

## **О некоторых проблемах законодательного обеспечения информационной безопасности бизнеса**

(выступление на конференции деловой газеты «Ведомости»  
«Информационная безопасность бизнеса. Реалии нового законодательства»,  
Москва, 1 ноября 2011 г.)

Мы полагаем, что проблема информационной безопасности бизнеса (далее буду сокращать – ИББ) – комплексная и ее решение требует таких же комплексных подходов.

Исходя из положений Доктрины информационной безопасности Российской Федерации ИББ можно определить как состояние защищенности от внутренних и внешних угроз интересов субъектов бизнеса в информационной сфере. А их интересы распространяются на три вида объектов:

информацию, имеющую для конкретного бизнеса коммерческую ценность, и права на нее;

информационные системы, в которых хранится и обрабатывается такая информация;

сети связи, по которым она передается.

Защита первых двух объектов, а также защита локальных (корпоративных) сетей связи полностью ложится на плечи предпринимателя, защита сетей связи общего пользования, которыми пользуются предприниматели для передачи информации - на собственников этих сетей (операторов связи).

**Внешние угрозы** реализуются в форме недобросовестной конкуренции и промышленного шпионажа.

Правовую базу защиты от внешних угроз ИББ составляют сегодня Федеральный закон № 135-ФЗ «О защите конкуренции» и ряд статей Уголовного кодекса РФ, устанавливающих ответственность за некоторые преступления, которые можно отнести к недобросовестной конкуренции и промышленному шпионажу.

Недобросовестная конкуренция включает, в том числе, такие действия как распространение ложных, неточных или искаженных сведений, которые могут причинить убытки хозяйствующему субъекту либо нанести ущерб его деловой репутации; незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну; незаконное приобретение и использование исключительного права на средства индивидуализации юридического лица, средства индивидуализации продукции, работ или услуг.

Признак недобросовестности – отсутствие согласия на указанные действия со стороны обладателя информации или правообладателя. При этом речь идет не только о разглашении, но и о других действиях с информацией - ее получении и использовании.

Незаконные модификация, блокирование, уничтожение информации это самостоятельное уголовное преступление, не связанное с недобросовестной конкуренцией.

***Внутренние угрозы*** интересам субъекта бизнеса в информационной сфере реализуются в результате недобросовестности и противозаконной деятельности персонала, а также недостаточно развитой и устойчивой системы обеспечения информационной безопасности. По мнению многих руководителей внутренние угрозы ИББ представляют для бизнеса наибольшую опасность.

Правовую базу защиты от внутренних угроз составляют, прежде всего, Трудовой кодекс Российской Федерации, Гражданский кодекс Российской Федерации, федеральные законы «О коммерческой тайне», «О персональных данных», «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», «О связи», «Об информации, информационных технологиях и о защите информации», «О лицензировании отдельных видов деятельности», «Об электронной подписи», «О техническом регулировании».

Итак, в целях обеспечения ИББ субъект бизнеса должен организовать защиту следующих объектов:

- 1) открытой информации, размещаемой на сайте организации;
- 2) имеющейся в организации информации ограниченного доступа, в том числе информации, составляющей государственную, коммерческую и профессиональные тайны; инсайдерскую информацию, персональные данные;
- 3) права на доступ к информации, необходимой для ведения бизнеса;
- 4) корпоративных информационных систем и сетей;
- 5) объектов интеллектуальной собственности, правообладателем которых является юридическое лицо.

Меры обеспечения ИББ субъект вправе устанавливать самостоятельно в соответствии с российским законодательством, за исключением случаев, когда федеральный закон и принимаемые в соответствии с ним нормативные правовые акты устанавливают обязательные для соблюдения требования. Например, требования по защите сведений, составляющих государственную тайну, требования по защите прав субъектов персональных данных, требования получения лицензии на отдельные виды деятельности, дополнительные требования по обеспечению информационной безопасности, установленные для объектов, оказывающих существенное влияние на безопасность государства в информационной сфере.

