перечисленных задач (я хочу сказать сначала по задачам)…

Да, прежде чем по задачам, я хочу внести предложение по организации нашего взаимодействия.

Вот Вы, Руслан, сказали по поводу представителей прессы. Я бы предложила, наверное, делать какие-то черновые заседания, где мы обсуждаем, ну, там внутренние какие-то элементы, и делать какие-то чистовые заседания вместе с прессой. Потому что потом читать то, что ты не говорил, не всегда бывает приятно. Потом надо будет отнекиваться: да нет, я не это имел в виду. Это все-таки сложно.

Но у нас сейчас пока вот так по сути хвастаться нечем. Мы только на самой, самой отправной точке находимся, и очень мало чего такого реального есть, что показать. Поэтому на этом уровне – ну чего "нижним бельем" трясти? Давайте, как-то вот разделим. Когда у нас будет, чего показывать, мы пригласим прессу. То есть делать какие-то там… Хотя бы там через заседание или, может быть, даже реже, с приглашением прессы, а всю остальную внутреннюю кухню оставить все-таки для экспертов, чтобы у нас было какое-то, ну, более свободное общение в этом смысле.

По поводу задач я хочу сказать. На мой взгляд, очень разумно сформулированные задачи. Они – с правильной точки зрения. Они, с одной стороны – довольно общие. С другой стороны они идут – ну там вот понимание, как функционирует государство, это хорошо. Потому что, например, вот альтернативные задачи здесь были представлены, задачи типа борьбы вообще со всеми родами киберугроз, она представляется не очень реалистичной. Она хорошая, конечно, но не знаю, как ее можно реалистично реализовывать.

Здесь мне единственная из списка задача, которая мне не очень ясна, – это обеспечение консолидации ведомственных информационных ресурсов. Она как бы не очень лежит в сфере информационной безопасности. И задача эта имеет двоякую реализацию.

Дело в том, что любая консолидация, надо понимать, приводит к увеличению возможных угроз. Это создает некий консолидированный объект, который проще атаковать. Всегда сложнее атаковать разрозненную сеть, разным образом организованную, чем четко описанный однозначно организованный объект.

В этом смысле мне представляется это не совсем понятным, чтобы хотелось здесь видеть. Если мы имеем в виду консолидацию, с точки зрения там информационной безопасности, ну, наверное, это вообще не правильно.

Если мы имеем в виду, что они должны озаботиться информационной безопасностью или построение каких-то принципов для ведомств, — это немножко другая история.

___

Можно я сразу очень коротко откомментирую? Мы здесь немножко… с одной стороны, мы абсолютно принимается то, что Вы говорите, Наталья Ивановна. Но мы-то о чем говорим? У нас государство, например, какое-нибудь ведомство заказывает себе систему документооборота. Вот оно платит деньги, проводит торги, платит там десятки, сотни миллионов рублей, ставит ее, ну, вроде как ее делают, оно вроде как ее ставит; а потом другое ведомство, очень похожее по структуре, точно также создает систему документооборота, точно также торгуется, платит столько же или еще больше за практически подобную работу. Мы говорим о некой, грубо говоря, ты создал государственную систему за деньги налогоплательщиков, ты положи ее в хранилище, где ее может взять как минимум другое ведомство. Вот мы в первую очередь об этом говорим.

Н.И. КАСПЕРСКАЯ

Да. Обеспечение хранилищ — это довольная сложная задача, которая на сегодняшний момент не решена. В этом стоит проблема. Все говорят об облачных технологиях, но первое, что связано с облачными технологиями, что, отдавая свою информацию в облако, ты можешь с ней мысленно распрощаться, потому что эта информация так и улетает в облако, да? Обеспечение безопасности в облаке сейчас — огромная проблема, которая не решена. По этой причине облачные технологии так плохо распространяются.

И дальше мы читаем, когда подзадачу, что минимизировать там число шлюзов, или обеспечить механизмы электронного межведомственного взаимодействия. Но эти подзадачи могут вызвать обратный эффект. То есть, по сути, мы говорим об унификации инфраструктуры. Но это задача, не связанная с безопасностью, это задача связанная, как вы говорите, тот пример, который Вы приводите, — это задача повышения эффективности функционирования госорганов. Безусловно, хорошая задача, отличная. Все отлично. Только какое отношение имеет к безопасности? Понимаете, с точки зрения безопасности консолидация всех госорганов в одном месте — это повышение уязвимости. Давайте мы подумаем все-таки на эту тему. Здесь двойственное у меня чувство этой задачи. Со всем остальным я согласна.

Р.У. ГАТТАРОВ

Пожалуйста.

И.А. БУХШТАБ

Во-первых, хотел, действительно, поблагодарить, потому что работа проделана большая. Да, не представился — Игорь Бухштаб, ЗАО "Линкс".

Вроде как все аспекты, связанные с тематикой сегодняшнего мероприятия, освящены. Есть некоторые маленькие дополнения, которые хотелось бы внести, причем я даже не знаю в какую из подзадач это внести, потому что, в принципе, если мы говорим про кибербезопасность, ну, как таковую, есть еще один вопрос, который просто выпал, называется: "Стандартизация объектов хранения". И это достаточно серьезный вопрос, потому что, собственно говоря, в зависимости от того в каких форматах мы храним информацию, мы либо сможем ее в дальнейшем использовать, либо не сможем, и вот куда это отнести, я, честно говоря, не знаю. Но мне логически кажется, что задача шесть, подзадача "Стандартизация объектов хранения", и может быть, сюда же можно отнести то, о чем говорила госпожа Касперская, — собственно говоря, это "Стандартизация регламентов информационного взаимодействия (межведомственного)". Вот в такой формулировке это, наверное, будет корректно и уместно. Все. Мне больше пока сказать нечего.

Р.У. ГАТТАРОВ

Журналисты просят представляться. Это был у нас Бухштаб Игорь Адольфович, директор ЗАО"Линкс". *(Оживление в зале.)*

Да, пожалуйста.

А.А. ВОРОБЬЕВ

Андрей Воробьев Ru-Center (hosting community). Вот, говорим про задачи. Собственно говоря, к задачам, наверное, придраться трудно, тем более что на первых заседаниях мы договорились, что это будут общие такие цели, какие-то не конкретные вопросы прописаны, потому что все-таки стратегия, документ…

А придраться к отсутствию в общих положениях такого понятия как раскрытие терминов и основных определений. Все дело в том, что мы копья поломали на комиссиях РАЭКа в связи с еще одним законом, который сейчас, закон об Интернете. Но я не знаю, будет ли это закон или это будет свод каких-то поправок.

Но само, то, что уже сегодня существует в законодательстве — то провайдер встречается, то оператор, то как-то еще его называют, то хостинг-провайдер, прописывают, и имеют с виду на самом деле гораздо более широкий круг субъектов, чем те компании, которые только услуги хостинга оказывают.

Вот, единство терминов обязательно должно быть, и хочется как-то еще нам, наверное, коррелировать работу над законом или сводом законов об Интернете.

Р.У. ГАТТАРОВ

Андрей Александрович, у меня сразу. Мы почему? То есть мы — а) мы уходим от технических вещей, потому что там, еще раз говорю, три тысячи и одно мнение. Вот я сколько помню как только уходим в термины, приходят сразу такие умные высоколобые мужчины и начинают такие вещи двигать. А может, мы попросим как раз Ru-Center совместно с РАЕКом сделать нам глоссарий такой…

А.А. ВОРОБЬЕВ

Практически он готов.

