УДК 35.077

Защита и обработка конфиденциальной информации

Зимницкая Л.В.
Белорусский национальный технический университет

В современной рыночной экономике обязательным условием успеха предпринимателя в бизнесе, получения прибыли и сохранения в целостности созданной им организационной структуры является обеспечение экономической безопасности его деятельности. Одна из главных составных частей экономической безопасности - информационная безопасность.

Необходимо помнить о том, что информацию очень сложно сохранить, не дать ей уйти за пределы организации.

С появлением новых технологий (компьютеры и оргтехника) защитить информацию становится все труднее. Множество конкурентов не упустят малейшей возможности получить конфиденциальную информацию фирмы-конкурента и использовать ее в своих целях. Для того чтобы избежать утечки информации, составляющей тайну фирмы, создаются службы по контролю за документами конфиденциального характера, их передвижением и хранением в организации.

Безопасность ценной документируемой информации определяется степенью ее защищенности от последствий экстремальных ситуаций, в том числе стихийных бедствий, а также пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам с использованием организационных и технических каналов, в результате чего могут произойти хищение и неправомерное использование злоумышленником информации в своих целях, ее модификация, подмена, фальсификация, уничтожение.

Документируемая информация, используемая предпринимателем в бизнесе и управлении предприятием, организацией, банком, компанией или другой структурой (далее - фирма), является его собственной или частной информацией, представляющей для него значительную ценность, его интеллектуальной собственностью.

Ценность информации может быть стоимостной категорией, характеризующей конкретный размер прибыли при ее использовании или размер убытков при ее утрате. Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например учредительные документы, программы и планы, договоры с партнерами и посредниками и т. д. Ценность информации может также отражать ее перспективное научное, техническое или технологическое значение.

Информация, имеющая интеллектуальную ценность для предпринимателя, обычно разделяется на два вида:

• техническая, технологическая: методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, результаты испытаний опытных образцов, данные контроля качества и т. п.;

• деловая: стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы, стратегия действий на рынке и т. п.

Ценная информация охраняется нормами гражданского, патентного и авторского права или включается в категорию информации, составляющую тайну фирмы. Выявление и регламентация реального состава информации, представляющей ценность для предпринимателя и составляющей тайну фирмы, - основополагающие части системы защиты информации. Состав ценной информации фиксируется в специальном перечне, определяющем срок и уровень (гриф) ее конфиденциальности (то есть недоступности для всех), список сотрудников фирмы, которым предоставлено право использовать эти сведения в работе. Перечень, основу которого составляет типовой состав защищаемых сведений фирм данного профиля, является постоянным рабочим материалом руководства фирмы, служб безопасности и конфиденциальной документации. Он представляет собой, классифицированный список типовой и конкретной ценной информации о проводимых работах, производимой продукции, научных и деловых идеях, технологических новшествах.

Конфиденциальность отражает ограничение, которое накладывает собственник информации на доступ к ней других лиц, то есть собственник устанавливает правовой режим этой

информации в соответствии с законом. Вместе с тем к конфиденциальным документам нельзя относить учредительные документы уставы предпринимательских структур, финансовую документацию, сведения о заработной плате персонала и другую документированную информацию, необходимую правоохранительным и налоговым государственным органам.

Под конфиденциальным документом понимается необходимым образом, оформленный носитель документированной информации, содержащий сведения, которые относятся к негосударственной тайне и составляют интеллектуальную собственность юридического или физического лица. Обязательным признаком конфиденциального документа является наличие в нем информации, подлежащей защите. К конфиденциальным относятся следующие документы:

- в государственных структурах - документы, проекты документов и сопутствующие материалы, относимые к служебной информации ограниченного распространения, содержащие сведения, отнесенные к служебной тайне, имеющие рабочий характер и не подлежащие опубликованию в открытой печати;

- в предпринимательских структурах и направлениях подобной деятельности— документы, содержащие сведения, которые их собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне фирмы, тайне мастерства;

- независимо от принадлежности - документы и базы данных, фиксирующие любые персональные (личные) данные о гражданах, а также содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т. п.

Главным направлением защиты документированной информации от возможных опасностей является формирование защищенного документооборота, то есть использование в обработке и хранении документов специализированной технологической системы, обеспечивающей безопасность информации на любом типе носителя.

Под защищенным документооборотом (документопотоком) понимается контролируемое движение конфиденциальной документированной информации по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в жестких условиях организационного и технологического обеспечения безопасности как носителя информации, так и самой информации.

Помимо общих для документооборота принципов защищенный документооборот основывается на ряде дополнительных принципов:

- ограничение доступа персонала к документам, делам и базам данных деловой, служебной или производственной необходимостью;
- персональная ответственность должностных лиц за выдачу разрешения на доступ сотрудников к конфиденциальным сведениям и документам;
- персональная ответственность каждого сотрудника за сохранность доверенного ему носителя и конфиденциальность информации;
- жесткая регламентация порядка работы с документами, делами и базами данных для всех категорий персонала, в том числе первых руководителей.

Защищенность документопотоков достигается за счет:

•одновременного использования режимных (разрешительных, ограничительных) мер и технологических приемов, входящих в систему обработки и.хранения конфиденциальных документов;

• нанесения отличительной отметки (грифа) на чистый носитель конфиденциальной информации или документ, в том числе сопроводительный, что позволяет выделить их в общем потоке документов;

• формирования самостоятельных, изолированных потоков конфиденциальных документов и (часто) дополнительного их разделения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;

• использования автономной технологической системы обработки и хранения конфиденциальных документов, не соприкасающейся с системой обработки открытых документов.