**Какие правовые условия для обеспечения ИББ существуют и насколько они эффективны? Рассмотрим это для каждого из объектов защиты.**

(1) Защита открытой информации, размещенной на сайте организации, это право организации и ограничения этого права не установлены.

(2) Что касается защиты информации ограниченного доступа, то здесь есть проблемы.

Прежде всего, отсутствует классификация информации ограниченного доступа, а количество видов такой информации уже перевалило за 40. Не установлены общие требования к формированию отдельных правовых режимов ограничения доступа к информации, права и обязанности обладателей информации, ответственность за ее разглашение.

По видам тайн.

Коммерческая тайна. После принятия четвертой части Гражданского кодекса Российской Федерации и внесения изменений в Федеральный закон № 98-ФЗ «О коммерческой тайне» понятие информации, составляющей коммерческую тайну, принципиально изменилось. Если прежде в состав этой информации могли входить сведения, составляющие секрет производства, то теперь информация, составляющая коммерческую тайну, практически отождествляется со сведениями, составляющими секрет производства (ноу-хау) в смысле статьи 1465 ГК РФ. Что это означает?

В обычаях делового оборота к коммерческой тайне относится, например, информация о потребителях и поставщиках, об условиях договоров поставок и предоставления услуг. Назвать эту информацию «секретом производства», значит исказить смысл этого термина. Но иного способа обеспечить конфиденциальность этой информации нет. Помимо обеспечения конфиденциальности информации, составляющей коммерческую тайну, что является условием защиты ее в этом режиме, руководитель вынужден исполнять все требования оборота этой информации как объекта исключительных прав.

Следует отметить, что проблемы реализации данного федерального закона известны и у ряда экспертов есть предложения по изменению отдельных положений закона и части четвертой Гражданского кодекса. Однако в Государственную Думу соответствующий законопроект не внесен.

Эта ситуация, как ни странно, влияет и на формирование правового института служебной тайны, потому что нужен режим, в котором можно

охранять информацию, имеющую коммерческую ценность, но не являющуюся секретом производства.

Служебная тайна. Часть организаций, плотно контактирующих с органами государственной власти, нередко получает документы с пометкой «Для служебного пользования» (ДСП).

Существующий на сегодняшний день порядок работы со служебной информацией определяется Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» и распространяется только на указанные органы.

Правовой режим обращения такой информации вне федеральных органов исполнительной власти законодательно не установлен, хотя данная категория информации (непосредственно или по смыслу) присутствует в большом количестве федеральных законов (около 40).

Базовый для данного законодательства Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет уровень законодательного регулирования – это федеральный закон, устанавливающий условия отнесения информации к сведениям, составляющим служебную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение (ст. 9). Федеральный закон, регулирующий порядок установления режима служебной тайны, не принят и ответственность не установлена.

С 2004 года в Государственной Думе находился на рассмотрении проект федерального закона «О служебной тайне», внесенный группой депутатов, включая меня. Однако рассмотрения как такового не было. Вначале мы дорабатывали проект по замечаниям органов государственной власти, внесли новую редакцию в 2006 году. И с тех пор нам не удавалось преодолеть позицию правительства, которое считает, что реализация

федерального закона потребует бюджетных затрат на техническую защиту информации, составляющей служебную тайну.

Мы считаем, что эта позиция спорна, потому что сейчас документы с пометкой «ДСП» широко используются и защищаются в органах государственной власти из имеющихся средств. Для нас очевидно, что практика широкого использования такой пометки в документах органов государственной власти всех уровней, в том числе направляемых в государственные и негосударственные организации, требует правового регулирования на уровне федерального закона (включая доступ к такой информации, ее передачу, хранение и уничтожение), а также установление ответственности за ее разглашение.

Вместе с тем, за прошедшие 5 лет было принято несколько федеральных законов, влияющих на концепцию рассматриваемого законопроекта (это введение в действие части четвертой Гражданского кодекса, федеральные законы о персональных данных и об использовании инсайдерской информации).

