тайны связана с совершенствованием организационно-правовых основ обеспечения информационной безопасности органов государственной власти в условиях постоянного и бурного развития средств информатизации.

Одной из весьма существенных проблем сохранности государственной тайны является угроза ее утечки по техническим каналам. Для недопущения этого в органах государственной власти необходимо на постоянной основе реализовывать комплекс профилактических мероприятий, среди которых:

- повышение безопасности информационных систем, включая сети связи органов внутренних дел;
- обеспечение защиты сведений, составляющих государственную тайну;
- мероприятия, направленные на гарантированное предотвращение несанкционированного проникновения на объекты органов внутренних дел и утечки информации по техническим каналам;
- совершенствование системы подготовки и переподготовки персонала по использованию современных средств защиты информации.

По данным специальных исследований, «наиболее уязвимым местом в сфере защиты информации являются действия технического персонала и пользователей информационных систем (умышленные и неумышленные), которые приводят к утечке информации, циркулирующей в этих системах» [10]. В этой связи открытые информационные системы при работе с открытой информацией должны контролироваться на предмет исключения попадания в них секретной и конфиденциальной информации по неумышленным и умышленным действиям технического персонала и пользователей.

Таким образом, в проблеме правового регулирования института государственной тайны в России необходимо выделить два аспекта: теоретический, связанный с несовершенством правовой теории государственной тайны, и практический, касающийся ее правоприменения, которое, в свою очередь, подразумевает организацию защиты и охраны государственной тайны.

Итак, даже небольшой анализ сложившейся практики правового регулирования государственной тайны наглядно демонстрирует насущную потребность оптимизации действующего законодательства Российской Федерации и совершенствования концепции защиты и охраны государственной тайны.

Литература

1. Закон Российской Федерации от 21 июля 1993 г. N 5485-1 (ред. от 01.12.2007 г.) «О государственной тайне» // Российская газета. 1993. N 182. 21 сентября.
2. *Трунов И.Л.* Процессуальное законодательство на защите частной жизни и ее тайн. http://www.trunov.com/content.php?act=showcont&id=388
3. Тайна и ее составляющие: современное регулирование. http://www.namvd.ru/sciense/dis/Autoref/468.html
4. *Горелик Л.А.* Гласность и рассекречивание тайн. http://www.jourclub.ru/5/572
5. Закон Грузии от 29 октября 1996 года N 455-Iс «О государственной тайне» // Парламентис уцкебани. 1996. 21 ноября. N 27-28/4. Пер. с грузинского. http://www.medialaw.ru/exussrlaw/index.htm; Закон Украины от 21 сентября 1999 года № 1079-XIV «О государственной тайне» // Ведомости Верховной Рады Украины. 1999. № 49. Ст. 428.
6. Закон Республики Армения «О государственной и служебной тайне», принят Национальным собранием 3 декабря 1996 года. http://www.medialaw.ru/exussrlaw/index.htm
7. *Мальцев В.А.* Защита государственной тайны в Российской Федерации на современном этапе ее развития // Конституционное и муниципальное право. 2008. N 4.
8. Федеральный закон от 22.10.2004 г. N 125-ФЗ (ред. от 13.05.2008 г.) «Об архивном деле в Российской Федерации» (принят ГД ФС РФ 01.10.2004 г.) // Российская газета. 2004. N 237. 27 октября.
9. Федеральный закон от 08.08.2001 г. N 129-ФЗ (ред. от 19.07.2009 г.) «О государственной регистрации юридических лиц и индивидуальных предпринимателей» // Российская газета. 2001. N 153-154. 10 августа.
10. *Аксенов С.Г.* Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Налоги. 2008. N 3(2).

Василий КИРИЛЕНКО

Создание общей системы мер информационной безопасности

Состояние информационной среды сегодня определяет уровень и возможности социально-экономического развития, обеспеченность обороноспособности и суверенитета страны. От положения дел в сфере информатизации в огромной степени зависит эффективность работы государственного аппарата, взаимоотношения государственной власти и общества. В этом сложном механизме одно из важных мест занимает деятельность по обеспечению информационной безопасности страны.

