лики от 8 ноября 2006 года № 178 "О противодействии терроризму".

Однако оценивая в целом положительно состояние антиэкстремистского законодательства, просматриваются и явные просчеты, к которым относятся: декларативость принимаемых законов и нормативно-правовых актов; недостаточная координация действий со стороны всех заинтересованных участников процесса их реализации; недостаточность и нестабильность финансирования мероприятий. В виду этого среди причин и условий распространения экстремизма следует признать также неэффективность правовой системы, которая проявляется в несовершенстве законодательства и правоприменительной практики, низкой эффективности субъектов противодействия экстремизму, либерализованном характере мер юридической ответственности, низком уровне правосознания и правовой культуры общества, отсутствии реальной работы по правовому воспитанию населения и др.

В этой связи совершенствование законодательства необходимо именно в силу недостаточной эффективности правоприменительной практики, которая без четких законодательных ориентиров зачастую не в состоянии проводить последовательную линию по борьбе с экстремизмом, по его профилактике.

Поэтому необходимо подвергнуть экспертизе действующие, а также разработать и принять законы и другие правовые акты в сферах этнокультурной и миграционной политики, противодействия экстремизму.

Разработать законодательные акты, предусматривающие ответственность владельцев электронных носителей информации, Интернет-сайтов, за пропаганду экстремизма и терроризма. Пока не выработана единая юрид ическая практика по признанию электронных носителей к СМИ, чтобы можно было использовать имеющиеся меры ответственности СМИ к электронным источникам информации.

Литература:

1. Закон Кыргызской Республики Закон Кыргызской Республики от 12 июня 1999 года № 50 "О политических партиях" // "Эркинтоо" от 25 июня 1999 года №51; "Ведомости Жогорку Кенеша Кыргызской Республики" 1999 г., № 11; "Бюллетень Верховного суда КР" № 2 (18).
2. Закон Кыргызской Республики от 15 октября 1999 года № 111 "О некоммерческих организациях" // "Эркинтоо" от 3 ноября 1999 г. № 86; "Ведомости Жогорку Кенеша Кыргызской Республики" 2000 г., № 2, ст. 102.
3. Закон Кыргызской Республики от 31 декабря2008 года № 282 "О свободе вероисповедания и религиозных организациях в Кыргызской Республике" (с дополнениями от 15.06.2011 г.) // "Эркинтоо" от 16 января 2008 года № 3; "Ведомости Жогорку Кенеша Кыргызской Республики" 2008 г., №10, ст. 1110.
4. Закон Республики Кыргызстан от 2 июля 1992 года№ 938-ХП "О средствах массовой информации" // "Свободные горы" от 4 августа 1992 года № 99.
5. Закон Кыргызской Республики от 8 ноября 2006 года № 178 "О противодействии терроризму" (с изменениями и дополнениями по состоянию на 26.07.2011 г.) // "Эркинтоо" от 17 ноября 2006 года № 85; "Ведомости Жогорку Кенеша Кыргызской Республики", 2006 г., № 10, ст. 854; "Нормативные акты Кыргызской Республики" от 24 ноября 2006 года №47.

Рецензент: дло.н., профессор Шерипов Н.

Акназаров З.К.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЮРИДИЧЕСКИХ ЛИЦ ГРАЖДАНСКО-ПРАВОВЫМИ СРЕДСТВАМИ

Z.K. Aknazarov

PROVISION OF INFORMATION SECURITY SERVICE OF CIVIL LEGAL REMEDIES

УДК: 347.47.48/15.343

Статья посвящена обеспечению информационной безопасности юридических лиц гражданско-правовыми средствами. По мнению автора информационную безопасность юридического лица можно определить как состояние защищенности от внутренних и внешних угроз в деятельности юридического лица, направленной на достижение его целей и задач, а также защищенность информации принадлежащей юридическому лицу.