В связи с этим, Комитетом Государственной Думы по безопасности было принято решение снять законопроект с рассмотрения через отклонение при рассмотрении его в первом чтении. Будем работать над новой концепцией законопроекта.<sup>1</sup>

Профессиональная тайна. Обязанность по защите профессиональной тайны и состав защищаемой информации проистекают из специальных законов, в том числе: законов о связи, о частной охранной и детективной деятельности, о нотариате, об охране здоровья граждан, банковской деятельности, об адвокатской деятельности и многих других.

Анализ содержания сведений, составляющих профессиональную тайну, свидетельствует о том, что в этом режиме охраняются, как правило,

---

<sup>1</sup> Интересующихся этой проблемой отошлю к нашей с Еленой Константиновной Волчинской статье в журнале «Государственная служба», № 2, 2011 год.

персональные данные и информация, составляющая коммерческую тайну, доверенные специалисту в рамках его профессиональной деятельности.

Однако общих требований по безопасности информации, составляющей профессиональную тайну нет, за исключением требований обеспечения ее конфиденциальности, требований закона об обеспечении безопасности персональных данных при их обработке и общих положений о защите информации, предусмотренных Федеральным законом «Об информации...».

Инсайдерская информация. Перечень инсайдерской информации установлен приказом Федеральной службы по финансовым рынкам от 12 мая 2011 г. и занимает 22 страницы. Интересно, что в состав инсайдерской информации может входить и информация, составляющая коммерческую, служебную, банковскую, налоговую и иную тайну.

Вместе с тем, в соответствии с законом, данный вид информации не является априори информацией ограниченного доступа (это временный режим). Закон устанавливает условия, при которых использование такой информации правомерно. Более того, законом установлены требования по раскрытию такой информации в определенных случаях. Однако юридические лица обязаны принять меры по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации.

За неправомерное использование инсайдерской информации установлена уголовная (Статья 185.6 УК РФ) и административная ответственность (Статья 15.21 КоАП РФ).

При этом закон не устанавливает требования к порядку защиты инсайдерской информации, за исключением отсылки к [законодательству](#) о государственной тайне и о налогах и сборах. В связи с чем возникает вопрос о мерах защиты инсайдерской информации, которые в случае ее неправомерного использования будут признаны судом достаточными.

Персональные данные. Вопросы совершенствования законодательства о персональных данных и анализа проблем правоприменения были в центре

внимания последние года три, поэтому нет необходимости особенно это комментировать. В последней версии федерального закона было учтено большинство предложений операторов информационных систем персональных данных, за исключением положений по обеспечению безопасности персональных данных и правовых режимов конфиденциальности персональных данных. Несмотря на концепцию совершенствования закона, выработанную на парламентских слушаниях, в окончательном тексте получила закрепление позиция правительства по данному вопросу. Жизнь покажет эффективность этих решений.

Тем не менее, ментальность наша начала меняться: и граждане стали внимательнее относиться к своим данным, и операторы учатся их защищать. Этот процесс в Европе занял не менее 10 лет. Мы пока в середине пути.

Проблема защиты персональных данных обостряется для тех, кто ведет электронный бизнес. Электронные магазины до сих пор собирают избыточную информацию о клиентах. Например, если товар доставляется по месту работы, зачем требовать домашний адрес. Да и к защите клиентских баз еще относятся недостаточно серьезно. Примерами тому недавние утечки данных, накапливаемых операторами связи.

Целям обеспечения ИББ служит и электронная подпись. В связи с расширением использования информационных технологий для ведения бизнеса (подготовка и заключение договоров в электронном виде, проведение электронных платежей, электронные торги и т.п.) остро встают вопросы защиты передаваемой информации от модификации, копирования и уничтожения, а также обеспечение неизменяемости маршрута сообщений и аутентификации адресата. Определенный вклад в решение этих задач может внести использование технологий электронной подписи.

Федеральный закон № 63-ФЗ «Об электронной подписи», принятый в апреле текущего года, позволил сделать шаг вперед в использовании электронных подписей разного вида.

