С Т Е Н О Г Р А М М А

заседания "круглого стола" на тему "Состояние и проблемы нормативно-правового регулирования технологического обеспечения информационной безопасности Российской Федерации"

19 апреля 2016 года

еб

Б.Б. ЖАМСУЕВ

Добрый день, уважаемые коллеги! Начинаем работу нашего "круглого стола". Напомню о том, что тема – "Состояние и проблемы нормативно-правового регулирования технологического обеспечения информационной безопасности Российской Федерации.

Председателем комитета Виктором Алексеевичем Озеровым поручено мне вести сегодняшнее заседание "круглого стола". Меня зовут Жамсуев Баир Баясхаланович, я являюсь заместителем председателя данного комитета.

Я от имени нашего комитета хотел бы прежде всего поблагодарить всех вас за то, что вы откликнулись на наше приглашение принять участие в работе "круглого стола" с очень актуальной на сегодняшний день темой – технологическое обеспечение информационной безопасности нашей страны. Вы понимаете, что в современных геополитических и экономических условиях эта тема выступает в качестве приоритетной задачи, и прежде всего субъектов обеспечения национальной безопасности.

Мы с вами с учетом всех последних событий, которые происходят в нашей стране, вокруг нашей страны, наблюдаем

достаточно серьезную заинтересованность и спецслужб иностранных государств, и криминальных структур к информационным ресурсам нашей страны, прежде всего органов государственной власти. Есть те, которые реально угрожают национальной безопасности нашей страны.

В связи с этим мы посчитали, что на заседание "круглого стола" необходимо пригласить не только представителей федеральных органов исполнительной власти, которые играют, конечно же, ведущую роль в решении задач в этой важнейшей сфере, но и ученых и практиков, которые ежедневно занимаются вопросами прикладного обеспечения информационной безопасности и подготовкой соответствующих специалистов.

Отмечу, что вопросы, связанные с информационной безопасностью Российской Федерации, нашли свое отражение и в Стратегии национальной безопасности Российской Федерации, которая была, как известно, утверждена Президентом нашей страны 31 декабря прошлого года. В качестве направления совершенствования информационной безопасности выделено совершенствование системы выявления и анализа угроз в информационной сфере, противодействия им. При этом уязвимость информационной инфраструктуры обозначена среди главных стратегических угроз национальной безопасности, а повышение уровня технологической безопасности, в том числе в информационной сфере, определено в качестве одного из главных направлений обеспечения национальной безопасности.

Подчеркну, что Совет Федерации, в частности наш Комитет по обороне и безопасности, постоянно проводит мониторинг правоприменительной практики в данной сфере. Вы знаете о том, что у нас создан специальный Совет по законодательному

обеспечению оборонно-промышленного комплекса и военно-технического сотрудничества. В рамках данного совета у нас создана секция радиоэлектронной промышленности, которая, на наш взгляд, достаточно эффективно работает и вносит достаточно хорошие рекомендации, проводит неплохой, хороший анализ, который позволяет нам видеть наиболее проблемные, уязвимые вопросы именно в этой отрасли.

Тем не менее специфические вопросы информационной безопасности, обозначенные тематикой сегодняшнего нашего "круглого стола", по нашему мнению, требуют участия специалистов, наверное, более узкого круга, узкого спектра. И в данной связи просил бы всех участников, которые будут сегодня выступать с сообщениями, с докладами, задавать вопросы, высказывать свое мнение, все-таки сосредоточиться на наиболее проблемных местах и на конкретных предложениях, не просто обозначить проблему, мы все умеем задавать вопросы, вываливать какие-то проблемы, мы их реально видим, ощущаем в повседневной практике. Но для того чтобы были выработаны конкретные предложения именно на нашей площадке, на площадке Совета Федерации, именно в плане правоприменительной практики с точки зрения реализации нормативно-правового и законодательного обеспечения в этой сфере, хотелось бы, чтобы ваши рекомендации носили более конкретный характер и, я бы сказал, такой разрешающий те проблемы, которые у нас сегодня здесь существуют.

ст

Поэтому просьба: именно проблема и ваше видение решения этой проблемы. Это было бы очень важно для того, чтобы, еще раз повторяю, наши рекомендации были бы полезны всем участникам и не только нашего "круглого стола", но и тех всех структур и всех

органов власти, ученых, практиков, которые работают или находятся в данной сфере.

Предлагается следующий регламент работы, уважаемые коллеги. Выступления — до семи минут, основные выступления, и обсуждение итогового документа — до пяти минут. Заседание планируется провести без перерыва, если не возражаете, в течение одного часа 30 минут — 45 минут. То есть мы где-то должны без пятнадцати четыре всю работу нашу закончить. Поэтому я просил бы всех выступающих, тех, кто будут участвовать в обсуждении, придерживаться строго регламента, который я сейчас вам обозначил.

Обращаю ваше внимание, что "круглый стол" у нас проводится в открытом режиме. Поэтому те люди, которые являются носителями секретной информации, прошу это особенно учитывать. Перед тем, как задать вопрос в ходе дискуссии, просьба отчетливо называть должность, фамилию, имя, отчество. Ведется стенограмма. И все ваши предложения, конечно же, будут затем обработаны, учтены в подготовке нашего итогового документа. Поэтому была бы просьба, если кто-то желает, можно заполнить, наверное, те места, которые не заняты, кто желает выступить, чтобы микрофон был вам доступен, и очень четко мы слышали все ваши предложения. *(Оживление в зале.)* Пришли уже, да? Вовремя сказали. Испугались, что займут, и пришли сразу же.

И просьба, если у кого-то есть более конкретные и достаточно, будем говорить, на ваш взгляд все-таки глубокие и конкретные предложения, которые должны заслуживать нашего внимания — есть микрофон напротив меня, просьба к нему и выступать по тем предложениям, которые вы хотели бы высказать.

Я сразу скажу о том, что в заседании нашего "круглого стола" принимают участие члены Комитета по обороне и безопасности

Совета Федерации. Присутствуют представители Аппарата Совета Федерации. Фамилий очень много, чтобы не задерживать, просто перечислю, какие структуры сегодня у нас представлены: Федеральная служба безопасности Российской Федерации, Федеральная служба охраны Российской Федерации, представители Министерства обороны, Федеральной службы по техническому и экспортному контролю, Министерство внутренних дел Российской Федерации, Министерство образования и науки, Министерство транспорта, Министерство энергетики. И присутствуют представители промышленности и научно-исследовательских и образовательных учреждений. Круг людей достаточно компетентный, широкий для того, чтобы у нас разговор с вами по данному вопросу получился.

Разрешите теперь слово предоставить инициатору проведения данного "круглого стола", члену Комитета Совета Федерации по обороне и безопасности Мархаеву Вячеславу Михайловичу. Пожалуйста, Вячеслав Михайлович.

В.М. МАРХАЕВ

Спасибо.

Уважаемый Баир Баясхаланович, Франц Адамович, уважаемые коллеги, добрый день! Развитие российского государства связано с переосмыслением роли информационной безопасности, поиском и определением направления и механизмов защиты информационного пространства. В настоящее время проблема информационной безопасности стоит еще более остро, поскольку значительно выросла роль накопления обработки и распространения информации, в частности, в принятии стратегических решений увеличилось количество субъектов информационных отношений и потребителей информации. Угрозы и вызовы современности вновь и вновь

обращают внимание на необходимость более тесного взаимодействия всех государств с целью осмысления сущности и масштабов проблем, выработки мер по их решению, твердой политической воли для реализации принятых обязательств и договоренностей.

Информационная революция коснулась практически всех отраслей народного хозяйства всего общества. Проблема информационной безопасности оказалась неразрывно связана со всеми другими аспектами безопасности, в том числе личной безопасностью, безопасностью государства и общества.

сб

Информационное оружие, которое стремительно развивается, может стать даже более опасным, чем ядерное. Информационное оружие может действовать избирательно. Оно может быть применено через трансграничные связи, сделать невозможным выявление источника этой атаки. Поэтому информационное оружие может стать идеальным средством для террористов, а информационный терроризм может стать угрозой существования государств, что делает информационную безопасность важным аспектом национальной и международной опасности. И роль этого аспекта будет только усиливаться.

Сегодня в интересах безопасности мы должны объединить ряды и попытаться рассмотреть систему противодействия новым угрозам и вызовам, главными из которых являются терроризм, экстремизм и кибертерроризм.

События последних лет лишний раз продемонстрировали всю важность технологий современного обеспечения информационной безопасности и трагические последствия их недооценки. Нет сомнения, что помимо интересов физической безопасности сегодня несоизмеримо возрастает спрос на средства защиты информации, но

какими бы эффективными не были эти средства, они мало чего стоят без квалифицированного персонала и соответствующих организационно-распорядительных документов.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры нескольких уровней, но главное – это правовые методы обеспечения информационной безопасности государства. То есть разработка нормативно-правовых актов, регламентирующих отношения в информационной среде и нормативно-методических документов по вопросам обеспечения информационной безопасности.

Важно отметить, что текущие сроки разработок и утверждение нормативно-правовых актов не поспевают за высокими темпами развития коммуникационных технологий, тем более за технологиями обеспечения информационной безопасности. В связи с этим, возможно, следует рассматривать механизмы принятия подзаконных нормативно-правовых актов.

