

6. РАЗВЕДЫВАТЕЛЬНЫЕ СВЕДЕНИЯ И ИНФОРМАЦИЯ

6.2. Источники конфиденциальной информации и способы получения доступа к ней

Конфиденциальная информация – это данные, доступ к которым ограничен в соответствии с законом. Такая информация может быть коммерческой, личной или же служебной [1].

Основные источники конфиденциальной информации:

- носители данных (документы);
- сотрудники предприятия, имеющие доступ к данным;
- технические средства обработки и хранения информации;
- методы коммуникации, используемые для передачи конфиденциальной информации.

Самым слабым элементом в системе конфиденциальных данных является человек.

Коммерческая тайна – это сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Профессиональная тайна – это конфиденциальная информация, которая стала известна лицу в силу исполнения им своих профессиональных обязанностей.

К ней относят:

- конфиденциальность источника информации в журналистике;
- банковская тайна;
- адвокатская тайна;

и др.

Для получения информации специалисту по бизнес-разведке необходим доступ к источнику информации при соблюдении законодательства.

Способы **доступа к информации** можно разделить на три группы:

- физическое проникновение к источнику информации;
- сотрудничество отдела бизнес-разведки с работником конкурента, имеющего доступ к интересующей информации;
- дистанционное снятие информации с носителя.

Скрытое проникновение имеет ряд преимуществ по сравнению с открытым, но требует тщательной подготовки и априорной информации о месте нахождения источника, возможных маршрутах движения и др.

Скрытое проникновение не может носить регулярного характера, так как оно связано с большим риском для специалиста по бизнес-разведке.

Канал распространения информации представляет собой путь перемещения ценных сведений из одного источника в другой в законном режиме. Увеличение числа каналов распространения информации порождает расширение состава источников ценной информации [2].

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 к конфиденциальной информации и как результат этого – кражу, уничтожение, фальсификацию, модификацию, подмену документов.

При отсутствии интереса конкурента угроза информации не возникает и в случае создания предпосылок для ознакомления с ней посторонних лиц.

Переход информации к третьему лицу может быть непреднамеренным, стихийным.

Подобный переход возникает в результате [3]:

1. Утери или случайного уничтожения документа;
2. Невыполнения, незнания или игнорирования сотрудником требований по защите информации;
3. Излишней общительности сотрудников;
4. Работы с конфиденциальными документами при посторонних лицах;
5. Использования конфиденциальных сведений в открытой печати, личных записях, неслужебных письмах;
6. Наличия в документах излишней конфиденциальной информации;
7. Самовольного копирования сотрудником документов в служебных целях.

Конкурент создает угрозу информации путем **установления контакта с источником информации** или преобразования канала распространения информации в канал ее утечки. Угроза предполагает намерение конкурента совершить противоправные действия по отношению к информации для достижения желаемой цели.

Утрата (утечка, потеря) информации предполагает несанкционированный переход ценных, конфиденциальных сведений к лицу, не имеющему права владения ими и использования их в своих целях для получения прибыли.

В том случае, когда речь идет об утрате информации по вине персонала, обычно используется термин «разглашение (огласка) информации». **Разглашение информации** осуществляется сотрудником в различных формах: устно, письменно, с помощью жестов, мимики, условных сигналов, лично или через посредников.

Список использованных источников

1. Бурдов С. Н. Сущность и отличительные признаки конфиденциальной информации // Правовое государство: теория и практика. – 2013. – № 4. – С.150–157.
2. Варлатая С. К. Шаханова М. В. Проблемы защиты и обработки конфиденциальных документов // Доклады ТУСУРа. – 2019. – № 1. – С. 46–48.
3. Шемяков А. О. Информационные ресурсы ВУЗа и оценка их безопасности // Труды МАИ. – 2012. – № 50. – С. 36.