ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ ОБЩЕСТВЕ

А.Л. Димова

Российский государственный университет
физической культуры, спорта и туризма

Под воздействием научно-технического прогресса кардинально повышлась роль информациоиной безопасности личности, общества и государства. В развитых странах информация и информационная инфраструктура уже стали критическими компонентами, факторами риска, воздействие на которые способно вызвать крупномаштабные аварии, военные конфликты, дезорганизовать государственное управление, финансовую систему, научные центры.

В настоящей статье расмотрено понятие системного обеспечения информационной безопасности, дается анализ вопросов обеспечения информационной безопасности.

О системном подходе к информационной безопасности

Система (греч Systeta - целое) определяется как упорядоченное множество закономерно связанных друг с другом с определенном порядке элементов, представляющих собой целостное образование, единство. Поэтому целостность и единство системы обеспечения информационной безопасности должны быть основаны на взаимодействии ее важнейшых и необходимых элементов: объекта, субъекта, принципов обеспечения, источников опасности, направленности опасных информационных потоков, целей и мер ее обеспечеиия.

Для познания и управления любым системным образованием важно раскрыть его состав, «набор» компонентов, выясиить их субстанциональную природу, поскольку все другие характеристики системы в эначительной мере зависят от ее состава. Единство элементов в системе достигается определенными системообразующими связами и отношениями.

Доминирование и актуальность системного подхода к обеспечению информационной безопасности могут быть обоснованы следующими положеииями:

1. Информация и информационная среда общества базируются на информационных системах т.е. организационно упорядоченных совокупностях документов (массивов документов) и информационных технологий, в том чиспе с использованием средств вычиспительной техники и связи, реализующих информационные процессы.

2. Защита информации представлает собой системное явление – это комплекс организационных, правовых, технических и технологических мер по предотвращению угроз информационной безопасности и устранению их последствий. Такое понимание вытекает из комплексного характера угроз информационной безопастности как факторов, создающих опасность функционированию и развитию информационной среды общества.

3. В принципах обеспечения информационной безопасности существенное место отводится системно-юридической составляющей. К таковым относят в первую очередь эаконность, прововую обеспеченность; баланс интересов личности, общества и государства; комплексностъ, системность; научность, объективность, интеграцию международными системами безопасности; зкономическую эффективность.

4. В стране сложилась система субъектов информационной безопасности, к числу которых относятся те органы и структуры, которые в той или иной мере занимаются ее обеспечением. На государственном уровне это органы не только испольнительной, но и законадательной, судебной власти, в том чиспе ведомства, специально занимающейся информационной безопасностью.

Их деятелъность, полномочия и компетенция в целом и в части, каса-ющейся информационной безопасности, облачены в правовую форму и детально регламентированы на уровне федерального законодательства.

Правовому регулированию подвержено также использование названными субъектами активных и пассивных технических средств обеспечения информационной безопасности, с помощью которых осуществляются меры по защите систем и связи, компьютерных сетей от несанкционированного проникновения и других угроз. Существует и достаточио развитая наука - криптология, занимающаяся защитой информации, хранящейся или передаваемой с помощью бумажных, электронных, акустических и других средств.

Очень важно также выяснение направленности потоков информации. По своей направленности опасные информационные воздействия возможно рзделитъ на два вида. Первый связан с выводом, утратой, хищением ценной информации. Если информация выводится из технических систем, то речь может идти о деяниях, образующих несанкционированное проникновение в компьютерные сети, базы данных и т.д. Второй вид информационных опасностей менее извесген и исследован: он связан с внедрением, вводом новой информации, дезинформации, что может привести не только к опасным ошибкам в деятельности, но и повлечь опасные аварии и катастрофы. Информационную безопасность этого вида допжны обеспечивать специальные государственные органы (по типу структуры США - информационно-психологичес-кой и информационно-технической борьбы). На основе соответствующих правовых предписаний они призваны нейтрализовывать акции дезиинформации, пресекать манипулирование общественным мнением, противодействовать радиоэлектронной борьбе, ликвидировать последствия компьютерных атак, давать этим общественно опасным деяниям адекватную юридическую оценку.

В месте с тем пресечение или искажение информационных потоков само по себе может таить информационную опасность, особенно если это позитивные, социально полезные потоки. Так, от субъекта (человека, коллектива, общества) может скрываться информация, на которую он имеет полное право. Предупреждение таких негативных аспектов в информационной сфере также осуществляется правовыми средствами, С учетом современных кибернетических разработок возможно научное прогнозирование появяения новых информационных угроз и системмое воздействие на детерминирующие их факторы.

Комплекс "Байконур" является сложной научно-технической системой внутри которой передаются, обрабатываются перерабатываются огромные потоки различной информации, которая зачастую является конфиденциальной. В современных условиях информация по подготовке к пуску и пуск ракет космического назначения в большинстве своем хранится в базах данных компьютеров. Проникновение в компьютерные сети и в базы данных, введение в них дезинформации может сорвать подготовку и пуск ракет космического назначемия и/или привести к тяжелым авариям и катастрофам.

А предпосылки этого сохраняются. В их числе неурегулированность законодательной базы Российской Федерации и Республики Казахстан по комплексу "Байконур", а также разночтения в подходах при решении вопросов фунционирования инфраструктуры космодрома, которые являются питательной средой и искушением для тех организаций и лиц, которым информационная безопасность либо безразлична, либо в ее нарушении они видят корыстный интерес.

Изложенное позволяет сделать некоторые выводы. Роль и значение информационной безопасности объективно возрастает, особенно в связи с бурной информатизацией общества, Отставание в обеспечении информационной безопасносги может привести в перспективе к опасной уязвимости компьютерных сетей космодромов и страны в целом, всей информационной, управленческой инфраструктуры.

Мы также показали, что информационная защищенность личности, общества и государства возможна только на основе системного подхода. Известно, что нынешняя нормативная база обеспечения информационной безопасности пока недостаточна и нуждается в дальнейшей разработке. На государственном уровне следует также особое внимание уделять предупреждению и парированию новых информационных опасностей, объективно увеличивающихся в связи с повышением информационной насыщенности общества.