Вместе с тем, в законе не решен главный вопрос: сферы допустимого и обязательного использования электронной подписи разных видов. Требования к электронной подписи должны быть включены в федеральные законы, предусматривающие использование таких подписей в различных правоотношениях. Такой подход имеет право на жизнь и он реализован во втором принятом Федеральном законе № 65-ФЗ, предусматривающем внесение изменений в связи с принятием Федерального закона «Об электронной подписи», однако этим законом изменения внесены в 6 федеральных законов, а следует их внести, как минимум, еще в 28.

Остались недостаточно определенными: правовой статус подписи юридического лица; права, обязанности и ответственность подписывающего лица и лица, принимающего подпись; процедуры проверки ЭП (в том числе проверки вида ЭП); условия и правовые последствия использования средств ЭП в автоматическом режиме. Не предусмотрена разработка технических требований к сервисам, предоставляемым УЦ.

Так что работы впереди еще много.

(3) Следующий объект защиты - право на доступ к информации, необходимой для ведения бизнеса. Реализация этого права осуществляется в рамках федеральных законов № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». Эти законы закрепляют права и юридических лиц на доступ к соответствующей информации.

Но немаловажное значение имеют условия доступа: платность, форма представления информации. В частности, мы с вами были свидетелями спора по поводу платности услуг Ростехрегулирования по предоставлению текстов национальных стандартов. Интересы общества отстаивал Институт развития свободы информации. Точку в этом споре поставил Верховный Суд, который своим решением от 2

февраля 2010 года фактически признал правомерным предоставление за плату текстов национальных стандартов. Справедливости ради, надо сказать, что новые стандарты размещаются на сайте Ростехрегулирования в формате PDF. Однако там же присутствует предупреждение, что эти тексты «не подлежат копированию, тиражированию и дальнейшему распространению». Понятно, что такая услуга позволяет только ознакомиться с документом и принять решение о целесообразности его приобретения за плату.

Необходимо отметить, что в целях обеспечения безопасности бизнеса, в том числе информационной безопасности, часто требуется проверка персональных данных принимаемых на работу лиц, в том числе документов об образовании. Полагаем, что организацию предоставления такой очень востребованной услуги может взять на себя Минобрнауки, для чего надо только создать федеральный банк таких документов.

Аналогичную услугу юридическим лицам может оказывать МВД России по проверке паспортных данных, тем более, что база данных там уже создана. При этом вполне возможно организовать предоставление информации таким образом, чтобы оно не нарушало требования Федерального закона № 152-ФЗ «О персональных данных».

(4) Защита локальных (корпоративных) компьютерных систем и сетей осуществляется собственниками этих объектов самостоятельно или с привлечением специализированных организаций. Правовую основу этой деятельности составляет Федеральный закон №126-ФЗ «О связи».

(5) Защита объектов интеллектуальной собственности, правообладателем которых является организация, осуществляется в соответствии с положениями части четвертой Гражданского кодекса Российской Федерации.

Особую проблему в этой связи представляет участвовавшие нарушения интеллектуальных прав в Интернете, в том числе авторских прав на дизайн и принципы организации корпоративных сайтов. Защита авторских прав, нарушаемых с использованием Интернета представляет собой глобальную

проблему в силу трансграничности Сети. Вместе с тем, в рамках юрисдикции России наше законодательство позволяет защищать эти права.

Обеспечивая информационную безопасность бизнеса, необходимо учитывать установленные законом ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.<sup>2</sup>

В связи с этим, необходимо обратить внимание на использование специальных технических средств, предназначенных для негласного получения информации (СТС). Эти средства в последнее время получили развитие и широко используются в бизнесе как в целях недобросовестной конкуренции, так и в целях защиты от нее.

Свободное использование таких технических средств<sup>3</sup> физическими и юридическими лицами запрещается Федеральным законом № 144-ФЗ «Об оперативно-розыскной деятельности». Этим же законом ограничивается разработка, производство, реализация и приобретение в целях продажи СТС индивидуальными предпринимателями и юридическими лицами, а также установлен особый порядок ввоза в Российскую Федерацию и вывоз за ее пределы указанных технических средств (только по лицензии).

---

<sup>2</sup> Это определено Федеральным законом «Об информации... (ст. 16)».