Р.У. ГАТТАРОВ

Тогда мы готовы взять его за основу, а дальше уже проработать.

И.Ю. ЛЕВОВА

Давайте тогда уж я, раз речь про проект зашла. Левова Ирина, Российская ассоциация электронных коммуникаций. Спасибо за проделанную работу. К сожалению, мы не смогли принять участие, за что я хотела бы отдельно извиниться. Это было связано с большим количеством отпусков в период вокруг новогодних праздников… Это означает, что дальше мы примем намного более активное участие, и, в частности, комиссия по информационной безопасности, киберпреступности подтвердила желание и возможность заняться этим вопросом более плотно. Что касается стратегии, то со вчерашнего дня, к сожалению, все члены комиссии не смогли дать какого-то определенного ответа в связи с тем, что ночь — это слишком мало.

Однако замечания у нас есть следующее. По поводу определения, действительно, их нужно определять, и, возможно, некоторые из заявленных являются лишними. Ну, это мы отдельно обоснуем и обсудим. А также мы хотели бы отметить, что не хватает, наверное, именно преамбулы и стратегических каких-то абзацев. То есть нужно очень четко объяснить зачем, в общем-то, мы этот документ пишем, какие цели он преследует, и некая классификация наверное киберугроз должна быть дана. Опять-таки готова, вот, как раз стратегический абзац, и такое что-то типа преамбулы взять на себя.

Ну и по поводу международного сотрудничества было бы интересно очень узнать, как вообще к этому документу все-таки относится МИД, и какого рода… как, каким образом эта стратегия соотносится с теми мероприятиями в области информационной безопасности, которыми сейчас занимается Министерство иностранных дел? Собственно, основные замечания все, и мы готовы в какие-то сроки, которые мы согласуем, предоставить замечания уже по тексту.

А.В. ЛУКАЦКИЙ

Алексей Лукацкий. У меня два было замечания. На самом деле я хотел бы Наталье оппонировать по поводу консолидации. Изначально вот эта задача, она ставилась все-таки немного по-другому. Там не было слова "Консолидация", там было "Государственные информационные ресурсы". И идея была вынести отдельную задачу по защите государственных информационных ресурсов. А консолидация здесь не совсем, действительно, она верная.

Минимизация числа шлюзов — задача она всегда спор вызывает: минимизировать, не минимизировать, но учитывая как сегодня госорганы и муниципальные органы подключаются к Интернет, обеспечивают свою безопасность, наверное, минимизировать число и контролировать все потоки, наверное, было бы правильнее, чем отдавать на откуп каждому госоргану и муниципалитету возможность ходить куда угодно, откуда угодно, и делать непонятно что, учитывая, что они все при этом еще подключаются к межведомственному взаимодействию. Именно в этом стояла задача.

И с точки зрения, на мой взгляд, оттуда выпало из задач, собственно, важные вещи, — это включение соответствующих программ обучения в вузы и в школы. *(Оживление в зале.)*

Это было в том варианте, который присылался, но не попало в итоговый. *(Оживление в зале.)* Нет в школах и в вузах этого в разделе культуры точно нет…

М.И. ШУБИНСКИЙ

Можно я скажу?

Р.У. ГАТТАРОВ

Пожалуйста. Представляйтесь.

А.В. ЛУКАЦКИЙ

Это специалист. А школы и вузы это совершенно другие.

М.И. ШУБИНСКИЙ

Шубинский Максим, Общественная программа "Чистый Интернет", Санкт-Петербург. Вообще, поддерживаю полностью по поводу обучения детей. Мы об этом говорили полгода назад. Вообще, ощущение, что немножко не хватает, может быть, подзадачи или задачи отдельной, которая бы звучала как "Содействие формированию систем профилактики киберпреступности", куда бы входило и обучение, так называемой, группы риска возможной — это дети, это пенсионеры, это, может быть, бизнес. Потому что, который… мы говорим, что данная программа направлена на бизнес. Но вот малый бизнес особенно… тоже вполне был группой риска, который является потенциальными жертвами киберпреступлений.

Это могла бы быть задача. И тогда подзадачей было бы как раз создание системы обучения, одной из подзадач, кроме вопросов, связанных с органами, скажем так, классической профилактикой, то, что МВД, допустим, занимается.

И если говорить уже об обучении, то вторая вещь, связанная с повышением квалификации персонала, госчиновников, госслужащих, то, что сейчас очень видно, как только мы начали работы, связанные с защитой информации в государственных

учреждениях, дикий дефицит людей, которые бы понимали, что такое защита информации, киберугрозы в государственных учреждениях, и совсем нет курсов повышения квалификации, ну, условно говоря, для пользователей кибербезопасности. То есть, если как мы говорим, программист и пользователь, для программистов, может быть, курсы есть, для пользователей курсов нет. И повышение квалификации именно пользователей, которые бы знали, к кому обратиться, в каком случае, что нужно делать, вот это в том числе и в госучреждениях очень большой дефицит сейчас. Спасибо.

Ю.В. НИКИТИНА-АТТИЛА

Юлия Никитина-Аттила, компания ЗАО "РОСА", в которую входит в том числе "ПингВин Софтвер", член РОСПО.

У меня по данному документу, с нашей стороны, есть одно замечание относительно задач и целей, хотя можно сказать, что это всё общо описано и всем понятны цели документа, мне хотелось, чтобы здесь, где у нас перечислены принципы, предложить обозначить, что бизнес тоже является субъектом, для которого создается данный документ. Гражданину говорится о государстве.

Дальше в задачах упомянуты все субъекты и государства, и граждане, и бизнес, но тем не менее хотелось, чтобы с самых первых строк было видно, что в интересах бизнеса данная стратегия также будет работать и создается в том числе и в интересах бизнеса.

И еще у меня есть одно предложение, оно касается задачи третьей. Простите, пожалуйста, сейчас скажу, задачи седьмой. Здесь говорится об организации поддержки отечественных производителей программного обеспечения, в том числе свободного программного обеспечения. Я как раз представляю сообщество СПО, и я хотела бы всем здесь присутствующим напомнить, что в принципе для того, чтобы у государства и у граждан в пользовании было разработанное, в том числе российскими производителями, свободное программное обеспечение, сделано уже довольно много. И напомнить историю про национальную программную платформу и Фонд алгоритмов и программ, который практически был подготовлен, но пока что Минкомсвязи не запущен в работу.

Если можно какую-то перекличку с проделанной работой, чтобы мы не побежали заново… Почему, если можно?

Р.У. ГАТТАРОВ

Работа была какая-то проделана, но мне кажется, что мы только в начале пути.

Ю.В. НИКИТИНА-АТТИЛА

Вы знаете, фактически фонд… Так как мы являлись одним из разработчиков, стояли у истоков разработки Фонда алгоритмов и программ, мы…

Р.У. ГАТТАРОВ

Я прошу прощения, но это немножко у нас отдельная тема СПО, мы ее отдельно прорабатываем.

Ю.В. НИКИТИНА-АТТИЛА

Тем не менее одна из задач очень сильно перекликается именно с этим вопросом.

Р.У. ГАТТАРОВ

Да, да. Но здесь Ваши предложения, на мой взгляд, учтены. А то, что Вы сказали, мы проработаем обязательно.