Одна из составляющих национальных интересов в информационной среде включает в себя развитие современных информационных технологий отечественной индустрии и информации, в том числе индустрии средств информатизации и обеспечения потребности внутреннего рынка ее продукции и выход этой продукции на мировой рынок. Также обеспечение накопления, сохранения и эффективного использования отечественных информационных ресурсов, что включает в себя прежде всего защиту от несанкционированного доступа обеспечения безопасности информационных, телекоммуникационных систем как уже развитых, так и создаваемых.

Наличие и доступность к достоверной информации о состоянии динамики и развития экономических, политических,

социальных и других процессов в обществе в решающей степени определяет возможность властных структур и общества в целом по выработке и реализации эффективных решений в военно-стратегической, политической и научно-образовательных сферах.

Информация, информационные коммуникации стали сегодня факторами, способными либо обеспечить стратегическую стабильность и развитие общества и государства, либо разобщить и дестабилизировать общество. Таким образом, информацию сегодня можно рассматривать как важнейший элемент системы выживания и, следовательно, национальной безопасности страны в целом.

В процессе функционирования нынешней системы безопасности можно выделить проблемы, относящиеся к системе обеспечения национальной безопасности в целом, а именно: отсутствие общеконцептуальных подходов к созданию логически и технически взаимосвязанной системы, гармонично сочетающей всю совокупность подсистемы информационного обеспечения, низкий уровень финансового и материально-технического обеспечения данной сферы управленческой деятельности, который характерен сегодня для субъектов обеспечения национальной безопасности практически всех уровней.

Усиливается технологический отрыв ведущих стран мира, и наращиваются их возможности для создания информационного оружия. Всё это может привести к созданию нового этапа развития гонки вооружения в информационной сфере с использованием глобальной информационной инфраструктуры.

Обеспечение информационной безопасности – это непрерывный процесс постоянной реализации способов и путей совершенствования и развития системы информационной

безопасности, непрерывный контроль выявления слабых мест и потенциально возможных каналов утечки информации.

ог

Информационная безопасность является одним из важнейших аспектов отечественной безопасности, на каком бы уровне ее не рассматривали – национальном, отраслевом, корпоративном или персональном. Комплексный подход к рассмотрению информационной безопасности предполагает всеобщее обсуждение и участие всех слоев общества. Думаю, участники "круглого стола" дополнят и раскроют сущность стоящих перед нами проблем, особенно в нормативно-правовом обеспечении, для выработки конкретных и эффективных рекомендаций. В завершение хотелось бы напомнить слова, ставшие как никогда актуальными сегодня: "Страна без собственного достойного оборудования – все равно, что государство без вооруженных сил". Спасибо.

Б.Б. ЖАМСУЕВ

Спасибо, Вячеслав Михайлович.

Пожалуйста, есть вопросы? Нет?

Тогда будем продолжать. У меня есть список людей, которые заранее записались для выступления, поэтому слово им предоставлю.

Пожалуйста, Чернов Дмитрий Евгеньевич, директор Департамента развития высоких технологий Министерства связи и массовых коммуникаций Российской Федерации.

Пожалуйста, Дмитрий Евгеньевич.

Д.Е. ЧЕРНОВ

Спасибо.

Я постараюсь достаточно коротко по тем инициативам, с которыми на сегодняшний день выступает министерство, прежде всего в законодательной части, потому что тема действительно очень

широкая. Количество угроз и количество необходимых, как с точки зрения законодательной, так и подзаконной активности, действий весьма велико. Я остановлюсь на двух вещах: на глобальной – это, собственно говоря, государственный суверенитет над интернетом и обеспечение его устойчивости и стабильности. И немного расскажу о тех законодательных инициативах, которые от нас исходят в рамках исполнения поручения Президента после Форума "Интернет Экономика" в части защиты персональных данных и личных данных граждан.

Собственно говоря, ни для кого не секрет, что работа наших сетей Интернет фактически реализована в виде некоей самоорганизующейся конструкции, в которой есть корпорация ICANN, которая занимается выдачей доменных имен. И зоны .RU и .РФ являются национальными доменами, то есть как кириллический, так и латинский домен. Но при этом все равно общее руководство осуществляется ICANN и по его правилам. И вторая история, которая тоже, в общем, модерируется не страной, – это выдача интернет-адресов и, собственно говоря, автономных систем, то есть адресация на физическом уровне, которая тоже происходит из-за рубежа. В нашем случае центр находится в Голландии.

Собственно, история с доменными именами тревожит не только Российскую Федерацию, но фактически все развитые страны, потому что все хотят представлять себе и участвовать в разработке тех правил и нормативов, которые используются при выдаче доменных имен. На сегодняшний день в корпорации ICANN происходят достаточно существенные подвижки, меняется руководство, и мы совместно в том числе с китайскими коллегами (с которыми мы недавно встречались) высказываем некую

консолидированную позицию, чтобы голос стран в национальных доменах был решающим.

Сейчас на организационном уровне министерство связи вошло в автономную некоммерческую организацию "Центр координации Интернета" (АНО КЦ). И фактически мы имеем право вето, то есть все внутренние процедуры сделаны. Но кроме этого готовятся поправки в закон "О связи", в которых суверенитет Российской Федерации над доменными именами в зонах .RU и .РФ и над ведением списка автономных систем и адресаций внутри Российской Федерации будет закреплен за федеральным органом исполнительной власти, и мы фактически получим право, возможность и обязательство управления этими двумя основными ресурсами.

тм

И считаем, что этой ситуацией национальный суверенитет России над доменной зоной и над Интернетом внутри наших границ будет в достаточной степени обеспечен. То есть там некие технологические мероприятия нами уже проведены, конечно, но здесь речь идет только о законе. Мы сейчас согласуем с заинтересованными ведомствами и с аппаратом текст закона. Я думаю, что он к лету будет готов и выйдет.

Немножко хотел бы остановиться на защите персональных данных, в документах об этом много говорится. С одной стороны, мы считаем, что федеральный закон № 152 в части защиты персональных данных фактически достаточно хорошо проработан, полностью соответствует требованиям. И мало того, скажем, Совет Европы фактически с большинством тех изменений или тех новелл, которые находятся в законе № 152, и не было в Европе, согласился. И сейчас в рамках "КАДАТы"(?) фактически позиция Российской

Федерации является, я бы сказал так, довлеющей. Там есть небольшие только у нас разногласия по поводу гостайны, но, по сути, все равно можно говорить о том, что наш закон о персональных данных всеми признается, считается хорошо проработанным и достаточно эффективно работающим.

Однако Президент дал нам поручение по защите личных данных, то есть была изменена формулировка. Суть угроз, которые в документах тоже есть, состоит в том, что кроме однозначно используемых данных (фамилия, имя, отчество), неких данных, которые к определяемому определенному лицу могут быть однозначно отнесены, существуют в Интернете гигантские наборы профилированных данных, когда про пользователя конкретно ничего не сказано, но при этом крупные корпорации, владеющие информационными ресурсами или находящиеся на сетях связи, способны профилировать группы пользователей по половому признаку, по признаку присутствия в тех или иных группах, по интересам и так далее. И при помощи этих профилей, не попадающих, по сути, в федеральный закон № 152, оказывать в том числе и деструктивное влияние на те или иные социальные группы. То есть, условно говоря, понимая, что люди с определенными интересами откликнутся на определенные призывы, не собирая по ним персональные данные, они, фактически работая с онлайн-пользователем, не с человеком, как в законе № 152, имеют возможность установить коммуникацию при помощи рассылок, мессенджеров, SMS-сообщений и так далее, и нанести тот или иной, но фактический ущерб.

К июню мы готовим доклад Президенту и будем выступать с законодательными инициативами именно в этой части, которая нам тоже представляется крайне важной. Но пока у нас только идет

обсуждение на открытой площадке и в Администрации Президента, мы готовим свою позицию по этому поводу. Спасибо.

Б.Б. ЖАМСУЕВ

Вопросы есть? Пожалуйста.

С.Е. СТАЛЕНКОВ

Сталенков Семен Егорович, генеральный директор ЗАОН НПЦ "НЕЛК".

Вопрос к закону о защите персональных данных. Приходится наблюдать постоянно такую ситуацию, когда пользователь не имеет права отказаться от предоставления возможности обрабатывать свои персональные данные. Примеров миллион, приведу простой.

Ведущая выставка по безопасности. Билет куплен заранее, приходишь, должен получить бэйдж, в обязательном порядке должен предоставить свои персональные данные. Отказаться от этого не можешь. Пробовал один раз, сказали: "Не нравится, разворачивайтесь и уходите". И это идет постоянно. С учетом того, что организаторы выставки иностранные компании, с участием иностранного капитала, многие интернет-ресурсы, где приходится регистрироваться пользователям, тоже являются с участием зарубежного капитала, эта услуга навязывается в обязательном порядке. Никакой ответственности организаторы не несут за то, что они действуют таким образом. Прошу учесть это при дальнейшей разработке и совершенствовании данного закона. Спасибо.

Д.Е. ЧЕРНОВ

Могу коротко прокомментировать. Не знаю, Роскомнадзора, по-моему, нет, они бы лучше меня ответили, хотя я думаю, что я отвечу примерно то же самое.

мв

Дело все в том – цель, для которой собираются эти данные. Вообще говоря, всегда можно обратиться и к контрольному органу, которым является Роскомнадзор, и к любому другому надзорному органу, который за наши с вами права отвечает.