С точки зрения правоохранительных органов, обеспечение информационной безопасности – вид деятельности, заключающийся в применении системы специальных и иных мер по защите информационного пространства и информационной инфраструктуры России от внешних и внутренних угроз и целенаправленному воздействию в интересах Российской Федерации на информационное пространство и информационную инфраструктуру противостоящей стороны.

Говоря о внешних угрозах, необходимо отметить, что наиболее квалифицированное, опасное и целенаправленное воздействие на информационные системы России осуществляют специальные подразделения иностранных государств. Выявлены и пресечены попытки противо-

Василий КИРИЛЕНКО – кандидат юридических наук, доцент

правного использования рядом российских и иностранных граждан открытых телекоммуникационных сетей (ОТКС), а также возможностей Интернета для передачи иностранным государствам интересующей их информации, в том числе закрытой.

Значительные проблемы нередко возникают при вхождении отечественных пользователей в международные информсистемы, в частности в Интернет. Многие преступления, совершенные с применением этой сети, очень схожи с обычными, такими как распространение конфиденциальной информации без согласия ее владельца, клевета, взлом компьютерных сетей, кража информации, пиратство, мошенничество. Вместе с тем Интернет порождает и некоторые специфические проблемы, которых нет в других открытых системах, действующих на территории одного государства.

В Вооруженных силах России из-за недостаточного финансирования по-прежнему предпочитают надежные сейфы. Но процессы информатизации затронули и их. Имеющиеся материалы уголовных дел свидетельствуют о том, что работа разведчиков сейчас существенно упростилась: закрытую информацию можно добывать с использованием Интернета, а секретные сообщения – посылать по электронной почте.

ЦРУ, Агентство национальной безопасности (АНБ), другие специальные подразделения и организации иностранных государств изучают возможности и методы проникновения в компьютерные сети своих потенциальных противников. Для чего, в частности, разрабатываются технологии противоправного внедрения различных компьютерных программ, которые длительное время не проявляя себя, способны активизироваться по команде в нужный момент. В случае кризисной ситуации электронные «диверсанты» могут дезорганизовать оборонную систему управления, транспорт, энергетику, финансовую основу другого государства.

Вместе с тем, по заключению специалистов, внутренние угрозы не менее серьезны, чем внешние. Мы всегда ищем виновного на стороне. А он среди нас. Различные информационные воздействия Запада были и раньше, они и сейчас продолжаются. Эти угрозы имеют как бы внешний источник, но реализуются нами самими, на территории нашего государства.

Для государственной, коммерческой и иной организации (фирмы) опасность в большей степени исходит из самой организации: от сотрудников, похищающих информацию или сведения о ее деятельности, в которой заинтересована конкурирующая или оппозиционная сторона, распространяющих ложную или недостоверную информацию. Но действуют эти сотрудники не по своей инициативе, а по заданию извне.

Опасность исходит и от хакеров. Их возрастающая квалификация и активность нередко ведут к взлому нестойких к дешифрованию систем. Слабая криптографическая защита компьютерных сетей, теснимая хорошо вооруженными в технологическом отношении программистами, наносит заметный ущерб экономической безопасности страны.

Поэтому ряд ведомств, банков и других учреждений реализуют планы создания собственных сетей засекреченной связи. Однако отсутствие серьезной научной базы и специалистов приводит к тому, что эти организации могут оказаться под контролем у более мощных конкурентов или разведок.

В условиях продолжающейся активизации специальных подразделений и организаций иностранных государств против Российской Федерации отечественные правоохранительные органы принимают меры по противодействию этой деятельности. Значительно активизировалась работа по выявлению, предупреждению и пресечению преступлений в сфере компьютерной информации, создающих угрозу нормальному функционированию органов государственной власти, кредитно-финансовой сферы, правоохранительных органов, объектов жизнеобеспечения. Приняты меры по созданию нормативно-правовой базы обеспечения информационной безопасности и борьбы с преступлениями в сфере компьютерной информации.