Ю.В. НИКИТИНА-АТТИЛА

Спасибо.

_____

Я просто последнее по поводу Фонда алгоритмов программ. Не столь важен сам по себе Фонд алгоритмов и программ, сколько важен на самом деле процесс стандартизации используемых программных средств и их аттестация, с точки зрения тех же самых киберугроз. И это вопрос, который действительно, наверно, в рамках кибербезопасности есть смысл поддержать. Спасибо.

Р.У. ГАТТАРОВ

Да, пожалуйста, коллега из Санкт-Петербурга.

И.Б. САЕНКО

Саенко Игорь Борисович, Санкт-Петербург, Институт СПИ РАН.

Прежде всего, я хочу сказать… начну со списка альтернативных задач, которые Александр Шепилов нам озвучил. На самом деле прозвучала такая мысль, что мы как бы должны чем-то пожертвовать, наверное. Но это неправильно, или я неправильно понял.

Эти задачи, которые прозвучали альтернативные, они мне представляются чрезвычайно все важными, и просто мы должны найти место в нашей стратегии, куда их надо поставить, потому что на самом деле там другая классификация, но ни в коем случае их опускать и выбрасывать не надо. Ну, например, такая задача, как форенсия, как борьба с киберпреступлениями и так далее. Она должна найти место и даже в той классификации тех задач, которые мы сейчас…

РЕПЛИКА

Их в обязательном порядке…

И.Б. САЕНКО

Да. Но, проглядев нашу версию, это пока еще не видно, но нужно их не потерять.

Дальше я хотел бы сказать относительно того, что в самом начале госпожа Касперская сказала. Задача четвертая относительно (если я не ошибаюсь) консолидации ведомственных информационных ресурсов.

Мне кажется, что здесь, наверно, неправильно поставлен вопрос, что консолидация именно информационных ресурсов. Либо я не понимаю, может быть, консолидация ведомственных средств, моделей, механизмов защиты информации или, скажем, обеспечения кибербезопасности. Вот в этом плане.

РЕПЛИКА

Там говорится о стандартах.

И.Б. САЕНКО

Потому что если мы говорим про чисто информационные ресурсы, то, скажем, … *(неразборчиво)* ведомстве они имеют степень конфиденциальности. Понятно о чем…

Р.У. ГАТТАРОВ

И поэтому никак не могут между собой разговаривать.

И.Б. САЕНКО

И как это реализовывать не понятно. А вот именно те механизмы защиты, которые реализовываются в разных ведомствах, а есть наработки, вот их (это государственная задача) надо как-то пытаться консолидировать.

И дальше я перепрыгну на международное сотрудничество. Дело в том, что наша организация, наш институт ведет достаточно давно уже несколько международных проектов,

и мы связаны напрямую со многими европейскими, американскими, с южноафриканскими организациями, которые занимаются вопросами именно кибербезопасности, борьбы с кибертерроризмом.

Знаете, неоднократно мы проводили два семинара в Санкт-Петербурге в 2010 году и в 2012 году по борьбе с кибертерроризмом, приезжали специалисты из-за рубежа и все они говорят, что борьба, обеспечение кибербезопасности – это, в частности, и борьба с кибертерроризмом. Это у нас где-то тоже вышло это понятие. Но если говорить про кибертерроризм, то тут победа, наша победа может быть только в том случае, если все страны объединят свои усилия. То есть это звучала такой постулат.

Ну, опять в плане каком усилия? Наподобие той консолидации, как мы говорим, консолидировать ведомственные возможности по борьбе. И здесь тоже получается, что Россия должна выступать на международном уровне, чтобы добиться такого объединения специалистов по борьбе с кибертерроризмом, чтобы пользоваться чужими наработками, другими наработками опять же во благо и свое благо, и благо других стран, потому что кибертерроризм – это терроризм, он не имеет национальности и вред приносит всем.

Есть еще замечания такие, наверно, более мелкие, которые в рабочем порядке… Например, первая задача. У меня есть по терминологии… Скажем, я начинаю читать слова: "Создать механизм мониторинга потенциальных киберугроз". Но опять же слово "потенциальных", например, я бы выкинул, потому что киберугрозы потенциально – это, значит, возможно. Но они такие разнообразные и могут быть непредсказуемыми. И если мы будем … *(неразборчиво)* защищаться, а они не предсказуемы, нас потом прихлопнут.

Есть еще такое замечание. Добавить сюда еще одну подзадачу. Это то, что называется упреждающее управление безопасностью или проактивное управление безопасностью. Это в рамках подзадач первой задачи.

Р.У. ГАТТАРОВ

Я прошу оформить это всё членам…

И.Б. САЕНКО

Это в рабочем порядке, не буду ваше время занимать.

Р.У. ГАТТАРОВ

Спасибо.

Уважаемые коллеги, я попрошу, в связи с тем, что у нас уже не только Наталья Ивановна высказалась, а еще несколько коллег мне отписались и сказали, давайте, чтобы отдельно в следующий раз нам не собираться, попросим… То есть, так или иначе, у нас уже все, кто хотел высказаться в публичной части, высказались.

У меня просьба к журналистам. Если будут какие-то вопросы, мы отдельно готовы выйти и их прокомментировать. А сейчас мы бы уже в закрытом режиме продолжили про некие технические вещи, о которых мы говорим.

Спасибо вам большое. Мы тогда через Пресс-службу или звоните мне, мы все комментарии уже дадим. Спасибо.

Уважаемый, извините, пожалуйста, а можно вернуть документ? Спасибо. Рабочая версия пока.

РЕПЛИКА

Теперь еще больше будет тайн…

Р.У. ГАТТАРОВ

Коллеги, если честно, то я подразумевал, что у нас будет закрытое совещание. В связи с тем, что совещание еще в рамках работы комитета, оно попало у нас в анонс общий.

И когда мне сегодня сказали, что будут журналисты, я попросил их не пускать. Но когда сказали, что их много и это будет неправильно, вот пришлось их все-таки пустить. И не исходя из того, что мы что-то секретное делаем, а ровно из того, что вот я сказал и Наталья Ивановна сказала, что потом получается, что какие-то вещи технические, два слова переставили, а для них смысл сохраняется, а для экспертного сообщества, там все говорят: дураки какие-то сидят, какую-то фигню обсуждают. Вот ровно из этого.

Теперь у нас закрытый режим. Пожалуйста, сейчас по существу.

РЕПЛИКА

На самом деле документ плохой. *(Смех в зале.)*

Р.У. ГАТТАРОВ

По существу. Светлана Васильевна, Вы что-то хотели.

С.В. КОНОВЧЕНКО

Спасибо. Я хотела бы несколько слов сказать по существу документа. Первое, пойдем сначала по документу. Конечно, хотелось бы поблагодарить тех, кто работал над этим документом. И будем надеяться, что работа будет продолжаться. Но ждем сайта, ждем, когда документ выйдет в краутсорсинг, когда к его обсуждению присоединится как можно больше людей. Хотя для того, чтобы его обсуждать, его еще нужно проработать в какой-то мере, чтобы выставить уже на всеобщее обсуждение.

Если говорить о самой первой части, это основные понятия, то хотелось бы отметить, что, наверное, когда мы будем готовить документ такой, как стратегия кибербезопасности Российской Федерации, мы должны опираться на те документы, которые уже приняты и утверждены, а не вводить новую терминологию. Тем более что в связи с терминологией происходит очень много споров в наших международных отношениях, на уровне наших международных отношений. Споров между Россией, например, и США, особенно между этими двумя странами.

