

There are no translations available.

## Глобальные аспекты культуры кибербезопасности: взгляд из России



## ГЛОБАЛЬНЫЕ АСПЕКТЫ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ: ВЗГЛЯД ИЗ РОССИИ

– Анатолий Иванович, проблемы, связанные с кибербезопасностью, решаются на самом высоком политическом уровне. Чем, на Ваш взгляд, вызвана озабоченность мирового сообщества и России этой проблематикой?

– Планета охвачена беспрецедентной информационной революцией, которая, по мнению многих экспертов, стала локомотивом и нервом глобализации. Наряду с несомненным позитивом ее феномен несет в себе принципиально новые глобальные вызовы и угрозы.

Учитывая это обстоятельство, Генеральная Ассамблея ООН 17 марта 2010 года приняла резолюцию (по докладу Второго комитета A/64/422/Add.3) «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур». Данная резолюция стала развитием ранее принятых резолюций (55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о борьбе с преступным использованием информационных технологий, 57/239 от 20 декабря 2002 года о создании глобальной культуры кибербезопасности и 58/199 от 23 декабря 2003 года о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур).

При этом данная проблематика тесно переплетается с резолюциями ООН о достижениях в области информационных технологий в контексте международной безопасности. Впервые этот вопрос был внесен в ООН по инициативе России еще в 1998 году (53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года и 64/25 от 14 января 2009 года).

Озабоченность России и мирового сообщества данной проблемой отнюдь не случайна. Наряду с сотнями тысяч разновидностей вирусов, квазивирусов, шпионских программ и, казалось бы, безобидных спама, по



Интервью члена оргкомитета «ИНФОФОРУМ», Председателя Отделения Российской академии естественных наук «Информационная глобализация», доктора исторических наук, профессора, Чрезвычайного и полномочного Посланника Российской Федерации **Анатолия Ивановича СМЕРНОВА** журналу «Безопасность России»

данным ЦРУ, более 120 стран мира разрабатывают принципиально новый вид оружия массового поражения – информационного.

Заметными вехами в решении столь важной для судеб мира проблемы стали итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), состоявшейся 10–12

декабря 2003 года в Женеве и 16–18 ноября 2005 года в Тунисе под эгидой ООН и ИМСЗ.

Признавая растущий вклад ИКТ во все сферы социума, ООН призвала правительства, деловые круги, организации, индивидуальных владельцев и пользователей ИКТ к ответственности за обеспечение безопасности и принятие над-

лежащих мер для ее укрепления. Особое место в резолюции уделено важности мандата Форума по вопросам управления Интернетом (в настоящее время проходит в пятый раз в Литве): «Все правительства должны иметь равные задачи и обязанности в сфере управления Интернетом на международной основе и обеспечения стабильности, безопасности и непрерывности Интернета».

В резолюции также отмечено, что угрозы надежному функционированию важнейшей инфраструктур ИКТ и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия.

В силу этого в резолюции подчеркнута, что национальные усилия должны подкрепляться обменом информацией и взаимодействием на международном уровне с тем, чтобы можно было эффективно противостоять новым угрозам, приобретающим все более транснациональный характер.

В этом контексте подготовленный Международный союзом электросвязи в 2009 году доклад об обеспечении защищенности ИКТ и передовой практике в области формирования культуры кибербезопасности основное внимание уделяет всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободу слова, свободу передачи информации и надлежащие правовые процедуры.

С учетом вышесказанного в резолюции ООН предлагается государствам-членам использовать инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур, призванный помочь им выявить области, в которых требуется принятие дополнительных мер, в целях повышения глобальной культуры кибербезопасности. Кроме того, рекомендовано государствам-членам и соответствующим региональным и международным организациям, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, поделиться сведениями о передовой практике и мерах, которые могли бы помочь другим странам в обеспечении кибербезопасности.

– Расскажите о роли России в решении этой глобальной проблемы.

– Как уже отмечалось выше, Россия инициативно и ответственно относится к данной проблематике. Наряду с активным участием в подготовке и подписании Окнаской карты ГИО (2000 год), документов ВВУЮ (Женева, Тунис), форумов по вопросам управления Интернетом и др. в России действуют Доктрина информационной

безопасности (2000 год), ФЦП «Электронная Россия» (2002–2010 годы), Стратегия развития информационного общества в России (2008 год), Концепция формирования в Российской Федерации электронного правительства до 2010 года (2008 год), а также ряд федеральных законов.