Article is devoted maintenance of information security of legal bodies -with civil-law means. According to the author information security of the legal person can be defined as a condition of securityfrom internal and external threats in the activity of the legal person directed on achievement of its purposes and problems, and also security of the information belonging to the legal body.

Юридические лица как участники гражданского оборота в своей деятельности в полной мере сталкиваются со всеми проявлениями информационной безопасности, или со всеми проблемами, которые нормы института информационной безопасности призваны решать.

Каждое юридическое лицо, независимо от его организационно-правовой формы или иных факторов, самостоятельно определяет средства и способы обеспечения информационной безопасности, учитывая существующие угрозы, исходя из своих интересов и потребностей, очерчиваемых целью, задачами и характером деятельности.

При этом на наш взгляд, уместно исходить из двух критериев: во-первых, любое юридическое лицо является субъектом информационных правоотношений, во-вторых, для разных юридических лиц задачи обеспечения информационной безопасности могут решаться по-разному. Исходя из этого представляется методически обоснованным оценивать значимость и масштабность конкретной проблемы по обеспечению информационной безопасности для определенных субъектов, в том числе юридических лиц.

Решение этой теоретической проблемы имеет и весьма практическую значимость. Методически представляется возможным и целесообразным в практическом отношении выявление, обобщение, и распространение на основе сложившегося опыта наиболее оправдавших себя и эффективных подходов и средств к обеспечению информационной безопасности юридических лиц.

Информационная безопасность юридического лица обычно определяется на основе приведенных подходов к пониманию информационной безопасности государства и ее обеспечения. Так, В.А.Северин полагает, что информационную безопасность предприятия можно определить как состояние защищенности его интересов в информационной среде от внутренних и. внешних источников угроз, последствиями которых может быть причинение ему материального ущерба .

По мнению Е. Волчинской, информационную безопасность бизнеса можно определить как состояние защищенности от внутренних и внешних угроз интересов субъектов бизнеса. А их интересы распространяются на три вида объектов: информацию, имеющую для конкретного бизнеса коммерческую ценность; информационные системы, в которых хранится и обрабатывается такая информация; сети связи, по которым она передается.

По мнению Журавлева Ю.А. "эти определения информационной безопасности юридического лица, важно дополнить указанием на защищенность деятельности юридических лиц, поскольку для массы юридических лиц эта деятельность разнообразна и по целям, и по задачам, и по объему, и по "включенности" в интересы более крупных структур (корпораций, объединений, общества, государства в целом). Следовательно, обеспечение информационной безопасности требует индивидуального подхода".

По нашему мнению, понятие информационной безопасности юридического лица можно определить как состояние защищенности от внутренних и внешних угроз в деятельности юридического лица, направленной на достижение его целей и задач, а также защищенность информации принадлежащей юридическому лицу.

Предложенное нами определение, на наш взгляд, в отличие существующих ставит во главу угла тезис о самостоятельном определении юридическим лицом цели и задачи обеспечения информационной безопасности. Дело в том, что основным подходом к пониманию информационной безопасности юридического лица и к решению задач по ее обеспечению, по нашему мнению, должен являться субъективный подход. У каждого юридического лица, интересы, цели и задачи в сфере обеспечения собственной информационной безопасности могут быть разные, на практике не существует универсальных критериев их определяющие. Можно определить только общие правовые и технические средства к решению юридическими лицами задач в области информационной безопасности, из них юридическое лицо, в соответствии с собственными интересами выбирает подходящие для своих целей и задач.

Согласно Концепции национальной безопасности основной задачей государства является повы-

шение безопасности информационных систем органов государственной власти. Обеспечивая собственную информационную безопасность, государство решает две задачи: развитие и модернизация сопутствующей инфраструктуры, расширение правового регулирования в сфере информационной безопасности.

Применительно к хозяйствующим субъектам государство решает иную задачу - создание условий данным субъектам для осуществления их информационной безопасности, т.е. обеспечивает предоставление им доступа к техническим и правовым средствам.