И поэтому переходить какие-то грани даже в терминологии, это иногда, может быть, делать уступки в дальнейшем каким-то шагам в международной сфере. И мы должны быть очень и очень осторожны. Мы должны проконсультироваться со специалистами, которые принимают в этом активное участие.

Кстати сказать, есть представитель от Министерства иностранных дел. Вы нам что-нибудь об этом скажете, наверное. Я знаю, Крутских Андрей Владимирович очень активно работает над этой темой и уже не один год. И все пункты, которые здесь имеют место быть, они уже находятся в работе. Поэтому нужно связаться со специалистами, занимающимися этой темой, и тогда можно то, что можно дополнить в этой стратегии, нужно будет дополнить.

Возвращаясь же к терминологии, я еще раз хочу сказать, что желательно опираться на те термины, которые уже как-то утверждены и как-то приняты. И вот в связи с этим у нас есть утвержденный документ "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления… (тра-та-та) и критических объектов". Вот если брать эти основные направления, то этот документ, он как раз и начинается с терминов. Может быть, что-то можно добавить. Но в основном, скорее всего, нужно опираться на эту терминологию, потому что другой, утвержденной, у нас нет.

Задача номер один. Действия. Создать государственный ситуационный центр. По поводу ситуационного центра единого разговор шел в Совете безопасности. Но это, оказалось, сделать совершенно невозможно. Более того, сейчас идет разговор, вернее, не просто разговор, а проводятся совещания, многочисленные совещания на межведомственном уровне о создании сети ситуационных центров. И даже при наличии сети, не просто единого ситуационного центра, а сети, пока еще не пришли к единому

пониманию, на каких основах, политических, технических, философских, будет эта сеть создаваться.

Это вопрос очень непростой, но то, что нельзя создать единую такую сеть, это совершенно однозначно.

С МЕСТА

(Говорит без микрофона.)… почему? В Китае есть такой центр, в Европе – там во многих странах, в Германии есть, в США есть. Почему мы-то не можем?..

С.В. КОНОВЧЕНКО

Единый ситуационный центр, который отслеживает все проблемы и в банковской сфере?

С МЕСТА (та же)

Есть главный, есть главный… *(Шум в зале.)* А сколько под ним там сидит, я не знаю.

С.В. КОНОВЧЕНКО

Этим занимается ФСБ, да, как правило, или какие-то структуры, которые отслеживают информацию самого секретного и глубокого уровня. Понимаете, да? Это просто уже другой уровень.

Р.У. ГАТТАРОВ

Я-то просто, про что хочу сказать: почему мы этим занимаемся? Вот у нас получается, что у нас ФСБ занимается этим, но никто даже здесь, грубо говоря, там до конца не понимает, а чем она занимается. И соответственно все люди не понимают, что их все-таки кто-то там… Ну они надеются, что кто-то их защищает, но до конца не понимают этого.

Поэтому и нужно создавать некие публичные структуры. Пускай они самые страшные вещи туда уходят, но какие-то публичные структуры должны быть у государства, потому что… Ну, когда-то у страны не было системы МЧС, ну вот до того, как пришел Шойгу. И она вроде, как и не нужна была. Потом она появилась. А притом, что… Сейчас вот представьте, что у нас не будет МЧС. Люди начнут волноваться.

_____

(Говорит без микрофона.) Можно я просто?.. Еще раз, чисто технически такой ситуационный центр модифицированный можно создать, причем именно, как надстройку над отраслевыми.

И здесь основная задача, на самом деле… То есть должна быть выстроена методология, что к какой угрозе относить, потому что угроза там кибератаки, например, может быть, в одном ведомстве, но разобраться в ней может только другое. Для этого нужен, грубо говоря, некий синхронизирующий механизм, который диспетчеризирует эту задачу точно так же, как диспетчеризируется любая техническая поддержка, связанная с функционированием того или иного сложного технического объекта, в соответствии с профессиональной пригодностью.

Сбор такой информации абсолютно технически не сложный, потому что построение вот этих самых электронных административных регламентов, о которых я сегодня уже говорил, позволяет, с одной стороны, извлекать проблему и её решать, может быть, коллективным образом, но при этом, не нарушая целостности тех информационных ресурсов, которые существуют в той или иной ведомственной системе.

Там как привести в глоссарий, с точки зрения, в разных ведомственных системах или там в частном сленге, возможно разное толкование одного и того же явления с совершенно

разными понятиями. Привести это тоже можно, потому что есть системы семантического разбора, которые могут приводить к тождеству между событиями.

Технически абсолютно реализуемая задача. Вопрос – как её строить, как её спроектировать, это другой вопрос, который, безусловно, там вот в Совете Федерации есть смысл обсуждать. Если вам интересно, мы можем вам рассказать про кое-какие опыты.

Р.У. ГАТТАРОВ
В Совете Безопасности.

_____(тот же)
Совет Безопасности, да. Прошу прощения.

Р.У. ГАТТАРОВ
Прокомментировать хотите? Давайте. Потом продолжим.

С МЕСТА
Действие номер один – создать государственный ситуационный центр. Действие номер два – создать сеть центров реагирования. Да?

Честно говоря, я думал, что это между собой взаимосвязанные как бы там получаются центры. И второе – это как бы разновидность ситуационного центра, только с меньшим количеством, может быть, задач решаемых, как бы подчиненных.

На самом деле, Вы правильно сказали, что надо создавать сеть ситуационных центров, но главный центр, он должен быть, конечно.

Я бы дальше предложил бы вот то, что раньше называлось "территориальные центры", а здесь можно ведомственные центры предложить. Вот они как бы подчиняются главному, а уже потом от ведомственных идет подчинение вот этих вот сетей центров реагирования, которые не в каждом ведомстве, каждой критической инфраструктуре там либо некритической, информационной. Вот такая система выстраивается управления, может быть, киберинфраструктуры, компьютерная там, кибер там сетевой инфраструктуры. Она, конечно, еще обсуждается, но в принципе где-то так.

Р.У. ГАТТАРОВ
Я вот, единственное, у меня вопрос. Мы имеем в виду аппаратные вещи или технические вещи?

РЕПЛИКА
(Говорит без микрофона.)… организационно-технические…

С МЕСТА (тот же)
И программные есть, и информационные… *(Шум в зале.)*

Р.У. ГАТТАРОВ
Нет-нет, аппаратные. Не аппаратно-технические, а аппаратные, то есть конъюнктурные… *(говорят одновременно).*

С МЕСТА (тот же)
Организационно-технические мероприятия. Есть такой официальный термин.

Р.У. ГАТТАРОВ
Нет, это не правильно. Есть политический, то есть, кто главный. Вот сказали: сейчас там главный ФСБ. Мы-то "за", но нам нужно сделать какую-то внешнюю инфраструктуру,

которая была бы понятна гражданину, бизнесмену, чтобы он понимал, куда ему бежать, что спрашивать, что делать.

_____

А мне кажется, что ФСБ – это один из агентов доставки и обработки информации, то есть на самом деле в таких структурах есть набор агентов. Это министерства: МВД, не знаю, там Минкомсвязь, Министерство иностранных дел. На самом деле это все источники первичной информации и профессиональной обработки этой информации. Должен быть диспетчер, который собирает проблемы и дальше раздает их по профессиональному признаку. Вот тогда будет, собственно говоря, результат… *(Оживление в зале.)*

Р.У. ГАТТАРОВ

Коллеги, давайте дослушаем.

