И.А. Гайченя,
соискатель кафедры
национальной безопасности РАГС

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Сегодня региональная пресса уделяет пристальное внимание проблемам информационной безопасности. Модно выделить несколько направлений данной темы: политика информационной безопасности, проводимая органами государственной власти; работа силовых министерств и ведомств в области информационной безопасности; подготовка кадров в образовательных учреждениях профессионального образования по специальности «Информационная безопасность» и проведение научно-практических конференций по защите информации; защита коммерческой информации; разработка защиты от новых компьютерных вирусов.

В ряде регионов образованы комиссии по информационной безопасности и защите информации при администрациях областей. Основные направления их работы: определение приоритетных вопросов защиты информации в исполнительных органах государственной власти области; поиск концептуальных подходов к обеспечению информационной безопасности в исполнительных органах государственной власти области; разработка предложений по формированию областной системы информационной безопасности; подготовка программы информационной безопасности исполнительных органов государственной власти области; разработка проектов постановлений и распоряжений Администрации области по вопросам информационной безопасности и защите информации, организация и проведение экспертизы проектов областных нормативных правовых актов на соответствие требованиям нормативных документов по информационной безопасности; выработка предложений по выполнению требований нормативных актов по информационной безопасности, обеспечению защиты информации организациями на территории области; рассмотрение результатов контроля эффективности принятых мер защиты информации в исполнительных органах государственной власти области.

Так, постановлением Администрации Новгородской области от 22 мая 2006 г. № 253 для совершенствования работ по противодействию техническим разведкам и технической защите информации

области, составляющей государственную тайну, образована постоянно действующая техническая комиссия по защите государственной тайны при Администрации области, утверждены Положение о постоянно действующей технической комиссии по защите государственной тайны при Администрации области и ее состав. В Калужской области постановлением губернатора от 21 апреля 2006 г. № 130 был утвержден новый состав комиссии по информационной безопасности при губернаторе области.

Управление информатизации Москвы объявило результаты открытого конкурса по выбору исполнителя городского государственного заказа на выполнение научно-исследовательских и опытно-конструкторских работ в рамках городской целевой программы «Электронная Москва» по теме: «Создание и развитие системы мониторинга событий информационной безопасности города Москвы». Победителем признано ЗАО «Инфосистемы Джет».

Международное сообщество давно следит за развитием высоких информационных технологий. Отмечаются следующие возможные угрозы: прерывание связи с самолетами, проникновение в базы данных крупных банков, катастрофы на крупных предприятиях – там, где можно отключить большие компьютерные системы.

В России ситуация с защитой информационных технологий пока сложная. Действующий закон устарел, а новый уже который год безуспешно обсуждают в Думе. На первый взгляд закон о защите информационной безопасности не затрагивает интересы простых граждан. Это не «дачная амнистия» и не монетизация льгот. Однако именно этот закон, как никакой другой, в час «Х» может спасти страну.

Эксперты приводят такой пример: создается «логическая бомба» (набор команд, внедряемых в программу), которая срабатывает при конкретных условиях: по истечении времени или при нажатии определенной клавиши. Внедренная, например, в систему управления поездами метрополитена, она может блокировать работу подземки, парализовав город.

Известен факт: операция «Буря в пустыне» оказалась столь удачной не только потому, что американские рейнджеры быстро бегали и метко стреляли. Иракцы закупили французскую систему ПВО, имеющую «дыры» в управлении, чем и воспользовались американцы, отключив ее спутниковым сигналом. Для верности они использовали и радиоэлектронное подавление.

К счастью для России, мы пока отстаем в информационных технологиях. По статистике Министерства связи, только каждый 12-й житель России умеет пользоваться Интернетом.

В ряде субъектов Российской Федерации уже накоплен положительный опыт решения вопросов информационной безопасности.

Принимаются стратегии инновационного развития, где особое внимание уделяется совершенствованию методов госуправления. Их важной составляющей является информационно-аналитическая система поддержки управленческих решений и система электронного документооборота. Они ориентированы на эффективную работу госаппарата. Например, в Республике Татарстан министерства и ведомства в своей работе активно используют возможности информационно-аналитической системы. С ее помощью формируются отчеты, осуществляются запросы по базам данных, анализируется тенденция социально-экономической динамики отдельных отраслей. В аппарате правительства, в республике в целом реализован проект безбумажной подготовки важнейших документов. Теперь к этой системе подключаются министерства и ведомства Татарстана.

В условиях формирования информационного общества информационный обмен требует не только открытости, но и защиты от постороннего доступа. В этой связи особую актуальность приобретает вопрос информационной безопасности. В настоящее время подготовлен проект Концепции информационной безопасности в республике. В этом документе на основе анализа современного состояния информационной безопасности определены основные цели и задачи, ключевые проблемы обеспечения защиты информации, разработан проект республиканской программы «Обеспечение комплексной информационной безопасности в Республике Татарстан». Программа определяет основные положения государственной политики в этой сфере, организационную структуру и принципы построения системы информационной безопасности. В мае 2006 г. объявлен конкурс на создание межведомственной системы информационной безопасности для выбора аппаратных решений, позволяющих решить задачи, поставленные в концепции и программе.

