Владение информацией о противнике - один из наиболее действенных способов конкурентной борьбы на рынке. Необходимость решения проблемы утечки конфиденциальной информации связана с выживанием и успешным ведением бизнеса компании.

Во-первых, ущерб от раскрытия конфиденциальной информации может выражаться в потере конкурентных преимуществ, упущенной коммерческой выгоде, санкциях со стороны регулирующих органов, административной и уголовной ответственности за раскрытие персональных данных, ухудшении морального климата в коллективе вследствие раскрытия информации о заработной плате работников, планируемых кадровых перестановках и т. п. Например, американская компания Victoria Secrets была оштрафована на 50 тыс. долл. за то, что не обеспечила надлежащей защиты своего Web-сайта электронной коммерции, в результате чего пострадали 560 клиентов, персональные данные которых оказались скомпрометированными.

Несмотря на то, что несанкционированное раскрытие информации является во многих случаях административно и уголовно наказуемым деянием, в условиях, когда информационное законодательство РФ еще полностью не сформировано, а процессы законотворчества сильно отстают от уровня развития информационных технологий, возникают существенные трудности в обеспечении юридической защиты интересов собственников конфиденциальной информации. Однако приемлемое решение всегда существует, и поиск этого решения должен осуществляться в рамках стандартной схемы «объекты - угрозы - контрмеры».

Во-вторых необходимо категорирование конфиденциальной информации

Состав сведений с грифом «конфиденциальная информация» варьируется в зависимости от предприятия и должен приводиться в «Перечне сведений ограниченного распространения», который утверждается руководителем организации. Информация, не попавшая в данный перечень, считается открытой. Опираясь на опыт защиты информации в коммерческих организациях и положения действующего законодательства, можно выделить следующие основные категории конфиденциальной информации:

сведения, составляющие коммерческую тайну организации;

персональные данные сотрудников организации (информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника);

сведения, составляющие конфиденциальную информацию третьих лиц (партнеров, клиентов, подрядчиков, контрагентов);

любые другие сведения, разглашение и/или неправомерное использование которых может нанести ущерб интересам организации.

К открытой информации относятся, например, сведения:

содержащиеся в сообщениях и отчетах, официально опубликованных компанией в соответствии с действующим российским законодательством;

содержащиеся в официальных пресс-релизах, а также рекламных сообщениях компании;

опубликованные в средствах массовой информации по инициативе третьих лиц и с разрешения руководства компании;

любая информация, не попадающая в категории, определяемые «Перечнем сведений ограниченного распространения», принятым в организации, и не являющаяся конфиденциальной по законодательству РФ.

В коммерческой организации наиболее остро стоит вопрос о защите коммерческой тайны, однако не менее важными являются сведения, составляющие конфиденциальную информацию третьих лиц, к которым могут относиться коммерческая тайна третьих лиц, персональные данные, служебная тайна и т. п., включая государственную тайну.

В третьих, Важной категорией конфиденциальной информации являются персональные данные сотрудников организации. Например, в США законодательство предусматривает строгое наказание за раскрытие персональных данных граждан. Соответствующие вопросы отражены в Privacy Act и HIPPA, последний определяет наказание до десяти лет лишения свободы или 200 тыс. долл. штрафа за умышленное раскрытие персональных данных.

В нашей стране вопросы защиты персональных данных пока недостаточно хорошо проработаны как на законодательном, так и на технологическом уровне. Однако правовая база все же была заложена в законе РФ «Об информации, информатизации и защите информации».

Помимо определения состава конфиденциальных сведений, информационные ресурсы организации нуждаются также в категорировании по уровню конфиденциальности. Это позволяет ввести дифференцированный подход к реализации защитных мер. Знания о составе информационных ресурсов организации и соответствующих уровнях конфиденциальности формализуются в виде единого «Реестра информационных ресурсов организации».