Современный опыт показывает, что:

- обеспечение информационной безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов и путей совершенствования и развития системы информационной безопасности, непрерывном контроле за ее работой, выявлении ее слабых мест, возможных каналов утечки информации и способов несанкционированного доступа к ней;
- информационная безопасность может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм – систему обеспечения информационной безопасности. Его функционирование должно контролироваться, обновляться и дополняться в зависимости от изменения внутренних и внешних условий, с учетом возможных информационных угроз;
- никакая система обеспечения информационной безопасности не может обеспечить требуемого уровня безопасности без надлежащей подготовки пользователей и соблюдения ими всех установленных правил сохранения конфиденциальности.

Основным компонентом системы обеспечения информационной безопасности можно считать организованную совокупность правоохранительных органов, средств, методов и мероприятий, обеспечивающих защиту информации от искажения, исчезновения, использования в ущерб жизненно важным интересам личности, общества и государства в информационной сфере. Эту систему ус-

ловно можно подразделить на две подсистемы: обеспечения безопасности открытой информации и обеспечения безопасности закрытой информации.

Вместе с тем децентрализация органов власти в Российской Федерации, реструктуризация экономики страны, придание большей самостоятельности регионам и отдельным городам областного подчинения (муниципалитетам) с развитой инфраструктурой обусловили появление такого понятия, как *муниципальный объект информатизации* (МЦОИ).

Обобщенные сведения и потоки данных, которые используются в процессе функционирования муниципального хозяйства, носят конфиденциальный характер. Если речь идет о деятельности стратегических объектов федерального подчинения, дислоцируемых на территории муниципалитетов, то отдельная информация о них относится к государственной тайне. Утечка, потеря, искажение или несанкционированный доступ к такой информации являются составной частью потенциальных угроз информационной безопасности государства в целом.

Поэтому государственная информационная политика должна исходить из того, что в системе обеспечения информационной безопасности возникает необходимость выделения подсистемы обеспечения муниципальной информационной безопасности (МИБ).

В интересах государственной информационной политики в сфере обеспечения информационной безопасности Российской Федерации необходима серьезная общетеоретическая проработка рассматриваемой проблемы, разработка и научное обоснование принципов и методов, строгой оптимизации всех мероприятий обеспечения информационной безопасности страны. Основным способом достижения указанной цели представляется переход всей проблемы обеспечения информационной безопасности с экстенсивных на интенсивные пути решения. А это в более конкретной постановке вопроса заключается в решении следующих научных задач: создание предпосылок для реализации упреждающей стратегии обеспечения информационной безопасности; разработка регулярных методик объективной (на количественном уровне!) оценки уязвимости информации и требуемого уровня ее защиты; синтеза оптимальных систем обеспечения информационной безопасности; обоснование необходимой инфраструктуры обеспечения информационной безопасности в общегосударственном масштабе.

В процессе обеспечения информационной безопасности необходимо учитывать и такую проблему, как соотношение права собственности (в гражданско-правовом его понимании) и права на информацию. Это актуальнейшая и важнейшая проблема на пути формирования государственной информационной политики в области информационного права и правового регулирования информационных отношений. Суть заключается в том, что право на информацию включает в себя, в том числе, и право на производство информации. И законодательство об интеллектуальной собственности (об авторском праве, о патентном праве) в первую очередь регулирует отношения по поводу производства информации. И СМИ – это тоже производство информации. Создание баз и банков данных самого разнообразного назначения – тоже производство информации. И все эти процессы как бы объединяются через уникальный объект – информацию.

Однако информационная сфера ряда регионов России в значительной мере определяется сформированным подконтрольным администрациям информационным пространством. На фоне стабильного и поступательного развития средств массовой информации по-прежнему основной проблемой остается их экономическая зависимость, что вынуждает активно работать по договорам об информационном обслуживании с органами власти, реализовывать рекламные акции. Так, в 2007 г. в бюджете Приморского края на эти цели были предусмотрены расходы на общую сумму свыше 130 млн рублей (два раздела бюджета), из них на информационное обслуживание АПК по договорам выделено около 30000 млн рублей. При этом различные политические и финансовые структуры Приморья продолжают активно втягивать средства массмедиа в сферу своих интересов. В результате в крае нет по-настоящему независимой прессы и телевидения. Участвующие в информационной сфере Приморья субъекты СМИ отражают точку зрения на происходящие в крае и стране политические и экономические процессы той или иной структуры, стоящей за конкретным изданием*.

