

Тайна за семью печатями

Охрана конфиденциальности сведений ограниченного доступа на предприятиях топливно-энергетического комплекса

Директор по развитию бизнеса НИП «Информзащита»
Михаил Емельяников

Предприятия ТЭК, как никакие другие, чувствительны к несанкционированным действиям с внутренней информацией. В условиях функционирования в жесткоконкурентном окружении технологические секреты, результаты разведки ресурсов, сведения о себестоимости продукции, оценка рынков и перспектив их развития, текущее финансовое состояние, условия и сроки кредитования, персональные данные работников, особенно составляющих интеллектуальную и профессиональную базу предприятия, – далеко не исчерпывающий список того, к чему нужно и должно ограничивать доступ. Доступ не только конкурентов, но и иных третьих лиц, в том числе проявляющих подозрительный интерес чиновников, потенциальных инвесторов, готовых при удобном случае поглотить попавшее в трудное положение предприятие, контрагентов, часто без каких-либо сомнений использующих в своих интересах конфиденциальную информацию партнеров. Наконец, доступ собственных работников, не всегда лояльных к предприятию, часть которых ищет пути дополнительного, пусть и незаконного, обогащения.



новления на предприятии режима коммерческой тайны, отнесения информации к данной категории, ввода ее в гражданский оборот (передачи третьим лицам). Закон «О персональных данных» определяет порядок охраны конфиденциальности сведений частной жизни граждан, их личной и семейной тайны, а также предоставления им доступа к собственным персональным данным, находящимся в распоряжении госорганов, предприятий и организаций страны – операторов персональных данных.

Отнесение информации к категории «коммерческая тайна» (ИКТ) является исключительно делом ее обладателя, который вправе относить или не относить к ней собственные производственные секреты и иные сведения любого характера (производственные, технические, экономические, организационные и другие), а также сведения о способах осуществле-

нистративной, дисциплинарной и даже уголовной.

Ситуация с ограничением доступа к информации о деятельности предприятия усугубляется принятием 9 февраля 2009 г. Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», вступающего в силу с 1 января 2010 г. В соответствии с этим законом к информации о деятельности госорганов и ОМСУ относится, в том числе, и информация, поступившая извне, т.е. от предприятий и организаций в указанные органы.

По запросу любого гражданина госорганы и ОМСУ обязаны предоставить ему истребуемую информацию о своей деятельности (в том числе полученную в ее рамках от коммерческих организаций), за исключением случаев, когда такая информация отнесена к сведениям, составляющим государственную или иную охраняемую законом тайну. При этом гражданин не обязан обосновывать необходимость получения информации, доступ к которой не ограничен.

Таким образом, уже после 1 января следующего года на законном основании чиновником может быть передана третьим лицам любая представленная предприятием в госорган или ОМСУ информация, если в ее отношении обладателем не были установлены огра-

Уже после 1 января следующего года на законном основании чиновником может быть передана третьим лицам любая представленная предприятием в госорган или ОМСУ информация, если в ее отношении обладателем не были установлены ограничения в виде грифа «Коммерческая тайна»

Законодательные ограничения

Особенности российского законодательства таковы, что просто, по произвольному решению руководителя, ограничить доступ к той или иной информации нельзя. В соответствии со ст. 3 ФЗ «Об информации, информационных технологиях и о защите информации», одним из основополагающих принципов правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации, является установление ограничений доступа к информации только федеральными законами. Этот тезис подтверждается ст. 5 того же закона: информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

На сегодняшний день применительно к деятельности предприятий ТЭК ограничение доступа к информации об их деятельности возможно на основании части 4 Гражданского кодекса РФ, вступившей в действие 1 января 2008 г., и федеральных законов «О коммерческой тайне» и «О персональных данных». Гражданский кодекс и ФЗ «О коммерческой тайне» регулируют вопросы уста-

ния профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам. Ограничения по отнесению к коммерческой тайне установлены рядом федеральных законов, но в любом случае к данной категории информации у третьих лиц не может быть свободного доступа на законном основании. Сведения будут составлять коммерческую тайну лишь после того, как в отношении них обладателем таких сведений будет введен режим коммерческой тайны.

В отличие от коммерческой тайны, в отношении персональных данных закон обязывает их обладателя (который в законе именуется оператором) принимать при обработке персональных данных необходимые организационные и технические меры для защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий. Невыполнение этого требования чревато для предприятия и его руководителей различными видами ответственности – гражданской, адми-

нистративной, дисциплинарной и даже уголовной. Учитывая широко используемые в конкурентной разведке методы добытия сведений через органы власти, в том числе и путем инициации необходимого запроса на предприятие знакомым или замотивированным бюрократам, риски утечки чувствительных сведений, не отнесенным законным порядком к сведениям ограниченного доступа, для предприятий существенно возрастают, при этом более чем проблематичным является привлечение виновных к ответственности и взыскание нанесенного ущерба. При таких попытках чиновник обособанно будет ссылаться на норму закона, обязывающего его предоставлять желаемую информацию, не имеющую ограничений в доступе.