Пожалуйста.

У меня просьба, выключить микрофон, тогда будет лучше слышно.

С.В. КОНОВЧЕНКО

Просто существует в государстве информация разного уровня тайны. И то, что делает одна организация, эта информация не может войти в другую организацию. И те организации, которые занимаются одного уровня информацией, они не могут работать, например, в общепринятом понимании на всю страну. То есть есть свои определенные какие-то полномочия у каждой организации.

И здесь вот, я повторюсь, этот вопрос очень сложный. Он до сих пор продолжается, он находится в обсуждении, потому что, несмотря на то, что над ним уже длительное время работают в Совете Безопасности, единого мнения не выработано пока.

Если же говорить о второй и третьей частях этого действия, то вы знаете, наверное, что 15 января был принят указ Президента о создании государственной системы, ну, о "сопке"(?), короче говоря, по сопке. И там некоторые ответы вот по второй части этого действия, они как бы уже предоставлены. Их можно будет посмотреть.

И последнее, на что я хотела бы… Не хотелось бы особенно задерживать ваше внимание, хотела бы вернуться опять-таки вот к МИДу, к важности того, чтобы проработать со специалистами вопросы по международному сотрудничеству. И плюс… Да, вот, если говорить, например, о задаче номер восемь и действии номер пять, то опять-таки это все тот же 31-С указ Президента.

Вещи, которые вы планируете, как что-то нужно сделать, оно уже прописано в каких-то законодательных актах.

_____

Светлана, все-таки "сопка" и 31-й указ касается только госорганов и критически важных объектов, а мы говорим о государстве, бизнесе и гражданском обществе.

С.В. КОНОВЧЕНКО

Вы знаете, я здесь гражданского общества вообще не вижу.

_____(та же)

Ну как? Вот, второй пункт – бизнес, гражданское общество. 31-й указ ни того, ни другого вообще не касается.

С.В. КОНОВЧЕНКО

Очень пунктиром. Я бы хотела, кстати, сказать, защитить вообще гражданина и гражданское общество, так как я представляю здесь интересы культуры и информационной

безопасности граждан. Мы надеемся, опять реанимируем работу над таким документом в Совете Безопасности, но вот она пока тоже получила какое-то слишком уж минимальное отражение, эта тема вот в данном документе.

Р.У. ГАТТАРОВ
Ну вот и образование, и культура.

С.В. КОНОВЧЕНКО
И последнее…

С МЕСТА
(Говорит без микрофона.)… можно вопрос? А вопросы устранения цифрового неравенства вы тоже решаете?

С.В. КОНОВЧЕНКО
Нет. Мы взяли пока только один аспект и работаем пока только над ним.

И последнее, о чем хотелось бы сказать. Вот просмотр проекта данного документа показал, что ориентироваться… Работа все-таки должна идти по классическому сценарию. Никуда не денешься. Необходимо все же создавать рабочую группу специалистов из министерств и ведомств, потому что они в основном нарабатывают регламентирующие акты, они аккумулируют то, что сделано и делается на государственном уровне, что будет делаться на государственном уровне в ближайшее время.

А экспертное сообщество, со своей стороны, оно должно привносить то, что… Все-таки государство, оно несколько консервативно, оно боится ошибиться и боится сделать нередко лишний шаг в сторону. Экспертное сообщество может предложить то, что является риском, но то, что продвигает любое общество.

И вот после этого соединять, можно проводить и совместные заседания. Но то, что должны присутствовать представители и от силовых ведомств, от ФСО, вот здесь мы даже не увидели в общем списке ни Министерства иностранных дел, ни ФСО, которые этим непосредственно занимаются. Видите, да? Прочие ведомства, вот так – прочие. Это не совсем хорошо. Даже дело не в том, что хорошо или плохо, а это не результативно. Мое предложение такое.

Р.У. ГАТТАРОВ
И буквально коротко. Все-таки мы здесь имеем опыт определенный по концепции "электронного парламента". Это очень сложный процесс. Всегда проще договориться с экспертами. Почему очень сложно договориться с ведомствами? У них у каждого своя поляна, они каждый думают о конкретных объектах своих и отстаивают в первую очередь некую субъектность. Это, наверное, и правильно. Любой человек это делает.

Мы изначально пытаемся сейчас сделать документ, некий экспертный, а потом уже садиться и разговаривать с ведомствами. Может быть, это неправильно, но как минимум, мне кажется, мы тогда сможет получить какой-то результат. Если мы сейчас изначально сядем с ведомствами, мы только в понятиях будем разбираться годик, потом годик будем формировать задачи, потом перейдем уже… Как раз у меня тогда кончатся полномочия. Ну, честно, я без всякого ерничанья здесь говорю. Мы изначально говорили о том, что мы готовы работать со всеми, но изначально не хотим делать такую большую, тяжелую конструкцию, потому что, на мой взгляд, она просто… Я просто, внутренне понимая свои ресурсы, я ее просто не смогу поднять. То есть без поддержки Щеголева, без поддержки, прямого включения руководства ФСБ, кого-то из вице-премьеров, ну, такая конструкция, она просто не взлетит.

Мы попытаемся сделать то, что можем со своей стороны. Я хочу еще раз, может быть, это было непонятно в первую очередь для экспертного сообщества, мы так собираемся идти. Мы очень ценим, например, вы же с нами здесь, по факту мы вас пригласили, вы с нами работаете. Также мы готовы работать с любым другим ведомством, но на предмете именно экспертной площадки, а не рабочих совещаний. Это следующий этап. Вот как-то так.

Представители МИДа. Пожалуйста.

А.А. РАДОВИЦКИЙ

Меня зовут Радовицкий Александр Александрович, МИД России, департамент по вопросам новых вызовов и угроз. Я представляю нашумевший в прессе департамент по информационной безопасности. На самом деле это отдел. Это будет отдел по международной информационной безопасности в рамках департамента. Абсолютно недавно создан.

Я так понимаю, что МИД первый раз на этом совещании. Я не знаю почему, но не суть. Просто с документом мы могли ознакомиться только сейчас, я вот сейчас его только увидел. Безусловно, это полезное только начинание. Это очень серьезный проект, пока это проект. Насколько я понял, был уже ряд заседаний, где это обсуждалось с участием ведомств, экспертов. Поэтому я сейчас не готов к формату …(?), здесь нужен серьезный анализ, проработка этого документа.

Как бы в части нашей компетенции могу сказать, что задачу девять уже в принципе многие выступавшие озвучили. Знаете, звучит: организовать международное сотрудничество. Оно уже организовано больше десяти лет, с 1998 года это организовано.

Р.У. ГАТТАРОВ

У нас конвенций куча не подписана международных.

А.А. РАДОВИЦКИЙ

У нас куча неподписанных конвенций… Конвенций у нас нет пока.

У нас есть концепция конвенции, у нас есть проект универсальной конвенции по борьбе с киберпреступностью, это пока проекты. Даже вы упоминаете концепцию конвенции, которая как раз была разработана под эгидой Совета безопасности. Это даже не проект, это концепция.

У нас есть в нашем правовом поле два межправсоглашения с ШОС о международной информационной безопасности и двустороннее с Бразилией. С Бразилией оно еще у нас не вступило в силу, потому что бразильцы не завершили внутригосударственные процедуры. По ШОС уже у нас окончательно оно вступило в силу. Но это уже детали, я не буду в них вникать, потому что это займет большое время дополнить этот список. У нас есть резолюция наша в ООН, у нас есть наши инициативы в ООН как официальные документы. И основная суть, что мы везде используем термин "международная информационная безопасность".

Я не знаю, насколько я подрывную работу сейчас веду, затрагивая, возвращаясь к теме терминов. Но как уже представитель Совбеза очень правильно отметил, кибербезопасность – это тот термин, сейчас в отсутствии журналистов я могу это говорить, тот термин, с которым мы боремся, потому что это термин, который используют наши западные партнеры. Этот термин, в нем заложена сужающая трактовка. Потому что, как вы отчасти правильно сказали, есть контент, но тут дело даже не в контенте.

Во-первых, в нашем правовом поле нет понятия кибербезопасности, что это такое, также как и нет в законодательствах большинства стран, в том числе и США. Есть в концепции, да, появляется. В законодательстве этого нет. Потом кто-то трактует кибербезопасность как безопасность Интернета, кто-то трактует как безопасность

компьютерную, то есть какую-то аппаратно-техническую. Он не включает всей сферы информационно-коммуникационных технологий.

В частности, в ООН, в ОБСЕ мы используем альтернативный компромиссный термин, кстати, который часто нехотя, но поддерживают наши западные партнеры, это безопасность в сфере использования ИКТ. Он наиболее компромиссный и при этом довольно всеобъемлющий. Но опять же я не буду повторять слова Совбеза, потому что задача девять – продвигать инициативы. Это называется международная информационная безопасность.

Р.У. ГАТТАРОВ

Я надеюсь, что мы нормально сейчас при Вашей помощи и поддержке сможем задачу девять сделать более корректной, тем более что уже целый отдел создан и так или иначе вы этим занимаетесь. Нам действительно здесь очень нужна ваша поддержка для более полной картины, в том числе и в этих вещах, связанных с информационной, с кибербезопасностью.

С МЕСТА

(Говорит не в микрофон. Не слышно.) … потому что информационная безопасность является сужающим термином.

ВОПРОС

Кто это сказал?

Р.У. ГАТТАРОВ

Наоборот, мне кажется, что информационная безопасность – это всеобъемлющий, самый широкий.

С МЕСТА

Понимаете, трактовка "информационный" может быть достаточно простая, то есть все, что связано с информацией. Она может не затрагивать, например, базовые технологии. И это вопрос вопросов. Потому что вы говорите, что кибербезопасность – сужающий термин, а я говорю, что информационная безопасность – сужающий термин. Понимаете, здесь действительно вопрос терминологии достаточно сложный, потому что информационная безопасность – это защита информации, это не защита базовых элементов. И в этом смысле нужно тогда находить такую формулировку, которая интересна… Я понимаю, что очень важны наши западные партнеры и так далее и …(?) друзья, но мы же говорим о нашем государстве. Соответственно, исходя из этого, мы должны четко понимать, о чем говорим мы.

Я понимаю кибербезопасность – это совокупность информационной безопасности, технологической безопасности, отраслевой безопасности.

Р.У. ГАТТАРОВ

Игорь, здесь на самом деле вопрос… Меня это на самом деле сильно настораживает. Если вопрос идет уже о неких международных историях и толкании в том, что признавать ли этот термин на уровне неких международных договоренностей, это очень проблематичная история.

Но я единственное чего не понимаю. Смотрите, если мы сейчас начнем заниматься или кто-либо, например, Совбез сейчас пока в активную фазу перейдет по информационной безопасности в разговорах, я думаю, что мы получим такой кусок негатива как внутри страны, так и со стороны извне.

Потому что нам скажут, что мы будем заниматься… журналисты тут же напишут, что мы будем заниматься, там, цензурой. Поэтому мне кажется, что наши, в том числе,

зарубежные партнеры, используя слово "кибербезопасность", минимизируют как раз вот эти некие информационные риски. Но это мое сугубо личное мнение.

Да, пожалуйста.

_____

Я бы не хотел пикироваться по вопросу кибербезопасности… информационная… Потому что у нас есть целый, скажем так, комплексный уже подход, в рамках которого мы говорим о терминологии. Это бы заняло сейчас какую-то ненужную лекцию, знаете, на час, на два. И дело тут даже, как я Вам отвечу, не в сужающем… Информационная безопасность — это понятие, которое есть в нашем правовом поле. Кибербезопасность — такого понятия в нашем правовом поле нет. Это раз.

А что касается… Руслан Усманович, как Вы правильно заметили совершенно, — это негативная реакция. Я могу говорить о негативной реакции извне в своей компетенции — это то, с чем мы боремся, это то есть основной наш… одной основной задачей МИДа, нашей внешней политики в области информационной безопасности является как раз разъяснительная задача насчет подходов Российской Федерации. Потому что у нас регулярно. Мы можем даже не говорить, мы на многих площадках слово "МИБ" — табу, слово "международной информационной безопасности". Но при этом "кибербезопасность" тоже табу. Мы пользуемся компромиссным термином… *(Оживление в зале.)* Но даже при таких условиях мы все равно получаем определенную негативную реакцию на многих площадках.

Р.У. ГАТТАРОВ

Ирина Левова.

И.Ю. ЛЕВОВА

Нет. Я не себе слово. Я хотела бы просить, чтобы Олег высказал… Тоже у нас выступил тоже специалист очень хороший по информационной безопасности, он стесняется просто.

О.

Я членом комиссии РАЭК являюсь, и также представляю центр аналитических исследований России. И сейчас просто возник опять этот сюжет с терминологическими противоречиями, и стоящими за ними понятийными противоречиями. Я хотел бы как раз заострить внимание на возможности компромиссного решения. Поскольку сейчас мы все-таки обсуждаем экспертный документ, а не законодательный какой-то документ, может быть нам в рамках этого экспертного документа попробовать пойти на компромисс и, по-моему, на первой встрече об этом уже говорилось, — выделить… договориться о том, что мы выделяем для себя кибербезопасность как просто отдельную более узкую нишу в рамках более широкой повестки задач информационной безопасности. И посмотреть возможно ли это, и будет ли это гармонично сочетаться с тем, что записано уже в имеющихся доктринальный документах российских, и законодательных актах? Потому что…

Р.У. ГАТТАРОВ

Нет, коллеги. Мы услышали всех. Мы, давайте, поручим… рабочая группа поручит мне и Александру Шипилову, в первую очередь. Если РАЭК и наш коллега, который компетентен в этих вещах, мы отдельно проведем встречу с МИДом или у вас на площадке, мы с удовольствием к вам приедем, посмотрим как вы живете, или вы к нам приезжайте, мы вам наши покажем пенаты. И отдельно проговорим уже по этим всем вещам и попробуем найти там… пройти между Сциллой и Харибдой, да, вот здесь. Вот как-то так.

Коллеги, еще есть желающие в закрытой части?

Наталья Ивановна, в закрытой части что-то скажите?
Да, пожалуйста.

ИЗ ЗАЛА

(Говорит не в микрофон. Плохо слышно.)