Не исключаю, так как я здесь цель не видел, не знаю зарегистрировались они как операторы персональных данных, прошли ли все необходимые процедуры, если все эти процедуры соблюдены (например, это большая выставка, они собирают большое количество людей), таким образом, в каком-то смысле, они борются с экстремизмом и терроризмом. Если такую цель при обработке данных они декларировали, то, наверное, они вам в праве и отказать. То есть тут просто так собирать персональные данные у нас в стране нельзя. И Роскомнадзор имеет все механизмы с тем, чтобы привлечь организацию, которая либо собирает их незаконно, либо собирает их законно, объявив, что такой сбор будет, но использует не для тех целей.

Что касается... это иностранная компания. В 152-ФЗ в сентябре были внесены поправки, которые совершенно четко определяют, как должен работать оператор с персональными данными в случае необходимости их к разведочной(?) передаче.

Мы все-таки не строим закрытую страну. Мы понимаем, и закон четко описывает: информация должна быть собрана и локализована на территории Российской Федерации. В случае если страна входит в список стран, в которых обеспечена надлежащая охрана персональных данных, эти данные могут быть переданы по каналам разведочной(?) передачи, но при этом: а) пользователь должен быть об этом уведомлен, то есть в самом соглашении должно быть написано, что это возможно; б) и должны быть соблюдены те формальные требования, которые у нас в стране существуют.

Этот вопрос все время задается, но, коллеги, закон очень точно описал как это делается. Если они считают, что... Мы же тоже зашли с вами и тоже отдали свои персональные данные, потому что такое правило прохода в здание Совета Федерации. Ничего в этом страшного нет.

Б.Б. ЖАМСУЕВ

Хорошо. Пожалуйста, еще вопросы.

Тогда у меня к вам вопрос будет. С учетом высокого уровня внедрения информационных технологий – государственное управление, о чем Вы сейчас упомянули, социальные отношения, как Вы оцениваете сегодня законодательное обеспечение безопасности таких объектов и государственного управления? Мы же понимаем то, что в результате любой хакерской атаки, компьютерской атаки можно парализовать работу всей государственной системы. На Ваш взгляд, насколько законодательно обеспечена безопасность этой системы на данный момент?

Д.Е. ЧЕРНОВ

Хороший вопрос.

Б.Б. ЖАМСУЕВ

Вы понимаете, о чем я речь веду?

Д.Е. ЧЕРНОВ

Дело в том, что законодательство по персональным данным выглядит... нас очень часто за это критикуют, с одной стороны говорят: "а что является персональными данными", а фамилия, имя, отчество плюс телефон". В принципе, законодатель... Вообще говоря, с точки зрения закона более на 80 процентов возможность работы есть, потому что построение в законах особенно любых закрытых списков (хакерская атака это только вот это, вот это и вот это), тот час же возникнет история, когда вот это не соблюдалось, появилась

какая-то еще новая угроза, ее в законе нет и возникает долгая и формальная процедура о внесении изменения в закон. *(Оживление в зале.)*

Подзаконные акты выпускаются быстрее и проще. Их зачастую не всегда хватает, но для этого нужны регуляторы в виде нас, ФСТЭК, ФСБ, которые готовят подзаконные акты. Мне не кажется, что какая-то гигантская правовая лакуна есть. Есть регулярная работа. Что-то появляется – мы потихонечку с тем темпом, с которым работаем, работаем. Мне не кажется, что здесь есть большой правовой...

РЕПЛИКА

(Говорит не в микрофон.) Необходима законодательная инициатива.

Д.Е. ЧЕРНОВ

Нет, законодательная инициатива... Законодательная работа есть. У нас три закона, три изменения в закон стоят. Но это просто некий такой регулярный процесс, который не остановится. Вот сейчас примем три и четвертый не потребуется, такого нет.

Б.Б. ЖАМСУЕВ

Я думаю то, что мы немного говорим о разных вещах. Я говорю о таком универсальном комплексном законе, который бы обеспечил безопасность критически важной информации. Вы говорите о дополнении в закон. Я речь веду о том, нужно ли сейчас с учетом высокого уровня информационных технологий, которые находятся и в системе государственной власти, принять основополагающий документ, который регулировал бы вопросы безопасности. Вот о чем. А не о дополнении на каждый хакерский выпад, на атаку, в тот же закон о связи. Вот о чем речь идет. *(Оживление в зале.)*

сз

Я понял Вас. У нас есть представители других структур, особенно Федеральной службы безопасности, я просил бы тоже более подробно ответить на этот вопрос о необходимости такого законопроекта.

Есть еще вопросы? Нет.

Двигаемся дальше. Семизорова Екатерина Владимировна, начальник отдела законодательства об обороне, безопасности и информации Департамента уголовного, административного и процессуального законодательства Министерства юстиции России.

Пожалуйста, Екатерина Владимировна, Вам слово.

Е.В. СЕМИЗОРОВА

Я хотела бы кратко... По нашему мнению, все-таки базовым, основополагающим документом была Стратегия национальной безопасности Российской Федерации, утвержденная указом Президента в декабре, которая определила основные направления развития законодательства, в том числе в сфере информационной безопасности. В частности, здесь очень важным является принятие стратегических, доктринальных документов, которые положат основу для разработки каких-то законодательных актов, подзаконных актов, которые будут в дальнейшем с учетом выявленных угроз обеспечивать соответствующее нормативно-правовое регулирование защиты.

Поэтому, по нашему мнению, все необходимые выявленные какие-либо лакуны, так скажем, которые в настоящее время не урегулированы, целесообразно в рамках вот этой работы сейчас осуществлять. В частности, существуют планы, в соответствии с которыми разрабатываются доктринальные стратегические

документы, в том числе и в сфере информационной безопасности. Все отраслевые органы работают с ними сейчас. То есть у нас такая оценка. В основном это важно, потому что это самый актуальный документ, который основу закладывает для дальнейшего развития законодательства. Спасибо.

Б.Б. ЖАМСУЕВ

Хорошо.

Будем двигаться дальше. Мурашов Николай Николаевич, заместитель начальника Центра ФСБ России. Пожалуйста.

Н.Н. МУРАШОВ

Коллеги, во-первых, я хотел бы (может быть, этого в моем выступлении нет) ответить на вопрос. Термин "компьютерная атака" у нас определен актом Президента. То есть есть соответствующий документ стратегического планирования, в котором очень четко определен термин "компьютерная атака". Он существует с 2012 года, и никаких проблем с его использованием в настоящий момент не имеется.

Второе. Отвечая на вопросы, переходя уже непосредственно к теме моего доклада, хотелось бы сказать, что в настоящий момент по распоряжению Президента Российской Федерации Федеральной службой безопасности совместно с Федеральной службой охраны и Федеральной службой по техническому и экспортному контролю, Министерством обороны и другими ведомствами проводится достаточно, на мой взгляд, большая работа, которая выражается в том числе и в подготовленных в настоящий момент и готовых для внесения в Правительство Российской Федерации законодательных актов.

С этой точки зрения наиболее важным (и с нашей точки зрения, и с точки зрения других ведомств) является обеспечение

безопасности критической информационной инфраструктуры. Руководствуясь этим положением, Президентом Российской Федерации было дано поручение Правительству Российской Федерации о разработке подобного закона, а Правительство поручило это ФСБ и вышеназванным ведомствам, о которых я говорю.

Объясняется это тем, что анализ современной обстановки показывает, что в последние годы наблюдается стабильный рост числа компьютерных атак на информационные ресурсы Российской Федерации. Спецслужбами иностранных государств, преступными сообществами ведется деятельность по сбору сведений, составляющих государственную тайну, получению информации о передовых разработках государства во всех отраслях производства, осуществляются крупномасштабные кражи персональных данных, систематические атаки на объекты критической информационной инфраструктуры с целью нарушения их функционирования.

Внедрение информационных технологий в государственное управление, экономику, социальные отношения ставит данные сферы в дополнительную зависимость от общей геополитической обстановки. Сфера информационно-коммуникационных технологий стала одной из площадок для реализации многочисленных угроз безопасности Российской Федерации. По данным за последние годы, исходя из различных методик оценки ущерба от вредоносных программ глобальный мировой ущерб составляет от 300 миллиардов до 1 трлн. долларов, то есть от 0,4 процента до 1,5 процента общемирового ежегодного валового национального продукта. Эти показатели имеют тенденцию к неуклонному росту.

вб

Я хотел бы здесь остановиться, что с точки зрения криминализации этих деяний Российская Федерация находится, пожалуй, на первом месте. Мы одна из немногих стран, где криминализировано уже само изготовление вредоносного программного продукта, а не его применение или использование в каких-либо целях. А в случае, если оно осуществляется должностными лицами, иными лицами, то эти преступления относятся к числу тяжких. К сожалению, наши иностранные коллеги периодически забывают про это. Я думаю, что им надо напомнить и иногда посоветовать самим криминализировать подобные деяния, тогда существенно облегчился бы способ борьбы с этим в первую очередь в международном плане. А так как сеть глобальна, то здесь, конечно, это имело бы еще большее значение.

В этих условиях стабильность социально-экономического развития Российской Федерации и ее безопасность, по сути, поставлены в прямую зависимость от надежности и безопасности функционирования информационных или коммуникационных сетей.

Одной из важнейших областей, как я уже сказал, является критическая инфраструктура. Концептуальный подход к обеспечению безопасности критической информационной инфраструктуры Российской Федерации дан в утвержденном в феврале 2012 года Президентом Российской Федерации документе стратегического планирования "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации". Подчеркну, что этот документ является открытым и находится в общем доступе, на сайте Совета Федерации приведен его официальный текст.

Основным принципом формирования государственной политики в этой области является неразрывная связь обеспечения безопасности отдельных инфраструктурных объектов с обеспечением безопасности всей критической информационной инфраструктуры в целом. Основные направления госполитики предусматривают решение комплекса задач. В первую очередь это государственное регулирование, совершенствование промышленной и научно-технической политики, развитие фундаментальной и прикладной науки, подготовка и повышение квалификации кадров.

В части совершенствования госрегулирования планируется и выстраивается система нормативно-правовых актов, включающих законодательный уровень (федеральные законы), подзаконные акты (указы, распоряжения Президента Российской Федерации, соответствующие постановления Правительства), конкретизирующие положения законов, и нормативно-правовые акты уполномоченных федеральных органов исполнительной власти, определяющие механизмы реализации законов и подзаконных актов применительно к специфике задач каждого ведомства.

В рамках создания подзаконных актов и документов стратегического планирования издан Указ Президента Российской Федерации от 15 января 2013 года № 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации", закрепивший координирующую роль ФСБ в построении и обеспечении функционирования данной системы. 12 декабря 2014 года Президентом Российской Федерации утверждена Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, определяющая

назначение, функции и принципы создания этой системы, а также виды обеспечения, необходимого для ее создания и функционирования.

Подчеркиваю, что все три документа, по крайней мере выписки из них, достаточно полные, находятся в общем доступе и доступны для нашей общественности.

Несмотря на очевидные успехи, к сожалению, в настоящее время, эффективное регулирование в данной сфере затруднено из-за отсутствия системообразующих законодательных актов, устанавливающих порядок отношений в сфере обеспечения безопасности критической информационной инфраструктуры.

Как я уже говорил, в этой связи ФСБ России совместно с заинтересованными ведомствами разработан законопроект "О безопасности критической информационной инфраструктуры Российской Федерации". Принятие этого федерального закона представляется делом исключительной важности. Это обуславливается тем, что, как было показано выше, нанесение ущерба критической информационной инфраструктуре (а к ней относятся системы информационного обеспечения и обеспечения функционирования в том числе и высших органов государственной власти, системы, имеющие отношение к обороне страны, обеспечению безопасности и правопорядка, а также критических отраслей промышленности) неизбежно нанесет ущерб по этим секторам. Подготовленный ФСБ России законопроект устанавливает основные принципы обеспечения безопасности критической информационной инфраструктуры, полномочия государственных органов Российской Федерации в области обеспечения безопасности, а также права, обязанности и ответственность лиц, владеющих на праве собственности и ином законном основании объектами

критической информационной инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

Вот здесь я хотел бы чуть-чуть остановиться и сказать нечто следующее: на самом деле, если мы возьмем 149-й закон, который является системообразующим законом вообще в области информационных технологий, то там ответственность за обеспечение безопасности информации возложено в первую очередь на собственников систем. Они отвечают за нее.

аб

Но, с другой стороны, практически никаких санкций по отношению к собственникам этих систем, которые не используют те или иные средства безопасности, не занимаются безопасностью систем, не занимаются соответствующим кадровым потенциалом, который должен эти системы иногда в очень сложных отраслях промышленности использовать, эта ответственность сейчас практически полностью отсутствует.

Второе. У нас размыта... Я уже говорил о том, что у нас есть статьи 272, 273 Уголовного кодекса, если мы посмотрим на опыт и Федеральной службы безопасности, МВД России, Следственного комитета, то иногда доказательная база по этим статьям собирается очень тяжело. Поэтому в том числе вот этот Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" идет пакетом вместе с изменением в Уголовный кодекс, где подготовка компьютерной атаки против объектов критической информационной инфраструктуры будет отнесена к тяжким преступлениям, соответствующим образом это и повышение меры наказания, это, самое главное, что возможность

его пресечения на стадии подготовки, что в отношении преступления по статьям 272, 273 сейчас очень тяжело происходит.

Как я уже сказал, закон подготовлен в комплекте, кроме того, в целях его реализации подготовлены изменения в Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс, Российской Федерации, Закон Российской Федерации "О государственной тайне" и Федеральный закон "О связи".

Таким образом, принятие законопроекта позволит создать правовую организационную основу для эффективного функционирования системы безопасности критической информационной инфраструктуры Российской Федерации, направленную на предупреждение возникновения каких-либо компьютерных инцидентов, а также существенно снизит общественно-политические, финансовые и иные негативные последствия для Российской Федерации в случае проведения против нее компьютерных атак.

К сожалению, процесс прохождения проекта федерального закона идет не так быстро, как хотелось бы. За последние два года законопроект трижды был возвращен Правительством Российской Федерации на доработку, причем согласованный со всеми ведомствами.

За это время законодательные акты аналогичного содержания приняты в Японии, Республике Корея, на финальной стадии проект директивы ЕС.

Когда мы начинали закон, действительно, мы были одними из первопроходцев именно с точки зрения законодательного акта. Аналогичный акт в силу специфики законодательства Соединенных Штатов Америки принят у них указом Президента, я говорю, в этом есть определенные различия в конституциях наших стран, там это

сделано таким образом. И большинство развитых стран мира сейчас в настоящий момент рассматривают или уже заканчивают рассмотрение в своих законодательных органах подобных законодательных актов.

С учетом изложенного, просили бы Комитет Совета Федерации по обороне и безопасности оказать нам необходимое содействие в продвижении и скорейшем принятии проекта вышеназванного федерального закона. Спасибо.

Б.Б. ЖАМСУЕВ

Спасибо большое.

Вопросы есть?

Николай Николаевич, у меня есть вопрос в связи с этим. Вот Вы правильно обратили наше внимание именно на этот проект закона, полагая, то что он очень важен с точки зрения обеспечения именно национальной безопасности. Я бы считал его краеугольным, потому что это касается системы именно государственной власти прежде всего.

Вот Вы сказали о том, что вроде бы проект согласован со всеми ведомствами, но Правительство его возвращает вам на доработку. Уже два года, насколько я понимаю, идет доработка данного закона. Скажите, пожалуйста, а вот основная причина, почему Правительство возвращает опять его на доработку, если он согласован? Я вот понять не могу этого... *(Микрофон отключен.)*

Здесь Вы не можете нам сказать?

Н.Н. МУРАШОВ

Сложно будет сказать мотив, по которому был возвращен закон. Формальным поводом послужило следующее, что... Дело в том, что... Как предусматривается формирование самой критической... *(Микрофон отключен.)*

св

Н.Н. МУРАШОВ

Он получает средства обнаружения и предупреждения компьютерных атак из госсистем за бесплатно, то есть за государственный счет они будут устанавливаться у него, он будет предупреждаться, и устанавливаться они будут непосредственно... Способ их установлен и Федеральной службой безопасности, и другими отраслевыми ведомствами, то есть все это делается.

Второе – он получает надежный зонтик в лице 10 лет за попытку атаки на него, потому что это действительно... Дело в том, что многие наши собственники за последнее время в электронной почте получали многочисленные угрозы от хакерских группировок, были случаи вымогательства, в первую очередь у объектов банковской системы. В настоящий момент такие попытки пресечены, но они осуществлялись уже международными группировками. И, в общем-то, нам потребовалось достаточно много сил и координации с нашими зарубежными партнерами, чтобы подобные факты пресечь.

Поэтому, конечно, такой закон... Да, действительно, он сложный, он важный, но я надеюсь, что в ближайшее время все же он окажется в Государственной Думе.

вш

Б.Б. ЖАМСУЕВ

Хорошо. Спасибо большое.

Я думаю, что мы, конечно, поддержим данный законопроект с учетом позиции нашего Комитета по обороне и безопасности. Вашу озабоченность мы понимаем, ее разделяем. И при поступлении уже непосредственно в Государственную Думу, конечно, будем

сопровождать и вместе с коллегами сделаем все, чтобы он был в ближайшее время принят.

Слово хочу предоставить еще одному представителю уполномоченного органа, который в том числе занимается вопросами защиты информации. Это Федеральная служба по техническому и экспертному контролю. Шевцов Дмитрий Михайлович – заместитель начальника управления данной службы. Пожалуйста.

Д.М. ШВЕЦОВ

Уважаемые коллеги! Во-первых, хотелось бы поддержать слова, которые были уже сказаны представителями Минюста, Минкомсвязи и ФСБ России. Мы всецело поддерживаем эти слова. Естественно, участвуем совместно в этой работе.

В своем выступлении я коротко расскажу о той деятельности, которую непосредственно осуществляет ФСТЭК России в части совершенствования нормативно-правового регулирования, технологического обеспечения вопросов информационной безопасности. За последние три года деятельность нашей службы была направлена на совершенствование требований по защите информации при ее обработке в различных информационных системах.

Так, в 2013 году ФСТЭК России были утверждены требования о защите информации, содержащейся в государственных информационных системах. Также в 2013 году были утверждены состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. И в 2014 году в соответствии с соответствующим поручением Президента Российской Федерации службой были утверждены требования к

обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами критически важных объектов.

Необходимо сказать, что все эти документы учитывают современные угрозы информационной безопасности, направленные на то, чтобы в информационных системах применялись современные информационные технологии. Надо отметить, что все эти документы, они не стационарные. Естественно, мы постоянно развиваем данные документы. Уже в определенные документы в этом году нами планируется внесение изменений, которое учитывает применение современных информационных технологий при построении информационных систем. Это и мобильные технологии, это и беспроводные технологии.

Что необходимо отметить? Большое внимание нашей службой уделено вопросам совершенствования требований к средствам защиты информации. Потому что без качественных средств защиты информации именно отечественного производства сложно обеспечить надлежащую и качественную защиту информации в информационных системах. Нашей службой также активно ведется эта работа. За последнее время нами был разработан целый ряд требований к средствам защиты информации от несанкционированного доступа. Это средства антивирусной защиты, это система обнаружения вторжений, средства контроля съемных машинных носителей информации. Также к средствам защиты информации от утечки по техническим каналам. Это и средства активной защиты по утечки по каналам ПЭМИН, акустическим операционным каналам утечки информации.

Надо отметить, что данные требования, они предъявляют не только требования безопасности к самой технологии. Эти

требования предъявляются к разработке и производству данных средств. Это действительно важно. Важно, чтобы средства разрабатывались соответствующим образом, чтобы эти средства соответствующим образом поддерживались, то есть осуществлялась техническая поддержка, своевременно выявлялись и устранялись уязвимости в средствах защиты информации.

В целях как раз своевременного учета угроз безопасности информации и устранения уязвимостей в информационных технологиях, применяемых средствах защиты информации ФСТЭК России совместно с ФСБ России, Минобороны России, МВД России, ФСО России, СВР России был разработан ресурс-банк данных угроз безопасности, который в марте прошлого года был введен в эксплуатацию, который включает в себя базу данных уязвимостей программного обеспечения информационных технологий. На что направлена эта база? Она направлена на то, чтобы уязвимости в информационных технологиях, средствах защиты информации своевременно выявлялись и устранялись.

Нами проводится активная работа по повышению качества именно отечественных средств, потому что самой важной проблемой на сегодняшний день является то, что отечественные разработчики, к сожалению, недостаточно внедряют при разработке средств процедуры безопасной разработки, достаточно плохо осуществляют тестирование этих средств, плохо проводят работы по выявлению и анализу уязвимостей.

При сертификации средств защиты информации мы данную работу проводим. И стремимся к тому, чтобы отечественные разработчики средств защиты информации данные мероприятия по безопасной разработке, по выявлению и анализу уязвимости, по

тестированию средств защиты информации внедряли у себя на производстве, у себя при разработке средств защиты информации.

В принципе всё, что хотелось бы сказать.

мг

Б.Б. ЖАМСУЕВ

Спасибо, Дмитрий Михайлович.

Есть вопросы к Дмитрию Михайловичу?

У меня один вопрос будет просто к Дмитрию Михайловичу, такой, укрупненный, чтобы не вдаваясь конкретно в цифры. Все-таки как Вы оцениваете уровень выполнения требований по защите информации в органах государственной власти на уровне федеральном и на уровне субъекта Федерации?

Д.М. ШЕВЦОВ

Нашей службой осуществляются контроль, защита информации в различных информационных системах. Но необходимо отметить, что в различных ведомствах отношение, естественно, разное. Можно выделить в лучшую сторону некоторые ведомства и в худшую. Но считаем, что не совсем достаточно, необходимо более внимательно относиться к вопросам защиты информации, необходимо обучать специалистов, и не только тех, которые непосредственно занимаются вопросами защиты информации, но и руководителей органов, и тех, кто применяет непосредственно информационные технологии при обработке информации. Все наши проверки направлены не только на то, чтобы выявить, например, какие-то недостатки, но и на то, чтобы как раз обучить, рассказать о том, как необходимо организовать защиту информации, как необходимо ее обеспечивать. Мы всецело оказываем содействие всем органам исполнительной власти и разъясняем, каким образом реализовывать требования по защите

информации, опять же, как организовать защиту информации в организации. Но вместе с тем пока уровень недостаточно высокий.

Б.Б. ЖАМСУЕВ

Хорошо. Спасибо.

Сейчас Дмитрий Михайлович говорил много о разработчиках. Я думаю о том, что предоставим слово тем людям, которые, насколько я понимаю, по тем должностям, которые они занимают, имеют отношение именно к этому.

Поэтому слово предоставляю Ромскому Георгию Алексеевичу, президенту консорциума "ОКБ Многофункциональные коммутационные системы".

Пожалуйста.

Г.А. РОМСКИЙ

Добрый день, уважаемые коллеги! В первую очередь разрешите поблагодарить за возможность довести надежды и чаяния отечественного производителя на столь высоком уровне. И хочу сказать, что сейчас, наверное, как никогда отечественные российские производители нуждаются в реальной государственной поддержке. Потому что, на наш взгляд, отсутствие долгосрочных векторов развития, которые ставят перед телекоммуникационной промышленностью именно государственные задачи о том, куда пойдет развитие технологий и что нам нужно сделать, нам этого сейчас не хватает. А учитывая, что у нас несколько сотен мелких, средних предприятий, которые так или иначе выпускают телекоммуникационное оборудование, часто конкурируют на нашем внутреннем рынке, мы пытаемся как-то объединяться в консорциумы (я вот являюсь президентом такого консорциума, куда входят несколько средних телекоммуникационных компаний). Но

без реальной государственной поддержки, конечно, продвинуться нам очень сложно.

Мы сейчас с удовольствием и с уважением наблюдаем за деятельностью Министерства связи и массовых коммуникаций, которое четко формулирует стратегию долгосрочного развития и для компаний, производящих программное обеспечение. Это и реестр программного обеспечения, это и те решения по созданию консорциумов с производителями программного обеспечения на принципах частно-государственного партнерства, когда государство совместно с бизнесом пытается решать важные задачи по разработке системного программного обеспечения, баз данных. Конечно же, нечто подобное хотелось бы видеть со стороны нашего государства и в области производства телекоммуникационного оборудования.

Сейчас хотелось немножко остановиться на термине "импортозамещение". Он у нас у всех на устах, но многие, даже на конференциях когда выступаем, понимает каждый немножко по-разному. Примерно есть вплоть до диаметрально противоположных мнений о том, что надо сделать все свое: собственная элементная база, собственное программное обеспечение, собственные производственные линии, либо достаточно локализовать импортные решения, ну или же просто замещать импортное оборудование одних западных производителей, государств, которые стали к нам не так дружественны, на другие западные или восточные решения.

св

У нас даже часто многие сейчас стали шутить, что импортозамещение у многих операторов связи складывается в том, что Cisco меняют на Huawei и так далее. Конечно, грустно наблюдать за этим процессом, но тем не менее мы не унываем и считаем, что совместно с государством здесь мы можем сделать

очень много. И поэтому, может быть, попробовать и акценты немножко сместить, то есть уйти от термина "импортозамещение" или использовать его четко по назначению, что импортозамещение – это следствие достижения нашей промышленности, независимости, суверенитета в ключевых технологических направлениях по производству телекоммуникационного оборудования, а весь фокус направить именно на достижение этой независимости и суверенитета. И понятно, что внутри, варясь в своем собственном соку, такого суверенитета сложно достичь.

Мы сейчас находимся, наверное, на границе новой технологической революции, мы видим, как быстро меняется наш окружающий мир, как информационные технологии входят во все сферы жизни – и государства, и бизнеса, и личности. Мы идем в мир интернет-вещей, а тут угрозы по безопасности заложены колоссальные. И без отечественных, нормальных, надежных доверенных решений здесь будет сложно обеспечить необходимый уровень безопасности.

Вот Вячеслав Михайлович в своем докладе привел высказывание основателя Huawei Жень Чжэньфэя о том, что страна без собственного оборудования, как страна без армии. В 1994 году китайское руководство услышало, и нам, бы, конечно, российским производителям, ту поддержку государственную, которую имеет Huawei.

А она в принципе... Можно уложить ее в три направления. Первое – поддержка по выходу на внешние рынки. Huawei пользуется практически неограниченными финансовыми ресурсами, для него дешевые... Операторам он предоставляет под 3 процента долговременные кредиты, с отсрочкой платежей. И даже у нас на внутреннем рынке очень сложно конкурировать в таких условиях.

Если говорить о таможенных условиях, экспортные пошлины на оборудование практически нулевые, у нас в России готовое оборудование также завозиться по нулевым пошлинам. Но в условиях отсутствия современной элементной базы тока, который необходим для производства современного конкурентоспособного телекоммуникационного оборудования, мы значительную часть вынуждены покупать на внешних рынках. Пошлины на комплектующие достигают 15 процентов. Да, в прошлом году мы видим: пошло движение в сторону снижения, многие позиции уменьшились, но тем не менее хотелось бы иметь, как, допустим, в том же Китае, что если комплектующая не производится на территории Китая, то практически нулевую таможенную пошлину они имеют.

Учитывая, что российских производителей достаточно большое количество, конечно, хотелось бы видеть стимулирование государства в таком важном направлении, как участие России в международных стандартизирующих организациях. Мы сейчас видим, что мир уходит от проприетарных решений, что все идут в сторону открытых технологий, открытых стандартов, и для этого в мире существует множество консорциумов, стандартизирующих организаций, которые уже сейчас объединяются и разрабатывают решения, допустим, по сетям следующего поколения, по программно-конфигурируемым сетям, по оптическим сетям. Это все сращивается в один клубок. К сожалению, российские представители, российские компании там находятся пока в стадии наблюдателей. И очень хорошо, что у нас появляются переводные документы и мы можем быть в курсе тех направлений, но без помощи государства, может быть, подумать о создании консорциума российских производителей, чтобы мы при соответствующей

государственной поддержке могли бы полноценно участвовать в этих стандартизирующих организациях, пытаемся туда влиять.

сб

Только так можно обрести определенную долю суверенитета.

Чтобы сейчас нам участвовать, к сожалению, и финансовые ресурсы не позволяют, и соответствующие налоговые условия. Мы все научно-исследовательские разработки вынуждены финансировать из прибыли. В то же время, как упомянутые китайские производители, до 10 процентов своего оборота они могут относить к себе в себестоимость, тем самым получая ключевые преимущества в области научно-технического прогресса.

Может быть, немножко сумбурно, волнуюсь, но нам бы казалось, если бы государство сделало госзаказ на перспективные телекоммуникационные технологии, организовало нечто подобное конкурсам тендера, как сделано для разработчиков программного обеспечения, мы бы, наверное, с удовольствием объединились, может, даже выделили какие-то ресурсы и вместе с государством начали вкладываться в действительно прорывные направления.

Пока мы пытаемся догнать, но пытаемся использовать те решения, которые за нас разработали, навязывают, а тут мы свободны... у нас же огромные возможности работать в том же ЕврАзЭС, в странах БРИКС. В этом плане нам нравится позиция и Министерства связи, которое активно продвигает кооперацию, но и производители отечественные готовы в этом направлении работать. Поэтому нам важно получить реальные стимулы на внутреннем рынке с точки зрения приведения законодательства как налогового, так и таможенного хотя бы с тем, чтобы мы были конкурентоспособными с западными компаниями и поддержку на

внешнем рынке. Без поддержки государства отечественных производителей на рынке никто не ждет.

Коротко так. Спасибо. Если есть какие-то вопросы, я готов ответить.

Б.Б. ЖАМСУЕВ

Спасибо, Георгий Алексеевич.

Есть вопросы? Пожалуйста.

_____

А что Вам сейчас мешает работать в том же международном союзе электросвязи? Он разрабатывает основные стандарты. Там есть представители западных частных фирм. Что мешает нашим производителям туда ездить?

Г.А. РОМСКИЙ

Во-первых, нашим производителям мешает финансовое ограничение. Чтобы выделить одному производителю человека на постоянную работу в этих группах...

_____ (тот же)

Там они не постоянные.

Г.А. РОМСКИЙ

Там все равно они...

_____ (тот же)

Командировочные расходы выносятся из соответствующих налогов.

Г.А. РОМСКИЙ

Они все равно существуют.

_____ (тот же)

264-я статья Налогового кодекса есть, там вообще налогов на них нет. Это производственная деятельность. Потом есть организация АДЭ. Ее председатель, насколько я знаю, был

председателем 17 комитета по безопасности. Что сейчас мешает использовать имеющийся потенциал?

Г.А. РОМСКИЙ

Имеющийся потенциал мешает использовать то, что мы недостаточно крупные, чтобы заявляться в этих организациях. Если бы мы объединились и пошли туда группой компаний...

_____ (тот же)

Но вот АДЭ есть, она частная организация. Она объединяет, насколько я понимаю, производителей программного обеспечения и телекоммуникационного оборудования. Она же есть.

Г.А. РОМСКИЙ

С АДЭ мы работаем.

Б.Б. ЖАМСУЕВ

Хорошо. Вопрос задан, ответ мы услышали.

Есть еще вопросы? Нет.

Идем дальше. Давыдов Владислав Владимирович, генеральный директор ЗАО "Искрауралтел" есть? Нет? Он был заявлен.

Тогда я предоставляю слово Дмитрию Владимировичу Сухомлинову, генеральному директору – главному конструктору ЗАО "Научно-производственное объединение "Мобильные информационные системы". Пожалуйста.

Д.В. СУХОМЛИНОВ

В этой области я представляю предприятие и разработчика систем защиты информации, которое работает в области информационной разработки системы управления информационных систем в интересах Министерства обороны.

ек

Ну, как бы здесь для нас опыт достаточно большой в разработке этих систем, и понятно, что в Министерстве обороны это

все оговорено соответствующими приказами. Мы ориентируемся на те законы, которые сегодня разработаны и действуют, в том числе взаимодействуем с органами ФСБ и ФСТЭК. Поэтому для нас это вопросы понятные. Единственное, конечно, необходимо, на мой взгляд, постоянно совершенствовать системы защиты информации, которые мы должны использовать в наших системах, потому что это сложные объекты информатизации, которые требуют соответствующей обработки грифованной информации. То есть здесь, конечно, надо постоянно совершенствоваться. И, безусловно, сегодня один из актуальных вопросов – сетевая организация защиты информации при сетевом взаимодействии сложных комплексов и систем. Вот это нас больше всего интересует, потому что информация подчас бывает достаточно высокого грифа секретности, и есть определенные опасения по поводу хакерских атак и возможного противодействия технических разведок западных государств, что повлияет на работу этих систем и целостность информации, которая функционирует в этих системах.

Поэтому я всячески поддерживаю развитие этого закона, чем скорее произойдет его внедрение и он будет принят, безусловно, это будет плюсом и движением вперед.

Б.Б. ЖАМСУЕВ

Спасибо.

Слово предоставляется Татухову Дмитрию Витальевичу, начальнику отдела 8-го Управления Генерального штаба Вооруженных Сил. Пожалуйста.

Д.В. ТАТУХОВ

Уважаемый Баир Баясхаланович, уважаемые коллеги! Тема моего сообщения касается подготовки кадров, но в преддверии пару слов из того, что я услышал, прокомментировать, если можно.

минобороны действует в рамках действующей правовой базы. Мы всегда исходим из реально сложившейся обстановки, поэтому, как уже было сказано, рядом внутренних ведомственных документов мы компенсируем те вопросы, которые, может, где-то законодательно до сих пор не закреплены.

Опять же, как было сказано коллегами из органов-регуляторов (ФСБ и ФСТЭК), мы включены в состав большинства межведомственных групп, находимся в курсе тех событий, которые происходят в рамках законотворчества в области информационной безопасности, и в своих внутренних документах, правовых актах мы ориентируемся и на терминологическую базу, ориентируемся на де-факто сложившиеся потребности органов военного управления, органов власти, которые взаимодействуют с Минобороны, таким образом на министерском уровне это нам позволяет сохранять более или менее равнопрочную защиту. Хотя проблем тоже хватает.

В своем выступлении Вячеслав Михайлович (как-то стало принято на него ссылаться) обратил внимание, и мы в своей практике сталкиваемся с этим, что немаловажна не только защищенная инфраструктура, но и квалифицированное ее обслуживание. Мы на протяжении ряда последних лет достаточно активно формируем систему органов защиты информации и сталкиваемся с тем, что базовая подготовка в школе не позволяет курсанту, который поступил в военный вуз, освоить программу, которая вытекает из квалификационных требований к специалистам по защите информации. Вместе с тем, мы принимаем дополнительные меры по селекции таких абитуриентов. В частности, мы два года практикуем дополнительную оценку по результатам ЕГЭ по информатике, и как ни странно получается, что хорошо знающие физику и математику, не всегда проходят по баллу ЕГЭ по

информатике, хотя, казалось бы, вступили в XXI век. Вот, если вкратце.

Хотелось бы несколько слов сказать, если позволите, о той системе подготовки, которая на данный момент сложилась в Минобороне.

ог

Я представляю управление Генерального штаба, которое непосредственно занимается организацией и защитой информации. И основные усилия, с учетом тематики нашего "круглого стола", сконцентрированы на обеспечении безопасности информации от несанкционированного доступа (со всеми вытекающими, то есть когда внутренний нарушитель рассматривается в качестве доминирующего); вопросах связанных с технической защитой информации как элементом противодействия техническим средствам разведки; противодействии компьютерным атакам, которые в последнее время с учетом той концепции, которую Президент утвердил, выведены, скажем так, в относительно самостоятельную отрасль; и немаловажные вопросы информационной безопасности СМИ. Вы знаете, что мы входим в информационное общество, и все всплески в СМИ зачастую гораздо больше ударяют по какой-то выполняемой задаче, нежели частные ошибки руководителей, ошибки персонала и тому подобное.

Не вдаваясь в сущность определения информационной безопасности, расскажу, как у нас выстроена система подготовки. Про первичный отбор я уже сказал. Мы имеем вуз, который специализируется на подготовке специалистов по защите, это Краснодарское военное училище. Также подготовка ведется сейчас во многих военных вузах по, скажем так, базовому минимуму, который касается информационных технологий. С 2002 года

Минобороны было принято ряд программ, направленных на создание базовых защищенных компьютерных технологий (так называемые БЗКТ(?)). Основой этих технологий являлось и является переход на доверенные среды (как здесь также было упомянуто, что с открытым исходным кодом), и в своей практике подготовки мы на это ориентируемся.

Основными направлениями совершенствования нашей системы подготовки мы видим поддержание учебно-методической и материально-технической базы на уровне, позволяющем обеспечить своевременность и актуальность получаемых знаний, непрерывное повышение квалификации профессорско-преподавательского состава, а также введение новых форм обучения, в том числе дистанционных.

В части поддержания материальной базы с советского периода (наверное, многие помнят) все базовые средства управления, которые использовались в войсках, имели установки, инсталляции в учебных комплексах, в училищах. Это достаточно качественная практика. Современные технологии нам даже дают в данном случае приоритет: мы на виртуальных машинах можем моделировать многие среды управления, что позволяет нам обучать информационным технологиям и применению конечных средств вооружения непосредственно в ходе учебного процесса.

