УДК 34.028

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

В.В. Боричевская

Полесский государственный университет

Вследствие пробелов в законодательном регулировании, организации управления финансами, отсутствия правовой базы для действенного контроля, банковская система Беларуси оказалась неподготовленной к развитию рынка и появлению большого количества новых альтернативных финансовых структур.

Безопасность банка, исходя из определения, содержащегося в Большом экономическом словаре, представляет собой состояние защищенности его жизненно важных интересов от недобросовестной конкуренции, противоправной деятельности криминальных формирований и отдельных лиц, способность противостоять внешним и внутренним угрозам, сохранять стабильность функционирования и развития в соответствии с уставными целями. Основным интересом банка (из числа жизненно важных) является приобретение, накопление и распределение в соответствии с уставными целями денежных средств и иных благ, основной целью деятельности банка является – извлечение прибыли.

В число необходимых условий функционирования банка является обязанность руководителя банка разработать и обеспечить эффективное функционирование внутренней системы обеспечения защиты интересов банка. Эта задача решается путем разработки соответствующей нормативной базы банка, а также организацией внутреннего контроля за соблюдением сотрудниками банка законодательства, нормативных актов и стандартов профессиональной деятельности.

Успешная деятельность банка в нынешних условиях невозможна без формирования и использования информации (информационных ресурсов) – отдельных документов или их массивов. Информационные ресурсы банка формируются путем создания, сбора и приобретения документированной информации о фактах, событиях, и обстоятельствах, имеющих отношение к кредитно-финансовой сфере. В целях создания оптимальных условий для удовлетворения информационных потребностей своих структурных подразделений, клиентов, а также органов государственной власти банк приобретает и использует информационные системы, информационные технологии и средства их обеспечения. Для этого привлекаются средства вычислительной техники и связи, обеспечивающие обработку, хранение и передачу информации.

Ответственность за неправомерные деяния в отношении объектов информатизации в целом и банка, в частности, установлена соответствующими нормами ГК РБ, УК РБ, КоАП РБ, ТК РБ, другими актами законодательства, а также корпоративными документами организаций – собственников информации.

Информацию банка, защищаемую законом от угроз преступного характера, можно разделить на:

1. Сведения конфиденциального характера, составляющие коммерческую и банковскую тайну. Ответственность за преступные посягательства на них предусмотрена ст. 255 УК "Разглашение коммерческой тайны".

2. Компьютерная информация. Уголовные наказания за преступное посягательство на этот вид информации установлены главой 31 УК РБ "Преступления против информационной безопасности".

Мировая практика показывает, что многие страны в настоящее время сталкиваются с небывалым ростом преступлений в банковской сфере, в том числе, связанных с использованием методов из сферы высоких технологий.

Согласно данным отечественных и зарубежных источников, преступные посягательства на информацию (прежде всего утечка конфиденциальной информации и злоупотребление конфиденциальной информацией) занимают одно из первых мест среди основных факторов риска, отрицательно влияющих на результаты экономической деятельности. В большинстве развитых иностранных государств такие деяния влекут применение весьма строгих санкций. Например, в США для лиц, злоупотребляющих информацией при заключении сделок с ценными бумагами, предусмотрены штрафы в 1 млн. долл. (для юридических лиц – 2,5 млн. долл.) либо тюремное заключение сроком на 10 лет. В Великобритании – денежный штраф в неограниченной сумме и (или) тюремное заключение до 7 лет, а для соучастников – 6-тимесячное содержание под стражей и (или) штраф 200 ф. ст. По оценке отечественных и зарубежных исследователей *кадры банка* являются важнейшим внутренним источником риска. При этом, прежде всего, имеются в виду риски, связанные с принятием персоналом ошибочных решений. Однако не исключены и угрозы, соединенные с противоправным поведением персонала.

Для создания эффективной системы противодействия организованной преступности в банковской сфере необходимо учитывать следующие исходные требования, выработанные на основе многолетней практики борьбы с преступлениями данного вида в зарубежных странах:

- Полностью избавиться от преступности в банковской сфере невозможно, однако ее можно контролировать;
- Чрезмерный контроль может, в свою очередь, вести к коррупции;
- Постоянные механизмы контроля неэффективны, т.к. никакая система правил (запретов) не застрахована от создания системы противодействия этим запретам и от коррумпированного влияния;
- Принятые с самыми хорошими намерениями нововведения зачастую превращаются в источник новых видов банковских правонарушений, коррупции и должностных преступлений.

Важными факторами повышения эффективности борьбы с преступностью в банковской сфере является совершенствование действующего законодательства, а также и сотрудничества банков и правоохранительных органов.