УДК 621.394/.396.019.3

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Н.Р. Шевко, старший преподаватель кафедры экономической теории, правовой статистики, математики и информатики Казанского юридического института МВД России, капитан милиции, кандидат экономических наук

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать. Проблема информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных. Каждый сбой работы компьютерной сети это не только «моральный» ущерб для работников предприятия и сетевых администраторов. По мере развития электронных платежей, «безбумажного» документооборота и других технологий серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приведет к ощутимым материальным потерям. Не случайно защита данных в компьютерных сетях становится одной из самых острых проблем в современном мире.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации[1] термин «информационная безопасность» используется в широком смысле. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина:

на доступ к информации,

на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития,

в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются:

в обеспечении интересов личности в этой сфере;

упрочении демократии;

создании правового социального государства;

достижении и поддержании общественного согласия.

Интересы государства в информационной сфере заключаются:

в создании условий для гармоничного развития российской информационной инфраструктуры;

в реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности;

в безусловном обеспечении законности и правопорядка;

в развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере. Одна из них включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России. Информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Таким образом, под *информационной безопасностью* понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

На сегодняшний день сформулированы базовые принципы информационной безопасности, которая должна обеспечивать:

– целостность данных – защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;

– конфиденциальность информации и одновременно ее доступность для всех авторизованных пользователей.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Значение защиты информации в современном информационном обществе трудно переоценить. Новая информационная инфраструктура создает новые опасности для информации.

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех уровней:

- законодательного;
- административного;
- процедурного;
- программно-технического.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Сами по себе лицензирование и сертификация не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за нарушения информационной безопасности. Реальность такова, что в России в деле обеспечения информационной безопасности на помощь государства рассчитывать не приходится.

Одной из мер обеспечения информационной безопасности является криптография. Все, что связано с криптографией, сложно не столько с технической, сколько с юридической точки зрения. Данный сервис является инфраструктурным, его реализации должны присутствовать на всех аппаратно-программных платформах и удовлетворять жестким требованиям не только к безопасности, но и к производительности. Пока же единственным доступным выходом является применение свободно распространяемого программного обеспечения.

Надежный контроль целостности также базируется на криптографических методах с аналогичными проблемами и методами их решения. Анализ защищенности — это инструмент поддержки безопасности жизненного цикла. С активным аудитом его роднит необходимость практически непрерывного обновления базы знаний и роль не самого надежного, но необходимого защитного рубежа, на котором можно расположить свободно распространяемый продукт.

Президентом Российской Федерации определены меры по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена.[2]

Установлено, что подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети «Интернет», не допускается. Государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, могут использовать только средства защиты информации, прошедшие сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю Российской Федерации.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем в соответствии с характером и важностью решаемых ими задач.

ПРИМЕЧАНИЯ

[1] Доктрина информационной безопасности РФ утв. Президентом РФ 09.09.2000 г. № Пр-1895.

[2] Указ Президента РФ от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена».