УДК [34:004](575.2) (04)

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

Х.М. Якубова

Рассматриваются вопросы, связанные с правовым обеспечением информационной безопасности в Кыргызской Республике.

Ключевые слова: информационная безопасность; защита информации; информационное правонарушение; коммерческая тайна; банковская тайна.

Понятие безопасности в информационной сфере опирается на общее понятие безопасности, которое можно определить как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. К основным объектам безопасности относятся: личность – ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальная целостность.

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства. Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

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 Кыргызской Республики. Национальная безопасность нашей страны существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [1].

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Под информационной безопасностью Кыргызской Республики понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Исходя из этого, информационная безопасность непосредственно связана с защитой информационной сферы, защита которой – важнейшая составная компонента информационной безопасности.

Таким образом, защита информационной сферы распадается на три направления:

1) защита информации от неправомерного доступа и воздействия на нее;

2) защита прав физических и юридических лиц на информацию;

3) защита общества и государства от вредной информации.

Понятие защиты информации следует отличать от понятия охраны информации. Охрана информации включает в себя любые средства, направленные на обеспечение интересов субъекта информационных правоотношений. Защита информации используется в тех случаях, когда информационные права уже нарушены или существует реальная угроза их нарушения [2].

Целями защиты информации являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Защита информации осуществляется как организационными, так и правовыми способами.

1. Организационные способы защиты информации.

В основе организационного аспекта защиты любой информации лежит принцип правильной организации движения информации, учитывающей методы обработки информации, организационно-управленческие концепции ее формирования и потребления. Информация, подлежащая защите, должна быть четко выделена из всей остальной, и для нее должны быть установлены особые правила обращения.

В частности, создание системы защиты информации предусматривает выявление возможных каналов утечки информации; оценку возможностей их перекрытия; установление ограничений на доступ к защищаемой информации; инструктирование персонала по работе с защищаемой информацией; использование криптографических и иных технических средств защиты информации и т.п.

2. Правовые способы защиты информации.

Правовые способы защиты информации предусматривают, прежде всего, создание юридической базы такой защиты, как в общегосударственном масштабе, так и в рамках одной организации. Правовую защиту обеспечивают также некоторые государственные органы, в первую очередь, органы суда и прокуратуры.

В соответствии с действующим законодательством собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.

Собственник документов, массива документов, информационных систем или уполномоченные им лица устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

К правовым способам защиты информации относится и установление особых правовых режимов информации, таких, как режим государственной тайны, коммерческой и банковской тайны и др.

В Кыргызской Республике вышеупомянутые виды тайн регулируют соответствующие законы: Закон Кыргызской Республики “О защите государственных секретов Кыргызской Республики” от 14 апреля 1994 г., Закон Кыргызской Республики “О коммерческой тайне” от 30 марта 1998 г. и Закон Кыргызской Республики “О банковской тайне” от 23 июля 2002 г.

Закон Кыргызской Республики “О защите государственных секретов” впервые определил круг вопросов, необходимых для обеспечения порядка и безопасности в этой сфере. В нем дано определение государственных секретов, названы виды сведений, составляющих в современных условиях содержание государственной тайны, порядок засекречивания сведений и их носителей, правила и способы защиты государственной тайны.

Исходя из определения, данного в законе, государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, разглашение которых может нанести ущерб безопасности нашей страны.

Закон Кыргызской Республики “О коммерческой тайне” к таковой относит информацию, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. К ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Таким образом, можно выделить три признака относимости информации к коммерческой тайне:

- информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- отсутствует свободный доступ к информации;
- обладатель информации принимает меры к охране ее конфиденциальности.

Первый признак означает, что к коммерческой тайне не могут быть отнесены сведения, которые заведомо не могут обладать коммерческой ценностью. Например, не может быть коммерческой тайной информация о планировке офиса фирмы и т.п.

Информация теряет свой статус коммерческой тайны в случае, если она становится общедоступной, т.е. отсутствует второй признак коммерческой тайны. Речь идет о случаях, когда сам владелец информации опубликовал ее в средствах массовой информации и тем самым сделал ее известной широкому кругу лиц [3].

Правовое регулирование банковской тайны в настоящее время осуществляется нормами Гражданского кодекса Кыргызской Республики, Законом Кыргызской Республики "О банках и банковской деятельности", а также вышеупомянутым Законом Кыргызской Республики "О банковской тайне".

Гражданский кодекс Кыргызской Республики устанавливает, что "банк гарантирует тайну банковского счета и банковского вклада операций по счету и сведений о клиенте". Более широкую формулировку содержит закон "О банках и банковской деятельности": "Кредитная организация гарантирует тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит законодательству".

Исходя из этого можно дать определение банковской тайны: банковской тайной являются сведения об операциях клиентов банка, о движении средств на банковских счетах, а также сведения о самом клиенте.

Наконец, защита информации и обеспечение информационной безопасности осуществляется также путем установления мер ответственности за информационные правонарушения.

Информационным правонарушением признается противоправное, общественно опасное, виновное деяние, за которое законодательством предусмотрена юридическая ответственность. Все информационные правонарушения в зависимости от степени общественной опасности можно подразделить на информационные проступки и информационные преступления.

За совершение информационного проступка к нарушителю могут быть применены меры дисциплинарной, материальной, административной или гражданско-правовой ответственности. Дисциплинарные проступки могут совершаться в процессе трудовой деятельности и связаны с неисполнением или ненадлежащим исполнением работником по его вине возложенных на него трудовых обязанностей. Примером дисциплинарного проступка в сфере защиты информации может служить ненадлежащее исполнение работником обязанности по использованию средств технической защиты компьютерной информации (например, игнорирование необходимости установления пароля), в результате чего была допущена утечка ценной информации.

Материальная ответственность также наступает, когда вред причинен организации ее работником при исполнении трудовых обязанностей и связан с непосредственным причинением материального ущерба.

За преступления в информационной сфере предусмотрена уголовная ответственность. В качестве примера можно привести разглашение государственной тайны, шпионаж и др. преступления.

Таким образом, для создания и поддержания необходимого уровня информационной безопасности, защищенности объектов безопасности в Кыргызской Республике, должны совершенствоваться существующая законодательная база и разрабатываться дополнительная система правовых норм, регулирующих отношения в сфере безопасности, определяться основные направления деятельности органов государственной власти и управления в данной области, формироваться эффективная система органов обеспечения информационной безопасности и механизм контроля и надзора за их деятельностью.

Литература

1. *Городов О.А.* Информационное право: учебник. М.: Проспект, 2007.
2. *Шиверский А.А.* Защита информации: проблемы теории и практики. М.: Юристъ, 1996.
3. *Копылов В.А.* Информационное право: учебник. М.: Юристъ, 2002. С. 103.