Постепенно страна становится по-настоящему современной, высокотехнологичной. Проходят те времена, когда власть и бизнес задумывались только о сиюминутных проблемах. Сегодня на первый план выходят проблемы безопасности: информационной, особенно в хозяйственной деятельности, и в масштабах государства в целом, понятие «коммерческая тайна», безопасность правоохранительной и розыскной деятельности. Безопасность и комфортное проживание граждан России на территории страны подразумевает также безопасность технологическую, криминогенную и экологическую. Главное, чтобы значительная часть разработок, демонстрируемых на различных выставках, нашла применение в будущем.

На Дальнем Востоке тоже займутся информационной безопасностью. Такое решение приняли на заседании межведомственной комиссии при полномочном представителе президента в Дальне-

восточном федеральном округе, куда впервые пригласили специалистов, отвечающих за обеспечение и доступ к информации. По словам помощника полпреда А. Дроздова, система безопасности в округе уже существует. Правда, она далека от совершенства. Он объяснил, что на территории Хабаровского края в особой охране от несанкционированного доступа к информации нуждаются предприятия оборонной промышленность, объекты энергетики и т. д. Бороться со всевозможными утечками информации в регионе намерены, до предела информатизировав все процессы на особо важных объектах, чтобы максимально исключить человеческий фактор. В частности, планируется ускоренными темпами развивать оптико-волоконную связь и спутниковую связь.

Большой резонанс вызвали в обществе два закона, подписанные Президентом России: «О персональных данных» и «Об информации, информационных технологиях и защите информации». В них речь идет о регламентации сбора баз данных на россиян. Этим занимаются не только спецслужбы, но и различные организации, например, банки, выдающие кредиты, управления соцзащиты, налоговые инспекции, больницы, ГАИ, отделы кадров и др. Не всегда эта информация доступна узкому кругу специалистов. Достаточно вспомнить, как некий издательский концерн рассылал по стране письма с сообщением, что компьютерная система этой фирмы выдала вашу фамилию в качестве победителя лотереи, разыгрывающей автомобиль. Многие озаботились вопросом: из каких же источников жулики заполучили списки с адресами россиян по всей стране и полным именем, отчеством и фамилией?

В прежних законах не существовало ограничений на объем данных, собираемых различными – как государственными так и коммерческими – структурами, и гражданин не мог требовать уничтожения информации о его личности. С принятием новых документов ситуация поменялась. Теперь никто не может требовать от гражданина сведений больше, чем нужно для заявленной цели. Наложен запрет на формирование баз данных, если нет гарантированной защиты этих сведений. Причем речь идет о необходимости получить согласие гражданина (а в ряде случаев письменное) на сбор и обработку его персональных данных. К персональным данным отнесены абсолютно все сведения – имя, фамилия, год и место рождения, адрес, семейное положение, зарплата, образование и т. д. Новый закон запретил вносить в базы данных сведения о национальности, политических и религиозных взглядах, интимной жизни и даже судимости. Единственная уступка в законе была сделана для спецслужб: в законодательный документ внесена оговорка о создании баз дан-

ных специальной категории, например для осуществления правосудия. Отныне необходимо регистрировать все базы данных в специально учрежденной организации. Она же станет следить за этими хранилищами информации. 7 августа 2006 г. новые законы вступили в силу.

В настоящее время на любых распространителей информации он накладывает жесткие обязательства. Причем касаются они не только информационных служб или иных специализирующихся компаний, а всех, кто предоставляет информацию неопределенному кругу лиц, в том числе владельцам сайтов. Такая информация должна включать в себя достоверные сведения о ее обладателе (владельце) или распространителе в форме и в объеме, достаточных для его идентификации. Кроме того, федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть. Такая новация должна защитить добросовестных граждан и организации от клеветы. Ведь на форумах и через бесплатные хостинги можно распространять и умаляющую честь и достоинство граждан информацию, а идентифицировать анонима крайне сложно. Правда, неясно, что делать с нарушителями. Дабы привлечь анонима к ответственности, его надо найти. Владелец сайта с форумом не может отвечать за вину пользователей, хотя по новому закону появляется право оклеветанного требовать удалить спорное сообщение. Предлагается защитить пользователей Интернета и от рассылки электронной рекламы. Причем получатель может отказаться от получения не только электронных, но и бумажных писем.

Аналогичная норма есть и во вступившем в силу 1 июля 2006 г. новом законе «О рекламе», но она касается только рекламных сообщений, а закон «Об информации» – любых. Из нового закона практически исключена основная декларация о праве на информацию. Теперь гражданин может требовать от госорганов только «информацию, непосредственно затрагивающую его права и свободы» и только в порядке, установленном законодательством. Юридические же лица вообще могут просить у госорганов только информацию, «необходимую в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности». В действующем же законе указывается на безусловное равное право всех на доступ к государственным информационным ресурсам, причем особо подчеркивается, что обращающийся «не обязан обосновывать перед владельцем ресурсов необходимость получения запрашиваемой ими информации». Исключение составляет информация с ограниченным доступом.

Таким образом, программы информационной безопасности, разрабатываемые в разных округах Российской Федерации, затрагивают много вопросов, касающихся личной, финансовой, международной информационной безопасности граждан. В них определяются приоритетные направления работы по вопросам защиты информации.