XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.IX: С.48-49, 2005.

УДК. 327

В.А.Кристи (5 курс, каф. МО), Д.Р.Ерофеев, ст. преп.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОНЯТИЯ В РАЗНЫХ СТРАНАХ

В наши дни информационные технологии получают все большее развитие. Прорыв в этой сфере последней четверти XX века вызвал у многих состояние интеллектуальной эйфории. Естественно, у информационных технологий есть свои слабые стороны. В последние годы они стали раскрываться все больше и больше. «Кибертерроризм», хакерство, компьютерный шпионаж – все это открытия последних 7-10 лет. Как ответная реакция на складывающуюся ситуацию в законодательстве многих стран примерно в это же время стали появляться статьи, а позже – целые акты, предписания, руководства, посвященные проблеме информационной безопасности. С другой стороны, процесс законодательного утверждения политики информационной безопасности происходил в каждой стране более или менее независимо, отсюда и по-разному расставленные приоритеты в данных актах вплоть до разного понимания самого термина «информационная безопасность». Сравнительный анализ определений данного термина производился на основе исследования законодательств шести стран: России, США, Канады, Японии, Индии и Европейского Союза (законодательство которого является обязательным к выполнению всеми странами-участницами ЕС). Приведем все шесть определений термина «информационная безопасность».

РФ – под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

США – термин «информационная безопасность» означает защиту информации и информационных систем от несанкционированного доступа, использования, раскрытия, изменения или уничтожения с целью обеспечения:

(A) целостности информации путем предупреждения ее неуместного изменения или уничтожения, что должно гарантировать подлинность и достоверность;

(B) конфиденциальности путем сохранения установленных ограничений на доступ и раскрытие, включая средства защиты личных тайн и информации о собственности;

(C) надежности путем предоставления своевременного и надежного доступа к информации и возможности ее использования; и

(D) защищенности от несанкционированного доступа путем использования цифрового удостоверения личности для подтверждения права пользователей на доступ к информации.

Канада – безопасность информации приобретает значение обеспечения защиты секретной информации от несанкционированного доступа и разглашения, которые могли бы привести к последствиям, противоречащим национальным интересам Канады.

ЕС – под сетевой и информационной безопасностью подразумевается способность сети или информационной системы сопротивляться случайным происшествиям, а также незаконным и злоумышленным действиям, которые подвергают риску надежность, аутентичность, целостность и конфиденциальность хранимой или передаваемой информации, а также функций, выполняемых или доступных через данные сети и системы.

Япония – информационная безопасность – защита конфиденциальности, целостности и надежности информационных ресурсов.

Индия – информационная безопасность означает сохранение конфиденциальности,

целостности и надежности информации.

Американский, европейский, японский и индийский варианты схожи. Все они говорят об информационной безопасности в техническом аспекте работы информационных сетей. Цель политики информационной безопасности – обеспечение такого уровня надежности коммуникационных сетей и информационных систем, при котором возможность несанкционированного доступа к ресурсам минимальна при максимально безотказной работе с авторизованными пользователями. Понятие информация в таком случае сводится лишь к тем ее видам, которые хранятся в электронном виде.

Более широко понимается информационная безопасность в РФ (и техническая, и морально-этическая составляющие). Сам термин «информация» не ограничивается ее электронными носителями. Российский вариант определения отличает больший упор на баланс между интересами личности, общества и государства в информационной сфере, в то время как практически все другие варианты (за исключением американского) ограничиваются регламентированием интересов государства и, максимум, бизнеса.

Канадское же законодательство вообще не признает термина «информационная безопасность». Близкое по звучанию понятие «безопасность информации» относится исключительно к охране секретной информации.

Выводы: трактовка термина «информационная безопасность» неоднозначна и зависит от приоритетов национальной политики. В РФ обеспечение информационной безопасности зависит от развития информационных технологий в стране, от доступа населения и предпринимательства к новейшим разработкам. Для стран с высоким уровнем развития информационных технологий главное – не допустить утраты информационных ресурсов на электронных носителях, на которых хранится большая часть стратегически важной информации – как относящейся к государственному управлению, так и экономических и технологических данных, утеря которых может привести к тяжелым последствиям для нации. Развитие информационных технологий приводит к стремительному росту внимания к понятию информационной безопасности. Законодательные акты, регулирующие отношения в информационной сфере, появились в законодательстве многих стран именно в последние 5-7 лет. Можно ожидать, что со временем термин «информационная безопасность» получит большую однозначность и за ним закрепится смысловая нагрузка, не зависящая от территориального признака или уровня развития информационных технологий.