Одним из важных документов последнего времени (май 2009 года) стала Стратегия национальной безопасности Российской Федерации до 2020 года. Ее пункт 109 гласит, что «угрозы информационной безопасности кода реализации настоящей Стратегии предотвращаются за счет совершенствования безопасности функционирования ИКТ систем критически важных объектов инфраструктуры и объектов повышенной опасности в России, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд, системы обеспечения национальной безопасности».

В этом контексте в России уточнены роль и обязанности заинтересованных сторон, стратегические процессы и участие, сотрудничество между государственным и частным секторами, деятельность в связи с инцидентами и восстановление после сбоев, а также правовые нормы и формирование глобальной культуры кибербезопасности.

Заметный вклад в столь важный процесс вносят институты гражданского общества, в т.ч. некоммерческое партнерство «Инфофорум».

В России разработано необходимое законодательство для расследования киберпреступлений и преследования лиц, виновных в их совершении, с учетом существующих механизмов, в т.ч. резолюций 55/63 и 56/121 Генеральной Ассамблеи о борьбе с преступным использованием ИКТ.

Что касается Конвенции Совета Европы о киберпреступности, то у российской стороны имеется особое отношение к ней. Данная Конвенция устанавливает правовые рамки лишь для борьбы с преступлениями против компьютерных систем или с «традиционными» преступлениями (отмывание денег, мошенничество, вымогательство), совершаемыми с использованием компьютерных систем. К сожалению, в Конвенции отсутствует понятие «кибертерроризм».

Россия не подписала Киберконвенцию, т.к. в любом случае у российской стороны остаются серьезные озабоченности по ее пункту «а»-статья 32, который в нынешней редакции фактически позволяет несанкционированный доступ одного государства к компьютерным данным другого государства. Российский взгляд разделяют многие государства, в т.ч. в формате СНГ,

ШОС, БРИК, ОДКБ и других международных и региональных организаций. В силу этого Россия выступает за подготовку универсального документа на сей счет под эгидой ООН.

– По каким сценариям ожидается развитие глобальной Сети в ближайшие несколько лет?

– С учетом стремительного процесса интертизации планеты эксперты Cisco и Monitor Group прогнозируют, что в течение ближайших 15 лет Интернет будет развиваться по одному из следующих сценариев.

Согласно их отчету *The Evolving Internet* («Растущий Интернет») первый сценарий называется *Fluid frontiers* («Жидкие границы»). Он описывает мир, в котором Интернет будет распространен еще больше, а его роль будет являться критически важной. В этом случае ожидается дальнейший рост мирового Интернет-предпринимательства вместе с ужесточением конкуренции в этой сфере, которая приведет к появлению огромного числа новых технологий.

Второй сценарий, *Insulate growth* («Небезопасное развитие»), описывает возможность того, что пользователи и организации столкнутся с ухудшением безопасности, страдая от бесчисленного количества кибератак. В этом случае аналитики ожидают, что появятся более безопасные альтернативы Интернету, однако они будут платными и дорогостоящими.

Третий вариант, *Short of the promise* («Не оправдать ожидания»), предполагает, что экономический застой во многих странах отразится и на развитии Интернета. В этом случае рецессия и протекционистская политика сильно замедлят рост Сети и появление инноваций.

Четвертый вариант предполагает развитие событий, в рамках которого Интернет станет жертвой собственного успеха: *Bursting at the seams* («Разрываясь по швам»). В этом случае спрос на различные веб-сервисы окажется так велик, что ИКТ не смогут справиться с объемами трафика.

Авторы предсказывают, что система управления Интернетом в будущем не сильно изменится, хотя тарифов для оплаты станет гораздо больше. QWERTY-клавиатура перестанет быть основным устройством управления, а пользователи, знакомые с Интернетом с детства, будут относиться к этой среде совсем иначе, чем нынешние. Прогнозируется, что основной рост в течение следующих 15 лет придется на развивающиеся страны, где доступ к нему пока невелик.

Все вышесказанное сценарии развития Интернета еще раз подчеркивают актуальность обеспечения культуры кибербезопасности, за которую последовательно выступает Россия. ■

[Скачать статью ...](#)