Определяющее влияние на состояние информационной сферы Приморского края продолжает оказывать стремление региональных политических сил в расстановке лоббируемых кандидатур на ключевых политических и административных позициях.

Наибольшую активность в данном направлении администрации отдельных регионов проявляют в интересах использования технологий управления информацией для выгодного влияния на общество и вытеснения «неугодных» политических фигур, с задействованием значительного финансового и административного потенциалов. При этом ряд из принимаемых государственных инициатив используются как информационные поводы для нагнетания протестной активности населения и смещения политических предпочтений электората.

Не меньшее влияние на информационною сферу регионов оказывают финансово-промышленные группы, использующие принадлежащие им СМИ в информационном обеспечении своих экономических интересов, что приводит к активному информа-

---

* В Приморском крае на 1 января 2007 года зарегистрировано в установленном порядке 736 СМИ, из них 519 печатных изданий (газет – 397, журналов – 93, иных печатных изданий – 29). Электронных СМИ – 203. Учредителями 40 СМИ являются государственные органы, 125 – органы муниципальной власти, 571 – частные лица.

ционному противоборству в информационной сфере.

Отмечается практика использования региональных СМИ различными адвокатскими и правозащитными организациями. Зачастую выражение позиции защиты в СМИ осуществляется не в рамках каких-либо направленных акций, а ввиду отсутствия у представителей массмедиа иных источников информации. Так, в ноябре 2006 года в Приморском крае работала объединенная следственная группа генеральной прокуратуры и МВД (ДЭБ) России, нацеленная на вскрытие преступлений на канале внешнеэкономической деятельности. В условиях полной информационной изоляции деятельности группы СМИ распространяли информацию, почерпнутую лишь на форумах в сети Интернет и из свидетельств так называемых «очевидцев» – в большинстве своем адвокатов, комментирующих события с выгодной для защиты стороны. Очевидно, что пребывание массмедиа в информационном вакууме способно привести к формированию негативного общественного мнения о деятельности правоохранительных органов.

Необходимость существенных изменений положения вещей вытекает из всего комплекса вопросов, которые отнесены действующими законодательными и правовыми актами к ведению правоохранительных органов. К ним относятся Федеральный закон от 03 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности» (в редакции последних изменений), Доктрина информационной безопасности Российской Федерации, Стратегия национальной безопасности Российской Федерации до 2020 года и другие. С учетом этих документов определяются следующие задачи по совершенствованию рассматриваемого направления деятельности, обозначенные автором:

- внести изменения и дополнения в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация;
- законодательно разграничить полномочия в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определить цели, задачи и механизмы участия в этой деятельности общественных объединений, организаций и граждан;
- разработать и принять нормативные правовые акты Российской Федерации, устанавливающие ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- уточнить статус иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры как регионов, так и России в целом;
- создать правовую базу для формирования в Российской Федерации региональных структур обеспечения информационной безопасности;
- создать действенную систему информационной безопасности на всех уровнях государственного и военного управления во главе с государственным исполнительным и координирующим органом управления, с подсистемами информационного, научного и правового обеспечения принятия решений;
- разработать концепцию обеспечения муниципальной информационной безопасности;
- построить модель потенциальных угроз муниципальной безопасности;
- разработать основные структуры муниципальных органов обеспечения информационной безопасности;
- разработать базовые нормативно-технические документы обеспечения муниципальной информационной безопасности;
- разработать систему защиты информации (СЗИ) муниципальных органов управления и др.

С учетом этого правоохранительным органам необходимо определиться с участием в построении подсистемы обеспечения муниципальной информационной безопасности, выделением сил и средств и т.д.

Словом, настало время серьезно переосмыслить законодательную основу, обеспечивающую защиту государственных и частных информационных систем обеспечения информационной безопасности.

В следующем номере:

«Основой системы корпоративных ценностей и корпоративной безопасности являются этические нормы. Когда сотрудники руководствуются нравственными нормами, это лучшая гарантия эффективности их профессиональной деятельности, а также личной, ведомственной и в конечном итоге национальной безопасности».

Член-корреспондент Академии педагогических и социальных наук, кандидат психологических наук М.А. БУРЕНКОВ