Начну с того, что вследствие резкого экономического спада обострилась конкурентная борьба, методы которой стали очень жесткими и, что самое главное – незаконными. Информация в настоящее время является как сильным, так и ценным оружием, однако для того, чтобы ее безопасно использовать, необходимо получить ее законным способом.

Так, имеется два вида разведки [1]:

- промышленный шпионаж, который включает незаконное добывание информации, недобросовестную конкуренцию;
- конкурентная разведка, представляющая сбор, а также обработку данных из разных источников в рамках закона для выработки решений в сфере управления с целью повышения конкурентоспособности предприятия.

Важно понимать разницу между конкурентной разведкой и промышленным шпионажем, которая состоит в законности методов получения информации. Другими словами, в промышленном шпионаже применяются все методы конкурентной разведки, однако в конкурентной разведке, в свою очередь, все имеющиеся методы промышленного шпионажа использоваться не могут.

Отмечу, что одним из ключевых средств получения информации является техническая разведка, которая проводится посредством различных специальных технических устройств. Тип используемых технических средств разведки, прежде всего, зависит от физической природы, а также особенностей демаскирующих признаков объектов, которые являются источниками информации [3, с. 347]. В определенном смысле, функции демаскирования также являются источниками информации, которые позволяют восстанавливать информацию.

На рынке России в настоящее время представлены самые разные современные технические средства промышленного шпионажа, к которым относятся: визуально-оптические, фотографические, телевизионные, тепловизионные (инфракрасные), акустические, радио-, радиотехнические и некоторые другие средства разведки. Их, в свою очередь, можно разделить на следующие группы:

- средства акустического контроля (радиозакладка);
- аппаратура для съема информации с окон;

- специальная звукозаписывающая аппаратура;
- микрофоны различного назначения и исполнения;
- электросетевые подслушивающие устройства;
- приборы для съема информации с телефонной линии связи и сотовых телефонов;
- специальные системы наблюдения и передачи видеоизображений;
- специальные фотоаппараты;
- приборы наблюдения в дневное время и приборы ночного видения;
- специальные средства радиоперехвата.

При этом перехват побочных электромагнитных излучений и наводок, безусловно, является достаточно «хлопотным» делом, а восстановление сигналов, соответственно, - это удел профессионалов.

Такие операции стоят весьма дорого, и эффект получается не всегда (за исключением перехвата радиационных дисплеев). Вследствие чего возникает явное желание установить в вычислительной технике специальные устройства, которые, питаясь от ее источников напряжения, передавали бы информацию в течение нескольких месяцев с фиксированной частотой на значительные расстояния (до 2 км). Наиболее перспективным в данном плане является внедрение таких устройств в клавиатуру, накопители на магнитных дисках и прочее.

Подчеркну, что внедрение программных закладок в настоящее время является перспективным направлением, задачей которых могут быть получение информации о паролях, кодовых комбинациях, обрабатываемых данных и передача собранных сведений заданному адресу по сети, электронной почте и т.д.

Сегодня это, скорее, гипотетическая угроза, однако она может быстро стать реальностью, благодаря возможности доставки таких программ на нужный компьютер. На самом деле, методы те же, что и для компьютерных вирусов, и сами закладки по сути являются вирусами. Одним из методов является введение вирусов путем подачи расчетных электромагнитных импульсов в цепь питания. Так, японцы и американцы особенно усердно работают над этим вопросом.

В заключение мне остается лишь подчеркнуть, что сегодня стало появляться все больше разнообразных средств, помогающих защищать информации в сети Интернет, а также препятствующих промышленному шпионажу, что по сути является противозаконным явлением [2, с. 99]. Важно грамотно подходить к системе защите информации не только на своем компьютере, но и в глобальной

сети Интернет.

Библиографический список

1. Дроздова, Л.А. Конкурентная разведка и промышленный шпионаж [Электронный ресурс] / Л.А. Дроздова // Студенческий научный форум. – 2017. – Режим доступа: https://scienceforum.ru/2017/article/2017034157 (дата обращения: 05.12.2019).

2. Зубков, Т.Н. Промышленный шпионаж и средства технической защиты от него / Т.Н. Зубков, Е.И. Прохоренко // Молодежный научный форум: технические и математические науки. – 2017. - № 6(46). – С. 94-99.

3. Чугаев, С.В. Проблемы защиты информации при ее обработке техническими средствами / С.В. Чугаев, В.В. Бурдюков, Д.Д. Чувашев // Актуальные проблемы права, экономики и управления. – 2016. - № 12. – С. 347-348.