

**К выступлению на пленарном заседании Инфофорума-Евразия  
10 июня 2010 года, 10:00, здание Правительства Москвы**

Уважаемые участники форума!

От имени Оргкомитета поздравляю вас с открытием 6-го Евразийского форума «Международные проблемы информационного взаимодействия и информационной безопасности».

На нашем форуме присутствуют представители 12 стран евразийского пространства, что сделает наши обсуждения более многогранными и целостными, позволит нам лучше понять друг друга и попытаться найти эффективные решения общих проблем.

Думаю, все вы согласитесь: мы живем в интересное время! Время стремительного изменения технологий, формаций, расстановок политических сил. Очевидно, что в этом мире выживет тот, кто максимально подчинит новые технологии интересам человека, целям развития страны, укрепления стабильности в мире. Поэтому объявленный Президентом России Д.А.Медведевым курс на модернизацию, в том числе модернизацию мышления, - не просто лозунг. Это фактор выживания.

В развитии новых информационных технологий мы наблюдаем выраженные отрицательные и положительные тенденции, которые, как мне кажется, не только дополняют, но и обуславливают друг друга.

Сохраняются негативные последствия финансового кризиса, который особенно сказался на лидерах отрасли, работа большинства технологичных компаний была дестабилизирована или даже полностью парализована: [банкротство компании Nortel](#); компания Microsoft впервые за последние 20 лет опубликовала в 2009 году [убыточный отчет](#), вслед за которым последовали массовые сокращения; корпорация Intel [закрывает пять фабрик](#) по производству микросхем и сокращении около 6 тыс. рабочих мест; [AMD в связи с ухудшением финансового положения сократила десятую часть сотрудников](#);

увольнения постигли даже сотрудников компании Apple. В России также существенно сократились инвестиции в отрасль.

На этом фоне увеличились масштабы компьютерной преступности (может быть за исключением спама), в России - на 25%. Киберпреступность приобрела более сложный технологичный характер, эксперты подтверждают ее организованность и коммерциализацию. Можно говорить о существовании рынка киберпреступности, причем его «участники» стремятся свой бизнес легализовать, используя различные серые схемы.

С расширением сфер и масштабов применения инфокоммуникационных технологий, увеличения количества пользователей Интернета в мире и в России (у нас это уже каждый третий), по оценкам экспертов, снизился уровень компьютерной грамотности, что также способствует росту преступности.

Эти негативные тенденции заставили активизироваться власть, гражданское общество и бизнес.

Можно отметить ряд серьезных шагов и решений органов государственной власти, направленных на реализацию Стратегии развития информационного общества в России, создание электронного правительства, предоставление государственных и муниципальных услуг населению в электронном виде, организацию электронного документооборота и эффективного межведомственного информационного взаимодействия.

Активизировалось общество, демонстрирующее полезные общегражданские и отраслевые инициативы в сфере защиты прав человека в информационном пространстве, развития киберкультуры и медиаобразования, профилактики киберпреступности.

Наконец, мы отмечаем примеры эффективного взаимодействия общества и власти в выработке государственных решений и формировании взаимовыгодного партнерства.

Эти положительные тенденции свидетельствуют о процессах «модернизации мышления», об осознании масштабов угроз, которые несет широкое проникновение в нашу жизнь инфокоммуникационных технологий, об

осознании личной ответственности за происходящее и понимании необходимости консолидации интеллектуального потенциала отрасли для взаимодействия с властными структурами.

Большинство, но, к сожалению, не все еще понимают, что безопасность, в том числе и информационная, начинается с себя.

Защити личный компьютер, задумайся о защите своих персональных данных и своей интеллектуальной собственности.

Защити семейный компьютер, задумайся о том, как он используется детьми в твое отсутствие, научи их хотя бы азам компьютерной культуры и кибербезопасности, установи «родительский контроль».

Руководители предприятий уже начинают осознавать, что защита от вирусов не спасет бизнес, существуют и более страшные и изощренные угрозы. Бессмысленно латать дыры, надо формировать продуманную политику информационной безопасности. При этом, внедряя новые технологии, не забывать, что самое уязвимое место в обеспечении безопасности – человек.

Государство у нас большое и не все надо делать на самом высоком уровне. Есть интересные региональные властные и общественные инициативы. Есть регионы, где реализуются серьезные инновационные проекты в сфере ИКТ. 20 апреля в рамках Второй Всероссийской конференции **«Электронный документооборот – требование времени»** мы наградили представителей Нижегородской и Самарской областей, Пермского края, Республики Татарстан, города Магнитогорска Челябинской области за лучшие решения по созданию систем коллективной обработки информации на федеральном, региональном и муниципальном уровнях. Эта конференция, кстати, продемонстрировала высокий интерес к региональным инициативам. Вместе с тем, мы понимаем, что проблемы информационной безопасности и применения инфокоммуникационных технологий для обеспечения безопасности человека в среде его проживания – гораздо шире. Поэтому было принято решение провести в рамках Евразийского форума первую конференцию **«Безопасный город»**. Она состоится завтра и пока будет касаться транспортных проблем,

решение которых для мегаполисов является сверхактуальным, а также будут обсуждаться вопросы управления безопасностью города с использованием ситуационных центров.

Хотим мы этого или не хотим, но Интернет стал неотъемлемым элементом нашей жизни, поэтому проблемы безопасного Интернета уже традиционно рассматриваются на мероприятиях Инфофорума. Мы обсуждали технические и юридические аспекты, а сегодня во второй половине дня предлагаем послушать участников общественных инициативах, направленных на защиту детей в Интернете, и обсудить, что надо делать для повышения социальной активности пользователей Интернета, для пресечения деятельности в Сети асоциальных субъектов.

В феврале были подведены итоги впервые проведенного в России Года безопасного Интернета. «Год безопасного Интернета» несомненно, позволил нам продвинуться вперед как в вопросах понимания стоящих проблем, связанных с использованием глобальной сети, так и в поиске эффективных решений. Удалось также аккумулировать потенциал значительного числа организаций, инициативно проявивших заинтересованность в «очищении» Интернета.

Год безопасного Интернета был насыщен мероприятиями, дал толчок интересным дискуссиям, но, главное, – начали реализовываться конкретные проекты. Появились специализированные порталы, горячие линии, проведены исследования и опросы, разработаны методики и рекомендации. В целом, оценивая результаты этой работы положительно, мы отдаём себе отчёт, что находимся лишь в начале сложного пути.

Опыт, приобретённый в «Год безопасного Интернета» необходимо реализовать в новых значимых проектах, привлекая к ним внимание всего общества: родителей, преподавателей, членов общественных и религиозных организаций, бизнес-сообщества, средств массовой информации. Гражданское общество может и должно предлагать власти организационные, технологические и законодательные решения, направленные на обеспечение

безопасности законопослушных пользователей Интернета, и в первую очередь, наиболее уязвимой категории пользователей - детей и юношества.

В связи с этой темой я хотел бы поздравить нас всех с получением Российской Федерацией нового русскоязычного домена **.РФ**. Этому событию был посвящен Первый российский форум по управлению Интернетом, который состоялся 13-14 мая. В рамках состоявшихся дискуссий звучали разные мнения по поводу перспектив использования этого домена. Как говорится, проживем-увидим. Мне кажется важным предложение участников форума, обращенное к национальным регуляторам, использовать, единый алфавит для отображения контактных данных владельцев доменов в целях обеспечения информационной безопасности и совместимости.

Говоря об Интернете и развитии информационного общества в нашей стране, нельзя не отдавать себе отчет в том, что мы живем в глобальном обществе, соответственно упомянутые угрозы носят глобальный характер и бороться с ними надо, объединяя усилия всех стран. Соответствующие процессы идут, в них участвуют как властные структуры, так и структуры гражданского общества. Например, негосударственные организации объединяются в сеть «горячих линий» по борьбе с детской порнографией (ИННОРТ - ИНХОП).

Россия инициативно участвует в формировании системы международной информационной безопасности в формате ООН, Евросоюза, Шанхайской организации сотрудничества, Организации договора о коллективной безопасности (ОДКБ), Союза независимых государств и других. Несмотря на сложности переговорного процесса определенные положительные результаты достигнуты. Но проблемы, конечно, остаются. Сегодня они будут обсуждаться представителями стран постсоветского пространства на заседании, организованном при участии ОДКБ.

Необходимость обеспечения международной информационной безопасности не снимает с нас обязанности формировать и реализовывать внутреннюю политику информационной безопасности. Пример подают США,

где в последние 2 года активно и планомерно разворачивается Комплексная национальная инициатива кибербезопасности, на реализацию которой выделяются беспрецедентные средства, создаются необходимые организационные структуры и механизмы управления их работой.

К сожалению, подобной программы в России нет, а в деятельности органов государственной власти недостает координации и научно-методического обеспечения. Даже в таком, более-менее понятном вопросе как создание официальных сайтов органов государственной власти (это первый этап формирования электронного правительства). Ведомства самостоятельно определяют требования к этим сайтам, поэтому затраты на создание и развитие сайта доходят до 11 млн. рублей (между прочим из государственного бюджета) при том, что по оценкам специалистов разработка даже крупного портала «с излишествами» обойдется существенно дешевле. А ведь впереди следующие этапы реализации электронного правительства! Вызывает большую озабоченность и явно не способствует укреплению безопасности тот факт, что многие официальные сайты органов государственной власти регистрируются на физических лиц и на коммерческие организации, реально располагаются за пределами России. Видимо, пора задуматься над оптимизацией государственных расходов, формированием единых требований, единой методической базы и технологического обеспечения.

Эти и иные вопросы обеспечения безопасности при осуществлении электронных госуслуг будут обсуждаться на Парламентских слушаниях В Государственной Думе 28 июня. Приглашаю принять участие.

В заключении хочу пожелать всем участникам Инфофорума-Евразия интересных встреч и обсуждений, слушать друг друга, использовать любую возможность поддержки и продвижения полезных для общества, для страны инициатив. На площадках Инфофорума традиционно встречаются представители органов государственной власти, бизнеса, науки и высшей школы, гражданского общества. Используйте эту возможность максимально продуктивно.