Действия, приводящие к неправомерному овладении конфиденциальной информацией

- владелец (источник) не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко по лучить интересующие его сведения;
- источник информации строго соблюдает меры информационной безопасности, тогда злоумышленнику приходится прилагать значительные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное, заходовое или беззаходовое;
- промежуточная ситуация — это у течка информации по техническим каналам, при которой источник еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник легко, без особых усилий может их использовать в своих интересах.

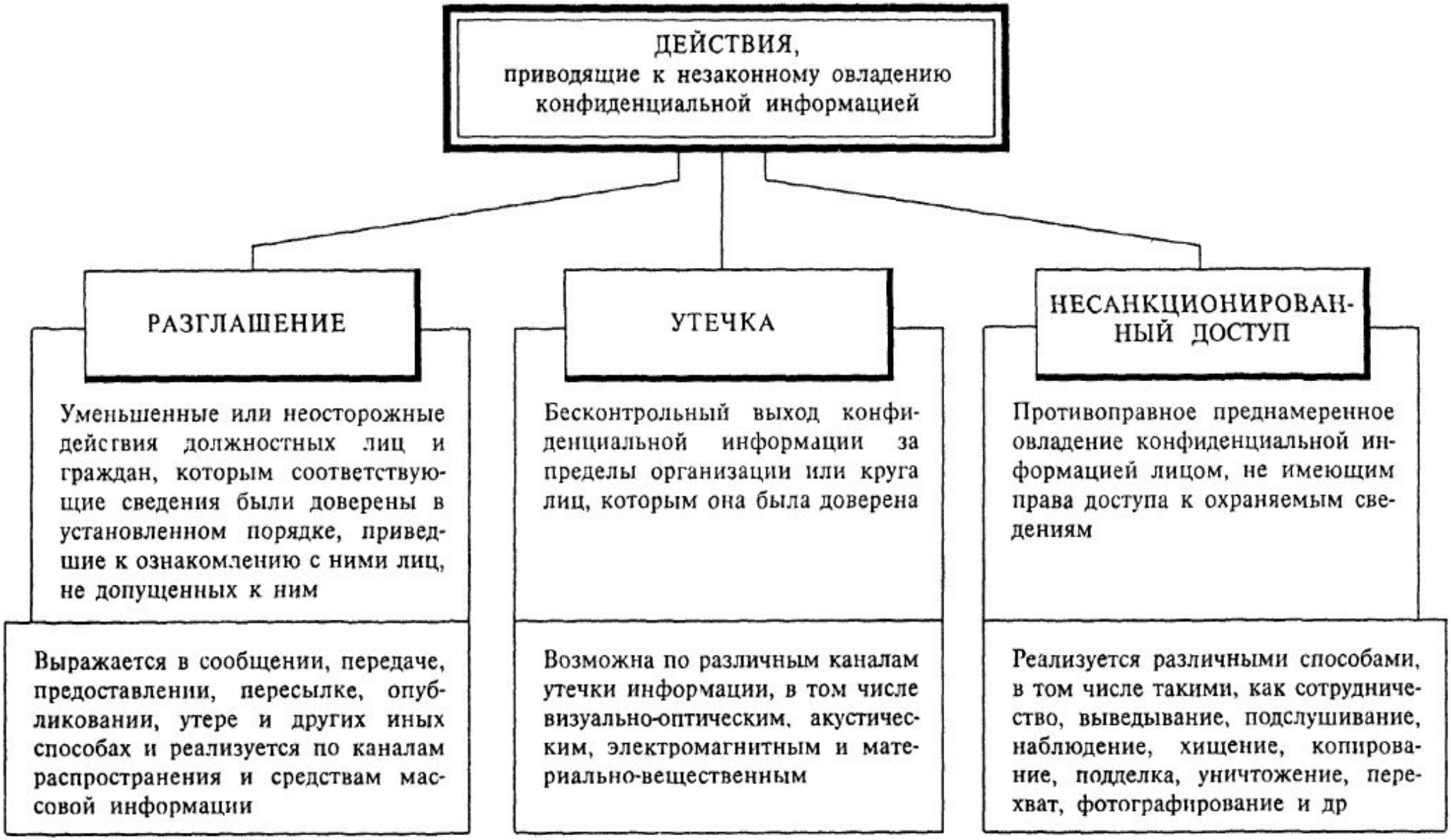
ДЕЙСТВИЯ,
приводящие к незаконному овладению конфиденциальной информацией
РАЗГЛАШЕНИЕ
Уменьшенные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения были доверены в установленном порядке, приведшие к ознакомлению с ними лиц, не допущенных к ним
Выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и других иных способах и реализуется по каналам распространения и средствам массовой информации
УТЕЧКА
Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
Возможна по различным каналам утечки информации, в том числе визуально-оптическим, акустическим, электромагнитным и материально-вещественным
НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП
Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям
Реализуется различными способами, в том числе такими, как сотрудничество, выведывание, подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, перехват, фотографирование и др

Рис. 7

Разглашение — это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и науч ной информацией.

Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и т. д.). Неформальные коммуникации включают личное общение (встречи, переписка), выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газе ты, интервью, радио, телевидение). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги (написанный текст) и др. С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации на визуально-оптические, акустические, электромагнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

Несанкционированный доступ к источникам конфиденциальной информации реализуется различны ми способами: от инициативно го сотрудничества, выражающегося в активном стремлении «продать» секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения — стационарных или в подвижном варианте, оборудованных самыми современными техническими средствами.

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направления обеспечения информационной безопасности — это нормативно-правовые категории, ориентированные на обеспечение комплексной защиты информации от внутренних и внешних угроз.


НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
- нормативно-правовые категории, определяющие комплексные меры защиты информации
ПРАВОВАЯ ЗАЩИТА
- Специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе
ОРГАНИЗАЦИОННАЯ ЗАЩИТА
- Регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая нанесение ущерба
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА
- Использование различных технических средств, препятствующих нанесению ущерба

Рис. 9


ХАРАКТЕРИСТИКИ ЗАЩИТНЫХ ДЕЙСТВИЙ
По ориентации
Персонал
Материальные и финансовые ценности
Информация
По характеру уг роз
Разглашение
Утечка
Несанкционированный доступ
По направлениям
Правовая
Организационная
Инженерно-техническая
По способам действий
Предупреждение
Выявление
Обнаружение
Пресечение
Восстановление
По охвату
Территория
Здание
Помещение
Аппаратура
Элементы аппаратуры
По масштабу
Объектовая
Групповая
Индивидуальная

Рис. 10