Повышение квалификации профессорско-преподавательского состава – здесь мы, скажем так, сталкиваемся с определенными трудностями, есть разрыв поколений. То есть старшее поколение в силу возраста больше сосредоточено на теории, на базовых... Но, к сожалению, офицер, который прибывает на должность офицера по защите информации, должен владеть множеством практических навыков. На базе ряда училищ также смотрели оцениваемое качество подготовки. Иногда возникает ситуация, что курсант, прошедший

подготовку по программе высшего обучения, несколько уступает на стадии выпуска из учебного заведения специалисту, который сосредоточен на непосредственном применении средств защиты. Это касается и технических средств защиты и средств защиты от НСД. Ну а средства обнаружения вторжения, утечки данных – это мы уже считаем, что нужно иметь несколько высоких квалификаций, то есть владеть одновременно и практикой программирования, и практикой администрирования, а также многими вопросами, понимать суть и физику технических каналов утечки.

Не буду останавливаться над, скажем так, многими вузами, которые участвуют. Скажу, что мы используем и привлекаем к службе в Вооруженных Силах также и выпускников ведущих вузов.

мг

Относительно территориальной распределенности у нас вузы, поставляющие офицеров запаса, назовем так, младших специалистов, которые находятся в резерве, по всей территории Российской Федерации, то есть условно можно выделить вузы, которые находятся на территории Западного военного округа, у него, в общем-то, преференции в этом вопросе. Вместе с тем и южный регион, в зоне ответственности Южного военного округа, и Центрального военного округа, и восточного. То есть, относительно потребностей у нас вузы распределены и емкость обучения позволяет обеспечить, в общем-то, квалифицированными специалистами.

В части комплектования здесь можно отметить то, что мы рассматриваем также вопрос, связанный с возможностью переподготовки с родственных специальностей специалистов, которые прошли обучение в области информационных технологий, радиотехнических систем, знающие вопросы радиоэлектронной

борьбы и тому подобное. В общем-то, как говорится, конвергенция знаний в нашем деле имеет место быть.

Все, что касается специальностей и адаптации граждан, прошедших подготовку в гражданских вузах, у нас создана система переподготовки на базе военных вузов, где, в общем-то, гражданские специалисты, уже квалифицированные, как имеющие диплом о высшем профильном образовании, мы их стараемся адаптировать к тем условиям военной службы, к особенностям применения информационных технологий в Вооруженных Силах, и, как следствие, мы получаем такую, достаточно взаимовзвешенную систему, где выпускники, допустим, МГТУ имени Н.Э. Баумана, Военно-космической академии, наших вузов друг друга дополняют. Все равно каждая школа каждого вуза имеет какие-то сильные и слабые стороны, здесь они в такие команды собираются, и мы видим в этом, в общем-то, хорошую тенденцию.

В части, касающейся дистанционного обучения, в прошлом году мы... скажем так, было названо это экспериментом. Эксперимент проводился относительно обучения без отрыва офицеров. Обычно это в форме сборов происходит, то есть они отрываются от своих повседневных обязанностей, пребывают, как правило, сюда, в центральный регион, с ними на базе какой-то из воинских частей проводят и занятия. Здесь мы пошли, и руководство Минобороны пошло с удовольствием, можно сказать, на решение проблем повышения квалификации, поскольку технологии, даже новый комплекс принимается – уже нужно какие-то особенности давать. Мы формируем это в электронные курсы, сейчас программа, скажем так, под патронажем Министра обороны по электронным учебникам, по формированию и повышению качества тех, по сути, уже баз знаний, которые будут сосредоточены в военных вузах,

должна дать такую, хорошую ступеньку для того, чтобы новое поколение, которое достаточно мотивировано на службу в Вооруженных Силах, уже имело современные знания, а где-то даже, может, и обгоняло по технологиям, то есть с опережающим развитием этого вопроса.

Наверное, у всех на слуху были идеи также с научными ротами, мы их также рассматриваем как такой источник комплектования органов защиты информации. Сейчас мы к этой системе, в общем-то, так адаптировались. Считаем качественным показателем результатов службы в научной роте – это желание гражданина продолжить службу по контракту уже, как правило, на офицерской должности. Мы в этом видим определенный плюс, и при отборе в эти подразделения мы смотрим, опять же, на профиль подготовки. У нас, к сожалению, на первых наборах превалировали специальности радиотехнического уклона, а сейчас мы смотрим больше на программистов, больше смотрим на специалистов в области информационной безопасности, специалистов по компьютерной безопасности как, в общем-то, такой, можно сказать, всеобъемлющий специалист, который готов и иностранную технику адаптировать, и готов участвовать в разработках, готов участвовать в различного рода военно-технических экспериментах, где использует как иностранное программное обеспечение, так и отечественное, так и находящееся еще в стадии разработки. Таким образом, такая система нам позволяет поддерживать уровень квалификации специалистов по защите информации на более-менее удовлетворительном уровне.

тм

Б.Б. ЖАМСУЕВ

Спасибо большое, Дмитрий Витальевич.

Уважаемые коллеги, у нас время ограничено, еще 15 минут работаем, с учетом того, что нам надо будет просто технически освобождать это помещение. В связи с этим (Дмитрий Витальевич много говорил и правильно по системе подготовки студентов в высших учебных заведениях), считаю необходимым послушать представителя как раз таких учебных заведений.

Слово предоставляется Лосю Владимиру Павловичу, проректору Московского института радиоэлектроники и автоматики. Он же является заместителем председателя Учебно-методического объединения по Центральному федеральному округу.

Пожалуйста, Владимир Павлович.

В.П. ЛОСЬ

Спасибо.

Уважаемые коллеги! Тема моего выступления "Проблемы материально-технического обеспечения подготовки кадров в области информационной безопасности". Ряд проблем был уже здесь обозначен, я конкретно остановлюсь на некоторых из них.

Прежде всего мы отталкиваемся от требований федеральных государственных образовательных стандартов, которые у нас есть в области информационной безопасности. Я просто пролистаю перечень, который минимально необходим для бакалавриата в отношении наличия в вузе тех или иных лабораторий. Это лаборатории физики, электротехники и электроники, сетей систем передачи информации, это техническая защита информации, это целый набор средств, которые реализуют защиту информации в тех или иных физических полях, это программно-аппаратные средства и так далее.

Почему в настоящее время поднимается эта проблема по материально-техническому обеспечению? В чем основные причины? Первая причина известна – это дороговизна оборудования, быстрое моральное старение этой техники. А остальные причины, на них бы я хотел обратить внимание. Сейчас реализуется упрощенная схема лицензирования образовательной деятельности в том числе и в области информационной безопасности. Если раньше для открытия той или иной специальности в области информационной безопасности в вуз выезжала комиссия Учебно-методического объединения и реально смотрела, что в вузе есть, какая база есть, какие преподаватели есть, которые способны реализовать образовательные стандарты, сейчас это не требуется. Вуз готовит пакет документов, отсылает в Министерство образования, выдается лицензия. И у нас число вузов, реализующих наши специальности, в последнее время значительно возросло. Но оценка Учебно-методического объединения показывает, что 30 процентов вузов не удовлетворяют требованиям по материально-техническому обеспечению.

Следующая причина – это снижение норматива бюджетных затрат на подготовку одного студента. Я дальше цифры назову. В то же время информационная безопасность остается соответствующим приоритетным направлением в соответствии с распоряжением Правительства, номер которого указан на слайде.

Что произошло у нас со стоимостными группами? Наши специальности, вообще вся укрупненная группа специальностей и направлений подготовки переехала из третьей группы, где предусматривался объем нормативных затрат на обучение одного студента в размере 114 тысяч на год, мы сейчас оказались во второй группе, где эти затраты оцениваются в 70 тысяч, оставаясь

приоритетными направлениями в соответствии с постановлением Правительства.

ст

Какие пути решения? Несколько таких тезисов хотелось бы назвать. В области нормативно-правового регулирования хотелось бы ввести особый порядок лицензирования образовательной деятельности в области информационной безопасности. Действительно я еще раз повторю, что некоторые вузы практически на пустом месте открывают специальности, руководствуясь тем, что народ идет, выпускники школ идут, модные специальности открывают. Но научить как следует ребят этих они не могут.

Второе. В рамках нормативно-правового регулирования, видимо, нужно принять какой-то нормативно-правовой акт о государственной поддержке приоритетных направлений подготовки, включая специальности по информационной безопасности, чтобы такого не оказывалось, что, находясь в приоритете, вдруг снижают нормативные затраты на обучение чуть ли не в два раза.

В области технологического обеспечения образовательного процесса хотелось бы, чтобы было реализовано предложение нашего федерального учебно-методического объединения, которое в прошлом году поддержал Совет безопасности, о создании учебно-научных производственных центров в федеральных округах на базе ведущих вузов. Речь идет о том, чтобы сосредоточить в рамках этих центров технические и преподавательские ресурсы и использовать эти ресурсы в интересах тех вузов, которые находятся в соответствующем федеральном округе. К сожалению, Министерство образования и науки на вот это решение пока не ответило с

прошлого года. Но, видимо, какое-то грандиозное решение готовится, мы об этом не знаем.

Направления деятельности таких центров сформулированы, они обсуждены. И есть варианты создания таких центров. Спасибо за внимание.

