Актуальные вопросы стратегии кибербезопасности:
соотношение российской и глобальной сетей

Актуальность международного форума по проблемам кибербезопасности весьма значительна, поскольку в жизни современного общества возрастающая роль информационных коммуникаций и соответствующих технологий фактически превращает институт Интернета в мощный геополитический фактор, в эффективный механизм глобального управления социальными и экономическими процессами, является достижением человечества и одновременно вызовом национальным интересам.

Глобальная информационная сеть – есть новое технологическое достижение человечества, стоит в ряду таких человеческих открытий, как радио, телефон и телевидение, обеспечивает новое прорывное развитие личности, общества и государства. В этой системе информационных коммуникаций происходит ускорение процессов межчеловеческих коммуникаций, стирание расстояний и границ, появляется высокая степень доступа к значительным массивам информации.

Современные информационно-коммуникационные технологии (ИКТ) выводят на новый уровень проблему детского воспитания, среднего и высшего образования, научно-исследовательского развития, ставят задачу подготовки высококвалифицированных кадров – специалистов в области программирования, криптографии, системного администрирования и нестандартного решения.

Достижения Интернета становятся очевидными и неоспоримыми явлениями современной жизни. Все больше и больше людей охвачены данной технологической системой. Сегодня трудно представить цивилизованное развитие, гармонизацию личности, демократизацию общества, гарантированное обеспечение прав и свобод граждан без Интернета и без электронного правительства. Вместе с тем, каждое научное открытие, каждая новая коммуникационная технология приводит к ситуации возникновения проблем защиты и безопасности субъектов и объектов данного процесса.

Современный мир столкнулся с такой проблемой, когда открытость информационной среды, стремительное развитие Интернета, усложнение компьютерных технологий, появление различного рода компьютерных сетей приводит к ситуации незащищенности личности, общества и государства от деструктивного и подрывного воздействия со стороны преступных, радикальных, экстремистских, политически опасных и вредных сил. На повестку дня выходит актуальная проблема повышения информационной безопасности локальных, национальных и международных систем коммуникаций. Не секрет, что определенные политические и преступные силы пыта-

ются использовать достижения Интернета, современных информационно-коммуникативных технологий в ущерб национальным интересам и безопасности России и других государств.

Фактически сегодня на Интернет завязаны не только социальные коммуникации между людьми, но и целые экономические и финансовые программы, системы обороны и правительственные порталы, бизнес и гражданские институты. Через Интернет определенные центры и подрывные силы способны и организуют новые технологии психологической и информационной войны, способные подавить волю человека, дезориентировать широкие социальные слои общества, вызвать локальную и глобальную дестабилизацию. Таким проявлением выступают экстремистские сайты, распространение нелегального контента (то есть запрещенной информации типа детской порнографии, идеологии терроризма, разработки оружия массового поражения и т.д.).

Технология Интернета создавалась интеллектуальным усилием научных кадров, а получило развитие и массовое внедрение благодаря политическим интересам определенных сил. На Интернет завязано всё: всемирная телефония, биржа, финансовые торги, розничная продажа, социальные контакты, практически все коммуникации. Признанным фактом можно считать, что сегодня никто не может отстраниться и (или) отказаться от применения Интернета.

Однако Интернет все больше и больше становится прообразом нового империализма, превращается в глобальную систему мирового контроля и управления, создает для одной силы возможность влиять на другие силы и процессы. Интернет практически превращается в реальный геополитический, геоэкономический и геостратегический фактор. Глобальная информационная паутина позволяет обеспечивать несанкционированный доступ к огромному массиву данных, влиять на них и разрушать.

Неслучайно откровения бывшего системного администратора ЦРУ и АНБ США Эдварда Сноудена вызвали широкую и болезненную международную реакцию на действия американских спецслужб в информационном пространстве, которые по существу создали глобальную систему электронного шпионажа, взлома практически всех используемых в сети Интернет стандартов криптографии, перехвата и обработки личных данных пользователей разных стран мира: СМС-сообщений, телефонных разговоров, переписки в социальных сетях и электронной почте. Разоблачения бывшего сотрудника американских спецслужб привели к серьезным проблемам международного порядка, вынудили президента США Б. Обама заявить о реформе АНБ и исключении в последующей практике национальной разведки контроль над перепиской и общением руководителей дружественных стран. Правда, что делать с лидерами госу-

дарств, которые не попадают в реестр союзников США, президент Б. Обама ничего не сказал.

Таким образом, актуализируется проблема стратегии обеспечения локальной, национальной и международной кибербезопасности. В современном мире развитие киберпространства, информационно-коммуникативных технологий находится в прямой зависимости от ряда факторов, включая от:

– детского воспитания;

– национального образования (уровня развитости средней и высшей школы);

– развитости науки (включая таких отраслей, как программирование, программные и аппаратные шифровальные комплексы, криптография, космическая отрасль);

– производства (создания и массового выпуска национальных электронных машин – компьютеров);

– национального и международного законодательства (повышения административной и уголовной ответственности в отношении хакеров, распространителей разрушительных вирусов и нелегальных контентов);

– правоохранительной, оборонительной и контрразведывательной системы.

