
Источники (обладатели) ценной, конфиденциальной документированной информации представляют собой накопители (концентраторы, излучатели) этой информации. К числу основных видов источников конфиденциальной информации относятся: персонал фирмы и окружающие фирму, люди; документы; публикации о фирме и ее разработках, рекламные издания, выставочные материалы; физические поля, волны, излучения, сопровождающие работу вычислительной и другой офисной техники, различных приборов и оборудования.

Документация как источник ценной предпринимательской информации включает:

- конфиденциальную документацию, содержащую предпринимательскую тайну (ноу-хау);
- ценную правовую, учредительную, организационную и распорядительную документацию;
- служебную, обычную деловую и научно-техническую документацию, содержащую общеизвестные сведения;
- рабочие записи сотрудников, их служебные дневники, личные рабочие планы, переписку по коммерческим и научным вопросам;
- личные архивы сотрудников фирмы.

В каждой из указанных групп могут быть:

- документы на традиционных бумажных носителях (листах бумаги, ватмане, фотобумаге и т.п.);
- документы на технических носителях (магнитных, фотопленочных и т.п.);
- электронные документы, банк электронных документов, изображения документов на экране дисплея (видеограммы).

Канал распространения информации представляет собой путь перемещения ценных сведений из одного источника в другой в санкционированном (разрешенном, законном) режиме или в силу объективных закономерностей. Например, обсуждение конфиденциального вопроса на закрытом совещании, запись на бумаге содержания изобретения. Увеличение числа каналов распространения информации порождает расширение состава источников ценной информации.

Источники и каналы распространения информации при определенных условиях могут стать объектом внимания конкурента, что создает потенциальную угрозу сохранности и целостности информации. Угроза безопасности информации предполагает несанкционированный (незаконный) доступ конкурента или нанятого им злоумышленника к конфиденциальной информации и как результат этого — кражу, уничтожение, фальсификацию, модификацию, подмену документов. При отсутствии интереса конкурента угроза информации не возникает даже в том случае, если создались предпосылки для ознакомления с ней посторонних лиц. Ценная информация, к которой не проявляется интерес конкурента, может не включаться в состав защищаемой, а содержащие ее документы контролируются только с целью обеспечения сохранности носителя.

Каналы утечки, которыми пользуются злоумышленники, отличаются большим разнообразием. Основными видами этих каналов могут быть следующие:

- установление злоумышленником взаимоотношений с сотрудниками фирмы или посетителями, сотрудниками фирм-партнеров, служащими государственных или муниципальных органов управления и другими лицами;
- анализ опубликованных материалов о фирме, рекламных изданий, выставочных проспектов и другой общедоступной информации;
- поступление злоумышленника на работу в фирму;
- работа в информационных сетях;
- криминальный, силовой доступ к информации, т.е. кража документов, шантаж персонала и другие способы;
- работа злоумышленника в технических каналах распространения информации.

Обнаружение канала разглашения (утечки) информации - сложная, длительная и трудоемкая задача. В основе ее решения лежит классификация и постоянное изучение источников и каналов распространения информации, выявление угроз информации и возможных каналов ее утечки, поиск и обнаружение реальных каналов утечки, оценка степени опасности каждого реального канала, подавление опасных каналов и анализ эффективности защитных мер, предпринятых для безопасности информации. Каналы разглашения (утечки) информации всегда индивидуальны и зависят от конкретных задач, поставленных перед злоумышленником.