Руслан Усманович, насчет этих(?) заманчивых предложений, спасибо, к вам приехать, и вас тоже с радостью мы пригласим. Но я предлагаю в любом случае какую-то такую подгруппу провести, и как уже было предложено несколько раз, в межведомственном формате. Потому что, опять же, в плане международного сотрудничества в сфере информационной безопасности мы работаем такой плотной уже многолетней команде ведомств с разработанной позицией, и то есть, как озвучили: ведомство это такое… я понимаю, бюрократы — такое болото, но при этом в плане информационной безопасности у нас абсолютно отработанные роли и согласованная позиция межведомственная. Абсолютно.

Поэтому лучше даже такую подгруппу провести, может быть, в рамках Совета безопасности, с участием обязательно ФСБ, ФСО…

Р.У. ГАТТАРОВ

Мы на самом деле… Мы когда начинали этот долгий путь, мы такую встречу производили. Только вот МИД мы как-то тогда не… кстати, это было до того как появился отдел. Но в любом случае у вас было… мы МИД как-то не отождествляли с этой работой. Мы на самом деле, знаете до чего договорились? То есть вот здесь были большие, в общем-то, достаточно большие начальники, там, замдиректора департамента был как раз ФСБ. Все были. И мы и все скептически очень отнеслись к этой истории. Они спросили: у вас деньги есть? Я сказал: нет. А вам кто-то это поручал? Я сказал: нет. Они сказали: "Ну, тогда мы как? Мы посмотрим со стороны. Если у вас будет что-то получаться, тогда мы примем участие." То есть они незримо и зримо с нами здесь и сейчас, и я так понимаю, что мы как в какой-то конкретной коммуникации с ними сейчас работаем. И то, что мы здесь еще собираемся, значит, мы идет в каком-то так или иначе в верном направлении. Это понимание.

Но я бы все-таки сначала провел встречу с МИДом отдельно. Услышал вашу позицию, ваши наработки, что сделано. А если вот, в принципе, уже прозвучало, там, минимум дважды и от Светланы, и от Вас, мы отдельно тогда проведем, опять же, я предлагаю без экспертов для того, чтобы это было как-то на чиновничьем языке. Соберем те ведомства, которые вы считаете… которые вы назвали, может быть, представителей Правительства еще позовем, Администрацию Президента… И я лично, например, разговаривал об этом с Игорем Олеговичем Щеголевым для того, чтобы это было более весомое совещание, мы договорились провести его у него в кабинете. Если вы считаете, что время уже пришло, значит, мы готовы… я готов это совещание инициировать.

Да, пожалуйста.

С МЕСТА

Руслан Усманович, насчет… я бы хотел сказать, что у нас у МИДа есть полное понимание, что документ — экспертам. Но единственное, что нас беспокоит и будет беспокоить больше всех в выше указанных даже силовых ведомствах, — это то, что документ публичный. То что публичный, значит, этот будет в доступе для наших западных партнеров. И вот это…

Понимаете, есть стратегия, разработанная в рамках госсектора исключительно. Есть какие-то… это будет экспертный документ, его природная экспертная разработка, совместно с бизнесом, с гражданским обществом. Но для нас — это наша база, это основа, это оружие внешнеполитической деятельности. И когда мы продвигаем одни инициативы,

исходя из общей межведомственной, у нас будет документ, где будет слово, с которым мы боремся, ну вы понимаете какая это ситуация.

Р.У. ГАТТАРОВ

Ну, есть компромиссное решение. То есть мы можем называть как угодно. Главное, чтобы вопросы, которые мы вкладывали в это название, не выпали из стратегии. *(Оживление в зале.)*

На самом деле я Вас понял. На самом деле мы можем что сделать? В рамках бреда, конечно, мы можем сделать какую-то… Пускай наша стратегия будет, таким, отвлекающим маневром, мы их дезориентируем, они потом подумают, что все-таки мы их дезориентировали, а мы их ее примем. На самом деле отдельно все эти вещи.

О.А. ТЕРЛЯКОВ

Мы можем, конечно, дезориентировать врага главное самим не запутаться в этом. В вопросах терминологии с коллегой соглашусь, потому что это язык на котором мы с вами общаемся. Как мы понимаем друг друга, так мы, значит, и вкладываем одинаковый смысл в этот документ. Поэтому МИД в этом вопросе поддержу.

И я не представился, прошу прощения, Терляков Олег, Администрация Президента, управление применения информационных технологий. Одну ремарку небольшую к документу сделаю, которая вызвала у меня опасения просто — это вопрос публичности относительно государственных органов.

То есть я вот здесь зачитаю немного, да, то есть государственные органы должны подготавливать отчет о готовности федеральных структур по организации защищенности, и отчетность о защите национальных инфраструктур. Вот у меня здесь вызывает небольшой момент — это такая, знаете, публикация состояния собственной обороноспособности.

_____

Все публикуют.

О.А. ТЕРЛЯКОВ

Нет. Не надо. Не так. Это не так. Никто не публикует. *(Оживление в зале.)*

_____ (тот же)

Я видел отчеты Счетной палаты. Там открытым текстом написано… Там же не написано: вот в этом ведомстве на этом маршрутизаторе такая-то дыра. Там говорится об общем состоянии защищенности.

РЕПЛИКА

Тогда надо конкретизировать.

ВОПРОС

Как?

Р.У. ГАТТАРОВ

Я ровно… некое общее состоянии. Понимаете, еще раз, у нас, слава богу, не происходило ничего страшного, пока не вскрыли ничего, не произошла какая-то катастрофа из-за этого. Так или иначе, наверное, скоро это там может, не дай бог, случиться. У нас метеорит в Челябинской области упал. Все ржут. А в Челябинске очень у многих стрессовая ситуация. Реально. Я-то просто здесь. Я там разговариваю: хи-хи, ха-ха… а ребята, те кто это пережили, они понимают, что в тот момент их никто не защищал. Просто никто. И не мог защитить. Вот и все. И это людей напрягает больше всего. И здесь, когда мы говорим об

общих каких-то… пусть выйдет человек в красивой форме, с пагонами, и у него там… какие-нибудь Интернет-войска, и скажет: мы защищены. Половина людей будет спать спокойно…

_____

Интернет-войска — это хорошо.

Р.У. ГАТТАРОВ

Вот и все. То есть я исхожу с точки зрения гражданина, в первую очередь. И скоро вот это все будет для гражданина точно так же, что наши, там, ядерные войска в полной боевой готовности, на нас никто не нападет. Не меньше сдерживающий фактор, а то и больше.

РЕПЛИКА

Тогда нам нужно убирать вот эту защиту критически важных объектов. Потому что политическая(?) инфраструктура у нас, конечно, защищена определенным образом, и не факт, что это надо делать достоянием общественности. *(Оживление в зале.)*

Нужно сделать просто уровень открытости. Мы так и говорим, что мы говорим о защите безопасности тех объектов, которые не являются, там…

Р.У. ГАТТАРОВ

А давайте мы не будем их убирать, а просто упомянем, что это… их нужно защищать, и все …*(Неразборчиво.)* и туда лезть не будем вообще. Как изначально ,в общем-то, мы и проговаривали.

Я с этим согласен.

РЕПЛИКА (та же)

То есть мы защищаем больше граждан, больше бизнес, больше организации несекретные. Тогда это нормально. Это как раз общественность …*(Неразборчиво.)*

Р.У. ГАТТАРОВ

Согласен. Левова, что скажите?