<sup>3</sup> К таким средствам относятся (согласно Постановлению Правительства от 01.07.96 № 770).

1. Специальные технические средства для негласного получения и регистрации акустической информации.
2. Специальные технические средства для негласного визуального наблюдения и документирования.
3. Специальные технические средства для негласного прослушивания телефонных переговоров.
4. Специальные технические средства для негласного перехвата и регистрации информации с технических каналов связи.
5. Специальные технические средства для негласного контроля почтовых сообщений и отправлений.
6. Специальные технические средства для негласного исследования предметов и документов.
7. Специальные технические средства для негласного проникновения и обследования помещений, транспортных средств и других объектов.
8. Специальные технические средства для негласного контроля за перемещением транспортных средств и других объектов.
9. Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.
10. Специальные технические средства для негласной идентификации личности.

Установлена уголовная ответственность за незаконное производство, сбыт или приобретение СТС, за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан с использованием СТС (ст. 138 УК РФ).

Предусмотрена и административная ответственность за нарушение правил производства, хранения, продажи и приобретения СТС (статья 20.23. КоАП РФ). Эти положения законодательства надо знать и учитывать при формировании систем ИББ.

Как уже упоминалось ранее, государством могут быть установлены для отдельных объектов дополнительные требования по обеспечению информационной безопасности.

В рамках полномочий ФСТЭК России выделена функция обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (так называемые ключевые системы информационной инфраструктуры),. Это информационные системы, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям. Такие системы могут функционировать, в том числе, в составе критически важных объектов.

Анализ законодательства свидетельствует о том, что объектный состав ключевых систем информационной инфраструктуры и состав критически важных объектов Российской Федерации могут различаться. При этом, если состав критически важных объектов определен секретными Постановлениями Правительства РФ, то состав ключевых систем информационной инфраструктуры и требования к таким системам законодательно не установлены. Таким образом, имеет место неопределенность объектов защиты, нарушение безопасности которых угрожает национальной безопасности.

В рамках указанных полномочий ФСТЭК России утвердил в 2007 году ряд документов методического характера, имеющих гриф «ДСП», которые стимулируют бизнес - субъектов к дополнительным капиталовложениям. Такое положение дел, по нашему мнению, не вполне соответствует конституционным принципам и условиям ограничения прав и свобод человека и гражданина.

Представляется более правильным исходить из необходимости обеспечения комплексной безопасности критически важных объектов, включая защиту информационных и телекоммуникационных систем этих объектов.

К числу критически важных объектов относятся, в том числе, негосударственные организации, вынужденные самостоятельно финансировать создание, поддержание и развитие системы комплексной безопасности. Требования к таким организациям, их права, полномочия органов государственной власти в отношении деятельности этих организаций должны быть установлены отдельным федеральным законом.

Что касается антитеррористической защищенности объектов, то соответствующий законопроект внесен в Государственную Думу и принят в первом чтении в мае этого года.<sup>4</sup> Понятно, что подготовка этого законопроекта стимулирована террористическими актами на объектах транспортной инфраструктуры.

В заключении хочу подчеркнуть следующее: в целом безопасность бизнеса это комплексная проблема и неверно сосредотачиваться на вопросах информационной безопасности, игнорируя, например, вопросы пожарной безопасности, поскольку информационные системы организации могут выйти из строя не только из-за DDos-атак или вирусов, компьютеры могут просто сгореть.

---

<sup>4</sup> Законопроект № 534519-5 «О внесении изменений в Федеральный закон "О противодействии терроризму" и Федеральный закон "О транспортной безопасности»

Проблема обеспечения информационной безопасности бизнеса становится сейчас очень острой, особенно с развитием электронного бизнеса. Решение проблемы достаточно затратно. Оптимизировать эти затраты можно только грамотно выстроив как сам бизнес так и систему его защиты. Причем жизнь доказывает: если построение этих систем идет параллельно или последовательно (на сложившуюся систему бизнеса «навешивается» система безопасности) – собственник проигрывает. Эти задачи необходимо решать одновременно.