Не секрет, что для борьбы с теми же хакерами и распространителями нелегальных контентов в системе правоохранительных органов должны создаваться специализированные подразделения для их выявления, предупреждения и пресечения незаконной деятельности.

Для защиты стратегических систем обороны, ядерного потенциала государства от несанкционированного доступа и разрушительных последствий актуализируется задача обеспечения вооруженных сил соответствующим командованием и формированием системы кибероборонны.

Для борьбы с разведывательно-подрывной деятельностью иностранных спецслужб в сфере информационных коммуникаций также необходимы специализированные подразделения (включая отдельные спецслужбы), которые могли бы обеспечивать контрразведывательный режим безопасности в киберпространстве. Неслучайно в системе спецслужб ряда государств на рубеже XX–XXI вв. стали создаваться специализированные подразделения в сфере кибербезопасности. В той же Турции, например, создана Национальная организация информационной безопасности (НОИБ), одной из задач которой выступает блокирование иностранных сайтов, где освещается тема геноцида армян в невыгодном для Турции ключе.

Укрепление национальной системы кибербезопасности во многом зависит от способности формирования национальной и локальной системы киберпространства,

включая интеллектуальное развитие через соответствующее детское воспитание, среднее и высшее образование, высокий уровень научно-исследовательского поиска, подготовку сообщества высококвалифицированных кадров в области системного программирования, криптографии, вирусологии, космической инженерии.

Здесь также необходима совершенная правовая база, позволяющая правоохранительной и контрразведывательной системе государства ограничивать, а при необходимости блокировать доступ к определенным сайтам и информационным системам, которые оказывают деструктивное и подрывное воздействие на киберпространство России.

Однако, как только в отечественных СМИ появляется информация о целесообразности какого-либо ограничения в системе Интернет (ограничения, блокирования или закрытия сайтов экстремистского и иного вредного толка), определенный корпус журналистов и их лоббисты поднимают громкие пропагандистские акции со стандартными обвинениями спецслужб и властей в попытках закрыть доступ к Интернету, нарушить права человека, зажать демократию и т.д. Такая атмосфера не способствует развитию системы кибербезопасности. Необходимо контрпропагандистское сопровождение подобных решений и правовое закрепление ответственности физических и юридических сил за попытку сопротивления и саботажа государственной политике повышения защиты национального киберпространства.

К сожалению, по всему миру выход в глобальную сеть Интернета зачастую происходит через спутник JPS, что автоматически ставит под контроль тех же США киберпространство целых стран. *В России сегодня ставится задача перехода на систему спутникового обеспечения Глонас. И эту традицию нужно активно развивать с целью формирования национальной системы Runet.*

В практике таких государств, как Северная Корея и Китай, уже функционируют различные системы защиты киберпространства, от тотально закрытой в северокорейском случае до сочетания национальной сети с санкционированным (контрольным) выходом в глобальную информационную сеть в китайском варианте. Этот опыт необходимо учитывать в своей национальной практике с целью создания более-менее обособленных систем ИТК, которые позволят в форс-можорных условиях работать локально и надежно, ограничивать и контролировать выход в глобальную сеть.

В рамках решения данной концептуальной задачи важно развивать соответствующее детское воспитание в плане культивации у малышей способности к нестандартному решению, развития логики и аналитического склада мышления. Видимо, в этой связи целесообразно восстановить в системе детского развития прежние кон-

структоры, исключить модульные системы конструирования, что не позволяет развивать личную логику, думать и решать маленькие задачи. В системе начального школьного образования, возможно, следует исключить использование компьютера, особенно по таким предметам как математика, чтение, рисование, труд.

В плане развития национальной высшей школы следует укреплять и развивать специализированные вузы по подготовке высококвалифицированных специалистов в области космической инженерии (например, изготовления нового поколения спутников), системного программирования, шифрования (криптографии), вирусологии и защитных программных систем, создания и серийного производства современных электронных машин (компьютеров).

Наконец, одним из ключевых элементов повышения кибербезопасности национальной информационной сети является периодический регламент компьютерных систем в государственных и коммерческих структурах по установленным общим и особенным техническим и правовым правилам и нормам.

Формирование эффективной системы кибербезопасности и локальной национальной информационной сети может позволить лишить монопольного господства в глобальной сети со стороны какой-либо силы, перевести проблему стратегии международной кибербезопасности в повестку актуальной мировой дипломатии и международного права. Это будет способствовать принятию нового и адекватного цивилизованным запросам международного права, регламентирующее и регулирующее глобальное информационное пространство, исключающее вмешательство во внутренние дела иностранного государства и распространение запрещенной информации, обеспечивающее защиту детей и подрастающего поколения от деструктивного воздействия сайтов экстремистского толка, ксенофобии, национализма, наркомании, проституции и т.д.

Полагаю, что высказанные предложения будут способствовать развитию процесса поиска совместных путей и решений повышения уровня кибербезопасности национальной и глобальной сети.

Член Совета при Президенте Российской Федерации
по межнациональным отношениям,
президент «Союза армян России» **А.А. Абрамян**