

УДК 347.734

**ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ СУБЪЕКТОВ ПРЕДПРИНИМАТЕЛЬСКОЙ  
ДЕЯТЕЛЬНОСТИ**

Полякова Любовь Григорьевна  
старший преподаватель кафедры гражданского и  
хозяйственного права учреждения образования  
«Могилевский государственный университет  
имени А. А. Кулешова»  
(г. Могилев, Беларусь)

*Современное общественное развитие характеризуется становлением информационного общества, где информация является важнейшим ресурсом во всех сферах его жизнедеятельности. В этих условиях проблема обеспечения безопасности информационных ресурсов приобретает особую актуальность. Информационная безопасность рассматривается как один из факторов эффективного развития предпринимательской деятельности.*

Информация в современных условиях – важнейший ресурс ведения бизнеса. Осуществление предпринимательской деятельности напрямую связано с получением, переработкой, хранением и использованием экономически ценной информации. В процессе предпринимательской деятельности образуется информация о самом субъекте предпринимательской деятельности, его контрагентах, сделках, платежах, совершаемых, в том числе, по публичным обязательствам, а также иного рода информация. При этом информация, обладателем которой является субъект предпринимательской деятельности, в зависимости от содержания и назначения может иметь разные правовые режимы: режим коммерческой тайны, режим банковской тайны, режим персональных данных и другие.

Согласно действующему законодательству информация делится на два вида – общедоступную информацию (информация, доступ к которой, распространение и (или) предоставление которой не ограничены) и информацию, распространение и (или) предоставление которой ограничено [1, ст. 15, 16]. Проблема обеспечения информационной безопасности напрямую связана с несанкционированным доступом к информации ограниченного доступа. Неправомерный доступ к коммерческой, банковской тайне и иной информации ограниченного доступа может нанести организации значительный материальный ущерб, а также имиджевые издержки. Опыт эксплуатации информационных систем и ресурсов в различных сферах жизнедеятельности 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 системы и информационные ресурсы.

В этих условиях проблема обеспечения безопасности информационных ресурсов приобретает особую актуальность. Информационная безопасность следует рассматривать как один из факторов эффективного развития предпринимательской деятельности. При этом информационная безопасность белорусских организаций рассматривается как элемент национальной безопасности [2, с. 19].

Основной целью обеспечения информационной безопасности субъекта предпринимательской деятельности выступает повышение надежности защиты информации в процессе ее обработки, хранения, передачи информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом, при использовании технических и программных средств.

На законодательном уровне под информационной безопасностью принято понимать состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [3, п. 4]. Следовательно, под информационной безопасностью субъекта предпринимательской деятельности следует понимать состояние защищенности информации и всей организации от преднамеренных или случайных действий, приводящих к нанесению ущерба ее владельцам или пользователям. Утечка информации может привести к серьезным проблемам для компании (от значительных финансовых убытков до полной ликвидации).

Среди основных направлений по информационному обеспечению предпринимательства можно выделить: организация и осуществление защиты конфиденциальной информации; разработка и внедрение локальных актов, например положения о коммерческой тайне; автоматизация информации по вопросам безопасности; проверка правил ведения закрытого делопроизводства; проверка работников на предмет соблюдения ими правил обеспечения информационной и экономической безопасности.

В системе обеспечения информационной безопасности реализуются правовые (законодательные), морально-этические, технологические, организационные (административные), программно-технические меры защиты информационной безопас-

ности. Правовые меры защиты носят в основном упреждающий, профилактический характер.

Правовое обеспечение информационной безопасности представляет собой деятельность законодательных и исполнительных органов государственной власти по разработке, реализации и контролю исполнения совокупности нормативных правовых актов, регламентирующих практическую деятельность по защите информации. Приоритетным направлением в обеспечение информационной безопасности в нашей стране было и остается развитие законодательства в этой сфере. Система законодательства в сфере обеспечения информационной безопасности включает в себя меры, направленные на установление правил участия в интернациональном информационном обмене, на развитие современных информационных и телекоммуникационных технологий, на защиту информационных ресурсов от несанкционированного доступа; разработку, распространение, внедрение средств и способов защиты информации; организацию и совершенствование системы обеспечения информационной безопасности.

Для обеспечения защиты информационных ресурсов возникает необходимость разработки политики информационной безопасности, включающей в себя обязательные требования к защите информационных ресурсов и информации, распространение и предоставление которых ограничено, а также требования к контролю за обеспечением безопасности и защиты информационных ресурсов.

Политика информационной безопасности организации – общие намерения и направления деятельности по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, официально сформулированные собственником (владельцем) информационной системы [4].

Политика информационной безопасности разрабатывается в соответствии с Конституцией, законодательством Республики Беларусь, регламентирующим вопросы обеспечения информационной безопасности. К направлениям по политике 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 и другое.

Основной целью, на достижение которой направлены все положения политики информационной безопасности, является защита субъектов информационных отношений от возможного нанесения им материального, физического или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня информационного и финансового риска.

Исходя из изложенного, под информационной безопасностью субъектов предпринимательской деятельности следует понимать состояние (положение) защищенности сбалансированных интересов самого субъекта предпринимательской деятельности и иных лиц, взаимодействующих с субъектом в области обращения, пользования, хранения информации, создания, обращения, пользования, сохранения информационных ресурсов. В демократическом социальном правовом государстве это состояние может быть достигнуто на основе баланса государственных, общественных и частных интересов в информационной сфере путем применения эффективных механизмов правовой защиты.

#### Список использованной литературы

1. 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.
2. Матвеев, А. А. Направления развития законодательства в сфере информационной безопасности // А. А. Матвеев, А. Ю. Чернолевский // Промышленно-торговое право. – 2017. – №9. – С. 17-21.
3. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Респ. Беларусь, 09 нояб. 2010 г., № 575: в ред. Указа Президента Респ. Беларусь от 24.01.2014 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.

4. О некоторых вопросах технической и криптографической защиты информации [Электронный ресурс]: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 30 авг. 2013 г., № 62: в ред. приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 11.10.2017 г.// ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.
5. Агамов, А. Н. Правовое регулирование обеспечения информационной безопасности : учеб. пособие / А. Н. Агамов, А. А. Шмелев. – М. : НЦПИ, 2002. – 126 с.