Режим коммерческой тайны

Единственным законным способом предотвратить утечку конфиденциальных сведений по подобным каналам является установление владельцем в отношении их режима коммерческой тайны. Такой режим позволяет владельцу интеллектуальной собственности, спо-

собной к охране в режиме коммерческой тайны, защитить свои интересы во взаимоотношениях с собственными работниками, контрагентами, государственными и муниципальными органами власти, средствами массовой информации, и даже с акционерами, независимыми директорами и рейдерами.

Предоставляя бизнесу правовую охрану коммерческой тайны и давая механизм ее реализации, государство в законодательных актах выдвигает обязательные

Единственным законным способом предотвратить утечку конфиденциальных сведений является установление владельцем в отношении их режима коммерческой тайны

требования, при выполнении которых предоставляется такая охрана со стороны институтов власти (судов, прокуратуры, правоохранительных органов), а также определяет условия передачи информации, составляющей коммерческую тайну, третьим лицам – юридическим и физическим, в том числе – работникам предприятий.

Требованиями, обуславливающими получение правовой помощи со стороны государственных институтов, являются:

- установление в организации режима коммерческой тайны путем реализации организационных мер и ввода в действие внутренних нормативных документов по охране конфиденциальности;
- организация разрешительной системы доступа персонала к ИКТ на основании трудовых договоров;
- передача ИКТ контрагентам на основании гражданско-правовых договоров (уступки исключительных прав на результаты интеллектуальной деятельности, лицензионных, о коммерческой концессии);
- организация контроля за соблюдением режима коммерческой тайны.

В соответствии с Федеральным законом «О коммерческой тайне» режим коммерческой тайны считается установленным на предприятии после принятия следующих мер по охране конфиденциальности информации:

- определения перечня информации, составляющей коммерческую тайну;
- ограничения доступа к ИКТ путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- организации учета лиц, получивших доступ к ИКТ, и (или) лиц, которым такая информация была предоставлена или передана (здесь имеются в виду как юридические, так и физические лица);

- урегулирования отношений по использованию ИКТ с работниками на основании трудовых договоров и с контрагентами – на основании гражданско-правовых договоров;
- нанесения на все материальные носители (документы), содержащие ИКТ, грифа «Коммерческая тайна» с указанием обладателя этой информации.

Важно, что все эти мероприятия должны выполняться не только на бумаге, но и переноситься в корпоративные информационные системы, где сосредоточена практически вся информация о деятельности современного предприятия. Это потребует создания эффективных процедур управления идентификацией пользователей информационных систем и доступом их к защищаемым ресурсам, выявления приложений и подсистем, где обрабатывается конфиденциальная информация, маркировки носителей конфиденциальных сведений в составе вычислительных систем. В большинстве случаев придется подумать об управлении электронными правами на использование документов в цифровом виде, что существенно затрудняет их несанкционированное использование (копирование на отчуждаемые носители, отправку по электронной почте, незаконную модификацию и т.п.), а также о мониторинге событий в информационной системе, связанных с несанкционированными действиями пользователей, находящихся внутри периметра системы, и злоумышленников, действующих извне – из глобальных информационных систем и сетей связи общего пользования.

Защита персональных данных

Как уже отмечалось выше, защита сведений о физических лицах – их персональных данных, является прямой обязанностью любого предприятия. Наряду с требованиями ФЗ «О персональных данных», это определяется главой 14 Трудового кодекса РФ, ст.86 которого требует, чтобы защита персданных работника от неправомерного их использования или утраты обеспечивалась работодателем за счет его средств в порядке, установлен-

ном Трудовым кодексом и иными федеральными законами, при этом все работники и их представители должны быть ознакомлены под росписью с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также их права и обязанности в этой области. При этом кодекс содержит норму, в соответствии с которой работники не должны отказываться от своих прав на сохранение и защиту тайны.

Требования к обеспечению безопасности обработки персональных данных помимо Трудового кодекса и Федерального закона № 152-ФЗ устанавливаются тремя специальными постановлениями Правительства РФ, а также нормативно-методическими документами ФСТЭК и ФСБ России – федеральных органов исполнительной власти, которые к тому же выполняют функции государственного контроля и надзора за реализацией установленных законодательством требований.

Большинство информационных систем персональных данных на крупном предприятии должно пройти процедуру аттестации или сертификации, подтверждающую выполнение требований, а работы по защите информации могут выполняться только специалистами, имеющими соответствующую квалификацию и опыт, для чего предусмотрено лицензирование деятельности по технической защите конфиденциальной информации, к которой относятся и персональные данные.

В заключение необходимо отметить, что организационные и технические меры по охране конфиденциальности информации ограниченного доступа являются весьма сложными и затратными. Однако их непринятие чревато утечкой существенной для предприятия информации, убытками, ухудшением конкурентного положения. А в случае с персональными данными – еще и рисками исков субъектов персональных данных и санкциями надзирающих и контролирующих органов, причем не только в виде штрафов, но и в виде запретов на обработку информации до устранения нарушений. **T**