Единственным исключением из этого правила, послужила информационная безопасность в банковских учреждениях Кыргызской Республики. В этой сфере государство определило конкретные цели и задачи, которые должна решать банковская организация, средства и методы обеспечения информационной безопасности. Так, Постановлением Правления Национального банка Кыргызской Республики от 3 июня 1998 года №16/8 была утверждена "Концепция обеспечения безопасности информационных систем в банковских учреждениях Кыргызской Республики", в котором отмечается что развитие банковских технологий и платежной системы, а также развитие компьютерной техники требует качественно нового уровня построения систем информационной безопасности и их постоянного развития. Особенно это связано с развитием системы электронных платежей, систем электронных торгов и других, в результате которого все большее количество пользователей будут получать доступ к информационным ресурсам. Вместе с ростом количества пользователей повышается уязвимость информационных систем, растет риск совершения экономических преступлений с использованием компьютерных систем. Таким образом, принятие нормативных документов и обеспечение безопасности информационных систем являются задачей первостепенной важности для всей банковской системы Кыргызской Республики.

Целью Концепции является определение стратегии обеспечения информационной безопасности в банковской системе Кыргызской Республики и сведение к минимуму возможных потерь, вызванных действиями злоумышленников, аварийными сбоями и ошибками персонала.

В других случаях юридические лица в сфере обеспечения информационной безопасности самостоятельно определяют собственные цели и задачи по обеспечению информационной безопасности, исходя из специфики своей деятельности, степени ее зависимости от информации и иных факторов. Когда цели и задачи определены, необходимо тщательно выбрать подходящие технические средства их достижения и реализации, а также соотнести эти цели и задачи с существующими нормами права, регулирующими эти отношения, субъектом которых юридическое лицо будет становиться и при необходимости создать собственные локальные правовые акты.

На основе рассмотренных подходов к обеспечению информационной безопасности юридических лиц, важно определить основные принципы ооеспечения информационной безопасности юридических лиц с учетом существующих государственных принципов в этой сфере.

Принципами обеспечения информационной безопасности юридических лиц являются, на наш взгляд, следующие:

Принцип законности - юридические лица при создании своей системы информационной безопасности должны использовать только законные способы и средства обеспечения информационной безопасности, пользоваться только теми механизмами, которые предоставлены законодателем или которые не запрещены законодательно.

Принцип самостоятельности - юридические лица самостоятельно должна определять свою политику обеспечения информационной безопасности исходя из специфики деятельности, а также определять какие меры в данной области должны приниматься и финансовые затраты в этом направлении.

Принцип открытости - означает необходимость обеспечения иным субъектам доступу на информацию которая должна быть предоставлена согласно законодательству Кыргызской Республики и не может быть конфиденциальной.

Принцип реальности поставленных задач означает то, что юридическое лицо должно относить к конфиденциальной только ту информацию, которую в состоянии защитить, или только та информация, получаемая извне, может быть применена при принятии решений, достоверность которой юридическое лицо может проверить.

Приведенные принципы определяют всю деятельность юридического лица по обеспечению собственной информационной безопасности, а также, должны учитываться при определении государственной политики в рассматриваемой сфере, поскольку, как мы отмечали выше, создание условий для обеспечения юридическими лицами своей информационной безопасности является одной из составляющих национальных интересов Кыргызской Республики в сфере обеспечения информационной безопасности.

В основе субъектного подхода к обеспечению информационной безопасности юридического лица лежат цели, которые юридическое лицо преследует в рассматриваемой сфере, определяемые, в свою очередь, назначением и положением юридического лица в социальной действительности. Любая организация должна стремиться к тому, чтобы обеспечить системный подход, как к своей основной деятельности, так и к сопутствующим и необходимым задачам, в частности, по обеспечению информационной безопасности.

Задача по обеспечению информационной безопасности является как правило, вспомогательной, обеспечивающей основную, уставную деятельность юридического лица. Обеспечение информационной, безопасности является безусловно необходимым, хотя и может выражаться в различных формах - от простого нераспространения конфиденциальной