УДК 347.734

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ: ПРАВОВОЙ АСПЕКТ

Полякова Любовь Григорьевна,
Могилевский государственный университет имени А. А. Кулешова
(г. Могилев, Беларусь)

В условиях развития информационного общества для любого субъекта предпринимательской деятельности, в том числе банка, одним из важнейших ресурсов ведения бизнеса является информация, которая имеет высокую экономическую ценность. Обеспечение безопасности информационных ресурсов и информационных систем в банковской сфере рассматривается как один из важнейших факторов эффективной деятельности банков.

С развитием информационного общества появилась потребность в защите его главного движущего фактора – информации. Опыт эксплуатации информационных систем и ресурсов в различных сферах жизнедеятельности общества показывает, что существуют различные и весьма реальные угрозы потери информации, приводящие к негативным последствиям. А развитие информационных технологий и их активное внедрение создает качественно новые угрозы несанкционированного воздействия на информационные ресурсы и информационные системы.

Осуществление банковской деятельности напрямую связано с получением, переработкой, хранением и использованием информации, имеющей высокую экономическую ценность. При этом следует заметить, что банковская информация может иметь разные правовые режимы в зависимости от содержания и назначения ее использования и затрагивает интересы, не только самого банка, но и его клиентов [1, с. 217]. Данная информация используется при работе с клиентами, партнерами, внутри банка, к ней имеет непосредственный доступ персонал банка, а так же существует множество внешних злоумышленников, заинтересованных в организации несанкционированного доступа к интересующей их информации. Любые действия пользователей на компьютерах и в сетях приводят к перемещению или к обработке информации. Кроме того, информация находится в стадии хранения на информационных ресурсах.

В этих условиях информационная безопасность банков становится важнейшим элементом безопасности банка в целом.

Под информационной безопасностью принято понимать защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений [2, с. 23].

Информационная безопасность не сводится исключительно к защите информации. Субъект информационных отношений может пострадать (понести убытки) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в обслуживании клиентов.

В качестве стандартной модели безопасности информационных ресурсов банков используется модель из трех категорий: конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право (исключение доступа к информации несанкционированных пользователей); целостность – избежание несанкционированной модификации информации (свойство сохранять неизменность или обнаруживать факт несанкционированного изменения информации); доступность – свойство своевременно и достоверно представлять требуемую информацию в соответствии с установленными правилами и правами доступа [3, п. 2].

Соответственно в банковском законодательстве под информационной безопасностью понимается многоуровневый комплекс организационных мер, аппаратно-программных и технических средств, обеспечивающих защиту от случайных и преднамеренных угроз, в результате реализации которых возможно нарушение свойств доступности, целостности, подлинности или конфиденциальности обрабатываемой, хранящейся или передаваемой информации [3, п. 2].

Основными целями обеспечения информационной безопасности банка являются повышение надежности защиты информации в процессе ее обработки, хранения и передачи; выявление уязвимостей системы обеспечения информационной безопасности, предупреждение реализации угроз, минимизация ущерба от реализации угроз информационной безопасности, повышение деловой репутации банка, которые достигаются при соблюдении правил и требований информационной безопасности, необходимых для получения оптимального баланса между надежностью и оперативностью функционирования банка.

В соответствии с нормами действующего законодательства в системе мер по защите информационной безопасности реализуются правовые, организационные (административные), технические (программно-технические) меры [4, ст. 29].

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы банка. В качестве правовых мер следует рассматривать действующие в Республике Беларусь нормативные правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Следует указать на необходимость постоянного совершенствования нормативной базы, регулирующей вопросы безопасного функционирования критически важных объектов информатизации [5, с. 17].

Обеспечение информационной безопасности банка достигается реализацией комплекса необходимых мер. Кроме правовых мер защиты, система обеспечения безопасности информации банка должна предусматривать организационные и программно-технические меры и средства защиты информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом, при использовании технических и программных средств.

Национальный банк Республики Беларусь устанавливает для банков и небанковских кредитно-финансовых организаций обязательные требования к безопасному функционированию объектов и безопасности оказания банковских услуг, защите информационных ресурсов и информации, распространение и (или) предоставление которых ограничено и осуществляет контроль за обеспечением безопасности и защиты информационных ресурсов в банках и небанковских кредитно-финансовых организациях [6, ст. 26].

Для обеспечения защиты информационных ресурсов в банках разрабатывается политика информационной безопасности, включающая в себя обязательные требования по защите информации, распространение и предоставление которой ограничено, а также требования к контролю за обеспечением безопасности и защиты информационных ресурсов в банках.

Политика информационной безопасности банка представляет собой официально принятую руководством банка систему взглядов на проблему обеспечения информационной безопасности банка.

Политика информационной безопасности разрабатывается в соответствии с законодательством по информационной безопасности Республики Беларусь, требованиям нормативных документов Национального банка Республики Беларусь.

К направлениям политики информационной безопасности относят: защиту помещений и объектов от несанкционированного доступа; защиту информации в бумажном документообороте; защиту информации от утечки по техническим каналам; возможные угрозы при проведении мероприятий и эксплуатации технических средств; обеспечение информационной безопасности в компьютерных сетях; обеспечение информационной безопасности в платежных системах, в том числе с использованием банковских платежных карточек и др.

Таким образом, информационная безопасность банков – один из важнейших факторов их эффективной деятельности. Информационная безопасность банка – это состояние защищенности объектов защиты (информационных ресурсов, технических и программных средств информационных технологий и т.д.), при котором обеспечивается их конфиденциальность, доступность и целостность. Безопасность информации определяется отсутствием недопустимого риска, связанного с несанкционированными и непреднамеренными воздействиями на информацию и на другие ресурсы информационной системы, используемые в банке. Неотъемлемым элементом информационной безопасности в банковской сфере является состояние защищенности сбалансированных интересов самого банка и его клиентов, взаимодействующих в области создания, обращения, пользования, сохранения информационных ресурсов.

Список источников

1. Полякова, Л. Г. Банковская информация: терминологический аспект / Л. Г. Полякова // THESAURUS : зб. навук. пр. / УА «Магілёўскі інстытут Міністэрства ўнутраных спраў Рэспублікі Беларусь». – Магілёў, 2016. – Вып. 2. – С. 215–219.
2. Агамов, А. Н. Правовое регулирование обеспечения информационной безопасности : учеб. пособие / А. Н. Агамов, А. А. Шмелев. – М. : НЦПИ, 2002. – 126 с.
3. Об утверждении Инструкции об организации системы внутреннего контроля в банках, открытом акционерном обществе «Банк развития Республики Беларусь», небанковских кредитно-финансовых организациях, банковских группах и банковских

холдингах [Электронный ресурс] : постановление Правления Национального банка Респ. Беларусь, 30 нояб. 2012 г., № 625 : в ред. постановления Правления Национального банка Респ. Беларусь от 29.06.2016 г. // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.

4. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : в ред. Закона Респ. Беларусь от 11.05. 2016 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.
5. Матвеев, А. А. Направления развития законодательства в сфере информационной безопасности // А. А. Матвеев, А. Ю. Чернолевский // Промышленно-торговое право. – 2017. – № 9. – С. 17–21.
6. Банковский кодекс Республики Беларусь [Электронный ресурс] : 25 окт. 2000 г., № 441-З : принят Палатой представителей 3 окт. 2000 г. : одобр. Советом Респ. 12 окт. 2000 г. : в ред. Закона Респ. Беларусь от 17.07.2018 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.