Основной угрозой безопасности информационных ресурсов ограниченного распространения является несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации и как результат – овладение информацией и противоправное ее использование или совершение иных действий. Целью и результатом несанкционированного доступа может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, подмена и т. п. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники коммунальных служб, экстремальной помощи, прохожие и др.), посетители фирмы, работники других организационных структур, а также сотрудники данной фирмы, не обладающие правом доступа в определенные помещения, к конкретному документу, информации, базе данных. Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом, но может и не быть им.

Обязательным условием успешного осуществления попытки несанкционированного доступа к информационным ресурсам ограниченного доступа является интерес к ним со стороны конкурентов, определенных лиц, служб и организаций. При отсутствии такого интереса угроза информации не возникает даже в том случае, если создались предпосылки для ознакомления с ней постороннего лица. Основным виновником несанкционированного доступа к информационным ресурсам является, как правило, персонал, работающий с документами, информацией и базами данных. При этом надо иметь в виду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий, а из-за невнимательности и безответственности персонала.

Следовательно, утрата информационных ресурсов ограниченного доступа может наступить:

• при наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации;

• при возникновении риска угрозы, организованной злоумышленником или при случайно сложившихся обстоятельствах;

• при наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией. Эти условия могут включать:

• отсутствие системной аналитической и контрольной работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов;

• неэффективную систему защиты информации или отсутствие этой системы;

• непрофессионально организованную технологию обработки и хранения конфиденциальных документов;

• неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе;

• отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа;

• отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

• бесконтрольное посещение помещений фирмы посторонними лицами.

Утрата информации характеризуется двумя условиями, информация переходит а) непосредственно к заинтересованному лицу – конкуренту, злоумышленнику или б) к случайному, третьему лицу. Под третьим лицом в данном случае понимается любое постороннее лицо, получившее информацию во владение в силу обстоятельств или безответственности персонала, не обладающее правом владения ею и, что очень важно, не заинтересованное в этой информации. Однако от третьего лица информация может легко перейти к злоумышленнику.

Переход информации к третьему лицу представляется достаточно частым явлением, и его можно назвать непреднамеренным, стихийным, хотя при этом факт разглашения информации, нарушения ее безопасности имеет место.

Непреднамеренный переход информации к третьему лицу возникает в результате:

• утери или неправильного уничтожения документа, пакета с документами, дела, конфиденциальных записей;

• игнорирования или умышленного невыполнения сотрудником требований по защите документированной информации;

• излишней разговорчивости сотрудников при отсутствии злоумышленника (с коллегами по работе, родственниками, друзьями, иными лицами в местах общего пользования, транспорте и т. п.);

• работы с документами ограниченного доступа при посторонних лицах, несанкционированной передачи их другому сотруднику;

• использования сведений ограниченного доступа в открытых документации, публикациях, интервью, личных записях, дневниках и т. п.;

• отсутствия маркировки (грифования) информации и документов ограниченного доступа (в том числе документов на технических носителях);

• наличия в документах излишней информации ограниченного доступа;

• самовольного копирования сотрудником документов в служебных или коллекционных целях.