Угрозы информационной безопасности России
и вопросы противодействия

Тема нашего заседания весьма актуальна, поскольку в жизни современного общества постоянно возрастает роль информационных коммуникаций и соответствующих технологий.

Это, с одной стороны, способствует гармоничному росту личности, является свидетельством высокого уровня развития общества и государства, позволяет более полно отражать конституционные права граждан. Но, с другой стороны, открытость информационной среды, стремительное развитие Интернета, усложнение компьютерных технологий, появление различного рода компьютерных сетей (социальных, правительственных, научных, корпоративных, домашних и др.) приводит к ситуации, когда определенные политические и преступные силы пытаются использовать достижения Интернета, современных информационно-коммуникативных технологий в ущерб национальным интересам и безопасности России.

В частности, нередко можно встретить активное использование компьютерных сетей для распространения заведомо ложной информации (так называемой дезинформации), разжигания расовой, национальной и религиозной ненависти и вражды, проведения кибервойн (кибертерроризма, кибердиверсий, кибершпионажа).

Наиболее очевидными угрозами становится использование Интернет-сетей (например, Facebook», «Skype», «YouTube», «Tweeter») для возбуждения протестных настроений в обществе, организации активного движения Сопротивления и массовых несанкционированных шествий для свержения правящих режимов, так называемые цветные революции по типу Украины, Грузии, Кыргызстана и стран Арабского Востока.

В современном мире появляются технологические возможности по созданию и распространению в информационной сети боевых компьютерных вирусов, направленных на целенаправленное подавление и разрушение отдельных программ, похищение банка данных, внесение системной дестабилизации в социальные отношения.

Все это свидетельствует о появлении новых угроз интересам безопасности общества и государства в информационной сфере, что требует постоянного совершенствования системы защиты киберпространства, включая развитие правовых норм, активизацию международного сотрудничества, взаимодействия органов власти, гражданского общества и бизнеса, а также обеспечение научно-технологического роста. Использование Интернет-технологий в практике преступных организаций и разведывательно-

подрывной деятельности приводит к необходимости повышения организации системы защиты и совершенствования системы безопасности государства в киберпространстве от внешнего нападения и действия внутренних преступных формирований.

Учитывая, что информационная безопасность является одним из важнейших составляющих общей системы безопасности государства, общества и личности, необходимо регулярно проводить комплекс мер, направленных на обеспечение данного вида безопасности. В этой связи, на мой взгляд, целесообразно:

1. Разработать концепцию эффективного взаимодействия государства, гражданского общества и бизнес-сообщества в сфере обеспечения безопасности киберпространства, в которой определить цели и задачи, предмет, формы и методы сотрудничества, полномочия сторон, важность периодического проведения технологического регламента эксплуатационных сетевых систем.

2. Повысить правовую ответственность физических и юридических лиц, участвующих в организации кибератак (распространение дезинформации и разрушительных вирусов, способных привести к большим разрушительным процессам, значительному ущербу и системной общественно-политической дестабилизации) в киберпространстве России.

3. Использовать принцип государственно-частного партнерства для вовлечения бизнес-инвестиций в научно-технологические исследования в целях обеспечения адекватного требованиям времени информационно-коммуникативного технологического роста, включая развития защитных технологий и противодействия кибервойнам.

4. Активизировать международное сотрудничество в рамках двусторонних и многосторонних отношений. При этом особое внимание обратить на вопросы оптимизации взаимодействия со странами-участницами ЕврАзЭС в плане формирования единой системы киберпространства и защиты от внешнего нападения.

5. Учитывая современные тенденции в системе организации специальных служб ведущих стран Запада по созданию спецподразделений для проведения Интернет-шпионажа и внешнего взаимодействия с разведслужбами дружественных государств, видимо, и нам следует наладить в рамках отдельного проекта соответствующее сотрудничество (обмен разведывательной информацией, подготовка кадров, техническое и технологическое сотрудничество) со спецслужбами стран-участниц ЕврАзЭС.

Полагаю, что высказанные предложения будут способствовать укреплению национальной безопасности России в информационной сфере.

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