Б.Б. ЖАМСУЕВ

Уважаемые коллеги, есть настаивающие что-то еще дополнить к тем вопросам, которые уже мы сегодня освещали, обсуждали? Пожалуйста. Представьтесь.

А.Е. КОЛУПОВ

Советник генерального директора Центрального научно-исследовательского института связи.

Вот здесь много сегодня коллеги концептуально говорили. Если можно, мою презентацию очень быстро запустить, я буквально две секунды эту актуальность прокомментирую, насколько это важно.

Б.Б. ЖАМСУЕВ

Еще раз представьтесь, пожалуйста.

А.Е. КОЛУПОВ

Советник генерального директора Центрального научно-исследовательского института связи Колупов Андрей Егорович. ЦНИИС.

Можно сразу второй слайд? В настоящее время активно развивается единая сеть передачи данных страны. Это идет в рамках развития программы "Информационное общество 2011—2020". Это Постановление Правительства 1240 от 2014 года. Этот проект уже реализуется. В рамках этого проекта (на слайде коротко указаны основные вехи этого проекта) есть такое понятие, как мониторинг единой сети передачи данных. И на магистральных узлах Ростелекома уже сейчас устанавливается некое типовое

оборудование мониторинга, которое предназначено соответственно за выполнение требований этой системы передачи данных органам власти.

Что мы видим, исходя из этого? Вот у нас сеть связи страны сейчас – единая, взаимоувязанная. Исторически так сложилось, что развивалось все хаотически, по региональному принципу. И это как не удивительно, прекрасно. Потому что нет единой точки отказа, у нас в каждом регионе своя система: где-то Huawei, где-то Juniper, где-то Cisco. Нет одной точки, где можно нажать и чтобы все сломалось. И это по факту так. Это раз.

Второе, что неочевидно. Поскольку сеть связи страны раньше жестко под контролем государства развертывалась, функционировала, то топология этой сети до настоящего времени не является публичной. Никто не знает. Я имею в виду в публичной информации. *(Оживление в зале.)*

ек

Но я бы так не сказал, Министерство обороны хорошо знает это.

С МЕСТА

(Говорит далеко от микрофона. Не слышно.)

А.Е. КОЛУПОВ

Я не об этом хотел сказать. О связанности наших объектов никто не знает. Никто не знает, какое детально оборудование стоит. Таким образом, уничтожить все связи страны, как ни странно, сейчас очень сложно.

При этом возникают некоторые угрозы. Я на слайде показал. Сейчас в рамках этого проекта... мониторинг ЕСПГ на все магистральные узлы связи на первом этапе, на втором этапе. И на сами непосредственно объекты органов власти (а таких объектов

планируется 50 тысяч в нашей стране) устанавливается некое типовое оборудование, которое по сути должно мониторить состояние этих каналов связи, услуг сети передачи данных. Тут возникают, как минимум, две угрозы. Первая угроза – съем информации, топология сети. Вторая угроза – получение информации об объемах информации (тавтология), которая циркулирует в этой сети. По количеству информации, приходящей на объект, можно понять статус этого объекта, его важность в системе государственного управления. Это на первом этапе. А на втором этапе это оборудование, при воздействии непосредственно с какой-то единой точки, если есть такая возможность и есть функция "недекларируемая возможность" или какая-то программная уязвимость, просто это оборудование может взять и положить всю сеть связи государства. Вот такая не совсем очевидная штука.

Как с этим бороться? Есть доктрина соответственно информационной безопасности, там эти угрозы уже написаны. Там же есть раздел, где написано, как с этим бороться. Просто время очень сжато, не буду долго говорить.

А дальше модель соответственно любого системного мониторинга, она представляет собой железо, операционную систему и некое СПО. В нижней части слайда указано, коллеги, что сейчас требование метрологически обеспечено и для применения на сети связи общего пользования. А вот в серединке оранжевым – нет таких требований, а это значит только одно, что сейчас в этом СПО и соответственно в той операционной системе, которая там, может быть все, что угодно. И как только мы развернем это на всю сеть связи страны, я уже сказал, что произойдет.

Какие пути? Пути очень простые. Коллеги прекрасно сказали о законе о критической информационной инфраструктуре (я сейчас

остановлюсь) – это готовый способ решения этой проблемы. Что произойдет? Мы определим, что объекты СПД – критические важные объекты, мы скажем, что соответственно это так и есть, мы скажем, что у каждого критического важного объекта есть своя категория опасности, и мы установим требования для каждого такого объекта. Тем самым мы выставим абсолютно конкретные требования и защитим сеть связи страны от этих вещей.

А на первом этапе можно было бы сделать очень просто, можно было бы рекомендовать использовать при таких масштабных проектах информационных сертифицированные операционные системы (их достаточное количество в нашей стране, сертифицированные коллегами из ФСБ и ФСТЭК России, из Министерства обороны России) и сертифицированные специальные программные средства. Вот, собственно говоря, что я хотел сказать.

Поэтому если такой закон будет принят, то это всем нам поможет спокойно спать. Спасибо, коллеги.

Н.А. МАХУТОВ(?)

Разрешите?

Б.Б. ЖАМСУЕВ

Да-да, Николай Андреевич(?), пожалуйста.

Н.А. МАХУТОВ(?)

За закон спасибо. А вообще какие-то требования по информационной безопасности в ЕСПД существуют?

А.Е. КОЛУПОВ

Строчка одна в приказе 55, я могу показать. Вот этот документ.

Н.А. МАХУТОВ(?)

Одна строчка про это? Все требования?

А.Е. КОЛУПОВ

Нет, я же поэтому и говорю, я поэтому и сказал.

Н.А. МАХУТОВ(?)

А сеть существует и работает? Правильно я понимаю? *(Оживление в зале.)*

Б.Б. ЖАМСУЕВ

Пожалуйста, вопрос – ответ.

А.Е. КОЛУПОВ

Я отвечу на Ваш вопрос. Только начато развертывание. В прошлом году пять субъектов федеральных органов исполнительной власти включены. В этом году планируется восемь. То есть она не развернута. Мониторинг ЕСПГ развернут сейчас на 133 объектах на оборудовании, к сожалению, импортного лендера. Этот проект только начинается.

Н.А. МАХУТОВ(?)

Но там только импортное оборудование, насколько я пониманию, в "Ростелекоме"? Правильно? Там отечественного вообще нет.

А.Е. КОЛУПОВ

Правильно. Но я же Вам...

Н.А. МАХУТОВ(?)

Хорошо. И еще третье я хочу сказать. Проект изменения в федеральный закон "О связи" существовал, и это вещь сейчас не такая особо закрытая. Но ведь принято решение о создании некой интегрированной сети связи, которая должна быть отделена от сети связи полностью.

А.Е. КОЛУПОВ

Все правильно. Но Вы говорите о неком будущем...

Н.А. МАХУТОВ(?)

Почему "будущем"? Системный проект готов.

ек

Я понимаю, проект ЕСПД отличается двумя вещами, которые здесь любой из специалистов подтвердит, что сеть общего пользования не устойчива к компьютерным атакам и никогда не будет устойчива вообще. Как можно создать на базе сети связи общего пользования систему, устойчивую к компьютерным атакам? Есть аксиома. Глубокая интеграция...

А.Е. КОЛУПОВ

Министерство связи говорит о том, что есть некий переходный период между тем, что Вы сказали, и данностью сейчас. Они говорят, что модель ЕСПД – это некий переходный период. А я сказал только одно, что да действительно сеть связи страны сейчас разрозненна и кусочки некоего "Телекома". А сейчас риск в чем? Угроза в чем? Что в эти разрозненные кусочки мы ставим абсолютно одинаковую железку, на которой можно нажать кнопочку, и вся сеть связи разрозненная ляжет.

А то, что Вы говорите, – это следующий шаг.

Б.Б. ЖАМСУЕВ

Спасибо большое.

Если есть еще вопросы, можно побеседовать после окончания нашего "круглого стола", выяснить все тонкости и нюансы.

Уважаемые коллеги, я хочу выразить большую благодарность всем, кто выступил, за то, что вы все подготовились, пришли с конкретными предложениями и проблемами, которые существуют, и представителям органов власти, и науки, и разработчикам.

Я скажу по решению. У нас есть такая практика по "круглым столам", естественно, все ваши выступления будут обобщены нашим аппаратом. Продолжим мониторить в данной области. Я считаю, что подтвердил и наш последний выступающий, что одним из краеугольных вопросов обеспечения в законодательном плане

безопасности критической информационной инфраструктуры Российской Федерации является тот законопроект, который подготовлен Федеральной службой безопасности. Я надеюсь на то, что мы общими усилиями... Это мы тоже должны отразить в нашем решении, что мы поддерживаем данный законопроект и говорим о необходимости скорейшего рассмотрения в Федеральном Собрании Российской Федерации, чтобы Правительством Российской Федерации соответствующим образом его внесло.

Я прошу Вячеслава Михайловича, как основного докладчика подключиться, руководить работой аппарата по обобщению всех замечаний и предложений, чтобы они легли в наш итоговый документ, а потом уже на комитете рассмотрим этот документ и разошлем в соответствующие структуры, органы государственной власти и всем, кто принимал участие в нашем "круглом столе".

Я еще раз повторяю, что мы будем мониторить это очень важное направление. Еще раз мы убеждаемся в том, что оно очень актуально, оно важно с точки зрения обеспечения национальной безопасности нашей страны.

Всем большое спасибо. Успехов и удачи!