И.Ю. ЛЕВОВА

Я считаю, что надо договариваться с мирной терминологией все-таки нужно ввести, как правильно говорит Олег, и все остальные члены комиссии тоже согласны с этим, что нужно ввести термины "кибербезопасность" и "киберпреступность". Но нужно вводить их как, может быть, как более узкие.

Р.У. ГАТТАРОВ

Ирин, я Вас уже пригласил. Поэтому Вы будете как раз эмоционально и аргументировано доказывать эту позицию.

И.Ю. ЛЕВОВА

Мы напишем. А Вы тогда пойдете в МИД с ними договариваться.

Р.У. ГАТТАРОВ

Мы можем.

_____

(Говорит не в микрофон. Плохо слышно.) Совет дайте. Если делать анализ международных последних концепций, допустим, Бразилии, США, Британии, очень есть важный такой полезный раздел, который можно было сюда добавить, так, в качестве общего

предложения, либо как подраздел понятий, понятийного аппарата, либо просто раздел угрозы, и написать "угрозы террористического", "угрозы криминального характера"… *(Оживление в зале.)* Это очень важный и полезный раздел. *(Оживление в зале.)*

Можно ввести раздел… *(Оживление в зале.)*

О.А. ТЕРЛЯКОВ

Да, здесь коллеги еще хочется добавить одну немаловажную вещь, что эта стратегия все-таки имеет свой срок. То есть должно: от какого до какого года она должна существовать, потому что реалии меняются, мы какие-то себе планы ставим.

И, в принципе, здесь еще один аспект: мы должны отталкиваться от того что есть, то есть провести какой-то анализ текущей ситуации. Она должна тоже в стратегии быть отражена.

Р.У. ГАТТАРОВ

Ну, то есть зафиксировать момент.

О.А. ТЕРЛЯКОВ

Да. В стратегии – нет, скорее отдельным документом.

Р.У. ГАТТАРОВ

Это отдельный документ, да. Мне так нравились статьи Владимира Путина, которые были абсолютно политическими, понятными, которые потом раз – и превратились в 11 указов. Сейчас, правда, вся исполнительная власть думает, что с ними делать, но вот понятный политический документ превратился в указ. Спасибо.

Коллеги, ну что?

И.Ю. ЛЕВОВА

Тогда по поводу сроков. Если действительно нужно указывать сроки, то, наверное, с этим вопросом надо определиться.

Р.У. ГАТТАРОВ

Я думаю, что вы не комиссии РАЭК это рассмотрите.

О.А. ТЕРЛЯКОВ

Я думаю, что должна быть стратегия, а потом уже можно определить сроки.

И.Ю. ЛЕВОВА

А вот нет, потому что в зависимости от сроков по-разному документ надо писать.

Р.У. ГАТТАРОВ

Чем больше будет срок, тем более общие формулировки там будут.

И.Ю. ЛЕВОВА

Ну да.

РЕПЛИКА

Преамбула…

Р.У. ГАТТАРОВ

Преамбула – это однозначно.

И.Ю. ЛЕВОВА

До 20-го нормально, все до 20-го напишут. *(Говорят все одновременно.)*

С МЕСТА

Что об этом думают наши потенциальные друзья – о сроках? Сколько они нам отводят – год, два, три, пять? Кто-нибудь знает?

_____

Можно на эту тему высказаться?

Р.У. ГАТТАРОВ

Пожалуйста.

_____(тот же)

Я, во-первых, полностью хочу согласиться с тезисом, который сейчас высказали, о том, что нужна действительно максимально подробная и четкая классификация угроз, которой сейчас пока нет (сегодня тоже уже говорили).

Р.У. ГАТТАРОВ

Мы ее ровно на прошлом совещании снесли. Раскритиковали в пух и прах и сказали, что если мы привяжемся к угрозам, то угрозы меняются: вот сегодня были одни угрозы, завтра будут другие угрозы, послезавтра будут третьи угрозы. То есть вот в таком виде, в каком о них Александр Александрович из МИДа сказал… их нужно писать тогда в таком общем-общем виде. А у нас они были в технических…

С МЕСТА

Но есть такие документы, как межправсоглашение с Бразилией и с ШОС, и там описывается… там есть классификация существующих угроз. Опять же вопрос классификации.

С МЕСТА

Вот в том варианте, который был (это Наталья Ивановна предлагала нам эту классификацию), там мы делили на угрозы личности, угрозы бизнесу и угрозы государству, ну и дальше…

Н.И. КАСПЕРСКАЯ

Это не я, это концепция…

Р.У. ГАТТАРОВ

Да. Ну и, соответственно, дальше они там дробились. Здесь вот именно такие общие – "кибертерроризм"… по-крупному берем.

_____(тот же)

Да, это может быть, допустим, та же классическая, существующая в МИДе триада угроз или, допустим, это может быть, если есть параллельная классификация и если среди присутствующих экспертов разные представители поддерживают разные классификации, можно создать в рамках стратегии как экспертного документа матрицу классификаций угроз. Почему нет? Но то, что она должна быть… Иначе непонятно, от чего мы защищаем наших граждан, наш бизнес и наши организации и зачем нам эта стратегия. То есть немножко все реалистичнее получается.

Р.У. ГАТТАРОВ
А Вы читали, например, стратегию Великобритании?

_____(тот же)
Да, конечно.

Р.У. ГАТТАРОВ
Где там угрозы-то?

_____(тот же)
Там прослеживается… там есть.

Р.У. ГАТТАРОВ
Но они вообще… главная цель – это цифровой суверенитет. Там есть угрозы, безусловно, но они ставят не угрозы во главу, а во главу ставят действия.

С МЕСТА
Согласен, согласен.

_____(тот же)
Во главу ставить не обязательно, но…
Р.У. ГАТТАРОВ
Коллеги, мы работаем больше полутора часов. Вот Левова уже компьютер сложила, это сигнал к тому, что РАЭК уже готов на комиссию выдвигаться и начать работать. *(Оживление в зале.)*
Давайте подытожим. Все замечания отработаем и пришлем вам для экспертного заключения.
Второе. В течение, я думаю, пары недель, может быть, трех недель мы запустим сайт – это точно.
Третья вещь. Мы отдельно проработаем вопрос, как я уже говорил, с МИДом и попробуем договориться, для того чтобы мы ни в коем случае не вредили нашей международной безопасности своей публичной историей. Я здесь абсолютно не ёрничаю, а действительно считаю, что если есть какая-то тактика, стратегия у МИДа, мы должны ее понимать и в рамках нее в том числе действовать, чтобы ни в коем случае не нарушить большую игру, что называется, международную политику. Вот эти вещи.
И следующее заседание давайте проведем в течение марта, отдельно договоримся по дате и, как договорились, давайте будем тогда уже в закрытом режиме. Мне кажется, он более комфортен. А все, что нужно, потому будем выдавать отдельным пресс-релизом с точными формулировками кто и что говорил.

Р.У. ГАТТАРОВ
Это мы обязательно сделаем, но кто задал вопрос, может и сделать ответ. Мы возьмем триаду угроз, которая есть…

С МЕСТА
Если МИД предложил документ ШОС, мы можем взять что-то оттуда. *(Оживление в зале.)*
Р.У. ГАТТАРОВ
Я когда говорил про то, что мы все записали, я и говорил про угрозы. Мы отдельно тогда совместно с РАЭК и, Наталья Ивановна, тогда с Вами и Лукацким это отработаем. *(Оживление в зале).* Спасибо, коллеги. Тогда закончим.