В настоящее время данная тема является особенно актуальной так, как «информация» является движущей силой в сфере предпринимательства. По сути своей утечка информации — это неконтролируемое распространение информации за пределы организации, помещения, здания, какой-либо территории, а также определенного круга лиц, которые имеют доступ к этой информации. В случае обнаружения утечки важно своевременно ее ликвидировать, но лучше всего заранее принять превентивные меры по защите информации с ограниченным доступом.

В природе существуют только 4 средства переноса информации – это световые лучи, звуковые волны, электромагнитные волны, а также материальные носители (бумага, фото, магнитные носители и т.д.). Эти средства являются составляющими любой системы связи, в которой помимо них обязательно присутствуют:

- источник информации,
- передатчик,
- канал передачи информации,
- приемник,
- получатель сведений.

Непосредственно сам человек может стать инициатором (намеренным или случайным) утечки информации, используя одно или несколько вышеназванных средств переноса информации. Поэтому работу некоторых систем связи необходимо контролировать, чтобы, с одной стороны, обеспечить безопасную, надежную и точную передачу информации, а с другой, защитить ее от незаконного доступа. И если канал должным образом не защищен и передача информации из исходной точки в другую происходит без ведома источника, то такой канал можно называть каналом утечки информации.

Защита от утечки информации требует проведения обязательных организационных и технических мер, которые позволят выявить вероятные технические каналы утечки информации, чтобы избежать их возможного использования.

выделяют 4 группы способов утечки информации:

- визуально-оптические каналы утечки информации,

- акустические каналы утечки информации,
- электромагнитные каналы утечки информации (или каналы утечки информации по ПЭМИН),
- материально-вещественные каналы утечки информации.

Примеры утечки информации в различных компаниях :

Во- первых, компания Zoom, в начале апреля 2020 года стало известно о появлении в даркнете данных более 500 тыс. учетных записей Zoom, которые были выставлены на продажу. Эти данные содержат адреса электронной почты, пароли, URL-адреса для организации закрытых встреч, а также идентификаторы персональной конференции

Во-вторых, компания Decathlon, в феврале 2020 года исследователи безопасности из компании VPNmentor обнаружили, что данные более 123 млн клиентов Decathlon оказались в открытом доступе из-за незащищенного сервера ElasticSearch.

В-третьих, компания Microsoft, 22 января 2020 года стало известно о том, что данные миллионов клиентов Microsoft оказались в открытом доступе. Это произошло из-за неправильной настройки базы данных Elasticsearch: её параметры были выставлены таким образом, что всю информацию из каталога мог просматривать любой желающий.

Главной целью злоумышленника является получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т.д.) в целях удовлетворения своих информационных потребностей. Возможно в корыстных целях и внесение определенных изменений в состав информации, циркулирующей на объекте конфиденциальных интересов. Такое действие может привести к дезинформации по определенным сферам деятельности, учетным данным, результатам решения некоторых задач. Более опасной целью является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов. Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способов доступа к информации. Чем большими информационными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе.